C O M U N E D I S T I N T I N O
P R O V I N C I A D I S A S S A R I
VIA TORRE FALCONE – TEL. 079/523508-523053– FAX 079/523628
www.comune.stintino.ss.it

Documento Programmatico sulla Sicurezza (D.P.S.)

Il presente Documento è stato elaborato dall'Ente secondo quanto indicato dall'art. 34, lett. g) D. Lgs. 196/03 e sulla base delle specifiche tecniche indicate nella Regola 19, contenuta nell'Allegato B al D. Lgs. 196/03

Analisi compiuta dei rischi che incombono sui dati personali trattati dall'Amministrazione Comunale e indicazione delle misure di sicurezza, organizzative, fisiche e logiche da adottare per assicurare l'integrità e la disponibilità degli stessi dati al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, delle informazioni, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta

REVISIONE N° 03

INDICE

Paragrafo 1.

INTRODUZIONE

Il Codice in materia di protezione dei dati personali, introdotto nel nostro ordinamento dal D. Lgs. 196/03, si apre, all'art. 1, con il solenne riconoscimento del Diritto di chiunque alla protezione dei dati che lo riguardano.

A questa dichiarazione fa poi seguito l'indicazione delle finalità del Codice: garantire che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali nonché della dignità dell'interessato, con particolare riferimento alla RISERVATEZZA, all'IDENTITA' PERSONALE e al DIRITTO ALLA PROTEZIONE DEI DATI PERSONALI.

Autonoma rilevanza presenta quindi, nel nostro ordinamento, il diritto alla riservatezza quale diritto della persona al rispetto della propria vita privata. Tale diritto tutela in generale l'interesse della persona a non essere esposta alla curiosità altrui: cioè l'interesse alla salvaguardia della intimità della propria sfera privata.

Il diritto al rispetto della vita privata è suscettibile di essere leso da diverse forme di ingerenza, ma è principalmente minacciato dal trattamento illegittimo dei dati personali. Per questa ragione il Codice fa riferimento alla riservatezza quale rispetto della vita privata quando afferma che il trattamento dei dati personali deve svolgersi nel rispetto dei diritti e delle libertà fondamentali con *particolare riferimento alla RISERVATEZZA.*

Per comprendere pienamente la *ratio* della normativa sulla riservatezza, è necessario ricordare che questa costituisce attuazione dell'art. 2 della nostra Costituzione, il quale "riconosce e garantisce i diritti inviolabili dell'uomo, sia come singolo sia nelle formazioni sociali ove si svolge la sua personalità."

Il D. Lgs. 196/03 eleva la protezione dei dati personali a posizione giuridica autonoma che assurge al rango di diritto fondamentale della persona.

Con il D. Lgs. 196/03 quindi e con l'applicazione dell'articolo 1 ("Chiunque ha diritto alla protezione dei dati personali che lo riguardano") si ha una forte inversione di tendenza rispetto al passato perché l'individuo diventa anche il proprietario dei propri dati personali e, i soggetti pubblici che li hanno in custodia e che li utilizzano per il perseguimento delle loro finalità istituzionali, ne sono i meri "gestori", tenuti al rispetto rigoroso dei principi dettati dal legislatore a tutela della riservatezza e all'osservanza dei diritti del soggetto al quale i dati si riferiscono (soggetto interessato).

Ma se l'ordinamento deve garantire protezione ad ogni tipo di informazione relativa a soggetti individuati o individuabili, va da sé che, nella vita sociale ed economica moderna, tale protezione non può essere assoluta poiché nessun individuo vive totalmente isolato rispetto alla collettività dei consociati. Occorre per questa ragione individuare strumenti che contemperino, da un lato, l'esigenza di tutela delle informazioni personali; dall'altro, la necessità che tali informazioni circolino per poter garantire lo sviluppo dei contatti e delle relazioni economiche e sociali necessarie per l'esistenza stessa della società.

Questo è l'obiettivo della normativa sulla tutela della riservatezza, che il legislatore ha creduto di poter raggiungere sia sottoponendo ogni forma di trattamento di dati personali a specifiche regole, sia sancendo la necessità del consenso da parte del titolare dell'informazione personale per sottoporre la medesima a trattamento.

In altre parole, poiché il dato personale, cioè l'informazione su qualunque circostanza riguardi la persona, è tutelato dall'ordinamento come un diritto fondamentale, al pari ad esempio del diritto alla salute, per poter incidere su di esso, quindi per poter acquisire il dato personale di terzi, comunicarlo o collocarlo in un archivio, è necessario il consenso dell'interessato, così come detto consenso è necessario per poter incidere sul bene "salute". Così come il medico deve acquisire il consenso del paziente per poter operare sul medesimo, allo stesso modo il soggetto che intende acquisire un'informazione personale relativa ad un terzo deve acquisire il consenso del medesimo.

Tuttavia il ragionamento indicato vale unicamente nei confronti dei trattamenti di dati personali svolti da soggetti privati e deve essere invece diversificato laddove essi siano posti in essere da Pubbliche Amministrazioni. Queste, infatti, sono

deputate istituzionalmente allo svolgimento di attività volte a realizzare fini di interesse collettivo: ne consegue che, laddove l'acquisizione, l'archiviazione o la comunicazione di dati personali sia necessaria per il raggiungimento di tali fini, non sarà necessario il consenso dell'interessato poiché le esigenze connesse alle attività di interesse collettivo assumono una rilevanza tale da comprimere le posizioni soggettive dei destinatari dell'azione amministrativa.

Pertanto la legge, prescinde dal consenso dell'interessato per i trattamenti di dati personali effettuati da Pubbliche Amministrazioni sebbene assoggetti tali trattamenti a numerose altre regole vigenti anche per i trattamenti di dati personali operati da soggetti privati.

In particolare, le PP.AA. possono prescindere dal consenso dell'interessato purché il trattamento di dati personali venga effettuato per adempiere a funzioni istituzionali e sempre nel rispetto dei limiti posti da norme di legge o di regolamento (art. 18 D. Lgs. 196/03).

La fonte di legittimazione al trattamento è dunque l'attività pubblicistica svolta dall'Ente, e in questo concetto rientrano tutti i suoi compiti, propri e delegati. Compiti istituzionali sono quindi le funzioni svolte in base a leggi, statali e regionali, a norme comunitarie ed anche alla normativa statutaria e regolamentare dell'Amministrazione interessata.

Vanno considerati quali compiti istituzionali anche le attività e le funzioni esplicate per dare esecuzione a previsioni derivanti dalla stipulazione di accordi di programma, di accordi ex art. 15 L. 241/90 e, in generale, per l'attuazione di tutti gli strumenti di amministrazione negoziata previsti da norme di legge. Il concetto di "funzioni istituzionali" di cui all'art. 18 del Codice va dunque inteso in senso ampio, come *attività rivolte al perseguimento degli interessi collettivi*, e può trovare fondamento, oltre che nella "legge" intesa a sua volta nel senso ampio suddetto, anche in atti di indirizzo emanati dagli organi di governo dell'Ente, a condizione che si tratti di atti assunti legittimamente.

Nel bilanciamento tra l'interesse alla tutela del diritto alla riservatezza che il singolo vanta sulle informazioni che lo riguardano, e l'interesse all'efficacia e speditezza nel perseguimento degli interessi collettivi da parte della Pubblica Amministrazione, la legge assegna quindi maggior rilievo al secondo elemento. Ciascun Ente, nella persona del Responsabile del trattamento dei dati, deve valutare di volta in volta se le operazioni di trattamento siano pertinenti e non eccedenti rispetto alla cura degli interessi pubblici che è tenuto a perseguire sulla base delle fonti sopradescritte.

Paragrafo 2.

SCOPO E AMBITO DI APPLICAZIONE DEL DOCUMENTO PROGRAMMATICO 2010

Il Documento Programmatico sulla Sicurezza, alla luce del combinato disposto degli artt. 31, 33, 34 e 35 del D. Lgs 196/03 e della Regola 19 codificata nell'Allegato B al citato Decreto, si inserisce nel novero delle **misure minime di sicurezza**.

La sua annuale predisposizione costituisce uno specifico adempimento imposto all'Ente dall'art. 34, comma 1, lett. g) del D. Lgs. 196/03 e dalla già richiamata Regola 19 del Disciplinare Tecnico, Allegato B al Codice sulla Privacy.

La mancata tempestiva predisposizione e adozione del DPS, è sanzionata con l'arresto sino a due anni secondo la previsione di cui all'articolo 169 del D. Lgs. 196/2003, così come modificato dalla Legge 27 febbraio 2009, n. 14 di conversione, con modificazioni, del decreto-legge n. 207 del 30 dicembre 2008.

In particolare, l'art. 31 prevede che "I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta."

Il successivo art. 34 dispone che "Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:

a) autenticazione informatica;

b) adozione di procedure di gestione delle credenziali di autenticazione;

c) utilizzazione di un sistema di autorizzazione;

d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;

e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;

f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;

g) tenuta di un aggiornato documento programmatico sulla sicurezza;

h) adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari."

L'art. 35 stabilisce che "Il trattamento di dati personali effettuato senza l'ausilio di strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:

a) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative;

b) previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;

c) previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati."

Infine la Regola 19 del Disciplinare Tecnico in Materia di Misure Minime di Sicurezza (Allegato B al D. Lgs. 196/03), nell'indicare le modalità tecniche da adottare a cura del Titolare, del Responsabile ove designato, e dell'Incaricato, in caso di trattamento con strumenti elettronici, sottolinea espressamente come "Entro il 31 marzo di ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari redige anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza contenente idonee informazioni riguardo:

1) l'elenco dei trattamenti di dati personali;

2) la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;

3) l'analisi dei rischi che incombono sui dati;

4) le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonche' la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;

5) la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui al successivo punto 23;

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

7) la 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;

8) per i dati personali idonei a rivelare lo stato di salute e la vita sessuale di cui al punto 24 (trattati da organismi sanitari e da esercenti le professioni sanitarie), l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

L'Ente Locale Comunale che, in quanto Pubblica Amministrazione svolge per espressa previsione normativa una serie di finalità istituzionali indefettibili rivolte ai cittadini ed alle imprese che comportano la gestione di una notevole mole di dati personali di cui una parte **sensibili** e **giudiziari**, ha l'obbligo di redazione periodica del Documento Programmatico sulla Sicurezza.

Il presente D.P.S., che costituisce la REVISIONE periodica n. 03 al Documento Programmatico già adottato dall'Ente, può essere definito e catalogato come il **Documento Programmatico - Piano Operativo Annuale delle Misure di protezione**, il **Manuale della sicurezza organizzativa, fisica e logica dell'Ente** in quanto contiene l'esaustiva indicazione e l'attenta analisi dei rischi propri del **sistema informatico** (Hardware, Software, collegamenti, copie di sicurezza) che ospita dati personali, sensibili e giudiziari trattati dall'Ente, **delle risorse umane**, **degli eventi naturali** ovvero **degli incidenti** che possono riguardare e coinvolgere i dati personali dell'Amministrazione e focalizza l'attenzione sulle contromisure necessarie per contrastare o quanto meno ridurre i citati rischi.

Il D.P.S. mira ad illustrare gli elementi di novità rispetto al passato caratterizzanti il **programma di adeguamento dell'Ente alle Misure di Sicurezza** previste per il trattamento dei dati personali, sensibili e giudiziari dal D. Lgs. 196/2003 e dal suo Disciplinare Tecnico contenuto nell'Allegato B al citato Decreto.

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

Giova infatti in questa ottica evidenziare come l'applicazione del D. Lgs. 196/03 all'interno dell'Ente rappresenti una valida occasione di miglioramento organizzativo e procedurale e dia lo spunto perché si proceda ad una radicale revisione e razionalizzazione degli archivi e della regolamentazione dell'accesso agli stessi.

Sicuramente, l'Analisi e la Valutazione delle Minacce, delle Vulnerabilità e del Rischio residuo da abbattere (Sezione 6 e Sezione 6.1) rappresenta uno dei temi più importanti di tutto il Programma di adeguamento in quanto l'evidenza del Rischio Residuo potrà comportare la necessità di interventi, in taluni casi anche molto onerosi, sulle infrastrutture e sugli apparati informatici del Comune.

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

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

Con il presente Documento Programmatico, l'Amministrazione Comunale procede:

1. all'attenta verifica e ricognizione dell'architettura informatica e tecnologica presente ed alla descrizione del contesto ambientale in cui i dati personali sono conservati e custoditi
2. all'aggiornamento dell'elenco dei trattamenti di dati personali, sensibili e giudiziari effettuati a qualsiasi titolo dai diversi uffici dell'Ente
3. alla predisposizione dello schema di Informativa effettuata ai sensi dell'art. 13 D. Lgs. 196/03, da inserire nella modulistica resa disponibile dall'Ente a favore dell'utenza
4. all'indicazione esaustiva della distribuzione dei compiti e delle responsabilità tra i soggetti coinvolti
5. all'indicazione delle misure di sicurezza già adottate
6. all'analisi compiuta dei rischi e delle minacce potenziali e reali che incombono sui dati personali trattati
7. all'analisi e all'indicazione compiuta delle misure di sicurezza ancora da adottare
8. all'individuazione dei criteri e delle modalità di ripristino della disponibilità dei dati
9. alla pianificazione degli interventi formativi previsti per i soggetti individuati quali Responsabili e Incaricati del trattamento dei dati personali
10. alla descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare
11. all'indicazione delle misure prescritte dal Garante relativamente alla funzione di amministratore di sistema dell'Ente.

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

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

detta rilevazione si procede alla compiuta analisi del contesto ambientale nel quale gli strumenti elettronici utilizzati per il trattamento dei dati sono ospitati.

2. Censimento aggiornato dell'elenco dei trattamenti di dati personali effettuati dall'Ente

Il censimento delle banche dati e dei trattamenti è indispensabile per individuare quali sono i processi gestionali dei dati personali eseguiti all'interno della struttura pubblica e per la corretta gestione dei dati personali assoggettati a particolari regole da parte del dettato normativo.

Operativamente, si procede ad effettuare *in loco* un nuovo Censimento completo delle Banche Dati contenenti dati personali, sensibili e giudiziari trattati a qualsiasi titolo dagli Uffici dell'Ente, con l'indicazione delle informazioni essenziali per ciascun trattamento e, in particolare:

a) l'Ufficio di riferimento all'interno del quale viene effettuato il trattamento;
b) la descrizione sintetica del trattamento effettuato dall'Ufficio;
c) l'individuazione della natura dei dati trattati (dati personali, dati sensibili e/o dati giudiziari);
d) l'Area/Settore all'interno del quale è incardinato l'Ufficio che effettua il trattamento;
e) la descrizione sintetica della tipologia degli strumenti elettronici utilizzati per trattare i dati;
f) la sommaria indicazione delle misure di sicurezza adottate.

Le predette informazioni sono contenute all'interno di una tabella che viene elaborata con riferimento a ciascun Ufficio/Servizio in cui si articola l'organizzazione del Comune.

Giova precisare che, secondo quanto dettato dall'art. 18, comma 2, D. Lgs. 196/03, presupposto generale per la legittimità del trattamento di dati personali da parte di un soggetto pubblico è la necessità del trattamento per lo svolgimento delle funzioni istituzionali proprie del soggetto stesso: "Qualunque trattamento di dati personali da parte di soggetti pubblici è consentito soltanto per lo svolgimento delle funzioni istituzionali".

Si evidenzia inoltre che, a norma dell'art. 18, comma 4, D. Lgs. 196/03, i soggetti pubblici, laddove operino nei limiti previsti dalle finalità istituzionali, **non devono richiedere il consenso degli interessati**, pur dovendo procedere ad effettuare l'informativa secondo quanto espressamente disposto dall'art. 13 D. Lgs. 196/03.

Tale principio *funzionale,* codificato dall'art. 18, comma 4, sostituisce il "principio del consenso dell'interessato" sancito dall'art. 23 del Codice per il trattamento di dati personali da parte di privati o enti pubblici economici.

Infatti, per il soggetto pubblico, l'inerenza del trattamento ai suoi fini istituzionali costituisce l'unico indispensabile presupposto che legittima il trattamento di dati personali: se il trattamento dei dati è necessario per perseguire le funzioni istituzionali, il consenso dell'interessato è irrilevante.

In caso di trattamento dei dati per fini istituzionali, l'eventuale richiesta del consenso al trattamento, costituisce un atto non solo inidoneo a produrre effetti abilitativi al trattamento da parte di soggetti pubblici, ma anche contrario ai doveri d'ufficio del pubblico dipendete che lo pone in essere realizzando, di fatto, un rallentamento del procedimento o comunque dell'azione della P.A.

3. Informativa effettuata ai sensi dell'art. 13 D. Lgs. 196/03, da inserire nella modulistica resa disponibile dall'Ente a favore dell'utenza.

In questa Sezione viene riportato lo schema di Informativa da inserire nella modulistica dell'Amministrazione Comunale al fine di ottemperare a quanto previsto dall'art. 13 D. Lgs. 196/03.

Con riferimento all'informativa infatti, si ricorda che questa è sempre dovuta, anche qualora il consenso, come nel caso di trattamento effettuato da soggetto pubblico nell'ambito delle finalità istituzionali, non sia per legge necessario.

Con riferimento ai soggetti pubblici, l'informativa costituisce un adempimento obbligatorio anche quando il trattamento sia previsto da una disposizione normativa. Soltanto laddove i dati siano raccolti presso soggetti diversi da quelli a cui i dati si riferiscono, l'informativa può non essere fornita se i dati sono utilizzati in base ad un obbligo di legge o di regolamento.

4. Distribuzione dei compiti e delle responsabilità all'interno dell'Ente

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

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

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

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

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

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

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

In questa sede si procede all'analitica disamina delle Minacce Potenziali e Reali che incombono sui dati e più in generale sull'intero Sistema Informativo dell'Ente.

6.1 Criteri adottati per la valutazione dei rischi

In questa sottosezione si procede all'illustrazione dei criteri adottati per la valutazione dei rischi e per la definizione del Rischio Residuo.

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

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

L'indicazione delle citate misure di sicurezza sarà realizzata suddividendo, nelle seguenti sottosezioni (7.1 e 7.2) le stesse misure in **Misure Minime di Sicurezza,** in ottemperanza al Disciplinare Tecnico (Allegato B al D. Lgs.

196/03) relativamente ai punti da 1 a 26 e **Misure Idonee,** da adottare sia relativamente alle Banche Dati censite che, in senso più esteso, in relazione all'intero Sistema Informativo dell'Ente ai sensi dell'art. 31 del D. Lgs. 196/03.

7.1 Indicazione analitica delle Misure Minime di Sicurezza (ex art. 33 D. Lgs. 196/03 e Disciplinare Tecnico Regole da 1 a 26)

In questa sottosezione si procede all'indicazione delle **Misure Minime di Sicurezza,** in ottemperanza a quanto previsto dall'art. 33 D. Lgs. 196/03 e al Disciplinare Tecnico (Allegato B al D. Lgs. 196/03) relativamente ai punti da 1 a 26.

7.2 Indicazione analitica delle Misure Idonee di sicurezza (ex art. 31 D. Lgs. 196/03)

In questa sottosezione si procede invece all'indicazione delle **Misure Idonee** da adottarsi affinché i dati personali oggetto di trattamento da parte dell'Ente siano custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, in modo da ridurre al minimo, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

8. Individuazione dei criteri e delle modalità di ripristino della disponibilità dei dati in caso di distruzione o danneggiamento degli stessi dati o degli strumenti elettronici

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

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

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

In particolare, i Responsabili e gli Incaricati del trattamento, riceveranno una adeguata formazione che li renda edotti sui rischi che incombono sui dati, sulle misure rese disponibili per prevenire eventi dannosi, sulle misure di sicurezza idonee ancora da adottare e sui profili di responsabilità che derivano in capo al singolo Responsabile/Incaricato del trattamento nei casi di trattamento posto in essere in violazione delle norme dettate in materia di protezione dei dati personali.

10. Trattamenti affidati all'esterno

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

11. Gli Amministratori di sistema

In questo capitolo sono indicate le misure, prescritte dal Garante per la Protezione dei dati personali con il Provvedimento a carattere del 27/11/08 (G.U. n. 300 del 24/12/08) e con il Provvedimento del 25/06/09 (G.U. n. 149 del 30/06/09), ai Titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema.

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

SEZIONE	OGGETTO	SINTETICA DESCRIZIONE DEL CONTENUTO
1	**L'architettura Informatica dell'Ente**	**Indicazione ed analisi della Struttura e dell'architettura informatica e tecnologica dell'Ente. Esame del contesto ambientale in cui i dati sono conservati e custoditi**
2	**Censimento dei trattamenti di dati personali**	**Monitoraggio analitico delle banche dati trattate a qualsiasi titolo dagli Uffici dell'Ente**
3	**Informativa all'Interessato ai sensi dell' art. 13 D. Lgs. 196/03**	**Modello di Informativa all'interessato da inserire in tutta la modulistica resa disponibile dall'Ente ai sensi dell'articolo 13 D. Lgs. 196/03**
4	**Articolazione delle Responsabilità all'interno dell'Ente**	**Individuazione dei compiti e delle responsabilità che incombono in capo all'Ente nella sua qualità di Titolare del trattamento ed in capo ai soggetti individuati all'interno dell'Amministrazione come Responsabili e come Incaricati del trattamento dei dati**
5	**Misure di Sicurezza già adottate dall'Ente**	**Indicazione delle misure di sicurezza di cui l'Ente già dispone**
6	**Analisi dei rischi che incombono sui dati personali trattati**	**Descrizione analitica dei rischi potenziali e reali che incombono sui dati personali trattati dall'Ente**
6.1	**Criteri adottati per la valutazione dei rischi**	**Illustrazione dei criteri adottati per la valutazione dei rischi e per la conseguente definizione del Rischio Residuo**
7	**Misure di sicurezza che l'Ente deve ancora adottare**	**Esaustiva individuazione delle misure di sicurezza previste dal dettato normativo che l'Ente dovrà provvedere ad adottare**
7.1	**Indicazione analitica delle Misure Minime di Sicurezza**	**Analisi ed individuazione delle Misure Minime di Sicurezza, in ottemperanza a quanto previsto dall'art. 33 D. Lgs. 196/03 e al Disciplinare Tecnico (Allegato B al D. Lgs. 196/03) relativamente ai punti da 1 a 26.**
7.2	**Indicazione analitica delle Misure Idonee di sicurezza**	**Indicazione delle Misure di sicurezza Idonee da adottarsi affinché siano ridotti al minimo, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta**
8	**Descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati**	**Indicazione dei criteri e delle procedure adottati dall'Ente per il ripristino dei dati in caso di loro danneggiamento o di inaffidabilità sopraggiunta dello strumento elettronico**
9	**Pianificazione degli interventi formativi**	**Indicazione sintetica dei contenuti e delle modalità di svolgimento degli interventi formativi che l'Ente porrà in essere**

10	**Trattamenti di dati personali affidati all'esterno**	**Descrizione dei criteri individuati dall'Ente 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.**
11	**L'Amministratore di Sistema dell'Ente**	**Indicazione delle misure prescritte dal Garante per la Protezione dei dati personali ai Titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema.**

Paragrafo 3.

DEFINIZIONI

Per fini metodologici e di omogeneizzazione del linguaggio con riguardo agli Organi Ispettivi e di Vigilanza, si riportano, di seguito, le definizioni relative ai termini più comunemente usati nel presente Documento Programmatico per la Sicurezza nel Trattamento dei Dati Personali, Sensibili e Giudiziari sulla base delle indicazioni contenute nel D. Lgs. 196/03.

Autenticazione informatica

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

Blocco

La conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento.

Banca Dati

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

Comunicazione elettronica

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

Chiamata

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

Comunicazione

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

Diffusione

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

Credenziali di autenticazione

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

Dato personale

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

Dati identificativi

I dati personali che permettono l'identificazione diretta dell'interessato.

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
- 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 D.P.R. 313/2002, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli artt. 60-61 del codice di procedura penale.

Dati relativi al traffico

Qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione.

Dati relativi all'ubicazione

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

Dato anonimo

Il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile.

Garante

L'autorità di cui all'art. 153, istituita dalla Legge 675/1996.

Incaricati

Le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile.

Interessato

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

Misure minime

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

Parola chiave

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

Posta elettronica

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

Sistema di autenticazione informatica

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

Responsabile

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

Reti di comunicazione elettronica

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

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/c della Direttiva 02/21/CE del Parlamento europeo e del Consiglio, del 07-mar-2002.

Sistema di autorizzazione

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

Strumenti elettronici

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

Titolare

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

Trattamento

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

Utente

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

Paragrafo 4.

ORGANIZZAZIONE E ARTICOLAZIONE DELL'ENTE

Il Comune è organizzato in Servizi alle quali sono preposti i dipendenti costituenti la dotazione organica dell'Ente.
Il personale di ruolo può essere in alcuni casi affiancato, nell'esercizio dell'attività istituzionale, da personale a tempo determinato e da collaboratori a progetto e/o da consulenti esterni all'uopo incaricati.

Sono presenti sette Servizi secondo quanto di seguito indicato.

SERVIZIO AFFARI GENERALI - Responsabile Sig. Agostino PILO

- Segreteria Generale – Contratti
- Servizi Demografici
- Personale
- Ufficio Protocollo
- Commercio
- S.U.A.P.

SERVIZIO FINANZIARIO – Responsabile Rag. Rosalba MADDAU

- Servizi Finanziari
- Economato

SERVIZIO TECNICO 1 - Responsabile Ing. Giovanni SPANEDDA

- Lavori Pubblici
- Urbanistica
- Portualità
- Demanio Marittimo

SERVIZIO TECNICO 2 - Responsabile Ing. Giuseppe MUNDULA

- Edilizia Privata
- Manutenzioni
- Ambiente
- Ecologia
- Verde
- Informatizzazione

SERVIZIO VIGILANZA - Responsabile Comandante Antonio DENEGRI

- Corpo di Polizia Municipale

SERVIZIO SOCIO/CULTURALE - Responsabile Dott.ssa Maria Lucia STACCA

- Servizi Sociali
- Politiche educative giovanili
- Pubblica Istruzione
- Biblioteca
- Cultura e Musei
- Turismo
- Sport
- Spettacolo

AREA TRIBUTI - Responsabile Dott.ssa Beatrice MADDAU

- Servizio Tributi
- Servizio ICI
- Servizio TARSU – TOSAP – PUBBLICITA'

Paragrafo 5.

TRATTAMENTI EFFETTUATI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

Anche per i trattamenti effettuati senza l'ausilio di strumenti elettronici, come quelli posti in essere per la gestione di archivi di dati contenuti su supporti cartacei, il Disciplinare tecnico contiene sia prescrizioni generali sia regole ulteriori e specifiche per i trattamenti di dati sensibili e giudiziari.

Questa tipologia di trattamenti coincide con i trattamenti di atti e documenti cartacei, in originale ed in copia, posti in essere senza l'ausilio dello strumento informatico.

Come per i trattamenti effettuati con strumenti elettronici, le persone che accedono ai dati devono essere preventivamente individuate e potranno svolgere le operazioni di trattamento esclusivamente se preventivamente designate quali Incaricati del trattamento dei dati.

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

Il Codice si preoccupa, all'art. 35, di indicare le regole tecniche e disciplinari per queste tipologie di trattamenti, prevedendo che:
"il trattamento di dati personali effettuato senza l'ausilio di strumenti elettronici e' consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:
a) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative;
b) previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;
c) previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati.

Inoltre, nell'Allegato B al D. Lgs. 196/03 (Disciplinare Tecnico in materia di Misure Minime di Sicurezza), nelle Regole 27, 28 e 29 che di seguito si riportano, sono indicate le Modalità tecniche da adottarsi a cura del titolare, del responsabile, ove designato, e dell'incaricato, in caso di trattamento con strumenti diversi da quelli elettronici:

27. Agli incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati puo' essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

28. Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli

incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

29. L'accesso agli archivi contenenti dati sensibili o giudiziari e' controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.

I principi che stanno alla base della previsione normativa sono tre:

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

L'insieme di questi principi comporta l'obbligo di impartire agli incaricati istruzioni scritte finalizzate al controllo e alla custodia degli atti e dei documenti loro affidati.
L'organizzazione dei profili di accesso e gli aggiornamenti periodici sono finalizzati al rispetto del principio che gli incaricati abbiano accesso ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati.
La distinzione utile per l'individuazione dei profili di incarico per questa modalità di trattamento è la natura dei dati. Sarà perciò necessario individuare i trattamenti di dati sensibili e giudiziari, differenziandoli da quelli comuni, conseguentemente organizzare i singoli profili di incarico o i gruppi omogenei di persone autorizzate alla stessa attività.
L'organizzazione delle misure di sicurezza comporta una preventiva ricognizione dei trattamenti cartacei che può essere fatta congiuntamente a quella per individuare le operazioni svolte con strumenti elettronici, anche per individuarne le correlazioni.
Il nuovo testo normativo riconosce la relazione tra incaricati e unità organizzative dell'Ente. Di norma nell'ambito dell'articolazione delle attività svolte dall'Ente, sono raggruppate nella stesso settore/servizio/ufficio lavorazioni aventi la stessa finalità. Tutte le risorse umane assegnate alla stessa unità, avendo profili di incarico simili, sono considerate, ai fini dei trattamenti, un gruppo omogeneo. Ciò consente di descrivere il profilo dei trattamenti svolti per l'unità organizzativa e di correlarlo a tutte le persone assegnate a quel settore determinato. Le attività, però, non sono mai definitive, ma dinamiche e mutevoli in ragione dell'evoluzione normativa e regolamentare del settore di riferimento. Da ciò discende l'obbligo di verifica periodica e relativo aggiornamento con cadenza almeno annuale.

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

La protezione dei dati, specialmente se sensibili o giudiziari, riguarda anche la conservazione, che deve avvenire in archivi ad accesso selezionato. Le procedure di accesso a tali archivi sono finalizzate all'identificazione degli incaricati. Infatti,

secondo la norma tecnica (punto 29 del disciplinare) già richiamata, "l'accesso agli archivi contenenti dati sensibili o giudiziari è controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate."

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

Anche per quanto attiene all'archivio storico si dovrà adottare la rigida procedura prevista dal citato punto 29 del Disciplinare Tecnico.

SEZIONE 1
ARCHITETTURA INFORMATICA E TECNOLOGICA DELL'ENTE
CONTESTO AMBIENTALE IN CUI I DATI SONO CONSERVATI E CUSTODITI

Il Sistema Informatico del Comune è impostato e strutturato secondo il modello **Client / Server**.
Esiste infatti una infrastruttura di Rete Locale che interconnette le diverse Unità di Elaborazione tra loro.
E' presente un Server di Dominio e di Autenticazione (**ACER ALTOS G710**) e circa 30 Personal Computers, dislocati presso i diversi uffici Comunali, che risultano logicamente e fisicamente collegati tra loro.

Non si registra la presenza, all'interno della Casa Comunale, di elaboratori isolati (Stand Alone), non collegati alla Rete Locale, sistematicamente utilizzati dai dipendenti.

In occasione del sopralluogo realizzato presso la sede dell'Ente in data 15 Giugno 2010, si è osservato che il Server di Dominio e di Autenticazione (**ACER ALTOS G710**), il secondo Server che ospita gli applicativi utilizzati per la gestione dei Tributi (**ACER ALTOS G540**) e gli apparati di Rete, sono stati localizzati al piano terreno dell'edificio comunale, all'interno di un piccolo locale, **non climatizzato** e sprovvisto di aperture naturali verso l'esterno (finestre), che comunica a mezzo porta con altro locale di deposito (provvisto di finestra e climatizzato) al quale si ha accesso dall'Ufficio Anagrafe.

Sia la porta di accesso al primo locale di sgombero che la porta di accesso all'ambiente ospitante i Server, vengono lasciate sistematicamente aperte e dunque liberamente accessibili sia da parte dei dipendenti che da parte degli amministratori dell'Ente senza che sia possibile procedere, considerata la destinazione promiscua dei locali, ad una disciplina rigorosa degli accessi e ad un controllo degli stessi.

Si rimarca che, l'ambiente ospitante i Server, ricavato all'interno di un ripostiglio / locale di sgombero, è separato dagli altri ambienti esclusivamente a mezzo di porta lignea, non idonea a garantire l'adeguata compartimentazione del locale anche ai fini antincendio.
Tale aspetto determina, in caso di principio di incendio negli ambienti circostanti, un alto rischio di propagazione dello stesso al locale Server che necessita pertanto di un intervento quantomeno preordinato a garantire un R.E.I. complessivo pari a 120.

Dettaglio relativo alla porta di accesso all'ambiente ospitante i Server – Piano Terreno Casa Comunale

All'interno dell'ambiente ospitante i Server si osserva inoltre, la presenza delle borchie dedicate alla telefonia con conseguente ulteriore criticità rappresentata dall'esigenza di consentire l'accesso ai tecnici Telecom per le ordinarie attività di manutenzione degli apparati TLC.

Dettaglio relativo alla presenza della borchia TELECOM all'interno del locale ospitante i Server.

Si osserva ancora che, mentre lo Switch, il Router ed il Firewall sono stati adeguatamente segregati all'interno di un armadi Rack sospeso munito di serratura, i Server sono stati posizionati sopra una mensola in assenza di qualsivoglia presidio atto a compartimentali efficacemente rispetto all'ambiente circostante.

Dettaglio relativo all'armadio Rack sospeso ospitante il Firewall, il Router e lo Switch.

Dettaglio relativo ai Server posizionati sopra una mensola in assenza di qualsivoglia forma di compartimentazione rispetto all'ambiente circostante.

Si evidenzia infine l'assenza di una linea elettrica dedicata ed autonoma rispetto all'impianto generale, per l'alimentazione delle macchine e degli apparati di rete.

APPARATI INTERMEDI DI RETE

Per la gestione della LAN Comunale, si evidenzia la presenza di uno SWITCH **LEVEL ONE FSW-2409 TFX** a 24 porte, con velocità di transito dei dati pari a 10/100 Mbps.

SWITCH LEVEL ONE FSW-2409 TFX

IL SERVER DI DOMINIO ACER ALTOS G710

Il Server di Dominio e di Autenticazione **ACER ALTOS G710** (Processore INTEL XEON - Sistema operativo WINDOWS 2003 SERVER), dotato di doppi HDD in Raid 1, gestisce e controlla il Dominio ovvero il raggruppamento delle utenze e delle risorse presenti nella Rete dell'Ente: conserva tutte le informazioni sulle utenze (ID e PASSWORD) e sui permessi di accesso alle risorse disponibili e verifica la validità delle login e delle password fornite dai Clients con cui viene permesso l'accesso alle risorse richieste.

Dettaglio relativo al Server di Dominio ACER ALTOS G710.

Con la configurazione RAID 1, i dati vengono scritti sui diversi dischi, così che uno sia copia speculare dell'altro e qualora dovesse esserci qualche problema e/o errore di scrittura-lettura, oppure ancora di perdita di dati, il sistema andrà a recuperare le informazioni sull'altro hard disk, così da garantire la continuità delle operazioni. Questa modalità oltre a massimizzare la sicurezza dei dati, in caso di rottura di un disco rende possibile, a sistema funzionante, la sostituzione dell'hard disk danneggiato, senza perdita di dati e necessità di spegnere e/o riavviare il sistema garantendo continuità al funzionamento del sistema.

Lo stesso Server di Dominio **ACER ALTOS G710**, ospita alcuni dei Programmi di Gestione utilizzati dagli Uffici dell'Ente. In particolare, sul Server di Dominio, sono ospitati i programmi per la gestione dei Servizi Demografici e del Protocollo Informatico sviluppati dalla Software House **MAGGIOLI SPA** e gli applicativi per la Finanziaria e le Paghe forniti all'Ente dalla **ZUDDAS srl** di Cagliari.

Sul Server di Dominio ovvero su altra macchina dedicata, dovranno con urgenza essere configurate cartelle dedicate in via esclusiva ad ogni singolo dipendente al fine della corretta esecuzione delle copie di backup.
In particolare sarà necessario configurare il sistema informatico comunale in modo tale che le cartelle di lavoro dei singoli utenti, all'interno delle quali si elaboreranno i documenti di competenza di ciascuno, non siano più residenti in locale sul singolo Client ma siano ospitate sul Server e, conseguentemente, il dipendente, non possa più elaborare i documenti sul proprio disco ma direttamente sulle cartelle residenti sul Server.

IL SERVER ACER ALTOS G540.

L'Ente dispone di un secondo Server, **ACER ALTOS G540** (Processore INTEL XEON - Sistema operativo WINDOWS 2003 SERVER), anch'esso dotato di doppi HDD in Raid 1, sul quale sono residenti gli applicativi per la gestione dei Tributi fornito all'Ente dalla **ZUDDAS srl** di Cagliari ed il Software utilizzato dall'Ufficio Tecnico per l'Urbanistica.


Dettaglio relativo al secondo Server, ACER ALTOS G540.

PROCEDURE PER IL BACKUP DEI DATI RESIDENTI SUI SERVER

Con riferimento alle procedure ed ai dispositivi utilizzati per il salvataggio dei dati e degli applicativi residenti sul Server di Dominio **ACER ALTOS G710** e sul Server **ACER ALTOS G540**, si evidenzia che oltre alla copia di sicurezza garantita dalla presenza di doppi Hard Disk uniti in Raid 1, l'Ente, al fine di offrire adeguata garanzia di integrità, disponibilità e riservatezza alle informazioni ivi residenti, ha provveduto ad acquistare e configurare un'Unità di Backup su cassette DAT integrata ai Server, attraverso la quale si procede, con frequenza codificata settimanale ed in modalità manuale, ad effettuare una copia di sicurezza dei dati ospitati su Cassette DAT.
Le cassette DAT utilizzate per la realizzazione delle copie di Backup dei Server, sono poi rigorosamente custodite in armadi muniti di serratura.

PROCEDURE PER IL BACKUP DEI DATI RESIDENTI SUI SINGOLI CLIENTS

Si evidenzia una situazione di forte criticità, che espone l'Ente a livelli di vulnerabilità non accettabili, sui singoli Clients che, in linea generale, o non provvedono alla esecuzione di copie di sicurezza ovvero provvedono con periodicità non sempre codificata o comunque non espressamente definita.
L'Ente, infatti, non ha ancora provveduto alla configurazione su Server (ovvero su altra macchina dedicata), di CARETLLE DEDICATE IN VIA ESCLUSIVA a ciascun dipendete per l'elaborazione dei documenti di competenza: tutti gli utenti della LAN Comunale, elaborano dunque i documenti relativi ai procedimenti loro attribuiti esclusivamente in locale sul singolo Client.
Inoltre, come detto, non sono adottate con sistematicità e rigore procedure codificate di salvataggio e messa in sicurezza dei dati: in questo modo, gli stessi dati e le informazioni residenti unicamente sul disco fisso di ciascun PC Client sono esposti al rischio di perdita delle caratteristiche primarie di disponibilità, integrità e riservatezza.

Al fine di rimuovere definitivamente l'attuale situazione di forte criticità e vulnerabilità, sarà necessario provvedere con urgenza alla definizione delle procedure interne per la corretta esecuzione delle copie di backup.
In particolare, si dovrà provvedere con immediatezza a configurare sullo stesso Server di Dominio ovvero su altro elaboratore, cartelle di lavoro dedicate in via esclusiva ad ogni singolo dipendente, alle quali dovrà avere accesso esclusivamente l'utente, da utilizzarsi per la corretta gestione dei dati al fine dell'esecuzione delle copie di sicurezza.

Sarà necessario configurare il sistema informatico comunale in modo tale che le cartelle di lavoro dei singoli utenti, all'interno delle quali si elaboreranno i documenti di competenza di ciascuno, non siano residenti in locale sul singolo Client ma siano ospitate direttamente sul Server ed il dipendente non possa più elaborare i documenti sul proprio disco locale ma direttamente sulle cartelle residenti sul Server.
Le citate cartelle dovranno essere accessibili esclusivamente dall'utente per il quale sono state configurate.

Per la gestione dei documenti condivisi tra più utenti si utilizzeranno invece differenti cartelle "di condivisione".

AUTENTICAZIONE PER L'ACCESSO ALLA RETE LOCALE

Il Server di dominio e Autenticazione (**ACER ALTOS G710**)**,** verifica l'identità dei Client per l'accesso alla Rete Locale attraverso la richiesta di una Password di Rete.
Si registra quindi una corretta gestione delle procedure per l'accesso alla Rete Locale dell'Ente.
Infatti, ogni utente può accedere alla LAN attraverso un codice identificativo (USER ID) e una PASSWORD. L'identificativo e la Password sono attribuiti in via esclusiva a ciascun dipendente individuato quale incaricato del trattamento dei dati e il Server di Dominio conserva tutte le informazioni sulle utenze e sui permessi di accesso alle risorse disponibili, previa verifica della validità delle login e delle password fornite dai Client.

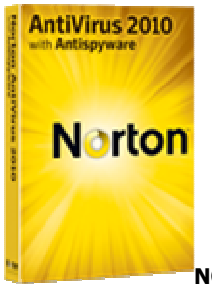
ANTIVIRUS

Nell'Ente non è presente una gestione centralizzata della distribuzione dell'Antivirus.

Tuttavia, i singoli Clients presenti in casa comunale (ed anche i Server) sono dotati di programmi Antivirus (**AVIRA McAfee, NORTON, AVG** Antivirus) che vengono aggiornati con cadenza codificata giornaliera ed in modalità automatica.

AVIRA Antivirus

McAfee Antivirus



NORTON ANTIVIRUS

AVG ANTIVIRUS

COLLEGAMENTO AD INTERNET E PROTEZIONE FIREWALL

L'accesso ad Internet da parte di tutti gli elaboratori collegati alla LAN Comunale, avviene attraverso il Router centralizzato **Telecom SPEEDTOUCH** su linea ADSL.

Da quanto rilevato e dichiarato in sede di sopralluogo, la connessione ad Internet risulta adeguatamente protetta grazie alla presenza di un Firewall Hardware (**CHECK POINT SAFE OFFICE 500**) opportunamente configurato con la chiusura delle porte logiche.

Dettaglio relativo al Router SPEEDTOUCH ed al Firewall CHECK POINT SAFE OFFICE 500

GRUPPI DI CONTINUITA'

In Comune, non è presente un gruppo di continuità centralizzato per tutti gli Uffici, idoneo ad evitare danni ai dati personali trattati nell'ipotesi in cui venga a mancare l'erogazione della corrente elettrica. L'unica forma di protezione adottata per contrastare gli eventuali sbalzi di tensione elettrica, è rappresentata dalla presenza di singoli gruppi di continuità collegati, in locale, a tutti gli elaboratori dell'Ente ed ai Server.

PROCEDURE PER L'AUTENTICAZIONE INFORMATICA

Per quanto attiene alla gestione del sistema e delle procedure per l'autenticazione informatica, si evidenzia quanto segue.

Per accedere al proprio PC, non si è provveduto ad attribuire a tutti i dipendenti individuati quali Incaricati del trattamento dei dati, una **credenziale di autenticazione** costituita da una User-Id e da una Password.

Inoltre la stessa Password (che rappresenta la componente riservata della credenziale di autenticazione), anche laddove attribuita, sebbene risulti essere conosciuta esclusivamente da ciascun incaricato, come espressamente previsto dalla Regola 4 dell'Allegato B al D. Lgs. 196/03, non sempre risulta essere composta da un numero di caratteri alfanumerici pari almeno ad otto (secondo quanto espressamente dettato dalla Regola 5 contenuta nel citato Allegato B al Codice).

La stessa Password, non viene autonomamente modificata da ciascun utente al primo utilizzo e, successivamente, con cadenza semestrale ovvero trimestrale nell'ipotesi di trattamento di dati sensibili o giudiziari (secondo quanto prevede espressamente il dettato normativo alla Regola 5 del già citato allegato B al Codice).

POSTA ELETTRONICA CERTIFICATA E SMART CARD

Non è presente un Server per la gestione della posta elettronica dell'Ente (MAIL SERVER).

L'Ente dispone di una utenza di posta elettronica certificata (PEC) utilizzata dall'Ufficio Anagrafe.

L'Ente ha provveduto all'acquisto di 2 Kit (lettori e relativo software di gestione), per le procedure di firma elettronica (SMART CARD). I citati dispositivi sono utilizzati dall'Ufficio Tecnico (Edilizia Privata – Manutenzioni) e dall'Ufficio Tributi.

SOFTWARE

Periodicamente sono installati gli ultimi aggiornamenti del Sistema operativo e delle applicazioni.

I Software gestionali utilizzati sono dotati di regolare licenza d'uso e si procede al loro aggiornamento ad ogni release del produttore.

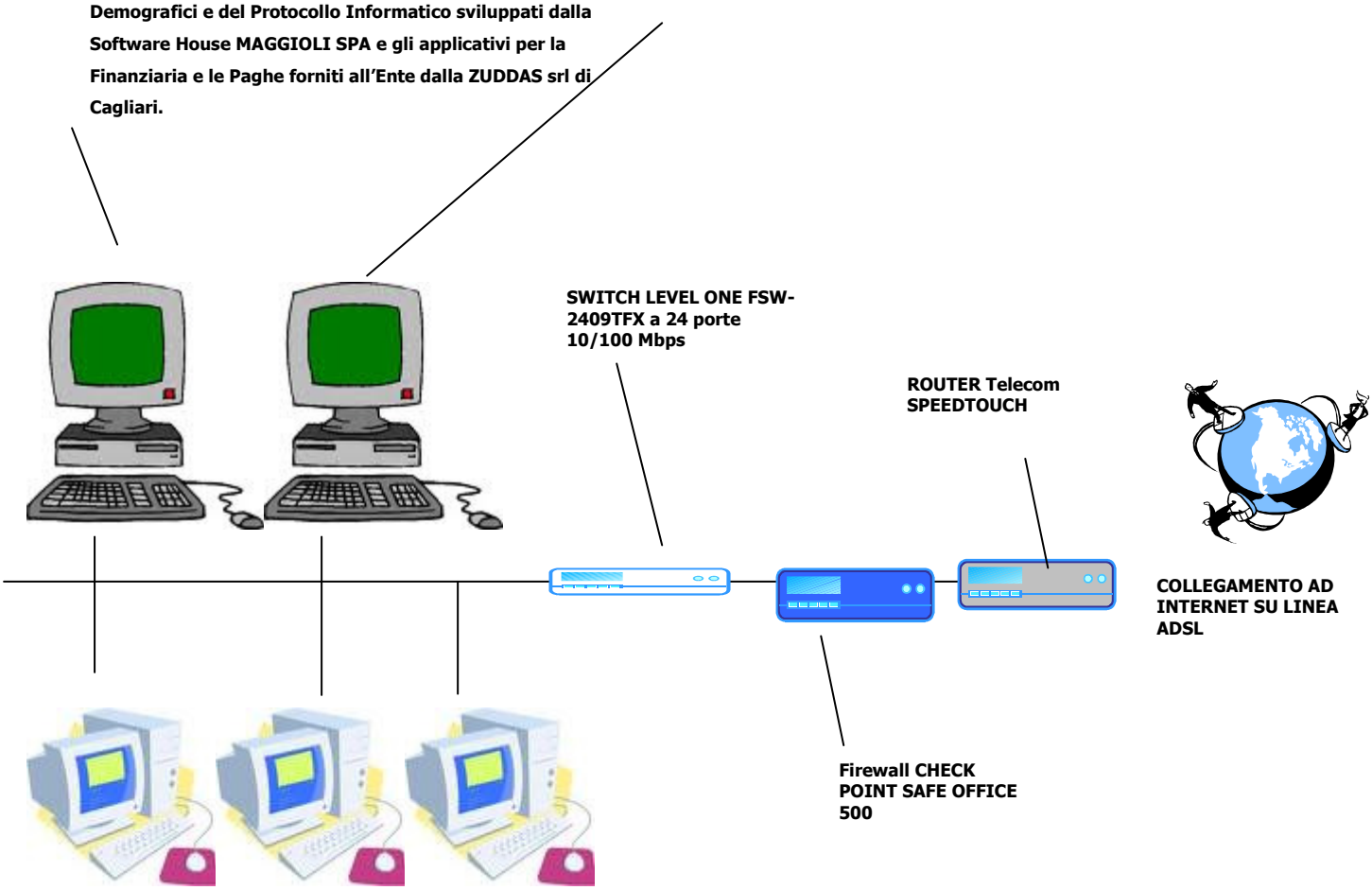
SEDE MUNICIPALE

Server ACER ALTOS G710 (Processore INTEL XEON - Sistema Operativo Windows 2003 Server) opera con le seguenti funzionalità:

- **Server di Dominio e di Autenticazione**
- **Ospita alcuni dei Programmi di Gestione utilizzati dagli Uffici dell'Ente. In particolare, sul Server di Dominio, sono ospitati i programmi per la gestione dei Servizi Demografici e del Protocollo Informatico sviluppati dalla Software House MAGGIOLI SPA e gli applicativi per la Finanziaria e le Paghe forniti all'Ente dalla ZUDDAS srl di Cagliari.**

Server ACER ALTOS G540 (Processore INTEL XEON - Sistema operativo WINDOWS 2003 SERVER), opera con le seguenti funzionalità:

- **Ospita gli applicativi per la gestione dei Tributi fornito all'Ente dalla ZUDDAS srl di Cagliari ed il Software utilizzato dall'Ufficio Tecnico per l'Urbanistica.**



SCHEDA SINTETICA RIASSUNTIVA

CARATTERISTICHE DEL SISTEMA INFORMATICO – TECNOLOGICO DELL'ENTE

- Il Sistema Informatico del Comune è basato sul modello **Client / Server**.
  Esiste infatti una infrastruttura di Rete Locale che interconnette le diverse Unità di Elaborazione tra loro.
- E' presente un Server di Dominio e di Autenticazione (**ACER ALTOS G710**) e circa 30 Personal Computers, dislocati presso i diversi uffici Comunali, che risultano logicamente e fisicamente collegati tra loro.
- Non si registra la presenza, all'interno della Casa Comunale, di elaboratori isolati (Stand Alone), non collegati alla Rete Locale, sistematicamente utilizzati dai dipendenti.
- Il Server di Dominio e di Autenticazione (**ACER ALTOS G710**), il secondo Server che ospita gli applicativi utilizzati per la gestione dei Tributi (**ACER ALTOS G540**) e gli apparati di Rete, sono stati localizzati al piano terreno dell'edificio comunale, all'interno di un piccolo locale, **non climatizzato** e sprovvisto di aperture naturali verso l'esterno, che comunica a mezzo porta con altro locale di deposito (provvisto di finestra e climatizzato) al quale si ha accesso dall'Ufficio Anagrafe.
  Sia la porta di accesso al primo locale di sgombero che la porta di accesso all'ambiente ospitante i Server, vengono lasciate sistematicamente aperte e dunque liberamente accessibili sia da parte dei dipendenti che da parte degli amministratori dell'Ente senza che sia possibile procedere, considerata la destinazione promiscua dei locali, ad una disciplina rigorosa degli accessi e ad un controllo degli stessi.
  Si rimarca che, l'ambiente ospitante i Server, ricavato all'interno di un ripostiglio / locale di sgombero, è separato dagli altri ambienti esclusivamente a mezzo di porta lignea, non idonea a garantire l'adeguata compartimentazione del locale anche ai fini antincendio.
  Tale aspetto determina, in caso di principio di incendio negli ambienti circostanti, un alto rischio di propagazione dello stesso al locale Server che necessita pertanto di un intervento quantomeno preordinato a garantire un R.E.I. complessivo pari a 120.
  All'interno dell'ambiente ospitante i Server si osserva inoltre, la presenza delle borchie dedicate alla telefonia con conseguente ulteriore criticità rappresentata dall'esigenza di consentire l'accesso ai tecnici Telecom per le ordinarie attività di manutenzione degli apparati TLC.
  Si osserva ancora che, mentre lo Switch, il Router ed il Firewall sono stati adeguatamente segregati all'interno di un armadi Rack sospeso munito di serratura, i Server sono stati posizionati sopra una mensola in assenza di qualsivoglia presidio atto a compartimentali efficacemente rispetto all'ambiente circostante.
  Si evidenzia infine l'assenza di una linea elettrica dedicata ed autonoma rispetto all'impianto generale, per l'alimentazione delle macchine e degli apparati di rete.
- Per la gestione della LAN Comunale, si evidenzia la presenza di uno SWITCH **LEVEL ONE FSW-2409 TFX** a 24 porte, con velocità di transito dei dati pari a 10/100 Mbps.
- Il Server di Dominio e di Autenticazione **ACER ALTOS G710** (Processore INTEL XEON - Sistema operativo WINDOWS 2003 SERVER), dotato di doppi HDD in Raid 1, gestisce e controlla il Dominio ovvero il raggruppamento delle utenze e delle risorse presenti nella Rete dell'Ente: conserva tutte le informazioni sulle utenze (ID e PASSWORD) e sui permessi di accesso alle risorse disponibili e verifica la validità delle login e delle password fornite dai Clients con cui viene permesso l'accesso alle risorse richieste.

Lo stesso Server di Dominio **ACER ALTOS G710**, ospita alcuni dei Programmi di Gestione utilizzati dagli Uffici dell'Ente. In particolare, sul Server di Dominio, sono ospitati i programmi per la gestione dei Servizi Demografici e del Protocollo Informatico sviluppati dalla Software House **MAGGIOLI SPA** e gli applicativi per la Finanziaria e le Paghe forniti all'Ente dalla **ZUDDAS srl** di Cagliari.

- **Sul Server di Dominio ovvero su altra macchina dedicata, dovranno con urgenza essere configurate cartelle dedicate in via esclusiva ad ogni singolo dipendente al fine della corretta esecuzione delle copie di backup.**

  In particolare sarà necessario configurare il sistema informatico comunale in modo tale che le cartelle di lavoro dei singoli utenti, all'interno delle quali si elaboreranno i documenti di competenza di ciascuno, non siano più residenti in locale sul singolo Client ma siano ospitate sul Server e, conseguentemente, il dipendente, non possa più elaborare i documenti sul proprio disco ma direttamente sulle cartelle residenti sul Server.
- L'Ente dispone di un secondo Server, **ACER ALTOS G540** (Processore INTEL XEON - Sistema operativo WINDOWS 2003 SERVER), anch'esso dotato di doppi HDD in Raid 1, sul quale sono residenti gli applicativi per la gestione dei Tributi fornito all'Ente dalla **ZUDDAS srl** di Cagliari ed il Software utilizzato dall'Ufficio Tecnico per l'Urbanistica.
- Con riferimento alle procedure ed ai dispositivi utilizzati per il salvataggio dei dati e degli applicativi residenti sul Server di Dominio **ACER ALTOS G710** e sul Server **ACER ALTOS G540**, si evidenzia che oltre alla copia di sicurezza garantita dalla presenza di doppi Hard Disk uniti in Raid 1, l'Ente, al fine di offrire adeguata garanzia di integrità, disponibilità e riservatezza alle informazioni ivi residenti, ha provveduto ad acquistare e configurare un'Unità di Backup su cassette DAT integrata ai Server, attraverso la quale si procede, con frequenza codificata settimanale ed in modalità manuale, ad effettuare una copia di sicurezza dei dati ospitati su Cassette DAT.

  Le cassette DAT utilizzate per la realizzazione delle copie di Backup dei Server, sono poi rigorosamente custodite in armadi muniti di serratura.
- Si evidenzia una situazione di forte criticità, che espone l'Ente a livelli di vulnerabilità non accettabili, sui singoli Clients che, in linea generale, o non provvedono alla esecuzione di copie di sicurezza ovvero provvedono con periodicità non sempre codificata o comunque non espressamente definita.

  L'Ente, infatti, non ha ancora provveduto alla configurazione su Server (ovvero su altra macchina dedicata), di CARETLLE DEDICATE IN VIA ESCLUSIVA a ciascun dipendete per l'elaborazione dei documenti di competenza: tutti gli utenti della LAN Comunale, elaborano dunque i documenti relativi ai procedimenti loro attribuiti esclusivamente in locale sul singolo Client.

  Inoltre, come detto, non sono adottate con sistematicità e rigore procedure codificate di salvataggio e messa in sicurezza dei dati: in questo modo, gli stessi dati e le informazioni residenti unicamente sul disco fisso di ciascun PC Client sono esposti al rischio di perdita delle caratteristiche primarie di disponibilità, integrità e riservatezza.

  Al fine di rimuovere definitivamente l'attuale situazione di forte criticità e vulnerabilità, sarà necessario provvedere con urgenza alla definizione delle procedure interne per la corretta esecuzione delle copie di backup.

  In particolare, si dovrà provvedere con immediatezza a configurare sullo stesso Server di Dominio ovvero su altro elaboratore, cartelle di lavoro dedicate in via esclusiva ad ogni singolo

dipendente, alle quali dovrà avere accesso esclusivamente l'utente, da utilizzarsi per la corretta gestione dei dati al fine dell'esecuzione delle copie di sicurezza.

Sarà necessario configurare il sistema informatico comunale in modo tale che le cartelle di lavoro dei singoli utenti, all'interno delle quali si elaboreranno i documenti di competenza di ciascuno, non siano residenti in locale sul singolo Client ma siano ospitate direttamente sul Server ed il dipendente non possa più elaborare i documenti sul proprio disco locale ma direttamente sulle cartelle residenti sul Server.

Le citate cartelle dovranno essere accessibili esclusivamente dall'utente per il quale sono state configurate.

Per la gestione dei documenti condivisi tra più utenti si utilizzeranno invece differenti cartelle "di condivisione".

- Nonostante nell'Ente non sia presente una distribuzione centralizzata degli aggiornamenti dell'Antivirus, i singoli Clients presenti in casa comunale (ed anche i Server) sono dotati di programmi Antivirus (**AVIRA McAfee, NORTON, AVG** Antivirus) che vengono aggiornati con cadenza codificata giornaliera ed in modalità automatica.
- L'accesso ad Internet da parte di tutti gli elaboratori collegati alla LAN Comunale, avviene attraverso il Router centralizzato **Telecom SPEEDTOUCH** su linea ADSL.
- Da quanto rilevato e dichiarato in sede di sopralluogo, la connessione ad Internet risulta adeguatamente protetta grazie alla presenza di un Firewall Hardware (**CHECK POINT SAFE OFFICE 500**) opportunamente configurato con la chiusura delle porte logiche.
- In Comune, non è presente un gruppo di continuità centralizzato per tutti gli Uffici, idoneo ad evitare danni ai dati personali trattati nell'ipotesi in cui venga a mancare l'erogazione della corrente elettrica. L'unica forma di protezione adottata per contrastare gli eventuali sbalzi di tensione elettrica, è rappresentata dalla presenza di singoli gruppi di continuità collegati, in locale, a tutti gli elaboratori dell'Ente ed ai Server.
- Per quanto attiene alla gestione del sistema e delle procedure per l'autenticazione informatica, si evidenzia quanto segue.

  Per accedere al proprio PC, non si è provveduto ad attribuire a tutti i dipendenti individuati quali Incaricati del trattamento dei dati, una **credenziale di autenticazione** costituita da una User-Id e da una Password.

  Inoltre la stessa Password (che rappresenta la componente riservata della credenziale di autenticazione), anche laddove attribuita, sebbene risulti essere conosciuta esclusivamente da ciascun incaricato, come espressamente previsto dalla Regola 4 dell'Allegato B al D. Lgs. 196/03, non sempre risulta essere composta da un numero di caratteri alfanumerici pari almeno ad otto (secondo quanto espressamente dettato dalla Regola 5 contenuta nel citato Allegato B al Codice).

  La stessa Password, non viene autonomamente modificata da ciascun utente al primo utilizzo e, successivamente, con cadenza semestrale ovvero trimestrale nell'ipotesi di trattamento di dati sensibili o giudiziari (secondo quanto prevede espressamente il dettato normativo alla Regola 5 del già citato allegato B al Codice).
- Non è presente un Server per la gestione della posta elettronica dell'Ente (MAIL SERVER).
- L'Ente dispone di una utenza di posta elettronica certificata (PEC) utilizzata dall'Ufficio Anagrafe.

- L'Ente ha provveduto all'acquisto di 2 Kit (lettori e relativo software di gestione), per le procedure di firma elettronica (SMART CARD). I citati dispositivi sono utilizzati dall'Ufficio Tecnico (Edilizia Privata – Manutenzioni) e dall'Ufficio Tributi.
- Periodicamente sono installati gli ultimi aggiornamenti del Sistema operativo e delle applicazioni.
- I Software gestionali utilizzati sono dotati di regolare licenza d'uso e si procede al loro aggiornamento ad ogni release del produttore.Esiste infatti una infrastruttura di Rete Locale che interconnette le diverse Unità di Elaborazione tra loro.

SEZIONE 2

L'ELENCO DEI TRATTAMENTI DI DATI PERSONALI EFFETTUATI DALL'ENTE

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

La ricognizione ed il censimento delle Banche Dati e dei Trattamenti sono stati realizzati mediante sopralluoghi effettuati presso ogni singolo ufficio dell'Ente con la collaborazione dei Responsabili del trattamento dei dati e degli Incaricati di volta in volta preposti al trattamento.

Per ogni Banca Dati individuata nel corso dell'attività di censimento è stato specificato:

- La denominazione sintetica della Banca Dati
- Il Settore/Area di riferimento
- L'ufficio dove la banca dati è detenuta, custodita e, più in generale, trattata
- La natura dei dati trattati (con la specificazione della tipologia: dati personali "comuni", dati sensibili o dati giudiziari)
- La tipologia di supporto sul quale sono registrati i dati (supporto cartaceo ovvero informatico)
- La tipologia dell'unità di elaborazione (con l'indicazione se si tratti di un elaboratore isolato, cioè non collegato alla LAN Comunale ovvero in Rete)
- La sintetica descrizione delle misure di protezione adottate.

SEZIONE 3

INFORMATIVA EFFETTUATA AI SENSI DELL'ART. 13 D. LGS. 196/03

L'informativa all'interessato deve essere resa dal Titolare (ovvero dal/dai Responsabile/i se designato/i) prima di iniziare la raccolta dei dati personali.

Ogni soggetto pubblico o privato che raccolga dati personali deve far conoscere al soggetto al quale i dati si riferiscono una serie di elementi ed informazioni espressamente indicati dall'art. 13 D. Lgs. 196/03 che costituiscono il contenuto minimo della stessa informativa.

In particolare, l'informativa deve contenere l'indicazione:

a) delle finalità e delle modalità del trattamento cui sono destinati i dati;
b) della natura obbligatoria o facoltativa del conferimento dei dati;
c) delle conseguenze di un eventuale rifiuto di rispondere;
d) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne

a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi;
e) dei diritti dell'interessato di cui all'articolo 7;
f) degli estremi identificativi del titolare e, se designati, del rappresentante nel territorio dello Stato ai sensi dell'articolo 5 e del responsabile. Quando il titolare ha designato più responsabili e' indicato almeno uno di essi (…).

Nella presente Sezione 3 del Documento viene riportato lo schema di Informativa all'Interessato che l'Ente utilizzerà inserendola nella modulistica resa disponibile all'utenza.

Schema di Informativa effettuata ai sensi dell'art. 13 D. Lgs. 196/03

Nello Schema di informativa che segue, le parti evidenziate in rosso, necessitano di un intervento integrativo per poter essere adeguate alla realtà operativa di volta in volta considerata.

La informiamo, ai sensi dell'art. 13 del Codice in materia di protezione dei dati personali (D.Lgs. 196/03), che il trattamento dei Suoi dati personali avviene secondo modalità idonee a garantire sicurezza e riservatezza ed è effettuato usando supporti cartacei, informatici e/o telematici per lo svolgimento delle attività della nostra Amministrazione atti a memorizzare, gestire e trasmettere i dati stessi.

Ai sensi dell'art. 4, comma 1 lett. a) D. Lgs. 196/2003, per "trattamento" si intende qualunque operazione o complesso di operazioni svolte con o senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modifica, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione la cancellazione e la distruzione dei dati personali anche se non registrati in una banca dati.

Ai sensi dell'art. 4, comma 1 lett. b) D. Lgs. 196/2003, per "dato personale" si intende 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.

Ai sensi dell'art. 4, comma 1 lett. c) D. Lgs. 196/2003, per "dati identificativi" si intendono i dati personali che permettono l'identificazione diretta dell'interessato.

Ai sensi dell'art. 4, comma 1 lett. d) D. Lgs. 196/2003, per "dati sensibili" si intendono 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.

Ai sensi dell'art. 4, comma 1 lett. e) D. Lgs. 196/2003, per "dati giudiziari" si intendono 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 D.P.R. 313/2002, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli artt. 60-61 del codice di procedura penale.

Ai sensi e per gli effetti del D. Lgs.196/2003 comunichiamo che i dati raccolti con la presente domanda, saranno trattati dall'Amministrazione Comunale esclusivamente al fine di espletare le attività di erogazione del servizio ..... nel rispetto del D. Lgs. 196/03 per il periodo necessario allo svolgimento dell'attività amministrativa correlata.

Il trattamento dei dati sarà improntato ai principi di necessità, correttezza, liceità, imparzialità e trasparenza; i dati saranno raccolti e registrati unicamente per gli scopi sopraindicati e saranno tutelate la Sua dignità e la Sua riservatezza.

Il conferimento dei dati è obbligatorio secondo quanto espressamente previsto dalla L. .....

Oppure, in alternativa:

Il conferimento dei dati è facoltativo, ma un eventuale rifiuto di fornirli comporterà l'impossibilità per il Comune di utilizzare i dati per le finalità indicate, con la conseguenza che non sarà possibile la erogazione dei servizi richiesti.

I dati raccolti con la presente domanda potranno essere comunicati agli altri soggetti pubblici individuati da norma di Legge o di Regolamento e/o diffusi in seguito a pubblicazione in albo pretorio.

Titolare del trattamento dei dati è il Comune inteso come Ente nel suo complesso.

Il responsabile del trattamento dei dati è ..... (nome e cognome del responsabile del trattamento dei dati se individuato).

L'interessato gode dei diritti di cui all'art. 7 del decreto legislativo 30 giugno 2003 n. 196, il cui testo è riprodotto qui di seguito:

Art.7 Diritti dell'interessato

1. 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.
2. L'interessato ha diritto di ottenere l'indicazione:
a) dell'origine dei dati personali;
b) delle finalità e modalità del trattamento;
c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;
d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2;
e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.
3. L'interessato ha diritto di ottenere:
a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati;
b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
c) l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.

4. L'interessato ha diritto di opporsi, in tutto o in parte:
a) per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;
b) al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

In particolare l'art. 7 D. Lgs. 196/03 conferisce agli interessati l'esercizio di specifici diritti. L'interessato può ottenere dal Titolare la conferma dell'esistenza o meno di propri dati personali che lo riguardano e la loro comunicazione in forma intelligibile. L'interessato può altresì chiedere di conoscere l'origine dei dati, le finalità e le modalità del trattamento, nonché la logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici, l'indicazione degli estremi identificativi del Titolare, dei responsabili nominati e dei soggetti o delle categorie di soggetti ai quali i dati possono essere comunicati o che possono venirne a conoscenza. L'interessato ha diritto di ottenere l'aggiornamento, la rettificazione, l'integrazione, la cancellazione, la trasformazione in via anonima o il blocco dei dati trattati in violazione di legge.

Le modalità di trattamento e le misure di sicurezza idonee alla protezione dei dati sono specificate nel Documento Programmatico sulla Sicurezza dei dati personali del Comune. Tale documento è stato redatto in conformità ai requisiti prescritti dal D. Lgs 196/03 e viene aggiornato annualmente anche in risposta all'evolversi delle tecnologie volte alla migliore la protezione dei dati.

Dichiaro di aver ricevuto tutte le informazioni di cui all'art. 13 del D. Lgs. 196/03 in relazione ai dati contenuti nei documenti allegati.

L'interessato al trattamento dei dati (art. 4, comma 1, lett. b D. Lgs. 196/03)

…… (Firma per esteso)

SEZIONE 4
DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITA' ALL'INTERNO DELL'ENTE

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

L'Ente, con Deliberazione della Giunta (Allegato 1, lettera A al presente Documento), provvede ad individuare i Responsabili del Trattamento (coincidenti con i responsabili di Area/Settore già esistenti nella pianta organica dell'Ente) e questi, conformemente al disposto normativo, designano con propria determinazione, gli Incaricati del trattamento dei dati, adottando gli atti di nomina e di designazione allegati alla presente sezione (Allegato 1, lettera C).
L'obbligo di protezione dei dati personali trattati riguarda il Titolare del trattamento, il Responsabile/i, gli Incaricati e più ampiamente chiunque sia tenuto all'adozione di misure di sicurezza, ivi compreso l'Amministratore del Sistema Informatico, che potrà essere interno o esterno all'Ente.

IL TITOLARE DEL TRATTAMENTO

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

L'art. 28 del Codice precisa che:
"Quando il trattamento è effettuato da una persona giuridica, da una Pubblica Amministrazione o da qualsiasi altro ente, titolare del trattamento è l'entità nel suo complesso che esercita (…)"
Nel Provvedimento del Garante per la Protezione dei Dati Personali, del 14/06/07 (G.U. n. 161 del 13/07/07), recante "Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico", si precisa definitivamente che in ambito pubblico "**per individuare il Titolare del trattamento, occorre far riferimento all'amministrazione o ente centrale o locale nel suo complesso, anziché a singole articolazioni interne o alle persone fisiche che l'Amministrano o la rappresentano (ad esempio, il ministro, il direttore generale o il presidente)."**

Il Titolare è dunque l'Ente nel suo complesso e non i singoli soggetti fisici che operano al suo interno. Sarà dunque l'Ente, che dovrà adempiere alle disposizioni contenute nel Codice sulla Privacy.
Al Titolare spettano le decisioni strategiche in materia di sicurezza nel trattamento dei dati anche qualora vengano nominati, per fini pratico – operativi, dei Responsabili.
Il Titolare è il centro di imputazione degli obblighi e delle responsabilità attribuite dalla legge.
Egli ha il compito, e i compiti del Titolare NON SONO DELEGABILI, di organizzare e vigilare sull'intero processo di trattamento dei dati. Egli è il destinatario delle sanzioni previste per il mancato rispetto delle relative norme: è una figura necessaria perché non ci può essere un trattamento di dati senza che vi sia un corrispondente Titolare.

Il Titolare:

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

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

IL RESPONSABILE DEL TRATTAMENTO

Secondo quanto disposto dall'art. 4, comma 1, lett. g) del Codice, per Responsabile si intende:
"la persona fisica (…) preposta dal Titolare al trattamento dei dati personali".
Questo significa che, mentre il Titolare esiste indipendentemente da qualsiasi atto di nomina, il Responsabile del Trattamento esiste solo se il Titolare del Trattamento (l'Ente nel suo complesso) esercita una delle facoltà ad esso concesse dalla Legge.
Recita infatti l'art. 29 del Codice che:
"il Responsabile è designato dal Titolare facoltativamente".
La nomina del Responsabile è pertanto facoltativa ma, allorquando il Titolare (l'Ente nel suo complesso sulla base di una deliberazione della Giunta Comunale) decida di procedere alla sua individuazione, sarà necessario che la scelta ricada su un soggetto che presenti caratteristiche di "esperienza, capacità ed affidabilità" e che "garantisca idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza."
Il fatto che la norma si preoccupi di dare delle indicazioni sulle caratteristiche soggettive e, in parte, professionali del soggetto da nominare quale Responsabile del trattamento ha un duplice significato. Da un lato essa tende a garantire che la tutela della riservatezza venga demandata a soggetti con determinate capacità ed esperienze. Dall'altro lato, essa indica il metodo per evitare che il Titolare incorra in quella che viene definita "culpa in eligendo", ossia un colposo errore di scelta che, oltre a rendere assolutamente INVALIDA la nomina, avrebbe anche l'effetto di ricondurre "*in toto*" ogni responsabilità in capo al Titolare.
Oltre ad avere i requisiti ora citati, la nomina del Responsabile deve seguire i criteri di forma stabiliti dalla norma.
In primo luogo la nomina deve avvenire con ATTO SCRITTO in cui vengono elencati specificamente i compiti assegnati al responsabile del trattamento.
Infatti, anche se l'atto scritto non risulta espressamente previsto dal legislatore, la necessità di produrre un atto scritto con l'indicazione della nomina del responsabile e dei compiti ad esso assegnati, è evidente dalla lettura del comma 4, dell'art. 29 del Codice, che stabilisce che "i compiti affidati al Responsabile devono essere analiticamente specificati per iscritto".

Inoltre il comma 5, dello stesso art. 29, stabilisce che "il Responsabile procede al trattamento attenendosi alle istruzioni impartite dal Titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza (…) delle proprie istruzioni".
E' importante sottolineare che i Responsabili possono essere più di uno.
Il Responsabile è per definizione il soggetto "preposto" dal Titolare al trattamento di dati personali. Se ne deduce che il responsabile nominato potrebbe occuparsi di tutte le fasi che costituiscono il trattamento medesimo e anche di più trattamenti. Ciò deve essere visto alla luce di quanto riportato nel Mansionario redatto dal Titolare all'atto della nomina del responsabile.
Le funzioni e l'ambito di operatività del Responsabile possono essere individuate solo attraverso le indicazioni fornite dal Titolare.

GLI INCARICATI DEL TRATTAMENTO

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

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

Devono essere nominati quali Incaricati del trattamento dal Titolare o dal Responsabile tutti i soggetti che, nella pratica, raccolgono i dati, li elaborano, li archiviano, li comunicano, li diffondono ecc.
In base a quanto disposto dall'art. 30, "la designazione degli Incaricati deve avvenire per iscritto e deve individuare puntualmente le operazioni del trattamento consentite all'incaricato."
Ai sensi della citata norma, è di fatto indispensabile che siano nominati Incaricati tutti i soggetti che in qualsiasi modo effettuano una o più operazioni nell'ambito del trattamento.
E' bene tenere presente che gli Incaricati nominati, possono effettuare solo le operazioni nei limiti di cui alla loro nomina e sotto il diretto controllo del Titolare o del Responsabile. Ciò significa prima di tutto che, come per la nomina del Responsabile, anche per gli Incaricati, deve essere redatto un apposito Mansionario attraverso il quale vengono fornite all'operatore tutte le indicazioni necessarie affinché egli operi correttamente negli ambiti consentiti.

Si ricordi che il Garante per la protezione dei dati personali in diversi Provvedimenti (Gar., 23.05.2000, in Boll. N. 13, p. 21) ha ricordato come in assenza di formale designazione quali Incaricati del trattamento dei dati, i dipendenti di un soggetto pubblico che, per lo svolgimento dei propri compiti vengano a conoscenza di dati personali, devono essere considerati come soggetti terzi rispetto al datore di lavoro, con conseguenti rilevanti limiti per la comunicazione ad essi e per l'utilizzazione da parte loro dei dati (e quindi per la stessa liceità del trattamento).
Tale designazione è infatti indispensabile in quanto permette di considerare legittimo il flusso delle informazioni personali nell'ambito degli uffici e tra i dipendenti del titola del trattamento.

Al fine di poter correttamente definire gli ambiti di competenza e responsabilità dei soggetti individuati quali Titolare, Responsabili ed Incaricati del trattamento dei dati nell'Ente, si inseriscono, nell'Allegato 1 al presente Documento, i Modelli di Assegnazione degli incarichi a Responsabili ed Incaricati del trattamento dei dati personali.

COMPITI E RESPONSABILITA'

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

Le misure adottate dovranno proteggere i dati personali ed i sistemi, quindi i programmi informatici, gli strumenti elettronici utilizzati, il sistema informativo nel suo complesso, gli atti ed i documenti cartacei, gli ambienti nei quali vengono svolte le operazioni di trattamento, ivi compresi gli archivi.

Così come per il Titolare anche per il Responsabile infatti, vige l'obbligo di fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati ivi compreso il profilo della sicurezza.

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

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

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

Il citato articolo 15 ha un rilievo straordinario.

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

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

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

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

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

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

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

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

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

Il titolare che tratta dati personali in modo lecito e sicuro, deve organizzare la loro protezione non solo con l'adozione delle misure di sicurezza minime ma anche con le più ampie misure idonee di sicurezza che tutelano l'interesse del soggetto al quale i dati trattati si riferiscono a che i suoi dati personali non costituiscano oggetto di trattamento in condizioni di carenza di sicurezza.

Per altro verso, si osserva che gli oneri da sostenere per l'adozione delle necessarie misure strutturali e tecnologiche di sicurezza, devono essere correttamente considerati, oltre che come spese finalizzate alla protezione della sfera giuridica dei terzi, anche in termini di investimento che comporta numerosi benefici diretti e indiretti per lo stesso Ente obbligato.

Tale investimento infatti, allontana l'eventualità di sostenere esborsi sicuramente più consistenti in caso di malfunzionamento del proprio sistema informatico o telematico (si pensi alla riparazione dei guasti, al ripristino del software, alla ricostruzione delle banche dati, al risarcimento del danno cagionato ai soggetti ai quali i dati si riferiscono).
Va inoltre considerato, che anche la tutela penale contro gli accessi abusivi ad un sistema informatico o telematico, assicurata dall'art. 615 *ter* del nostro codice penale, e quella contro la detenzione abusiva di codici di accesso a sistemi informatici o telematici, prevista dal successivo art. 615 *quater*, è riconosciuta solo se il sistema è "protetto da misure di sicurezza".

ALLEGATO A

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

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

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

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

Inoltre, ciascun Responsabile del trattamento dei dati:

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

SEZIONE 5
MISURE DI SICUREZZA GIA' ADOTTATE DALL'ENTE

CASA COMUNALE

Interventi sulle Infrastrutture

- ⇨ Gli Uffici dell'Ente contenenti fisicamente le banche dati sono protetti con sistemi antincendio regolarmente manutenzionati e sottoposti a revisione secondo la periodicità stabilita dalla norma (estintori a polvere e a CO2).
- ⇨ Sono presenti grate metalliche alle finestre situate al piano terreno della Casa Comunale.
- ⇨ I locali nei quali viene effettuato il trattamento dei dati personali dispongono di impianto di climatizzazione.

Strumenti - Rete LAN / Internet - Antivirus

- ⇨ I Server ed i singoli elaboratori sono protetti contro gli eventuali sbalzi di corrente elettrica da singoli gruppi di continuità presenti su ogni macchina idonei ad evitare danni ai dati personali trattati nell'ipotesi in cui venga a mancare l'erogazione della corrente elettrica.
- ⇨ Il Server di Dominio e di Autenticazione **ACER ALTOS G710**, sul quale sono ospitati i programmi per la gestione dei Servizi Demografici e del Protocollo Informatico sviluppati dalla Software House **MAGGIOLI SPA** e gli applicativi per la Finanziaria e le Paghe forniti all'Ente dalla **ZUDDAS srl** di Cagliari, è dotato di doppi HDD in Raid 1.
- ⇨ Anche il secondo Server **ACER ALTOS G540,** sul quale sono residenti gli applicativi per la gestione dei Tributi fornito all'Ente dalla **ZUDDAS srl** di Cagliari ed il Software utilizzato dall'Ufficio Tecnico per l'Urbanistica, dispone di doppi HDD in RAID 1.
- ⇨ Con riferimento alle procedure ed ai dispositivi utilizzati per il salvataggio dei dati e degli applicativi residenti sul Server di Dominio **ACER ALTOS G710** e sul Server **ACER ALTOS G540**, si evidenzia che oltre alla copia di sicurezza garantita dalla presenza di doppi Hard Disk uniti in Raid 1, l'Ente, al fine di offrire adeguata garanzia di integrità, disponibilità e riservatezza alle informazioni ivi residenti, ha provveduto ad acquistare e configurare un'Unità di Backup su cassette DAT integrata ai Server, attraverso la quale si procede, con frequenza codificata settimanale ed in modalità manuale, ad effettuare una copia di sicurezza dei dati ospitati su Cassette DAT.
  Le cassette DAT utilizzate per la realizzazione delle copie di Backup dei Server, sono poi rigorosamente custodite in armadi muniti di serratura.
- ⇨ Il Server di dominio e Autenticazione (**ACER ALTOS G710**)**,** verifica l'identità dei Client per l'accesso alla Rete Locale attraverso la richiesta di una Password di Rete.
  Si registra quindi una corretta gestione delle procedure per l'accesso alla Rete Locale dell'Ente.
  Infatti, ogni utente può accedere alla LAN attraverso un codice identificativo (USER ID) e una PASSWORD. L'identificativo e la Password sono attribuiti in via esclusiva a ciascun dipendente individuato quale incaricato del trattamento dei dati e il Server di Dominio conserva tutte le informazioni sulle utenze e sui permessi di accesso alle risorse disponibili, previa verifica della validità delle login e delle password fornite dai Client.
- ⇨ Nonostante nell'Ente non sia presente una gestione centralizzata della distribuzione dell'Antivirus, i singoli Clients presenti in casa comunale (ed anche i Server) sono dotati di programmi Antivirus (**AVIRA McAfee, NORTON, AVG** Antivirus) che vengono aggiornati con cadenza codificata giornaliera ed in modalità automatica.
- ⇨ L'accesso ad Internet da parte di tutti gli elaboratori collegati alla LAN Comunale, avviene attraverso il Router centralizzato **Telecom SPEEDTOUCH** su linea ADSL.

⇨ Da quanto rilevato e dichiarato in sede di sopralluogo, la connessione ad Internet risulta adeguatamente protetta grazie alla presenza di un Firewall Hardware (**CHECK POINT SAFE OFFICE 500**) opportunamente configurato con la chiusura delle porte logiche.

Organizzazione

⇨ Sono programmati Corsi di Formazione in materia di Privacy e di Sicurezza Informatica rivolti a tutti i Dipendenti.

⇨ I Software gestionali utilizzati sono dotati di regolare licenza d'uso e vengono aggiornati periodicamente ad ogni release del produttore.

⇨ Sono installati periodicamente gli ultimi aggiornamenti del sistema operativo.

⇨ L'Ente dispone di una utenza di posta elettronica certificata (PEC) utilizzata dall'Ufficio Anagrafe.

⇨ L'Ente ha provveduto all'acquisto di 2 Kit (lettori e relativo software di gestione), per le procedure di firma elettronica (SMART CARD). I citati dispositivi sono utilizzati dall'Ufficio Tecnico (Edilizia Privata – Manutenzioni) e dall'Ufficio Tributi.

SEZIONE 6
L'ANALISI E LA VALUTAZIONE DEI RISCHI E DELLE MINACCE CHE INCOMBONO SUI DATI PERSONALI OGGETTO DI TRATTAMENTO

L'art. 31 D. Lgs. 196/03 prevede espressamente che "i dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta."

I dati inoltre, devono essere integri, disponibili quando necessario e conosciuti solo da quei soggetti, individuati espressamente come Incaricati del trattamento dei dati, che hanno necessità di accedervi per lo svolgimento delle funzioni istituzionali proprie dell'Ufficio al quale sono preposti.

L'Ente è consapevole del fatto che sui dati personali, sensibili e giudiziari oggetto di trattamento da parte degli Uffici incombono una serie di "**minacce potenziali** ovvero **reali**" che potrebbero determinare la compromissione di una o più delle qualità fondamentali che, per espressa previsione normativa, i dati personali oggetto di trattamento debbono sempre possedere e cioè:

a) la **disponibilità,** che assicura che l'accesso ai dati sia disponibile quando necessario. Per garantire questa "qualità" è necessario che l'accesso alle informazioni o alle risorse informatiche sia negato senza autorizzazione;

b) l'**integrità,** che garantisce della accuratezza e della completezza dei dati e delle informazioni custodite e contenute all'interno degli elaboratori ovvero sui supporti magnetici o ottici utilizzati per il salvataggio dei dati. Per garantire questa "qualità" si rende necessario codificare ed adottare delle corrette procedure per il backup

dei dati e nel contempo evitare che le informazioni correttamente salvate possano formare oggetto di modifica o di accesso senza autorizzazione;

c) la **riservatezza,** che garantisce che i dati e le informazioni siano conosciute ed accessibili solo ed esclusivamente al personale autorizzato. Il rispetto della citata "qualità" si ottiene negando l'accesso alle informazioni a tutti i soggetti, interni ovvero esterni all'Amministrazione, che non siano legittimati al trattamento ed alla conoscenza degli stessi dati da una espressa previsione normativa oppure da necessità legate all' espletamento di funzioni istituzionali.

Per garantire il rispetto di queste qualità è necessario conoscere ed analizzare le minacce che potrebbero incidere sulle stesse.

Per un soggetto Pubblico come l'Amministrazione Comunale, i danni che possono essere provocati agli archivi, comunque gestiti dall'Ente, che contengono informazioni personali, sensibili o giudiziarie, si possono distinguere in due macro – categorie:

- I DANNI RICOLLEGABILI AD ATTIVITA' UMANE
- I DANNI DERIVANTI DA EVENTI NATURALI, INCIDENTI, GUASTI MECCANICI.

I danni che una persona, autorizzata/legittimata o meno al trattamento può apportare, volutamente o inconsciamente, alle banche dati si possono classificare nelle seguenti ipotesi:

- Accesso non autorizzato ad informazioni
- Modifica non controllata del contenuto delle Banche Dati con conseguente perdita delle caratteristiche di **correttezza, completezza e congruità logica** dei dati stessi
- Distruzione delle Banche Dati
- Copia non autorizzata dei dati contenuti nelle Banche Dati Comunali
- Malfunzionamento del Servizio
- Interruzione del Servizio
- Inserimento nelle pagine web del Comune di frasi o immagini non in linea con i fini Istituzionali propri dell'Ente
- Inserimento nelle pagine web del Comune di informazioni non corrette, false o fuorvianti
- Utilizzo, mediante impersonamento informatico, di macchine ed indirizzi dell'Amministrazione per il compimento di attività illecite.

Come si è detto, esistono però altri fattori di rischio non legati ad attività umane ma derivanti da eventi naturali, incidenti, avarie, guasti meccanici, che possono comunque determinare malfunzionamenti o, nei casi più gravi, interruzione di servizi, di cui è necessario tenere conto nella presente analisi.

A tal fine l'Ente ha realizzato un'Analisi del Rischio attraverso le seguenti **fasi**:

1. Ricognizione dettagliata delle Banche Dati trattate a qualsiasi titolo dagli Uffici dell'Ente con particolare riferimento al contesto tecnologico e ambientale nel quale il trattamento viene posto in essere anche in ordine alla eventuale presenza di misure preventive e protettive già adottate dall'Ente;
2. Identificazione dei rischi e delle minacce che incombono sui dati, sugli strumenti e sugli ambienti di cui sopra;
3. Identificazione dei criteri per la valutazione dei rischi.

La **Fase 1,** le cui risultanze sono emerse nella Sezione 2 "Elenco dei trattamenti di dati personali effettuati dall'Ente" ha consentito di rilevare e censire in modo analitico tutte le Banche Dati possedute e trattate dal Comune con l'indicazione delle seguenti informazioni principali:

- La denominazione sintetica della Banca Dati
- Il Settore/Area di riferimento
- L'ufficio dove la banca dati è detenuta, custodita e, più in generale, trattata
- La natura dei dati trattati (con la specificazione della tipologia: dati personali "comuni", dati sensibili o dati giudiziari)
- La tipologia di supporto sul quale sono registrati i dati (supporto cartaceo ovvero informatico)
- La tipologia dell'unità di elaborazione (con l'indicazione se si tratti di un elaboratore isolato, cioè non collegato alla LAN Comunale ovvero in Rete)
- La sintetica descrizione delle misure di protezione adottate.

La **Fase 2** e la **Fase 3** formano oggetto di studio della presente Sezione e mirano alla corretta identificazione degli elementi da valutare per l'analisi dei rischi gravanti sui dati personali trattati dall'Ente.

ANALISI DI DETTAGLIO E IDENTIFICAZIONE DEI SINGOLI FATTORI DI RISCHIO

Gli elementi da valutare per l'analisi del rischio, sono i seguenti:

- **A) LE RISORSE UMANE**
- **B) LE RISORSE HARDWARE**
- **C) I SOFTWARE**
- **D) I DATI PERSONALI**
- **E) I COLLEGAMENTI**
- **F) I SISTEMI DI SICUREZZA**
- **G) GLI EVENTI NATURALI**
- **H) GLI INCIDENTI**

Il dettaglio delle minacce e dei rischi propri di ciascun elemento valutato appare essere il seguente:

A. LE RISORSE UMANE

A.01 Insufficiente conoscenza del sistema informatico o dell'applicazione

In alcuni casi, il dipendente individuato quale Incaricato del trattamento dei dati, può involontariamente compiere azioni che comportano un danno semplicemente perché non è perfettamente a conoscenza delle conseguenze del suo operato a causa di una mediocre conoscenza del sistema o dello strumento informatico ovvero non ha una sufficiente conoscenza dell'applicazione.

Il danno che può essere provocato varia a seconda del comportamento posto in essere e può determinare:

- Un blocco momentaneo della stazione di lavoro
- Un blocco che può coinvolgere anche altri utenti della Rete
- L'inserimento, la modifica o la cancellazione (e dunque la perdita) non voluta di informazioni e dati
- L'invio di dati personali, sensibili o giudiziari a soggetti non autorizzati

- La visione di dati personali, sensibili o giudiziari a soggetti non autorizzati

A.02 Insufficiente conoscenza dei rischi e delle misure di sicurezza

Si osserva talvolta negli Incaricati del trattamento dei dati, una sorta di superficialità di comportamento con riferimento alle problematiche relative alla sicurezza informatica. Superficialità dovuta, in genere, ad una non puntuale conoscenza dei gravi rischi che possono determinarsi quale conseguenza di una condotta non improntata al rispetto delle norme tecniche dettate dal D. Lgs. 196/03.

I comportamenti più ricorrenti che si possono ascrivere a questa categoria sono:

- La diffusione nell'ambito dell'Ufficio, tra colleghi, della componente riservata della credenziale di autenticazione o PASSWORD
- La mancata effettuazione periodica di copie di sicurezza dei propri documenti ed archivi
- La circostanza che venga lasciata la propria stazione di lavoro accesa e collegata quando ci si assenta per qualsivoglia ragione dall'Ufficio
- La circostanza che vengano lasciate, liberamente fruibili, stampe e tabulati contenenti dati personali, sensibili o giudiziari

A.03 Distrazione

La distrazione può essere di tipo "fisico" ovvero "logico".

La distrazione di tipo fisico, in genere, comporta direttamente danni alla strumentazione ed alle attrezzature e, in alcuni casi, indirettamente e conseguentemente danni ai dati (si rovescia la tazzina di caffè sulla tastiera, si rovescia la bottiglia dell'acqua sull'unità centrale, si urta una stampante facendola cadere e danneggiandola).

La distrazione di tipo logico invece, determina in genere esclusivamente danni ai dati trattati (durante la sessione di lavoro l'Incaricato del trattamento viene distratto da una telefonata e dimentica di salvare il documento su cui stava lavorando ovvero preme inavvertitamente dei tasti che provocano l'esecuzione di un comando non voluto).

A.04 Negligenza

La negligenza appare per certi versi simile alla distrazione ma, presuppone un comportamento "colposo" da parte del dipendente.

Il caso che si può ipotizzare è quello dell'Incaricato del trattamento dei dati che abbia il proprio elaboratore posizionato accanto ad una finestra e che, durante una giornata di forte pioggia, lasci aperta la finestra determinando l'esposizione della macchina all'acqua piovana ed il conseguente danneggiamento della stessa.

A.05 Incidente

Si tratta di un evento non imputabile in modo diretto, alla condotta umana ma a caso fortuito ovvero a forza maggiore.

Il danno, in questo caso, può essere la conseguenza di un corto circuito, di un incendio, di un allagamento e così via.

A.06 Atto doloso

E' senza dubbio il più grave e pericoloso dei rischi legati al fattore umano in quanto presuppone una precisa volontà indirizzata alla manomissione ovvero alla distruzione delle strumentazioni o dei dati trattati.

B. LE RISORSE HARDWARE

B.01 Obsolescenza

L'obsolescenza delle attrezzature, che nel campo informatico è particolarmente rapida, più che rappresentare un fattore di rischio "attivo", può impedire l'attivazione e l'implementazione di misure di sicurezza fisiche o logiche che si rendano opportune per eliminare o ridurre alcuni rischi.

L'esempio che può essere fatto è quello che si riferisce alla impossibilità tecnica di installare su un vecchio elaboratore un sistema di cifratura dei dati che richiede processori di una certa potenza e sufficiente memoria.

B.02 Avaria

Come tutte le macchine, anche le strumentazioni informatiche sono soggette ad avarie che possono renderle inutilizzabili per periodi più o meno lunghi.

A seconda del tipo di guasto si può avere solo il blocco dell'attività della postazione di lavoro oppure anche il danneggiamento o la perdita dei dati (si pensi al caso di avaria dell' hard disk).

B.03 Distruzione

La distruzione, volontaria o dovuta a caso fortuito o forza maggiore, comporta una perdita totale della funzionalità della stazione di lavoro e dei dati residenti sulla stessa.

B.04 Furto

Il furto equivale sostanzialmente ad una distruzione totale del bene e quindi determina la perdita dei dati residenti sullo stesso.

B.05 Manomissione

La manomissione posta in essere su apparecchiature hardware determina dei malfunzionamenti.

Si tratta nella maggior parte dei casi di un intervento doloso, generalmente attuato da persona esperta, tendente ad impedire il corretto funzionamento della stazione di lavoro ad esempio mettendo fuori uso le testine di lettura e scrittura dei dischi oppure alterando la formattazione degli stessi per rendere non più rintracciabili le informazioni.

Ci possono essere anche delle ipotesi nelle quali la manomissione risulta essere la causa di una manovra sbagliata compiuta dall'operatore involontariamente oppure per imperizia o distrazione.

In altri casi ancora, la manomissione dell' hardware risulta essere la conseguenza di un'infezione da virus.

A) I SOFTWARE

C.01 Malfunzionamento

Il presupposto di partenza è rappresentato dalla considerazione che il perfetto software non esiste.

Partendo da tale premessa è possibile individuare alcune tipologie di danno che il malfunzionamento del software può provocare:

- danno economico e di immagine per l'Amministrazione che si trova ad utilizzare ovvero a pubblicare dati non corretti
- danno economico per l'Amministrazione quando l'errato funzionamento di un programma provoca errori nell'adempimento di operazioni obbligatorie o nella gestione di procedimenti
- danno gestionale per l'Amministrazione quando il citato malfunzionamento provochi un rallentamento o, addirittura un blocco, delle normali attività lavorative

- danno organizzativo ed economico nell'ipotesi in cui risulti necessario destinare risorse umane e finanziarie alla ricerca di una soluzione per il malfunzionamento verificatosi

C.02 Virus

I Virus possono attaccare e danneggiare più o meno profondamente anche i software installati sulle macchine ed i dati contenuti sugli stessi.

C.03 Distruzione

Un programma, o una sua parte, può essere distrutto sia intenzionalmente che accidentalmente (si pensi ad una errata operazione dell'utente, ad uno sbalzo elettrico, ad un malfunzionamento dell' hardware).

Oltre al danno derivante dal blocco temporaneo di tutta l'attività basata sul software distrutto, c'è da considerare l'eventualità che non ne sia possibile la ricostruzione.

Quest'ultima eventualità può verificarsi in una delle seguenti situazioni:

- mancanza di copie di riserva del software
- software installato su un'unica macchina e quindi non replicabile da altre stazioni di lavoro
- software sviluppato esternamente da società non più presenti sul mercato
- software sviluppato internamente e non documentato o del quale si è persa la documentazione
- software particolarmente obsoleto per il quale non c'è più manutenzione.

C.04 Duplicazione non autorizzata

Il danno derivante dalla duplicazione non autorizzata dei programmi di gestione utilizzati, consiste nella violazione delle norme vigenti nel nostro ordinamento che prevedono questa fattispecie come reato. Infatti, a titolo esemplificativo, l'art. 22, comma 8, D. Lgs. 196/03 prevede espressamente il divieto di diffondere informazioni sullo stato di salute e, l'art. 167 D. Lgs. 196/03 punisce questo reato, con la pena della reclusione da uno a tre anni.

Purtroppo, la diffusione non arrestabile dell'uso improprio della posta elettronica, la presenza di masterizzatori e supporti di memoria esterni, rendono praticamente impossibile per l'Ente un controllo totale su questa tipologia di eventi spesso posti in essere superficialmente dagli stessi dipendenti.

C.05 Obsolescenza

Il rischio derivante dall'obsolescenza dei programmi si traduce nell'incapacità degli stessi di rispondere correttamente alle mutate esigenze operative e normative degli Uffici dell'Ente.

C.06 Modifica non controllata

Si tratta del tipico effetto dovuto ad una infezione da Virus. In alcuni casi però, può avvenire a seguito di una modifica volontaria di un programma, realizzata in fretta o da personale che non conosce esattamente la procedura, che determina, a cascata, modifiche impreviste.

B) I DATI

D.01 Accesso non autorizzato

Secondo quanto espressamente previsto dal D. Lgs. 196/03, ogni dipendente individuato quale Incaricato del trattamento dei dati deve poter accedere esclusivamente a quelle informazioni che risultino essere necessarie, pertinenti e non eccedenti per svolgere correttamente il proprio lavoro e porre in essere l'attività istituzionale propria dell'Ufficio.

E' dunque necessario verificare che l'accesso ai dati personali, sensibili e giudiziari sia rigorosamente controllato.

La concreta possibilità che si verifichi una ipotesi di accesso non autorizzato a dati personali trattati su supporto informatico si può avere nelle seguenti situazioni:

- distrazione ovvero negligenza di un Incaricato del trattamento dei dati (il quale, per esempio, lascia incustodita la propria postazione di lavoro collegata)
- conoscenza della Password di un altro Incaricato
- carenze nel sistema e nelle procedure di attribuzione e gestione dei profili di autenticazione e di autorizzazione degli utenti.

Un'ulteriore possibilità di accesso ai dati deriva dal non corretto utilizzo delle stampe che contengono informazioni personali, sensibili e giudiziarie.

Spesso succede infatti che, dette stampe, prodotte come supporto al lavoro d'ufficio, vengano lasciate sulla scrivania anche nei momenti in cui il posto di lavoro non è presidiato oppure, quando non servono più, vengono gettate nel cestino della carta senza procedere invece alla distruzione vera e propria del documento a mezzo di presidio "distruggi – documenti".

Altro caso significativo di accesso ai dati non autorizzato si verifica nelle ipotesi in cui il fax dell'Amministrazione venga posizionato in area non presidiata. Il posizionamento dell'apparecchio ricevente in luogo non presidiato, accessibile normalmente a tutto il personale dipendente ed anche al pubblico, rende estremamente probabile che comunicazioni contenenti dati personali, sensibili e giudiziari, vengano viste (ed in alcuni casi anche asportate) da persone estranee sicuramente non legittimate all'accesso a quella tipologia di dati.

Si rende necessario provvedere con somma urgenza al posizionamento dell'apparecchio fax all'interno dell' Area Organizzativa Omogenea di Protocollazione (all'interno dell'Ufficio Protocollo) che deve risultare presidiato ovvero inaccessibile a tutti i soggetti non legittimati.

D.02 Modifica non autorizzata

La modifica non autorizzata di dati personali può essere il risultato di una operazione, volontaria o involontaria, posta in essere dall'utente oppure la conseguenza di un Virus.

Non è possibile ipotizzare di impedire agli Incaricati del trattamento la modifica dei dati in quanto, questo impedimento determinerebbe l'impossibilità di svolgere la normale attività istituzionale dell'Ente. Si rende pertanto necessario, incidere sul sistema delle autorizzazioni.

Se la modifica è opera di un utente, occorre distinguere tra volontarietà ed involontarietà. Nel primo caso, ci si trova di fronte ad un comportamento doloso, quindi più grave e presumibilmente più difficile da scoprire.

Nel caso invece di modifica involontaria, questa potrebbe derivare dal malfunzionamento di un programma oppure da un difetto delle misure di sicurezza relative all'assegnazione delle autorizzazioni ai dipendenti.

D.03 Distruzione

Anche la distruzione dei dati potrebbe essere il risultato di un'attività umana (volontaria o involontaria) oppure la conseguenza di un guasto hardware.

D.04 Mancanza di congruità

La mancanza di congruità di dati personali contenuti nello stesso data base ovvero in data base diversi, comporta la inattendibilità delle informazioni che se ne ricavano e, conseguentemente, l'inutilità complessiva della raccolta e del trattamento dei dati in oggetto.

La non congruità può essere "originale" ovvero esistere sin dal momento del primo caricamento dei dati, oppure può essere derivata da un'operazione, volontaria o involontaria, successiva.

Al momento del caricamento iniziale delle banche dati, che derivano da archivi cartacei diversi, è molto difficile garantire la congruità fra le due applicazioni, delle informazioni immesse ed è altrettanto difficile garantirla durante le fasi di aggiornamento dei dati.

La situazione risulta essere ancora più complessa nell'ipotesi in cui, lo stesso tipo di informazione risulti essere gestita da un numero superiore di banche dati.

D.05 Esportazione illegittima

L'esportazione illegittima di dati, oltre al danno patrimoniale che può determinare in capo all'Amministrazione, si può configurare come una forma indiretta di accesso non autorizzato alle informazioni trattate dall'Ente.

E' infatti evidente che l'esportazione, proprio perché illegittima, consente la conoscenza di dati personali, sensibili e giudiziari da parte di persone fisiche o giuridiche che non dovrebbero entrare nella disponibilità degli stessi.

L'esportazione illegittima di dati può avvenire verso l'esterno dell'Ente ma anche verso l'interno (comunicazione ovvero fornitura di dati ad un altro servizio comunale per scopi non istituzionali).

C) I COLLEGAMENTI

E.01 Malfunzionamento

I collegamenti possono essere di diverso tipo: quelli che riguardano il funzionamento delle apparecchiature (tipicamente la rete elettrica) e quelli che riguardano invece il flusso dei dati (rete di trasmissione dati).

Il malfunzionamento della rete elettrica (sbalzi di tensione) può provocare momentanei blocchi delle apparecchiature oppure, nei casi più gravi, rottura di alcune componenti con possibile danneggiamento ovvero addirittura perdita dei dati registrati.

Il malfunzionamento della rete di trasmissione dei dati può generare lievi anomalie quali ad esempio la temporanea mancanza di connettività sulla Rete Locale ovvero verso il Web; tuttavia, una non corretta gestione della infrastruttura informatica, ovvero la mancata manutenzione periodica, può determinare conflitti o anomalie sia logiche che fisiche tali da pregiudicare la sussistenza delle qualità di sicurezza sui dati trattati quali disponibilità, integrità e riservatezza.

E.02 Interruzione

L'interruzione è, sostanzialmente, una forma grave di malfunzionamento che, oltre ad eventuali danni fisici alle apparecchiature e conseguenti danni ai dati, comporta inevitabilmente anche il fermo di tutte o di parte delle attività istituzionali.

E.03 Intercettazione

L'intercettazione equivale ad un accesso non autorizzato ai dati tramite collegamento alle linee di trasmissione dati.

Può essere involontaria (malfunzionamento della linea di comunicazione) ma più spesso si tratta di azioni dolose effettuate da esperti.

D) SISTEMI DI SICUREZZA

F.01 Incompletezza

Per quanti sforzi l'Ente si impegni a porre in essere per la predisposizione di un sistema di sicurezza conforme al dettato normativo, è sempre possibile che rimangano dei varchi aperti o per una incompleta analisi dei rischi, o per qualche errore nell'implementazione del sistema oppure ancora per l'avvento di nuove tecniche di "penetrazione e forzatura" non sufficientemente conosciute.

F.02 Illeggibilità delle copie di backup

Tutti i supporti magnetici, per loro stessa natura, tendono ad un progressivo degrado, con conseguente possibilità che si determini la perdita totale o parziale dei dati memorizzati.

Naturalmente, più un supporto è economico o obsoleto (floppy disk) più è soggetto a deterioramento ma, persino sui CD-ROM o sui DVD non si hanno garanzie sulla effettiva durata della registrazione.

Risulta comunque estremamente pericolo per gli Uffici dell'Ente accorgersi che non si ha la possibilità di ripristinare ed utilizzare una copia di sicurezza realizzata e, sulla quale, evidentemente, si faceva affidamento.

Può inoltre verificarsi che, per un mero errore materiale, la copia di sicurezza venga fatta su un supporto sbagliato, già utilizzato per altre diverse copie, con l'effetto di cancellare quelle precedenti che vengono perse.

E) EVENTI NATURALI

G.01 Terremoto

La Sardegna in generale e conseguentemente anche il territorio su cui è costruita la Caca Comunale non risultano essere a rischio sismico. Si ritiene pertanto di dover valutare questa tipologia di rischio come non significativa.

G.02 Alluvioni

Sulla base dei dati storici in possesso dell'Amministrazione, non possiamo classificare la zona su cui sorge la Casa Comunale come a rischio di alluvione.

Tuttavia, potrebbero essere danneggiate dall'acqua, se questa dovesse raggiungere altezze sensibili, alcune stazioni di lavoro appoggiate al pavimento (PC di tipo Tower) negli uffici ubicati al piano terreno della Casa Comunale.

F) INCIDENTI

H.01 Incendio

E' il rischio di una reazione incontrollata e non voluta fra l'ossigeno dell'aria (comburente) e un qualsiasi materiale ad esso affine chimicamente (combustibile) iniziata per effetto di un innesco (temperatura o intimo contatto) che continua con sviluppo di calore, e conseguente aumento di temperatura, perciò autoalimentandosi.

A) Comburente:
- trattandosi di ossigeno che è presente nell'aria si trova dappertutto.

B) Combustibile:
- nei magazzini e depositi per materiali vari infiammabili come vernici, oli, grassi, solventi, gomma, plastica, imballaggi, oltre ai rifiuti differenziati temporaneamente stoccati,ecc.;
- negli archivi per la quantità di materiale cartaceo;

- negli uffici e nei locali presenti in Casa Comunale per il carico di incendio determinato dalla presenza degli arredi e dei materiali cartacei.

C) Temperatura di innesco:

- la fonte più comune è l'impianto elettrico oltreché l'incompatibilità di attrezzature che non sono pertinenti alla destinazione d'uso dei locali quali fotocopiatori e apparecchi riscaldanti con potenza assorbita maggiore di 1Kw e non dotati di interruttore omnipolare.

H.02 Cedimento strutturale

La Casa Comunale non presenta rischi di cedimento o improvviso collasso strutturale. Infatti, eventuali cedimenti sarebbero sicuramente preceduti da segni evidenti (crepe, rigonfiamenti ecc) facilmente diagnosticabili dai tecnici comunali.

H.03 Campi elettro-magnetici

E' noto ormai che i campi elettro-magnetici danneggino i supporti informatici alterando le informazioni registrate.
Se la potenza del campo è sufficiente, si possono avere anche blocchi o malfunzionamenti delle apparecchiature elettro-meccaniche, elettriche ed elettroniche.
Non vi sono però, nelle vicinanze della Casa Comunale, fonti di emissione di potenza tale da creare problemi di questo genere. Inoltre, va evidenziato che la loro eventuale presenza, creerebbe disagi notevoli anche alle persone che lavorano nella zona per cui il rischio assumerebbe sicuramente caratteristiche più gravi.
Molto più banalmente, si possono avere danneggiamenti ai supporti informatici ed alle apparecchiature se queste vengono posizionate vicino a motori elettrici abbastanza potenti e non schermati (condizionatori, stufe elettriche, ascensori).

SEZIONE 6.1
CRITERI ADOTTATI PER LA VALUTAZIONE DEI RISCHI

Una volta individuati i rischi e le minacce analiticamente, occorre procedere alla valutazione degli stessi nel contesto comunale, attraverso una indicizzazione del tipo di danno o di lesioni possibili.

In particolare, nel processo di valutazione, si tiene conto di due indici fondamentali:

- la **PROBABILITA'** di accadimento del danno **(P):** riguarda la frequenza riscontrata o riscontrabile
- La **GRAVITA'** del danno **(G):** da valutarsi sia in termini quantitativi (valore del bene, costi di riparazione, tempi di fermo macchina) che qualitativi (danno all'immagine dell'Ente, interruzione di pubblico servizio).

Il **Rischio Residuo che l'Ente avrà la necessità di abbattere** quindi altro non è che la risultante della probabilità di accadimento di un evento (o di un atto) e la sua gravità: l'indice **RR** è dato proprio dal prodotto **PXG.**
Attribuendo a **P** un valore compreso tra **1** e **5** ed a **G** ugualmente una valore compreso tra **1** e **5** si otterrà il valore di **RR** compreso tra **1** e **25.**

PROBABILITA' (P)	**1.** IMPROBABILE
	2. POCO PROBABILE
	3. MEDIAMENTE PROBABILE
	4. MOLTO PROBABILE
	5. ESTREMAMENTE PROBABILE

GRAVITA' (G)	**1.** MINIMO
	2. LIEVE
	3. MEDIO
	4. GRAVE
	5. GRAVISSIMO

Il numero, indicato con la lettera **RR (Rischio Residuo),** dato dal prodotto dei fattori arbitrari **PXG,** è per l'Ente un indice della gravità dello specifico rischio residuo.

Legenda Rischio Residuo (RR)

Il Rischio Residuo è stato valutato in termini di:

✓ accettabilità;

⦸ non accettabilità.

con il seguente significato:

✓ **<u>accettabilità – Valori di RR compresi tra 1 e 10</u>**

riferita sia a basse probabilità di accadimento della minaccia-evento dannoso, che a contenuta gravità del danno.

⦸ **<u>non accettabilità – Valori di RR compresi tra 11 e 25</u>**

riferita sia a medio-alte probabilità di accadimento della minaccia-evento dannoso che ad un livello medio-alto di gravità del danno.

SEZIONE 7

MISURE DI SICUREZZA DA ADOTTARE DALL'ENTE PER GARANTIRE LA INTEGRITÀ E LA DISPONIBILITÀ DEI DATI, NONCHÉ LA PROTEZIONE DELLE AREE E DEI LOCALI IN CUI QUESTI SONO CONSERVATI E CUSTODITI – ALLEGATO B AL D. LGS. 196/03 REGOLA 19.4

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

Le Misure di Sicurezza da adottare saranno di due tipologie:

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

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

La differenza tra le due categorie di misure, che sono entrambe parimenti obbligatorie, risiede fondamentalmente nel diverso regime di responsabilità in caso di omissione.

L'omessa adozione delle necessarie misure idonee e preventive può, infatti, comportare, ai sensi dell'art. 15 D. Lgs. 196/03, la responsabilità civile di chi ha cagionato danni patrimoniali o non patrimoniali ad altri per effetto del trattamento, mentre la mancata adozione delle *misure minime di sicurezza,* integra, oltre ai possibili profili di responsabilità civile, anche il reato di cui all'art. 169 del Codice ed è quindi penalmente sanzionata.

La disciplina delle misure PREVENTIVE ed IDONEE è contenuta negli articoli 31 e 32 e si limita ad indicare alcuni criteri generali di individuazione delle misure da adottare, visto che le misure idonee non possono essere predeterminate in modo preciso, dovendo essere adattate alle diverse tipologie di trattamenti.

Con riferimento invece alle misure MINIME di sicurezza, il Codice introduce una disciplina articolata su due livelli. Infatti, il D. Lgs. 196/03 indica agli articoli 34 e 35 i principi che devono informare la disciplina delle misure minime di sicurezza, rimandando poi al Disciplinare Tecnico ed ai suoi aggiornamenti – da operare con decreti del Ministero della giustizia di concerto con il Ministero per le innovazioni e le tecnologie – il compito di attuare tali principi in modo puntuale così da assicurare il rispetto del principio di tassativa individuazione delle fattispecie penali, ivi inclusa la fattispecie incriminatrice di cui all'art. 169 del Codice.

In tal modo si consegue il duplice risultato di agevolare il costante aggiornamento delle misure minime in base all'evoluzione tecnica ed all'esperienza maturata nel settore (considerato che il procedimento di adozione dei decreti ministeriali è più rapido rispetto a quello previsto per l'adozione di un regolamento governativo) e di assicurare, nel contempo, che tale aggiornamento abbia luogo in un quadro di principi stabile e definito dalla legislazione di rango primario.

SEZIONE 7.1

MISURE MINIME DI SICUREZZA ART 33 D. LGS. 196/03 – DISCIPLINARE TECNICO (ALLEGATO B AL D. LGS. 196/03) REGOLE DA 1 A 26

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

Secondo quanto previsto dall'art. 4, comma 3, lett. a) D. Lgs. 196/03, per **Misure Minime** si intende "il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31."
La sicurezza viene dunque considerata come l'insieme di soluzioni tecniche, informatiche, organizzative, logistiche e procedurali necessarie per ridurre al minimo i rischi di distruzione o perdita dei dati trattati. La sicurezza non è perciò intesa come un mero fatto tecnico.

Le misure minime di sicurezza sono puntualmente identificate da parte del Legislatore a causa della previsione della sanzione penale per la loro mancata adozione che vincola al rispetto del principio di tassatività della sanzione penale.
In via prioritaria l'Ente procederà all'adozione delle seguenti Misure Minime Di Sicurezza previste dal Codice sulla Privacy agli articoli 33 e 34 e dal Disciplinare Tecnico nei punti da 1 a 26 e non ancora rese pienamente operative all'interno degli Uffici dell'Amministrazione.
Saranno prescritte per tutte le Banche Dati contenenti informazioni di natura personale, di natura sensibile e di natura giudiziaria, le seguenti Misure Minime di Sicurezza in aderenza al disposto normativo.

Per contrastare i rischi descritti nella precedente **Sezione 6** di cui ai Punti **A.02 "Insufficiente conoscenza dei rischi e delle misure di sicurezza" - D.01 "Accesso non autorizzato"** si osserveranno le regole dettate espressamente dalle seguenti norme:
1) D. Lgs. 196/03 - Art 34 comma 1. lett. a) e b): autenticazione informatica, procedure di gestione delle credenziali di autenticazione.
2) Allegato B - Disciplinare Tecnico - Punti 1, 2, 3, 4, 5, 6, 7, 8, 9.

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

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

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

Misure di sicurezza da adottare

Il dettato normativo sopra richiamato comporta che tutti i dipendenti dell'Ente che svolgono una o più operazioni di trattamento dei dati siano stati preventivamente individuati quali Responsabili ovvero quali Incaricati del trattamento con atto formale di designazione.
Ai soggetti individuati quali Responsabili ed Incaricati sono fornite idonee credenziali per l'autenticazione della loro identità (parole chiave, codici di accesso, smart card) riferite all'accesso ad un solo specifico trattamento oppure a più trattamenti, oppure ancora a determinate operazioni di un trattamento.

Il sistema informatico sarà preventivamente impostato per consentire l'associazione delle credenziali a specifici trattamenti, ad insiemi di operazioni ovvero a insiemi di trattamenti.
Il riconoscimento da parte del sistema delle credenziali permette il superamento della procedura di autenticazione.
Si procederà a prevedere come obbligatorio, per l'accesso agli strumenti elettronici contenenti dati personali, l'uso corretto, il mantenimento e la gestione del sistema di credenziali costituito da:

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

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

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

Misure di sicurezza da adottare

La norma obbliga il Titolare ad impartire istruzioni agli Incaricati con la prescrizione dell'elencazione delle cautele da adottare per garantire la segretezza della componente riservata della credenziale.
All'atto della consegna formale delle credenziali di autenticazione all'Incaricato si provvederà a notificare allo stesso i criteri da seguire per la corretta gestione delle credenziali ricevute. In particolare è fatto obbligo di:

- evitare di trascrivere la credenziale in fogli "volanti";
- evitare di digitare la componente riservata della credenziale in presenza di terzi.

La parola chiave non deve contenere riferimenti agevolmente riconducibili all'incaricato
La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri alfanumerici.

Misure di sicurezza da adottare

La lunghezza minima della Parola Chiave è stata scelta dal Legislatore sulla base di calcoli matematici per migliorarne la sicurezza.
Non viene indicato con esattezza dalla norma come deve essere composta la Parola Chiave ma viene negata la possibilità di utilizzare parole facilmente individuabili da malintenzionati come ad esempio il proprio nome o quello di un familiare del soggetto interessato.

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

- non usare il proprio nome, cognome o parti di essi;
- non usare il nome del coniuge, dei figli, dei genitori, la targa della propria autovettura, il codice fiscale o combinazioni di essi;

- non usare date facilmente collegabili: data di nascita, data del matrimonio, etc;
- non usare nomi presenti nel vocabolario italiano o di altre lingue;
- non invertire la parole (es. servizi = izivres);
- non utilizzare parole, termini di uso diffuso e familiare, anche se non presenti in vocabolario;
- utilizzare insieme numeri, caratteri minuscoli e maiuscoli;
- evitare di ripetere caratteri in posizioni adiacenti;
- Fare ricorso, ove possibile, per facilità mnemonica a parole chiave ricavate da frasi lunghe, composte da numeri, caratteri minuscoli e maiuscoli.

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

Misure di sicurezza da adottare

La validità di una parola chiave non può essere superiore a sei mesi.
Il termine massimo per la modifica è dimezzato a tre mesi per i trattamenti di dati sensibili e giudiziari perché tali dati richiedono protezioni e garanzie maggiori.
Dovrà essere definita nel sistema informatico, con l'assistenza di un soggetto competente a tale scopo incaricato, e con l'ausilio di idonei programmi, la procedura per la gestione in forma automatica dell'obbligo di modifica immediata e successivamente con periodicità semestrale (ovvero trimestrale nel caso di trattamenti di dati sensibili e giudiziari) della parola chiave.

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

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

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

Misure di sicurezza da adottare

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

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

- cancellazione dell'account di un incaricato, previa segnalazione in tal senso del Responsabile, nei casi di cessazione dal servizio, mobilità esterna o interna, assenza per malattia o altra causa per periodi superiori ai sei mesi;

- cancellazione dell'account ove l'incaricato abbia perso le abilitazioni per il trattamenti dai dati.

Per contrastare i rischi descritti nella precedente **Sezione 6** di cui ai Punti **A.01 "Insufficiente conoscenza del sistema informatico o dell'applicazione" – A.02 "Insufficiente conoscenza dei rischi e delle misure di sicurezza" – B.05 "Manomissione" - C.02 "Virus" – C.06 "Modifica non controllata" – D.01 "Accesso non autorizzato" – D.02 "Modifica non autorizzata"** si osserveranno le regole dettate espressamente dalle seguenti norme:

1) D. Lgs. 196/03 – Art. 34, comma 1, lett. c): utilizzazione di un sistema di autorizzazione.

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

3) Allegato B – Disciplinare Tecnico – Punto 9, 10,12, 13, 14, 15, 16, 17.

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

Misure di sicurezza da adottare

La normativa richiamata demanda al Titolare il compito di predisporre istruzioni scritte per gli incaricati del trattamento affinché, durante una sessione attiva di trattamento dei dati, lo strumento utilizzato non rimanga incustodito.

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

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

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

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

In tal caso la custodia delle copie delle credenziali di autenticazione è organizzata garantendo la relativa segretezza e individuando, preventivamente per iscritto, i soggetti incaricati della loro custodia, i quali dovranno informare tempestivamente l'incaricato dell'intervento effettuato affinché questi provveda al rientro al lavoro alla autonoma sostituzione della parola chiave.

Misure di sicurezza da adottare

Sarà fatto obbligo di adottare la seguente procedura operativa:

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

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

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

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

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

Misure di sicurezza da adottare

La normativa richiamata disciplina inoltre l'ipotesi in cui agli stessi dati accedano più incaricati con profili di AUTORIZZAZIONE DIVERSI. Ad esempio, alcuni incaricati possono solo consultare i dati ma non modificarli mentre altri sono autorizzati al loro aggiornamento, rettifica o cancellazione.
L'Ente procederà secondo le seguenti indicazioni:

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

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.

Misure di sicurezza da adottare

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

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

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

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

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

- ❑ Consultare, esaminare e diffondere messaggi specializzati di virus alert;
- ❑ Nella posta elettronica, quando si introducono allegati, nel caso vengano inviati documenti scritti con MS Word, si usi il formato RTF e non quello .Doc;
- ❑ Configurare le schermate in modo che sia possibile visualizzare l'estensione dei files;
- ❑ Non aprire allegati che contengano un'estensione doppia;
- ❑ In caso di ricezione di una e-mail con oggetto insolito, effettuare un controllo con il mittente prima di aprire l'eventuale allegato;
- ❑ Non considerare le icone mostrate dagli allegati come garanzia dell'integrità del software;
- ❑ In caso di ricezione di e-mail non richieste o con contenuti insoliti, non eseguire senza aver preventivamente valutato la circostanza, collegamenti a indirizzi web presenti nel testo della e-mail;
- ❑ Controllare bene che i CD masterizzati e scambiati siano immuni da virus;
- ❑ Evitare di prelevare software da sorgenti poco affidabili.

Per contrastare i rischi descritti nella precedente **Sezione 6** di cui ai Punti **B.01 "Obsolescenza" – C.01 "Malfunzionamento" – C.05 "Obsolescenza"** si osserveranno le regole dettate espressamente dalle seguenti norme:

1) D. Lgs. 196/03 – Art. 34, comma 1, lett. e): protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici.
2) Allegato B – Disciplinare Tecnico – Punto 17.

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

Misure di sicurezza da adottare

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

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

La verifica dovrà produrre un documento tecnico che dia indicazioni su quanto segue:

- evidenza dei sistemi hardware obsoleti e da dismettere;
- disponibilità di patch, fix, service pack e nuove versioni da fornire agli utenti, ove possibile tramite sistemi centralizzati di distribuzione.

Per contrastare i rischi descritti nella precedente **Sezione 6** di cui ai Punti **A.02 "Insufficiente conoscenza dei rischi e delle misure di sicurezza" – B.02 "Avaria" – B.03 "Distruzione" – B.04 "Furto" – B.05 "Manomissione" – C.02 "Virus" – C.03 "Distruzione" – C.06 "Modifica non controllata" – D.02 "Modifica non autorizzata" – D.03 "Distruzione" – E.01 "Malfunzionamento" – E.02 "Interruzione" – F.02 "Illeggibilità delle copie di backup" – H.03 "Campi elettro – magnetici"** si osserveranno le regole dettate espressamente dalle seguenti norme:
1) D. Lgs. 196/03 - Art 34, comma 1 lett. f): adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi.
2) Allegato B – Disciplinate Tecnico – Punto 18.

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

Misure di sicurezza da Adottare

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

In alcuni casi l'attività di salvataggio dei dati viene trascurata, non considerata o non fatta in maniera sistematica. Per questa ragione il Legislatore ha voluto tutelare l'integrità e la disponibilità dei dati con una prescrizione tecnico-organizzativa considerata di base nella cultura della sicurezza informatica.
La produzione sistematica di copie di sicurezza è un processo articolato e di complessa gestione che richiede tempo.
L'Ente, procederà ad adeguare la propria condotta ai dettami legislativi secondo le specifiche di seguito riportate:

- si individueranno specifiche procedure attraverso le quali sarà previsto l'obbligo tassativo di effettuazione delle copie di sicurezza secondo quanto previsto dalla norma.

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

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

All'interno di ciascun servizio, sarà definita una procedura per quanto concerne:

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

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

Per contrastare i rischi descritti nella precedente **Sezione 6** di cui ai Punti **A.02 "Insufficiente conoscenza dei rischi e delle misure di sicurezza" – C.04 "Duplicazione non autorizzata" – D.01 "Accesso non autorizzato" – D.02 "Modifica non autorizzata" – D.03 "Distruzione" – D.05 "Esportazione illegittima"** si osserveranno le regole dettate espressamente dalle seguenti norme:

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

2) Allegato B – Disciplinate Tecnico – Punto 20.

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.

Misure di sicurezza da adottare

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

- Conoscenza dei dati da parte di persone non autorizzate;
- Distruzione o perdita totale o parziale dei dati;

- Danneggiamento dei dati;
- Diffusione di documenti, anche riservati;
- Impossibilità di svolgere operazioni di trattamento dei dati;
- Diffusione di programmi informatici infetti;
- Rallentamento delle capacità del sistema;
- Perdita di tempo.

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

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

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

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

A livello più generale si imporrà:

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

Per contrastare i rischi descritti nella precedente **Sezione 6** di cui ai Punti **A.02 "Insufficiente conoscenza dei rischi e delle misure di sicurezza" – B.02 "Avaria" – B.03 "Distruzione" – B.04 "Furto" – B.05 "Manomissione" – C.02 "Virus" – C.03 "Distruzione" – C.06 "Modifica non controllata" – D.02 "Modifica non autorizzata" – D.03 "Distruzione" – E.01 "Malfunzionamento" – E.02 "Interruzione" – F.02 "Illeggibilità delle copie di backup" – H.03 "Campi elettro – magnetici"** si osserveranno le regole dettate espressamente dalle seguenti norme:

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

2) Allegato B – Disciplinate Tecnico – Punto 21, 22, 23.

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

Misure di sicurezza da adottare

Dovranno essere adottate procedure formali affinché:

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

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

Misure di sicurezza da adottare

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

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.

Misure di sicurezza da adottare

- All'interno di ciascuna Area si provvederà affinché per i sistemi che contengono dati sensibili o giudiziari (per i quali è previsto un tempo certo di ripristino compatibile con i diritti degli interessati non superiore a sette giorni) sia previsto un sistema hardware di emergenza (backup) che possa garantire le condizioni minime essenziali di funzionamento dello stesso, sino al ripristino del sistema principale, previa regolare effettuazione delle copie di backup dei dati e del sistema operativo unitamente ad una procedura formalizzata che descriva in modo chiaro ruoli, compiti e scadenze, tempi e modalità di ripristino;
- si provvederà a correggere eventuali bugs (errori) del sistema operativo e degli applicativi.

Per contrastare i rischi descritti nella precedente **Sezione 6** di cui ai Punti **B.02 "Avaria" – B.05 "Manomissione" – C.01 "Malfunzionamento" – C.04 "Duplicazione non autorizzata" – D.01 "Accesso non autorizzato" – D.02 "Modifica non autorizzata" – D.05 "Esportazione illegittima" – E.01 "Malfunzionamento" – E.02 "Interruzione" – E.03 "Intercettazione"** si osserveranno le regole dettate espressamente dalle seguenti norme:

1) Allegato B - Disciplinare Tecnico - Punti 25 e 26

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

Misure di sicurezza da adottare

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

SEZIONE 7.2
MISURE DI SICUREZZA IDONEE ART. 31 D. LGS. 196/03

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

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

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

Le misure idonee di sicurezza sono disciplinate dall'art. 31 del Codice, articolo che impone al titolare del trattamento dei dati personali di predisporre tutte le misure di sicurezza idonee a ridurre al minimo "i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta".

A questo punto, si pone come necessaria un'importante considerazione: se l'adeguamento alle "misure minime" implica l'assenza di responsabilità penali, tale adeguamento non è di per sé sufficiente per affrancarsi da responsabilità civile qualora l'evoluzione tecnologica renda disponibili accorgimenti ulteriori che soddisfino le misure dichiarate "idonee".

Ciò perché - ai sensi dell'art. 15 del Codice - "chiunque cagiona danno ad altri per effetto del trattamento dei dati personali è tenuto al risarcimento ai sensi dell'art. 2050 c.c.".
L'art. 2050 c.c., infatti, (norma alquanto rigorosa, dettata in tema di esercizio di attività pericolose) prevede che l'esercente l'attività pericolosa - e quindi, nel nostro caso, il titolare del trattamento - vada esente da responsabilità solo se riesca a dimostrare di aver adottato tutte le misure idonee ad evitare il danno. In caso contrario, ai sensi del 2° comma dell'art. 15 D. Lgs. 196/03, egli dovrà rispondere anche del danno non patrimoniale eventualmente sofferto.

Come si evince facilmente, l'adeguamento alla previsione di legge poc'anzi citata (art. 2050 c.c.) è particolarmente difficoltoso. Secondo la giurisprudenza, infatti, può provare di aver adottato ogni misura idonea chi dimostri di aver rispettato "tutte le tecniche note" - anche solo astrattamente possibili - all'epoca del fatto (cfr. Tribunale di Milano, 19 novembre 1987, in Foro Italiano, 1988, I, 144).

Da altro punto di vista, è opportuno precisare che nell'ambito dei danni da risarcire non sarà incluso il solo pregiudizio patrimoniale (nelle note forme del "danno emergente" e del "lucro cessante"), ma anche il danno morale, come si desume dal chiarissimo tenore dell'art.15 D. Lgs. 196/03.

L'espressa estensione al trattamento di dati personali della risarcibilità del danno non patrimoniale è sintomatica della particolare attenzione che il Legislatore ha voluto rivolgere ai danneggiati, dal momento che il danno che ricorre più frequentemente è proprio quello relativo alla sfera morale dell'individuo, di cui sarebbe stata altrimenti esclusa la risarcibilità (stante il precetto dell'art. 2059 c.c.).

Il titolare ed il responsabile, perciò, oltre a quelle minime previste, devono anche adottare misure di prevenzione "idonee" a ridurre - per quanto possibile - i rischi, prevenibili e prevedibili, che incombono sui dati.

Riassumendo quindi quanto appena evidenziato, l'Ente dovrà:
a) osservare il livello di sicurezza minimo di legge (per evitare conseguenze penali);
b) approntare le misure di sicurezza ulteriori, che in base al caso concreto si potevano predisporre (altrimenti dovrà risarcire i danni eventualmente cagionati a terzi).

Si osserva, il richiamo esplicito del testo di legge al **PROGRESSO TECNICO**, che consente una "forbice" interpretativa particolarmente ampia all'interno della quale far rientrare le varie e possibili misure di sicurezza.

Ciò spiega il percorso seguito dal Legislatore che ha portato all'adozione di due diversi regimi di responsabilità nel caso di violazione di misure minime o di misure idonee, assegnando alle prime una rilevanza penale e, alle seconde, una rilevanza essenzialmente civile, con valutazioni da compiere al verificarsi del caso concreto e tenuto conto dello stadio di progresso tecnologicamente raggiunto e delle soluzioni concretamente disponibili sul mercato.

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

L'Analisi dei Rischi esplicitata nella Sezione 6 ed i criteri per la valutazione degli stessi esposti nella Sezione 6.1, hanno consentito di rilevare le **Minacce Reali** che insistono, in senso generalizzato e trasversale, su tutti i Servizi dell'Ente senza distinzione e, di conseguenza, su tutti i dati di ogni specifica Banca Dati censita.

I Rischi Residui risultanti devono essere abbattuti o quantomeno ridotti (ex Art. 31 D. Lgs. 196/03) al fine di evitare che i dati possano andare incontro ai seguenti eventi dannosi:

EVENTO DANNOSO	QUALITA' A RISCHIO DI PERDITA		
	DISPONIBILITA'	INTEGRITA'	RISERVATEZZA
Insufficiente conoscenza del sistema o dell'applicazione – Codice A.01	✔	✔	✔
Insufficiente conoscenza dei rischi e delle misure di sicurezza – Codice A.02	✔	✔	✔
Distrazione – Codice A.03	✔		✔
Negligenza – Codice A.04	✔	✔	✔

Incidente – Codice A.05	✔	✔	
Atto doloso – Codice A.06	✔	✔	✔
Obsolescenza Hardware - Codice B.01	✔		✔
Avaria Hardware - Codice B.02	✔	✔	
Distruzione Hardware - Codice B.03	✔	✔	
Furto Hardware - Codice B.04	✔	✔	✔
Manomissione Hardware - Codice B.05	✔	✔	✔
Malfunzionamento Software – Codice C.01	✔	✔	
Virus – Codice C.02	✔	✔	✔
Distruzione Software – Codice C.03	✔	✔	
Duplicazione non autorizzata Software – Codice C.04			✔
Obsolescenza Software – Codice C.05	✔		✔
Modifica non controllata Software – Codice C.06	✔	✔	
Accesso non autorizzato ai dati – Codice D.01			✔
Modifica non autorizzata dei dati – Codice D.02	✔	✔	✔
Distruzione dei dati – Codice D.03	✔	✔	
Mancanza di congruità dei dati – Codice D.04	✔	✔	
Esportazione illegittima di dati – Codice D.05			✔
Malfunzionamento collegamenti – Codice E.01	✔	✔	
Interruzione collegamenti – Codice E.02	✔	✔	
Intercettazione collegamenti – Codice E.03			✔
Incompletezza Sistemi di sicurezza – Codice F.01	✔	✔	✔
Illeggibilità delle copie di backup – Codice F.03	✔	✔	
Terremoto – Codice G.01	✔	✔	
Alluvione – Codice G.02	✔	✔	
Incendio – Codice H.01	✔	✔	
Cedimento strutturale – Codice H.02	✔	✔	✔
Campi elettro – magnetici – Codice H.03	✔	✔	

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

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

In senso generale si provvederà a sensibilizzare l'Amministrazione sulla problematica relativa alla Sicurezza nel trattamento dei Dati Personali, Sensibili e Giudiziari realizzando una serie di interventi (rivolti a ridurre il Rischio Residuo derivante dalle minacce rilevate) al fine di garantire l'applicazione delle Misure di Sicurezza Idonee secondo quanto di seguito meglio dettagliato.

EVENTO DANNOSO	RISCHIO RESIDUO	MISURA IDONEA DA ADOTTARE
❑ **Insufficiente conoscenza del sistema o dell'applicazione – Codice A.01** ❑ **Insufficiente conoscenza dei rischi e delle misure di sicurezza – Codice A.02** ❑ **Distrazione – Codice A.03** ❑ **Negligenza – Codice A.04**	✓ ⊘ ✓ ✓	**Per contrastare il rischio residuo derivante dalle minacce rappresentate dagli Eventi Dannosi indicati con i Codici A.01 – A.02 – A.03 – A.04, saranno adottate le seguenti misure:** ■ Conformemente a quanto previsto dalla Regola 19.6 contenuta all'interno dell'Allegato B al D. Lgs. 196/03 "Disciplinare Tecnico in materia di misure minime di sicurezza", saranno periodicamente previsti 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. ■ Sarà curata la formazione "continua" dei Responsabili e degli Incaricati in tema di Sicurezza nel trattamento dei Dati ed in particolare sulla corretta gestione delle Unità di Elaborazione, in armonia con quanto previsto nella Sezione 9 del presente documento. ■ Saranno impartite, chiare istruzioni scritte riguardanti i compiti assegnati agi incaricati in tutte le fasi di trattamento dei dati personali. ■ Saranno parimenti emanate direttive che diano univoche istruzioni di comportamento e indicazione chiare sulle modalità operative da tenere, che risultino sufficientemente elastiche per adattarsi alla maggior parte delle situazioni ma puntualmente rigide con riferimento a quelle situazioni giudicate ad alto rischio. ■ Sarà curata la formazione continua degli Incaricati sul tema specifico della custodia e buon uso delle credenziali. ■ Saranno emanate specifiche norme volte a sensibilizzare gli incaricati sull'uso corretto delle credenziali e sulle sanzioni previste in caso di omissione di tale adempimento.

EVENTO DANNOSO	RISCHIO RESIDUO	MISURA IDONEA DA ADOTTARE
❑ **Incidente – Codice A.05**	⊘	**Per contrastare il rischio residuo derivante dal verificarsi della minaccia di <u>incidente</u>, identificata con il Codice A.05, saranno adottate le seguenti misure:** ■ Saranno verificati e resi pienamente efficienti tutti i dispositivi antincendio presenti negli ambienti in cui sono effettuati trattamenti di dati personali. ■ Se valutato necessario sarà incrementato il numero degli estintori a polvere e ad Anidride Carbonica. ■ Saranno emanate specifiche informazioni e raccomandazioni ed avvisi in armonia con quanto già previsto dalla vigente normativa in tema di Sicurezza sul Lavoro (D. Lgs. 81/08 e successive modificazioni e integrazioni).

EVENTO DANNOSO	RISCHIO RESIDUO	MISURA IDONEA DA ADOTTARE
❑ **Atto doloso – Codice A.06** ❑ **Furto Hardware – Codice B.04**	⊘ ⊘	**Per contrastare il rischio residuo derivante dalle minacce rappresentate dagli Eventi Dannosi indicati con i Codici A.06 – B.04, saranno adottate le seguenti misure:** ■ I locali nei quali si effettuano trattamenti di dati personali ed i locali ospitanti il Server e gli apparati di Rete, saranno sempre presidiati dal personale incaricato nelle ore d'ufficio e chiusi a chiave in caso di prolungata assenza del personale. La chiave deve essere diversa per ogni locale. ■ Tutti i documenti contenenti dati personali sensibili e giudiziari, devono essere custoditi in armadi e cassetti rigorosamente chiusi a chiave. ■ Fuori dagli orari di lavoro nessun tipo di documento deve essere lasciato incustodito. ■ L'Ente provvederà alla installazione ed al potenziamento di sistemi antintrusione. ■ Le chiavi degli armadi non devono essere universali. In caso di prolungata assenza del personale e fuori dagli orari di lavoro non devono essere lasciate incustodite nel rispettivo ufficio ma dovranno essere custodite da ogni singolo incaricato del trattamento con copia depositata presso ciascun responsabile in busta chiusa e sigillata. ■ La bacheca con all'interno le chiavi degli Uffici sarà posta in un luogo non accessibile da utenti esterni. ■ Si darà adeguata informativa affinché sia segnalato tempestivamente da parte del personale dipendente qualsiasi evento significativo che possa costituire una minaccia per la sicurezza degli ambienti. ■ Si provvederà a dotare tutto il personale dell'Ente di un cartellino di identificazione ai sensi delle vigenti normative. ■ L'accesso all'archivio storico deve essere controllato. Per accedere a tale archivio le persone devono essere preventivamente autorizzate e nel caso in cui l'accesso avvenga dopo l'orario di chiusura devono essere identificate e registrate.

EVENTO DANNOSO	RISCHIO RESIDUO	MISURA IDONEA DA ADOTTARE
❑ **Obsolescenza Hardware – Codice B.01** ❑ **Avaria Hardware – Codice B.02**	✓ ✓	**Per contrastare il rischio residuo derivante dalle minacce rappresentate dagli Eventi Dannosi indicati con i Codici B.01 – B.02, saranno adottate le seguenti misure:** ■ Tutte le Unità di Elaborazione saranno acquistate o noleggiate con un periodo di garanzia "in loco" pari almeno a tre anni. ■ Si provvederà a censire e catalogare tutte le Unità di Elaborazione dell'Ente al fine di disporre di un quadro sempre aggiornato del livello di obsolescenza tecnica e degli interventi tecnici effettuati sulle macchine. ■ Si procederà con gradualità alla dismissione dell' hardware tecnologicamente obsoleto. ■ Si provvederà ad adottare una politica di acquisto delle Unità di Elaborazione di tipo Server con caratteristiche di ridondanza nei dischi (Mirroring o RAID), negli alimentatori elettrici e nelle schede di rete.

EVENTO DANNOSO	RISCHIO RESIDUO	MISURA IDONEA DA ADOTTARE
❑ **Distruzione Hardware – Codice B.03** ❑ **Manomissione Hardware – Codice B.05** ❑ **Distruzione Software – Codice C.03** ❑ **Duplicazione non autorizzata Software – Codice C.04** ❑ **Modifica non controllata Software – Codice C.06**	⊘ ⊘ ✓ ✓ ✓	**Per contrastare il rischio residuo derivante dalle minacce rappresentate dagli Eventi Dannosi indicati con i Codici B.03 – B.05 – C.03 – C.04 – C.06, saranno adottate le seguenti misure:** ■ I locali ove si effettuano trattamenti di dati personali ed i locali ospitanti il Server e gli apparati di Rete, saranno sempre presidiati dal personale incaricato e chiusi a chiave in caso di prolungata assenza del personale. La chiave deve essere diversa per ogni locale. ■ L'Ente provvederà alla installazione ed al potenziamento di sistemi antintrusione. ■ La bacheca con all'interno le chiavi degli Uffici sarà posta in un luogo non accessibile da utenti esterni. ■ Si darà adeguata informativa affinché sia segnalato tempestivamente da parte del personale dipendente qualsiasi evento significativo che possa costituire una minaccia per la sicurezza degli ambienti e dei dati. ■ Si provvederà a dotare tutto il personale di un cartellino di identificazione ai sensi delle vigenti leggi. ■ Conformemente a quanto previsto dalla Regola 19.6 contenuta all'interno dell'Allegato B al D. Lgs. 196/03 "Disciplinare Tecnico in materia di misure minime di sicurezza", saranno periodicamente previsti 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. ■ Sarà curata la formazione "continua" dei Responsabili e degli incaricati in tema di Sicurezza nel trattamento dei Dati ed in particolare sulla corretta gestione delle Unità di Elaborazione, in armonia con quanto previsto nella Sezione 9 del presente documento. ■ Saranno impartite, chiare istruzioni scritte riguardanti i compiti assegnati agi incaricati in tutte le fasi di trattamento dei dati personali. ■ Saranno parimenti emanate direttive che diano inequivoche istruzioni di comportamento e modalità operative da tenere, sufficientemente elastiche per adattarsi alla maggior parte delle situazioni ma puntualmente rigide con riferimento a quelle situazioni giudicate ad alto rischio. ■ Sarà curata la formazione continua degli Incaricati sul tema specifico della custodia e buon uso delle credenziali. ■ Saranno emanate specifiche norme volte a sensibilizzare gli incaricati sull'uso corretto delle credenziali e sulle sanzioni per l'Ente in caso di omissione di tale adempimento.

EVENTO DANNOSO	RISCHIO RESIDUO	MISURA IDONEA DA ADOTTARE
❑ **Malfunzionamento Software – Codice C.01** ❑ **Obsolescenza Software – Codice C.05** ❑ **Mancanza di congruità dei dati – Codice D.04**	✓ ✓ ✓	**Per contrastare il rischio residuo derivante dalle minacce rappresentate dagli Eventi Dannosi indicati con i Codici C.01 – C.05 – D.04, saranno adottate le seguenti misure:** ■ Sarà realizzato e mantenuto sempre aggiornato un inventario delle risorse software dell'Ente che permetta di avere costantemente sotto controllo il software installato al fine di poter procedere celermente alla revisione dei contratti in essere per la fornitura del software nei casi di entrata in vigore di nuovi disposti normativi ovvero in tutte le ipotesi di esigenze legate all'organizzazione degli Uffici dell'Ente. ■ Implementazione costante delle misure informatiche tese a garantire la correttezza, completezza e congruità dei dati trattati. ■ Acquisto puntuale delle licenze d'uso per i software gestionali utilizzati dai diversi Uffici dell'Ente e dei periodici aggiornamenti. ■ Si procederà ad una progressiva omogeneizzazione delle versioni dei sistemi operativi delle unità di elaborazione alle ultime versioni in commercio (Windows, Linux o altri sistemi operativi, Ms-Office, privilegiando i programmi OPEN SOURCE ed applicando la norma sul riuso del software in P.A.). ■ Saranno emanate Regole di Comportamenti rivolte a tutto il personale specificanti l'obbligo di utilizzare solo ed esclusivamente software con regolari diritti di proprietà da parte dell'Ente.

EVENTO DANNOSO	RISCHIO RESIDUO	MISURA IDONEA DA ADOTTARE
❑ **Virus – Codice C.02**	✓	Per contrastare il rischio residuo derivante dal verificarsi della minaccia "Virus", identificata con il Codice C.02, saranno adottate le seguenti misure: ■ Si provvederà a mantenere in piena efficienza il Software Antivirus. L'automatismo e la tempestività degli aggiornamenti disponibili per tutto il personale elimineranno in modo significativo i rischi derivanti da tale minaccia. ■ L'Ente si doterà di un server antivirus da sistema Centralizzato in modo da provvedere in tempo reale alla distribuzione del software e degli aggiornamenti agli utenti collegati in rete.

EVENTO DANNOSO	RISCHIO RESIDUO	MISURA IDONEA DA ADOTTARE
❑ **Accesso non autorizzato ai dati – Codice D.01** ❑ **Modifica non autorizzata dei dati – Codice D.02** ❑ **Distruzione dei dati – Codice D.03** ❑ **Esportazione illegittima di dati – Codice D.05**	⊘ ✓ ⊘ ⊘	**Per contrastare il rischio residuo derivante dalle minacce rappresentate dagli Eventi Dannosi indicati con i Codici D.01 – D.02 – D.03 – D.05, saranno adottate le seguenti misure:** ■ I locali ove si effettuano trattamenti di dati personali saranno sempre presidiati dal personale incaricato nelle ore d'ufficio e chiusi a chiave in caso di prolungata assenza del personale. La chiave deve essere diversa per ogni locale. ■ Tutti i documenti contenenti dati personali sensibili e giudiziari, devono essere custoditi in armadi e cassetti chiusi a chiave. ■ Fuori dagli orari di lavoro nessun tipo di documento deve essere lasciato incustodito. ■ Le chiavi degli armadi non devono essere universali. In caso di prolungata assenza del personale e fuori dagli orari di lavoro non devono essere lasciate nel rispettivo ufficio ma dovranno essere custodite da ogni singolo incaricato del trattamento con copia depositata presso ciascun responsabile in busta chiusa e sigillata. ■ Saranno mantenuti in piena efficienza e se possibile potenziati, in tutti gli uffici, i sistemi di antintrusione soprattutto in quelli collocati al Piano Terra più agevolmente raggiungibili dall'esterno. ■ La bacheca con all'interno le chiavi degli Uffici sarà posta in un luogo non accessibile da utenti esterni. ■ Si darà adeguata informativa affinché sia segnalato tempestivamente da parte del personale dipendente qualsiasi evento significativo che possa costituire una minaccia per la sicurezza degli ambienti. ■ Si provvederà a dotare tutto il personale degli uffici di un cartellino di identificazione ai sensi delle vigenti leggi. ■ Saranno emanate procedure formali per l'accesso controllato e regolamentato nei locali ove ha luogo la custodia dei supporti magnetici o ottici. ■ Saranno rafforzate e sottoposte a periodica revisione le misure di identificazione ed autenticazione dell'utente in rete LAN da parte dei Server Gestionali affinché in ogni rete interconnessa vengano rispettati i relativi requisiti di sicurezza definiti dalle specifiche politiche; ■ Saranno sottoposte a periodica revisione le regole di apertura delle porte necessarie per i servizi pubblici in produzione (tipicamente server web, server di posta, DNS, FTP); ■ L'Ente si doterà di un firewall perimetrale. ■ Tutte le stazioni di lavoro sulle quali vengono effettuati trattamenti di dati personali saranno protette a monte da un sistema di Protezione Personale contro le Intrusioni (Firewall Personale). ■ Sarà sottoposto a periodico monitoraggio il funzionamento del Firewall effettuando periodici test di simulazione di intrusione. ■ Saranno emanate specifiche norme volte a sensibilizzare gli incaricati sull'uso corretto delle credenziali e sulle sanzioni per l'Ente in caso di omissione di tale adempimento. ■ Sarà verificato periodicamente il rispetto delle procedure di cui sopra.

EVENTO DANNOSO	RISCHIO RESIDUO	MISURA IDONEA DA ADOTTARE
❑ **Malfunzionamento collegamenti – Codice E.01** ❑ **Interruzione collegamenti – Codice E.02** ❑ **Intercettazione collegamenti – Codice E.03**	✓ ✓ ✓	**Per contrastare il rischio residuo derivante dalle minacce rappresentate dagli Eventi Dannosi indicati con i Codici E.01 – E.02 – E.03, saranno adottate le seguenti misure:** ■ Sarà rafforzato l'esercizio di efficaci strumenti di controllo del traffico in rete tesi ad evidenziare il traffico anomalo e far sì che in ogni rete interconnessa vengano rispettati i relativi requisiti di sicurezza definiti dalle specifiche politiche, al fine di non creare danni o disservizi; ■ Saranno emanate specifiche regole di comportamento verso tutto il personale al fine di renderlo edotto sull'uso consapevole e corretto della Rete Locale e di Internet. ■ I cablaggi della rete locale saranno mantenuti in cabalette sigillate o protette, possibilmente, sottotraccia. ■ Saranno mantenuti efficaci sistemi di identificazione ed autenticazione dell'utente in rete. ■ Saranno mantenuti efficaci sistemi software di controllo delle Intrusioni in rete. ■ Sarà promosso l'utilizzo della crittografia ed in particolare della Firma Digitale, con l'obiettivo di realizzare la sicurezza dei servizi di rete attraverso una infrastruttura tecnologica di crittografia a Chiave Pubblica (PKI). ■ I Server ed i singoli elaboratori saranno collegati ad un gruppo di continuità che sia in grado di garantire una stabilizzazione dell'energia elettrica erogata. Tale gruppo, in conseguenza di un'improvvisa assenza di energia, garantisce un'autonomia temporale necessaria ad avviare le corrette procedure di spegnimento dell'elaboratore.

EVENTO DANNOSO	RISCHIO RESIDUO	MISURA IDONEA DA ADOTTARE
❑ **Incompletezza sistemi di sicurezza – Codice F.01**	⊘	**Per contrastare il rischio residuo derivante dalle minacce rappresentate dall' Evento Dannoso indicato con il Codice F.01, saranno adottate le seguenti misure:** ■ Si procederà ad un costante monitoraggio delle attività poste in essere dagli Incaricati del trattamento che espongono i dati personali trattati a situazioni di rischio. ■ L'Ente adotterà una politica di massimo coinvolgimento dei servizi e degli uffici al fine della messa a punto e della manutenzione di misure di sicurezza efficaci ed efficienti. ■ Si procederà a testare periodicamente l'efficacia dei sistemi di sicurezza adottati dall'Ente al fine di garantire che i dati personali oggetto di trattamento siano custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta (Art. 31, D. Lgs. 196/03)**.**

EVENTO DANNOSO	RISCHIO RESIDUO	MISURA IDONEA DA ADOTTARE
❑ **Illeggibilità / mancata effettuazione delle copie di Backup – Codice F.02**	⊘	Per contrastare il rischio residuo derivante dal verificarsi della minaccia "Virus", identificata con il Codice F.03, saranno adottate le seguenti misure: ■ Si provvederà alla corretta esecuzione delle copie di sicurezza dei dati residenti sul/sui Server e sui singoli elaboratori. ■ Si provvederà all'acquisizione di supporti magnetici o ottici per la memorizzazione dei dati (CDR, CDRW, DVD, nastri, floppy) con caratteristiche di alta affidabilità. ■ Si provvederà alla custodia delle copie di backup (in numero adeguato alle necessità) in luogo adeguato, sufficientemente distante dall' ambiente in cui vengono trattati i dati e protetto da agenti ambientali (tale da non risentire delle conseguenze delle minacce di un eventuale evento distruttivo o corruttivo dei sistemi hardware). ■ Si provvederà alla custodia delle copie dei dati sensibili e giudiziari in armadi o contenitori muniti di serratura,

SEZIONE 8
DESCRIZIONE DEI CRITERI E DELLE MODALITÀ PER IL RIPRISTINO DELLA DISPONIBILITÀ DEI DATI IN SEGUITO A DISTRUZIONE O DANNEGGIAMENTO (REGOLA 19.5 E REGOLA 23 ALLEGATO B AL D. LGS. 196/03).

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

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

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

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

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

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

L'attività pratica di ripristino della disponibilità dei dati consiste nell'eseguire una nuova installazione di tutti i file di dati, dei programmi, del software di base che l'evento indesiderato ha alterato o distrutto, ovvero nella sostituzione delle componenti tecnologiche hardware che hanno provocato l'interruzione dei trattamenti. La nuova installazione avviene

utilizzando le più aggiornate copie di sicurezza fatte su supporti o sistemi di riserva, accertandone preventivamente l'integrità.

La previsione da parte del Legislatore dell'obbligo di "istruzioni organizzative e tecniche" che prescrivano il salvataggio dei dati con una cadenza almeno settimanale mira a fare in modo che, in caso di "disastri informatici" non venga meno uno degli obiettivi principali della sicurezza nel trattamento dei dati: la disponibilità dei dati stessi.
In considerazione della capienza dei moderni supporti di memorizzazione, la cadenza settimanale del backup dei dati si configura come una misura letteralmente MINIMA (Regola 18 Allegato B al D. Lgs. 196/03) e sarebbe opportuno orientare gli Uffici dell'Ente verso una procedura di backup dei dati automatizzata a cadenza giornaliera.

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

Esso sarà composto da due categorie di azioni:

⇨ Azioni o Misure Preventive

⇨ Azioni di Ripristino

Piano di Continuità Operativa - Misure Preventive

1. Saranno osservate tutte le prescrizioni normative in ordine all'ambiente fisico, all' hardware ed al software su cui risiedono i dati secondo le prescrizioni contenute nella Sezione 7, 7.1 e 7.2 - Misure Minime di Sicurezza e Misure Idonee di Sicurezza .

2. Saranno effettuate con regolarità le copie di sicurezza dei dati secondo le prescrizioni specificate dalla Regola 18 del Disciplinare Tecnico. In particolare, saranno impartite istruzioni organizzative (e messi a disposizione gli strumenti) che prevedano il salvataggio dei dati con frequenza almeno settimanale.

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

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

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

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

Piano di Continuità Operativa - Azioni di Ripristino

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

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

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

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

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

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

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

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

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

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

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

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

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

CRITERI E PROCEDURE PER IL SALVATAGGIO	LUOGO DI CUSTODIA DELLE COPIE DI BACK UP	PERIODICITA' DEL BACK UP
Con riferimento alle BANCHE DATI ed alle informazioni ospitate sui Server ACER ALTOS G710 e ACER ALTOS G540, disponendo questi elaboratori di doppi HDD uniti in RAID 1, la copia di sicurezza dei dati residenti, è effettuata contemporaneamente ed in modalità automatica sui diversi supporti (mirroring) al fine di assicurare la presenza di copie speculari delle informazioni.	**Il back up viene effettuato in modalità automatica dai Server sugli HDD uniti in RAID.**	**Quotidiano/Automatico**
Sempre con riferimento alle procedure ed ai dispositivi utilizzati per il salvataggio dei dati e degli applicativi residenti sul Server di Dominio ACER ALTOS G710 e sul Server ACER ALTOS G540, si evidenzia che oltre alla copia di sicurezza garantita dalla presenza di doppi Hard Disk uniti in Raid 1, l'Ente, al fine di offrire adeguata garanzia di integrità, disponibilità e riservatezza alle informazioni	**Le cassette DAT utilizzate per la realizzazione delle copie di Backup dei dati residenti sui Server, sono rigorosamente custodite in armadi muniti di serratura.**	**La copia di sicurezza dei dati residenti sui Server è effettuata su cassette DAT con periodicità codificata settimanale ed in modalità manuale.**

ivi residenti, ha provveduto ad acquistare e configurare un'Unità di Backup su cassette DAT integrata ai Server, attraverso la quale si procede, con frequenza codificata settimanale ed in modalità manuale, ad effettuare una copia di sicurezza dei dati ospitati su Cassette DAT. **Le cassette DAT utilizzate per la realizzazione delle copie di Backup dei Server, sono poi rigorosamente custodite in armadi muniti di serratura.**		
Si evidenzia una situazione di forte criticità, che espone l'Ente a livelli di vulnerabilità non accettabili, sui singoli Clients che, in linea generale, o non provvedono alla esecuzione di copie di sicurezza ovvero provvedono con periodicità non sempre codificata o comunque non espressamente definita. **L'Ente, infatti, non ha ancora provveduto alla configurazione su Server (ovvero su altra macchina dedicata), di CARETLLE DEDICATE IN VIA ESCLUSIVA a ciascun dipendete per l'elaborazione dei documenti di competenza: tutti gli utenti della LAN Comunale, elaborano dunque i documenti relativi ai procedimenti loro attribuiti esclusivamente in locale sul singolo Client.** **Inoltre, come detto, non sono adottate con sistematicità e rigore procedure codificate di salvataggio e messa in sicurezza dei dati: in questo modo, gli stessi dati e le informazioni residenti unicamente sul disco fisso di ciascun PC Client sono esposti al rischio di perdita delle caratteristiche primarie di disponibilità, integrità e riservatezza.** **Al fine di rimuovere definitivamente l'attuale situazione di forte criticità e vulnerabilità, sarà necessario provvedere con urgenza alla definizione delle procedure interne per la corretta esecuzione delle copie di backup.** **In particolare, si dovrà provvedere con immediatezza a configurare sullo stesso Server di Dominio ovvero su altro elaboratore,**	**Non sono adottate con sistematicità e rigore procedure codificate di salvataggio e messa in sicurezza dei dati: in questo modo, gli stessi dati e le informazioni residenti unicamente sul disco fisso di ciascun PC Client sono esposti al rischio di perdita delle caratteristiche primarie di disponibilità, integrità e riservatezza.**	**La frequenza con la quale vengono effettuate le copie di Backup dei dati residenti in locale sui singoli Clients, allo stato attuale, non è né definita né espressamente tipizzata.**

cartelle di lavoro dedicate in via esclusiva ad ogni singolo dipendente, alle quali dovrà avere accesso esclusivamente l'utente, da utilizzarsi per la corretta gestione dei dati al fine dell'esecuzione delle copie di sicurezza. **Sarà necessario configurare il sistema informatico comunale in modo tale che le cartelle di lavoro dei singoli utenti, all'interno delle quali si elaboreranno i documenti di competenza di ciascuno, non siano residenti in locale sul singolo Client ma siano ospitate direttamente sul Server ed il dipendente non possa più elaborare i documenti sul proprio disco locale ma direttamente sulle cartelle residenti sul Server.** **Le citate cartelle dovranno essere accessibili esclusivamente dall'utente per il quale sono state configurate.** **Per la gestione dei documenti condivisi tra più utenti si utilizzeranno invece differenti cartelle "di condivisione".**		

SEZIONE 9

PREVISIONE DI INTERVENTI FORMATIVI

Disciplinare Tecnico

La formazione è da sempre considerata dal legislatore uno strumento strategico per lo sviluppo professionale, gestionale ed organizzativo.

Per questa ragione, l'attività formativa deve necessariamente essere concepita come continua, sistematica e mirata alla concreta realtà operativa dell'Ente.

Nel caso di trattamento di dati personali, è lo stesso legislatore a rilevare l'importanza e la necessità della formazione nella Regola 19.6 dell'Allegato B al D. Lgs. 196/03 che prevede espressamente che nel Documento Programmatico sulla Sicurezza devono essere contenute idonee informazioni riguardo la "previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali".

La formazione deve essere intesa sia come momento di conoscenza e di approfondimento di nuove tematiche e di corrette modalità di lavoro che come percorso di apprendimento che incide su stili di comportamento e abitudini.

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

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

L'utilizzo da parte del Legislatore della parola "previsione" si deve interpretare nel senso che non è sufficiente che la formazione avvenga *una tantum,* ma è necessario che sia continua, ogniqualvolta avvengano cambiamenti di mansione degli incaricati, vengano introdotti nuovi strumenti o modalità con cui i dati sono trattati, oppure vi sia il rischio che si verifichino gravi problemi in ordine alla sicurezza.
Il Comune provvederà all'erogazione della formazione in favore di Responsabili ed Incaricati del trattamento in occasione dell'ingresso in servizio, di cambiamento di mansione, di introduzione di modifiche significative al presente Documento Programmatico sulla Sicurezza ovvero agli strumenti informatici o alle procedure di trattamento e gestione dei dati personali da parte dell'
L'Ente è consapevole che l'adeguamento alla norma, avrà un impatto considerevole sulla propria organizzazione interna.
Nel corso delle precedenti annualità l'Ente ha realizzato percorsi formativi specialistici in materia di riservatezza nel trattamento dei dati personali rivolti a tutti i soggetti che a qualsiasi titolo trattino dati personali nell'ambito dell'Amministrazione.
Per il futuro l'Ente ha elaborato un programma formativo finalizzato a perseguire i seguenti obiettivi principali:

- consentire il raggiungimento dell'adeguamento alla norma da parte dell'Ente rendendo i discenti edotti sui rischi che incombono sui dati e sulle misure di prevenzione e protezione disponibili per prevenire eventi dannosi;
- informare gli operatori in relazione ai profili di responsabilità personale e patrimoniale previsti dalla vigente normativa in materia;
- analizzare la problematica del contemperamento tra tutela del diritto alla riservatezza nel trattamento di dati personali in relazione e altri diritti fondamentali in Pubblica Amministrazione come il diritto alla trasparenza dell'azione amministrativa o il diritto all'accesso agli atti;
- estendere il programma formativo oltreché agli incaricati direttamente coinvolti nel trattamento dei dati, come previsto dal Disciplinare Tecnico, a tutte gli altri soggetti che a qualsiasi titolo interagiscono in questo processo.

I soggetti coinvolti nel Piano Formativo apparterranno alle seguenti categorie:

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

Le tematiche trattate saranno le seguenti:

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

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

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

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

Gli interventi formativi potranno essere realizzati sia a cura degli stessi soggetti individuati quali Responsabili del trattamento dei dati che da parte di soggetti esperti, esterni all'Amministrazione, incaricati espressamente per l'effettuazione dei percorsi formativi di cui si è detto.

SEZIONE 10
TRATTAMENTI DI DATI PERSONALI AFFIDATI ALL'ESTERNO
REGOLA 19.7 ALLEGATO B al D. LGS. 196/03

Disciplinare Tecnico

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

Nello svolgimento dei propri compiti istituzionali il Titolare del trattamento può ricorrere ad altri soggetti cui affidare determinate attività. In tale ipotesi, deve essere precisato il ruolo assunto da questi soggetti, i quali, ai sensi della disciplina in materia di protezione dei dati personali, possono essere considerati, alternativamente, come semplici collaboratori esterni del Titolare quando coadiuvino quest'ultimo trattando dati personali anche al di fuori della relativa struttura, ma nell'ambito di un'attività che ricade nella sfera di titolarità e di responsabilità del Titolare oppure, come figure soggettive del tutto distinte da esso, che decidono autonomamente in ordine al trattamento delle informazioni. Nel primo caso, tali soggetti esterni costituiscono parte sostanziale del primo Titolare (e dovranno essere individuati come Incaricati ovvero come Responsabili del trattamento); nel secondo caso, invece, sono da considerarsi autonomi Titolari.
Da ciò deriva che, nel caso in cui l'Ente affidi ad un privato alcune operazioni di trattamento, qualora il soggetto affidatario sia considerabile "Incaricato" o anche "Responsabile" del trattamento, seguirà lo speciale regime previsto dalla norma per i soggetti pubblici; viceversa, qualora il soggetto esterno affidatario figuri come Titolare autonomo dovrà seguire le regole stabilite per il trattamento da parte di soggetti privati.

Si ricorda che, rivestono la qualità di "Incaricati esterni del trattamento" i privati (solo le persone fisiche possono essere designate quali Incaricati) che ricevano da un soggetto pubblico l'incarico del trattamento di dati personali connesso all'espletamento dei compiti istituzionali dell'Amministrazione da svolgersi sotto la diretta sorveglianza e secondo le indicazioni di quest'ultima, che conserva la qualità di "Titolare del trattamento e di Responsabile del trattamento". In questo caso al soggetto esterno non competono decisioni di fondo sulle finalità e sulle modalità di utilizzazione dei dati, ma solo limitati margini di autonomia in ordine al concreto svolgimento del servizio ed a scelte tecnico-operative. Nell'ambito di tale configurazione del rapporto, il privato è legittimato ad utilizzare i dati in possesso dell'Amministrazione rimanendo però vincolato ad usarli per le sole finalità perseguite dalla P.A. e sulla base del particolare regime previsto per quest'ultima.
Rivestono invece la qualità di "Responsabili del trattamento" i privati che sulla base di un contratto ovvero di una convenzione ricevano da un soggetto pubblico l'incarico di gestire integralmente un Servizio o porzione dello stesso che comporti il trattamento dei dati personali connessi all'espletamento dei compiti istituzionali delegati dall'Amministrazione.

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

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

A mero titolo esemplificativo e non esaustivo, si evidenzia che l'Ente provvede ad affidare all'esterno, sulla base di convenzioni, la gestione dei seguenti Servizi/attività:

- **Assistenza domiciliare – Cooperativa A.S. – Cooperativa di Assistenza Sociale – Sassari**
- **Assistenza educativa – Cooperativa A.S. – Cooperativa di Assistenza Sociale – Sassari**
- **Trasporto scolastico – FERRALIS VIAGGI – Olmedo**
- **Mensa Scolastica – "Consorzio Conserva" – Porto Torres**

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

Misura da adottare
Il soggetto esterno affidatario di operazioni di trattamento su Banche Dati dell'Ente fornirà le seguenti garanzie: **1.** di essere consapevole che i dati che gestirà nell'espletamento dell'incarico ricevuto, sono dati personali e, come tali, gli stessi potranno essere trattati ai soli fini dell'espletamento dell'incarico in essere con l'Amministrazione **2.** di ottemperare agli obblighi previsti dal Codice per la protezione dei dati personali

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

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

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

SEZIONE 11

GLI AMMINISTRATORI DI SISTEMA – PROVVEDIMENTO A CARATTERE GENERALE DEL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI DEL 27/11/08 – G.U. N. 300 DEL 24/12/08 MODIFICATO DAL PROVVEDIMENTO A CARATTERE GENERALE DEL 25/06/09 – G.U. N. 149 DEL 30/06/09

Gli "amministratori di sistema" sono figure essenziali per la sicurezza delle banche dati e la corretta gestione delle reti telematiche. Sono esperti chiamati a svolgere delicate funzioni che comportano la concreta capacità di accedere a tutti i dati che transitano sulle reti istituzionali. Ad essi viene affidato spesso anche il compito di vigilare sul corretto utilizzo dei sistemi informatici di una pubblica amministrazione.

Per questo il Garante ha deciso di richiamare l'attenzione di Enti Locali e Pubbliche Amministrazioni, sulla figura professionale dell' amministratore di sistema e ha prescritto l'adozione di specifiche misure tecniche ed organizzative che agevolino la verifica sulla sua attività da parte di chi ha la titolarità delle banche dati e dei sistemi informatici.

Le ispezioni effettuate in questi anni dall'Autorità hanno permesso di mettere in luce in diversi casi, una scarsa consapevolezza da parte di organizzazioni grandi e piccole del ruolo svolto dagli amministratori di sistema. I gravi casi verificatisi negli ultimi anni, hanno evidenziato una preoccupante sottovalutazione dei rischi che possono derivare quando l'attività di questi esperti sia svolta senza il necessario controllo da parte del Titolare.

Le misure e le cautele dovranno essere adottate entro il prossimo 15 Dicembre 2009 (alla luce della proroga contenuta nell'ultimo Provvedimento del 25/06/09) da parte di tutte le aziende private e da tutti i soggetti pubblici, compresi gli uffici giudiziari, le forze di polizia ed i servizi di sicurezza.

Il Garante per la Protezione dei dati Personali, in data 27/11/08 (G.U. n. 300 del 24/12/08) ha adottato un provvedimento a carattere generale al fine di prescrivere ai Titolari di trattamenti effettuati con strumenti elettronici, le misure da adottare nella attribuzione delle funzioni di amministratore di sistema.

Il Garante ha adottato questo importantissimo Provvedimento dopo aver rilevato l'esigenza di intraprendere una specifica attività rispetto ai soggetti preposti ad attività riconducibili alle mansioni tipiche dei c.d. "amministratori di sistema", nonché di coloro che svolgono mansioni analoghe in rapporto a sistemi di elaborazione e banche di dati, al fine di evidenziarne la rilevanza rispetto ai trattamenti di dati personali anche allo scopo di promuovere presso i relativi Titolari e nel pubblico la consapevolezza della delicatezza di tali peculiari mansioni nella "Società dell'informazione" e dei rischi a esse associati.

Il Garante riscontra l'esigenza di consentire più agevolmente, la conoscibilità dell'esistenza di tali figure o di ruoli analoghi svolti in relazione a talune fasi del trattamento all'interno di Enti e ritiene necessario promuovere l'adozione di specifiche cautele nello svolgimento delle mansioni svolte dagli amministratori di sistema, unitamente ad accorgimenti e misure, tecniche ed organizzative, volti ad agevolare l'esercizio dei **doveri di controllo da parte del Titolare**.

Il Garante è consapevole del fatto che, lo svolgimento delle mansioni di amministratore di sistema, anche a seguito di una sua formale designazione quale Responsabile o Incaricato del trattamento, comporta di regola la concreta capacità, per atto intenzionale, ma anche per caso fortuito, di accedere in modo privilegiato a risorse del sistema informativo e a dati personali cui non si è legittimati ad accedere rispetto ai profili di autorizzazione attribuiti. Per questo motivo, il Garante intende richiamare l'attenzione su tale rischio in particolar modo per le Amministrazioni e gli Enti (di seguito sinteticamente individuati con l'espressione "titolari del trattamento" ex art. 4, comma 1, lett. f) del Codice) che impiegano, in riferimento alla gestione di banche dati o reti informatiche, sistemi di elaborazione utilizzati da una molteplicità di incaricati con diverse funzioni, applicative o sistemistiche.

In particolare il citato Provvedimento a carattere generale, sottolinea:

- che i Titolari del trattamento dei dati, sono tenuti, ai sensi dell'art. 31 del Codice, ad adottare misure di sicurezza "idonee e preventive" in relazione ai trattamenti svolti, dalla cui mancata o non idonea predisposizione possono derivare responsabilità anche di ordine penale e civile (artt. 15 e 169 del Codice);
- che l'**individuazione di soggetti idonei a svolgere le mansioni di amministratore di sistema riveste una notevole importanza**, costituendo una delle scelte fondamentali che, unitamente a quelle relative alle tecnologie, contribuiscono a incrementare la complessiva sicurezza dei trattamenti svolti, e va perciò curata in modo particolare **evitando incauti affidamenti**.

Le novità di maggior rilievo introdotte con il Provvedimento riguardano:

- **La registrazione degli accessi** ovvero, l'adozione di sistemi di controllo che consentano la registrazione degli accessi effettuate dagli amministratori di sistema ai sistemi di elaborazione e agli archivi elettronici. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi.
- **La verifica della attività** ovvero, almeno annualmente, il Titolare del trattamento dei dati deve verificare la rispondenza dell'operato degli amministratori di sistema alle misure organizzative, tecniche e di sicurezza previste dalla legge per i trattamenti di dati personali.
- **L'Elenco degli amministratori di sistema** ovvero, ciascun soggetto pubblico dovrà riportare in un documento interno da mantenere aggiornato e disponibile in caso di accertamento da parte del Garante gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco dettagliato delle funzioni ad essi attribuite.
- **Verifica dei requisiti** ovvero, dovranno essere valutate con attenzione esperienza, capacità, e affidabilità della persona chiamata a ricoprire il ruolo di amministratore di sistema, che deve essere in grado di garantire il pieno rispetto della normativa in materia di protezione dei dati personali, compreso il profilo della sicurezza.