**Allegato parte integrante**
ALLEGATO B

# DISPOSIZIONI ESPLICATIVE IN TEMA DI PROTEZIONE DEI DATI PERSONALI, MISURE DI SICUREZZA E MODULISTICA

Attuazione delle disposizioni contenute
nel “Codice in materia di protezione dei dati personali”
(Decreto legislativo 30 giugno 2003, n. 196)

INDICE

# INTRODUZIONE

Il diritto alla protezione dei dati personali è particolarmente rilevante nell'ambito dell'attività amministrativa. Esso richiede di bilanciare la necessità degli enti pubblici di acquisire, e trattare, informazioni sui cittadini, in funzione dell'attuazione dei compiti istituzionali, con l'interesse di questi ultimi all'efficienza dell'Amministrazione e alla tutela dei propri dati. D'altra parte, non può nascondersi come lo sviluppo tecnologico, e l'evoluzione delle reti telematiche, espone il singolo individuo ad un rischio di abuso, anche inconsapevole, della sfera privata e delle informazioni che lo riguardano.
Per far fronte alla situazione descritta, la legge 31 dicembre 1996, n. 675, ispirandosi alla Direttiva europea 95/46/CE, aveva disciplinato in modo più preciso questa materia. Successivamente, nel 2003, è stato emanato il Decreto legislativo 30 giugno 2003, n. 196, contenente il Codice in materia di protezione dei dati personali, che ha recepito, formalmente, le direttive europee in tema di protezione dei dati personali.
E' utile ricordare come la tutela dei dati personali dei cittadini sia solo una faccia di una medaglia il cui rovescio è rappresentato dalle misure di sicurezza, ed in particolare dalle misure di sicurezza informatica, visto che ogni dato personale anche se conservato come documento cartaceo, viene quasi sempre preventivamente trattato con apparecchiature informatiche.
Il Titolare, attraverso la sistematizzazione e razionalizzazione delle disposizioni emanate dalla Giunta provinciale in materia di tutela dei dati personali e di sicurezza, ha predisposto il presente documento per facilitare l'applicazione di una normativa, a dir poco complessa. Questo provvedimento vuole essere uno strumento operativo, a disposizione dei vari soggetti che assumono ruoli, operativi e direttivi, di responsabilità nel trattamento dei dati personali. In particolare, mira a fornire ai Dirigenti, e ai vari operatori (Responsabili e Incaricati del trattamento, Amministratori di sistema), precisazioni in ordine alle varie misure (organizzative, procedurali, tecniche e logistiche) da applicare, per garantire il richiesto livello di sicurezza dei trattamenti gestiti dall'Amministrazione provinciale. Tramite la codificazione dei compiti e degli adempimenti richiesti, i vari soggetti coinvolti nella gestione dei dati personali, compresi i collaboratori esterni dell'Amministrazione provinciale, avranno presente l'estensione ed i limiti delle loro responsabilità.

L'Allegato si articola in quattro sezioni:

- una sintetica parte introduttiva (Sezione I), propedeutica alla conoscenza delle finalità e dei principi generali che reggono il trattamento di dati personali da parte dei soggetti pubblici;
- una Sezione II, di carattere operativo, specificatamente dedicata all'individuazione puntuale delle misure di sicurezza che i vari soggetti dell'Amministrazione provinciale sono tenuti a rispettare;
- una terza Sezione (III) che, al fine di semplificare l'attività di Responsabili e Incaricati del trattamento, accorpa in un unico documento le principali regole attinenti al trattamento dei dati attraverso dispositivi di videosorveglianza
- un'ultima parte (Sezione IV) relativa alla modulistica.

Per facilitarne la reperibilità, il testo del presente documento è disponibile in Internet, sul sito dedicato alla protezione dei dati personali all'indirizzo **http://privacy.provincia.tn.it** .

# SEZIONE I: CONTESTO NORMATIVO

## 1. ATTI DELLA PROVINCIA AUTONOMA DI TRENTO

1. ***DELIBERAZIONE DELLA GIUNTA PROVINCIALE*** 30 dicembre 1999, n. 7911 (revocata e sostituita dalla presente deliberazione): “Legge 31 dicembre 1996, n. 675 (Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali). Trattamento di dati sensibili da parte della Provincia di Trento: individuazione dei dati sensibili trattabili e delle operazioni consentite per il perseguimento di rilevanti finalità di interesse pubblico, ai sensi dell’articolo 22, comma 3 bis. Istruzioni ai Responsabili del trattamento dei dati personali”.

2. ***DELIBERAZIONE DELLA GIUNTA PROVINCIALE*** **23 novembre 2001, n. 3077** (revocata e sostituita dalla presente deliberazione): “Articolo 31 della legge provinciale 30 novembre 1992, n. 23. Individuazione delle modalità di redazione, di pubblicazione di comunicazione e di rilascio degli atti contenenti dati idonei a rivelare lo stato di salute”.

3. ***DELIBERAZIONE DELLA GIUNTA PROVINCIALE*** **23 dicembre 2002, n. 3216** (revocata e sostituita dalla presente deliberazione): “Revoca della deliberazione n. 2192 di data 6 marzo 1998, recante "Prime disposizioni concernenti l'applicazione della legge 31 dicembre 1996, n. 675 e s.m., in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali", e contestuale approvazione di nuove disposizioni generali concernenti l'applicazione della legge n. 675/1996”.

4. ***DELIBERAZIONE DELLA GIUNTA PROVINCIALE*** **23 dicembre 2002, n. 3217** (revocata e sostituita dalla presente deliberazione): “Articolo 15 della legge 31 dicembre 1996, n. 675, in materia di tutela dei dati personali - Misure minime di sicurezza - Revoca della deliberazione della Giunta provinciale n. 657 di data 22 marzo 2000, in materia di misure minime di sicurezza, e adozione di un nuovo provvedimento di attuazione delle misure minime di sicurezza per il trattamento dei dati personali previste dalla legge”.

5. ***DELIBERAZIONE DELLA GIUNTA PROVINCIALE 30 DICEMBRE 2003, N. 3372*** (revocata e sostituita dalla presente deliberazione) (Revoca della deliberazione n. 34 di data 17 gennaio 2003, concernente direttive esecutive per l'applicazione della legge 31 dicembre 1996, n. 675, e approvazione delle nuove direttive esecutive per l'applicazione del decreto legislativo 30 giugno 2003, n. 196, recante "Codice in materia di protezione dei dati personali")

6. ***DELIBERAZIONE DELLA GIUNTA PROVINCIALE 9 FEBBRAIO 2007, N. 232*** (revocata e sostituita dalla presente deliberazione) rimarrà in vigore, limitatamente al periodo necessario per la sua sostituzione, la procedura prevista dall’Allegato B della deliberazione). (Documentazione formale delle procedure operative di sicurezza delle informazioni attuate dalle strutture organizzative dipendenti dalla Giunta provinciale: approvazione dei documenti “Misure di sicurezza generali”, “Procedura operativa per lo sblocco di password bloccate e per l’azzeramento (reset) di password” e “Procedura operativa per l’accesso a dati presenti su server o pc e accesso a casella di posta in assenza dell’Incaricato”)

7. *DELIBERAZIONE* ***DELLA GIUNTA PROVINCIALE 17 OTTOBRE 2008, N. 2643***(Procedure operative di sicurezza delle informazioni attuate dalle strutture organizzative dipendenti dalla Giunta provinciale: approvazione del documento “Procedura operativa per la

gestione dei dispositivi di videosorveglianza*")* ***(INTEGRATA DAL PRESENTE PROVVEDIMENTO)***

8. ***DELIBERAZIONE DELLA GIUNTA PROVINCIALE 20 NOVEMBRE 2009, N. 2752 (***Direttive in tema di Amministratori di Sistema per Informatica Trentina)

9. ***DELIBERAZIONE DELLA GIUNTA PROVINCIALE 7 MAGGIO 2010, N. 1037 (***Utilizzo della rete Internet, della posta elettronica, delle attrezzature informatiche e telefoniche – Approvazione disciplinare***)***

I testi delle deliberazioni, qualora vigenti, unitamente ad alcune note e/o circolari esplicative ed organizzative ed alla normativa in materia di privacy, sono disponibili in Internet sul sito *dedicato alla protezione dei dati personali, all'indirizzo* ***privacy.provincia.tn.it***. .

.

## 2. FINALITA' DELLA LEGGE E DEFINIZIONI.

### 2.1 Che cosa disciplina il Codice in materia di protezione dei dati personali?

La legge 31 dicembre 1996, n. 675, che ha recepito la direttiva 95/46/CE del 24 ottobre 1995 in materia di protezione dei dati personali, e tutta la normativa collegata, sono state sostituite dal Codice in materia di protezione dei dati personali, entrato in vigore il 1 gennaio 2004. Il Codice disciplina il trattamento dei dati personali, al fine di garantire che si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali (art. 2, comma 1).
Il nuovo testo in materia di protezione di dati personali tutela, in particolare, alcuni diritti della persona, che l'articolo 2 della Costituzione qualifica come inviolabili e fondamentali, quali:

- **il diritto alla riservatezza**, vale a dire il diritto che ognuno può esercitare per mantenere libera, da ingerenze esterne, la propria vita privata.
- **il diritto all'identità personale**, che è il diritto che ogni individuo può esercitare per utilizzare, in esclusiva, il proprio nome e altri elementi identificativi della propria persona.

### 2.2 Quali sono i dati personali?

**Dato personale** è qualunque informazione (e non solo quelle di carattere riservato) che consenta di individuare con certezza una persona fisica in modo diretto o indiretto, vale a dire anche quando l'identificazione sia possibile attraverso il collegamento di più informazioni, di per sé non significative se singolarmente considerate. Il D. Lgs. n. 196/2003 definisce come **dati identificativi** i dati che permettono **l'identificazione diretta** dell'interessato, e **dati identificabili** quelli che, pur non essendo direttamente associati a persone fisiche, ne permettono l'individuazione, **solo indirettamente**, attraverso qualsiasi altra informazione.
Il Codice in materia di protezione dei dati personali individua, tra i dati personali, le seguenti categorie**: dati sensibili, dati giudiziari, altri dati particolari, dati comuni.**
Questa classificazione è stabilita in funzione del diverso livello di riservatezza intrinseco che caratterizza le varie tipologie di dati, delle diverse precauzioni che la legge richiede per il loro utilizzo, per la loro custodia e per il loro trattamento e della oggettiva diversa pericolosità per l'individuo, derivante da un eventuale illecito trattamento.
Una recentissima innovazione legislativa (D.L. n. 201/2011 convertito nella legge n. 214/2011) ha sottratto, dall'ambito di applicazione del Codice, i dati relativi alle persone giuridiche; ne consegue che, attualmente, nel concetto di dati personali rientrano solo quelli relativi alle persone fisiche.

### 2.3 Cosa sono i dati sensibili?

Sono i dati personali, individuati dall'art. 4, comma 1, lettera d, del D. Lgs. n. 196/2003, 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.
La definizione di dato sensibile è tassativa: sono considerati tali solo i dati specificamente indicati nell' apposita norma, indipendentemente dal carattere di riservatezza o di particolare rilevanza che un individuo, o il senso comune, può attribuire ad altre tipologie di dati (ad esempio: codice identificativo della carta di credito, reddito, stato di separazione ecc.).
A tutela della sicurezza dei dati sensibili sono imposte misure particolarmente rigide, che sono illustrate nella Sezione II del presente documento, sia per quanto riguarda i presupposti di legittimazione del trattamento, della comunicazione e della diffusione, sia con riferimento alle misure tecniche, organizzative e logistiche da adottare per il loro trattamento e per la loro conservazione.

**2.4 Cosa sono i dati giudiziari?**

Sono i dati personali indicati dall'articolo 4, comma 1, lettera e) del D. Lgs. n. 196/2003, idonei a rivelare i provvedimenti di cui al D.P.R. n. 313/2002, art. 3, comma 1, lettere da A ad O, e da R a U (casellario giudiziale, anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti), o la qualità di imputato o indagato (artt. 60 e 61 c.p.p.).
In particolare, sono dati giudiziari:

a) i provvedimenti giudiziari penali di condanna definitivi, anche pronunciati da autorità giudiziarie straniere se riconosciuti ai sensi degli articoli 730 e seguenti del codice di procedura penale, salvo quelli concernenti contravvenzioni per le quali la legge ammette la definizione in via amministrativa, o l'oblazione limitatamente alle ipotesi di cui all'articolo 162 del codice penale, sempre che per quelli esclusi non sia stata concessa la sospensione condizionale della pena;
b) i provvedimenti giudiziari definitivi concernenti le pene, compresa la sospensione condizionale e la non menzione, le misure di sicurezza personali e patrimoniali, gli effetti penali della condanna, l'amnistia, l'indulto, la grazia, la dichiarazione di abitualità, di professionalità nel reato, di tendenza a delinquere;
c) i provvedimenti giudiziari concernenti le pene accessorie;
d) i provvedimenti giudiziari concernenti le misure alternative alla detenzione;
e) i provvedimenti giudiziari concernenti la liberazione condizionale;
f) i provvedimenti giudiziari definitivi che hanno prosciolto l'imputato o dichiarato non luogo a procedere per difetto di imputabilità, o disposto una misura di sicurezza;
g) i provvedimenti giudiziari definitivi di condanna alle sanzioni sostitutive e i provvedimenti di conversione di cui all'articolo 66, terzo comma, e all'articolo 108, terzo comma, della legge 24 novembre 1981, n. 689;
h) i provvedimenti giudiziari del pubblico ministero previsti dagli articoli 656, comma 5, 657 e 663 del codice di procedura penale;
i) i provvedimenti giudiziari di conversione delle pene pecuniarie;
l) i provvedimenti giudiziari definitivi concernenti le misure di prevenzione della sorveglianza speciale semplice o con divieto o obbligo di soggiorno;
m) i provvedimenti giudiziari concernenti la riabilitazione;
n) i provvedimenti giudiziari di riabilitazione, di cui all'articolo 15 della legge 3 agosto 1988, n. 327;
o) i provvedimenti giudiziari di riabilitazione speciale relativi ai minori, di cui all'articolo 24 della legge 27 maggio 1935, n. 835;
r) i provvedimenti giudiziari relativi all'espulsione a titolo di sanzione sostitutiva o alternativa alla detenzione, ai sensi dell'articolo 16 del decreto legislativo 25 luglio 1998, n. 286, come sostituito dall'art. 15 della legge 30 luglio 2002, n. 189;
s) i provvedimenti amministrativi di espulsione e i provvedimenti giudiziari che decidono il ricorso avverso i primi, ai sensi dell'articolo 13 del decreto legislativo 25 luglio 1998, n. 286, come modificato dall'art. 12 della legge 30 luglio 2002, n. 189;
t) i provvedimenti di correzione, a norma di legge, dei provvedimenti già iscritti;
u) qualsiasi altro provvedimento che concerne a norma di legge i provvedimenti già iscritti, come individuato con decreto del Presidente della Repubblica, ai sensi dell'articolo 17, comma 1, della legge 23 agosto 1988, n. 400, su proposta del Ministro della giustizia.

Non si considerano dati giudiziari i provvedimenti di cui alle lettere p) e q) del predetto art. 3 DPR 313/2002 (sentenze dichiarative di fallimento; decreto di chiusura del fallimento; decreto di omologazione del concordato fallimentare e delle sentenze di interdizione, inabilitazione e revoca), poiché, in queste ipotesi, prevale l’esigenza di pubblicità rispetto alla tutela della riservatezza.
Anche tali dati sono tutelati, sotto il profilo della sicurezza, con apposite misure organizzative e gestionali (Sezione II).

### 2.5 Cosa sono gli altri dati particolari?

Si tratta di un'ulteriore categoria, prevista dall'articolo 17 del Codice in materia di protezione dei dati personali, intermedia tra dati sensibili e comuni, il cui trattamento presenta rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che può determinare. Il loro trattamento è ammesso nel rispetto di misure ed accorgimenti a garanzia dell'interessato, ove prescritti dal Garante (possibili esempi potrebbero essere rappresentati dai dati che indicano la posizione geografica, di persone o cose, attraverso una rete di comunicazione elettronica; dai dati relativi al rischio di solvibilità economica; da quelli relativi alla situazione patrimoniale ecc.)).

### 2.6 Cosa sono i dati comuni?

Sono tutti i restanti dati personali, non compresi nei precedenti paragrafi 2.3 e 2.4 .

### 2.7 Cos'è una banca dati?

È qualsiasi insieme di dati personali organizzati in modo da renderne possibile o agevole la consultazione e il trattamento.
Non è da considerare tale, pertanto, la sola "raccolta" informatizzata, bensì tutte le raccolte di dati personali, a prescindere dallo strumento usato per il trattamento dei dati, comprendendo anche strumenti di archiviazione quali i supporti audiovisivi, ottici, fotografici e le "raccolte" cartacee. Ai fini dell'applicazione delle misure di sicurezza, sono rilevanti non solo le banche dati ufficiali, ma anche le semplici raccolte di dati personali finalizzate all'ordinaria gestione dell'attività amministrativa.

### 2.8 Che cos'è il trattamento di dati personali?

Costituisce trattamento di dati personali (articolo 4, comma 1, lettera a, del Codice in materia di protezione dei dati personali) qualunque operazione o complesso di operazioni, svolti con o senza l'ausilio di mezzi elettronici o comunque automatizzati, 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.
La riservatezza dei dati è sempre tutelata indipendentemente dalle modalità di gestione (manuale o con strumenti elettronici).

### 2.9 Cosa sono la comunicazione e la diffusione?

La **comunicazione** è un'operazione del trattamento che consiste nel portare i dati personali **a conoscenza di uno o più soggetti determinati** (identificabili in modo univoco e determinato), diversi dall'interessato cui i dati stessi si riferiscono, in qualunque forma, anche mediante la loro messa a disposizione per la consultazione.
Non si considera comunicazione lo scambio di dati tra strutture interne dell'Amministrazione, o tra queste ultime e soggetti esterni individuati come Responsabili o Incaricati del trattamento nell'ambito di attività di *outsourcing* o in base ad atto convenzionale (ad es.: affidamento all'esterno di compiti dell'Amministrazione). In tal caso anche i soggetti esterni che collaborano con la Provincia vengono considerati "articolazioni" della stessa.
La **diffusione** è un'operazione del trattamento che consiste nel portare dati personali **a conoscenza di soggetti indeterminati**, in qualunque forma, anche mediante la loro messa a disposizione per la consultazione.
Tipica forma di diffusione è quella che si realizza tramite registri o albi pubblici, ovvero con la pubblicazione delle deliberazioni e determinazioni ai sensi dell'art. 31 della legge provinciale 1992, n. 23.

**2.10 Quali sono i presupposti che legittimano il trattamento dei dati personali da parte della pubblica amministrazione?**

Ai sensi dell'art. 18 del D. Lgs. n. 196/2003, il trattamento di dati personali da parte dei soggetti pubblici, esclusi gli enti pubblici economici (il cui regime è equiparato a quello dei privati), è consentito soltanto:
per lo svolgimento delle funzioni istituzionali;
nei limiti dettati da leggi e regolamenti.
Pertanto, di fronte a qualsiasi trattamento, il Responsabile del trattamento stesso (Dirigente) deve verificare:
che il trattamento sia connesso con **l'esercizio delle funzioni istituzionali** (principio di **pertinenza**) e che le stesse finalità **non siano perseguibili attraverso il trattamento di dati anonimi (principio di necessità)**;
che le modalità del trattamento siano tali da determinare il minor sacrificio possibile del diritto alla riservatezza dei terzi (principio di **non eccedenza**);
che il trattamento, ed in particolare le modalità adottate, **non sia difforme dalle norme di legge e di regolamento**;
che vengano adottate le **misure di sicurezza**.
Come tutti i soggetti, anche le amministrazioni pubbliche devono applicare quanto previsto dall'articolo 3 del Codice in materia di protezione dei dati personali (principio di necessità). I sistemi informativi e i programmi informatici vanno configurati riducendo, al minimo, l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.
Anche quando l'Amministrazione persegue finalità istituzionali mediante gli strumenti del diritto privato (disciplina del rapporto di lavoro, attività contrattuale, ecc.), ai fini della normativa sulla protezione dei dati personali essa è comunque da considerarsi soggetto pubblico, avendo rilevanza l'aspetto soggettivo della stessa e non la natura dei rapporti gestiti.
Ulteriori e particolari presupposti - che sono illustrati nella Sezione II del presente documento (paragrafo 4.2 *"Disposizioni speciali per il trattamento di dati personali sensibili e giudiziari"*, paragrafo 4.5.1.2 nella sezione "*Autorizzazione al trattamento dei dati sensibili e giudiziari*", paragrafo 8.5. "*Misure di sicurezza relative ai supporti di memorizzazione"* e capitolo 9. "*Trattamento di dati su supporti non informatici"*) - sono previsti per la legittimazione al trattamento dei dati sensibili.

**2.11 Per il trattamento di dati personali da parte della pubblica amministrazione, è necessario il consenso dell'interessato?**

In presenza dei presupposti giuridici illustrati al punto precedente, la pubblica amministrazione può legittimamente trattare i dati personali, **senza acquisire il consenso** dell'interessato (art. 18, comma 4, D. Lgs. n. 196/2003).
Al contrario, **l'acquisizione del consenso dell'interessato non legittima l'Amministrazione a trattare dati per finalità diverse** da quelle istituzionali o a effettuare operazioni non consentite da leggi o regolamenti. Nei confronti della pubblica amministrazione, pertanto, il consenso non rimuove il limite dato dalla mancanza dei presupposti che legittimano il trattamento.

**2.12 Quali sono i presupposti che legittimano la comunicazione e la diffusione dei dati personali da parte dei soggetti pubblici?**

La disciplina si differenzia a seconda del soggetto destinatario.

**Comunicazione e diffusione da parte di soggetti pubblici:**

Comunicazione a soggetti pubblici

La comunicazione dei dati **da un soggetto pubblico ad altri soggetti pubblici, esclusi gli enti pubblici economici, è ammessa** (art. 19, comma 2, del D. Lgs. n. 196/2003) quando è prevista da norme di legge o di regolamento. La comunicazione è ammessa anche quando non sia prevista, espressamente, da alcuna norma; in tal caso, l'Amministrazione deve darne comunicazione preventiva al Garante. I dati possono essere comunicati al richiedente una volta che siano trascorsi 45 giorni dall'inoltro al Garante, senza che la medesima Autorità abbia adottato diversa determinazione.

Comunicazione a privati o enti pubblici economici

La comunicazione dei dati personali da parte di soggetti pubblici, a privati o a enti pubblici economici, è ammessa solo quando sia prevista da norme di legge o di regolamento (art. 19, comma 3, del Codice)

Diffusione

**La diffusione, da parte di un soggetto pubblico, è ammessa solo quando sia prevista da norme di legge o di regolamento** (art. 19, comma 3, del Codice).

## SEZIONE II: MISURE DI SICUREZZA

## 3. MISURE DI SICUREZZA IN GENERALE

### 3.1 Considerazioni generali

Le **misure di sicurezza** sono costituite dal complesso delle misure organizzative, tecniche, informatiche, logistiche e procedurali volte a **ridurre**, al minimo, i **rischi** di:
**distruzione o perdita, anche accidentale, dei dati,**
**accesso non autorizzato;**
**trattamento non consentito o non conforme alle finalità della raccolta**,
**modifica dei dati** in conseguenza di interventi non autorizzati o non conformi alla regole.

Tutti i Titolari sono tenuti ad adottare misure minime individuate dal Codice in materia di protezione dei dati personali, e secondo le modalità previste nel Disciplinare tecnico allegato al Codice stesso (c.d. Allegato B). Va sottolineato come l'articolo 31 del D. Lgs. n. 196/2003 non faccia differenza tra violazione della riservatezza dei dati personali propriamente detta - quale si avrebbe ad esempio nel caso di accesso a dati sensibili da parte di terzi non autorizzati - e distruzione o perdita accidentale di dati già legittimamente raccolti e trattati.
La mancata custodia dei dati è comunque causa di un danno, e il responsabile del pregiudizio è sanzionato. Dalla distruzione o dalla perdita dei dati, infatti, derivano varie conseguenze, tutte connotate da evidente gravità: ad esempio, il blocco delle attività (che, per inciso, rappresenta anche un disservizio), costi gestionali imprevisti, danno di immagine. Poiché il privato, inoltre, deve poter fare affidamento sui dati che ha già comunicato alla pubblica amministrazione, ne consegue che, in caso di negligente custodia, può richiedere il risarcimento del danno.
Per i motivi esposti, il soggetto che non adotta le misure minime di sicurezza (mancata conformità al Disciplinare Tecnico in tema di misure minime) è sanzionato penalmente; ma se, in aggiunta, non ha adottato misure idonee, può anche essere chiamato a rispondere, in sede civile, di risarcimento dei danni provocati.
Ai sensi dell'art. 31 del D. Lgs. n. 196/2003, le misure di sicurezza adottate per il trattamento dei dati personali devono essere:

- adeguate in relazione alle conoscenze acquisite in base al progresso tecnico e tali da ridurre, al minimo, i rischi di distruzione dei dati o di accesso non autorizzato;
- adottate in via preventiva e differenziate in base alla natura dei dati e alle specifiche caratteristiche del trattamento.

La mancata adozione delle misure di sicurezza può dar luogo a responsabilità penale e civile (per il risarcimento dei danni), secondo quanto illustrato nella tabella:

| **Mancata adozione di:** | **Conseguenze:** | |
|---|---|---|
| | Resp. Penale | Resp.Civile |
| misure di sicurezza minime | Sì | Sì |
| misure di sicurezza idonee | No | Sì |

In altre parole, esistono due diversi livelli di responsabilità.
L'Amministrazione deve individuare, preventivamente, misure di sicurezza che devono rispettare almeno i parametri di sicurezza minimi definiti nel Codice in materia di protezione dei dati personali (articoli 33, 34, 35 e 36); se le misure di sicurezza adottate non rispettano i parametri minimi contenuti nel regolamento, scatta la **responsabilità penale**.
Ma l'individuazione di misure che rispettano i parametri minimi, non è sufficiente a liberare, da ogni responsabilità, il soggetto che effettua il trattamento. Se le misure adottate *non sono idonee ad*

*evitare il danno*, può essere comunque accertata la **responsabilità civile** di coloro che hanno effettuato il trattamento.

Le conseguenze della **mancata adozione di misure minime di sicurezza** possono quindi essere le seguenti**:**

**sanzione penale** arresto sino a due anni o sanzione amministrativa pari ad un quarto del massimo previsto (E 30.000,00)) (articolo 169 del Codice in materia di protezione dei dati personali)

**sanzione amministrativa** (da 10.000,00 a 120.000,00 Euro) (art. 162, comma 2-bis, del Codice in materia di protezione dei dati personali)

**risarcimento del danno** - nel caso le misure adottate non siano idonee ad evitare il danno - è previsto dall'art. 15 legge del Codice in materia di protezione dei dati personali, che rinvia all'art. 2050 (relativa allo svolgimento di attività pericolose). In questo tipo di responsabilità è prevista una presunzione speciale di colpa a carico del responsabile del danno (in questo caso chi effettua il trattamento): il responsabile ha l'onere della prova di aver adottato *tutte quanto era possibile per evitare il danno*, mentre il danneggiato deve solo dimostrare l'esistenza del danno.

Le conseguenze della **mancata o inadeguata adozione di misure di sicurezza idonee** possono quindi essere le seguenti**:**

**risarcimento del danno** - nel caso le misure adottate non siano idonee ad evitare il danno - è previsto dall'art. 15 legge del Codice in materia di protezione dei dati personali, che rinvia all'art. 2050 (relativa allo svolgimento di attività pericolose). In questo tipo di responsabilità è prevista una presunzione speciale di colpa a carico del responsabile del danno (in questo caso chi effettua il trattamento): il responsabile ha l'onere della prova di aver adottato *tutte quanto era possibile per evitare il danno*, mentre il danneggiato deve solo dimostrare l'esistenza del danno.

E' superfluo ricordare che la mancata applicazione delle misure di sicurezza determinate dal Titolare del trattamento (Giunta provinciale con riferimento alle misure generali) e delle ulteriori indicazioni impartite dal Responsabile/Dirigente e dal Dirigente del servizio competente in materia di informatica, per quanto riguarda le ulteriori istruzioni operative integrative, può dare adito a **responsabilità disciplinare**.

Poiché il parametro previsto dalla legge, per l'accertamento dell'eventuale responsabilità civile, è quello dell'**idoneità** delle misure ad evitare il danno, le misure di sicurezza elencate nel presente documento non rappresentano una limitazione alla adozione, da parte dei Responsabili del trattamento, di ulteriori misure idonee a garantire livelli di protezione maggiori, e più adeguati, alle singole situazioni.

Infine, va ricordato che le regole concernenti le misure di sicurezza servono anche ad indirizzare il personale al corretto utilizzo delle dotazioni informatiche dell'Amministrazione, anche ai fini della salvaguardia del patrimonio tecnologico della stessa. Infatti, tra le finalità implicite della legge sulla tutela dei dati personali, vi è anche il perseguimento di un processo di crescita culturale del personale dell'amministrazione pubblica.

**3.2 Prescrizioni operative in tema di misure di sicurezza**

Tutti i dipendenti, e in particolare gli Incaricati del trattamento, devono garantire la sicurezza delle informazioni attraverso la salvaguardia della loro a) riservatezza, b) integrità e c) disponibilità e devono attenersi alle "**Prescrizioni in tema di Misure di Sicurezza**", specificate nel paragrafo 14 del presente Allegato B.

In particolare, gli Incaricati devono:

a) assicurare che le informazioni siano accessibili solo a coloro che sono autorizzati a trattarle;
b) salvaguardare l'accuratezza e completezza delle informazioni e del loro trattamento;
c) assicurare che gli utenti autorizzati abbiano accesso alle informazioni, e ai beni ad esse associati, nel momento in cui lo richiedono.

I sistemi e le reti d'informazione sono sottoposti a rischi interni ed esterni, ed è quindi necessario che tutti sappiano e siano consapevoli che, a causa dell'interconnettività e dell'interdipendenza tra sistemi, falle in materia di sicurezza, su un componente del sistema, possono propagare i loro effetti fino ad incidere, gravemente, sull'integrità dei sistemi, delle reti, delle banche dati, degli archivi e arrecare danni ad altri.

Le misure di sicurezza informatica devono tener conto della natura dei dati, delle specifiche caratteristiche del trattamento e delle conoscenze acquisite in base al progresso tecnico. Ai trattamenti devono essere applicate le misure minime di sicurezza, indicate dagli artt. 33-35 del Codice in materia di protezione dei dati personali, e dettagliate nel Disciplinare tecnico (Allegato B).

In sintesi, le misure minime che garantiscono i principi della sicurezza informatica sono:

- utilizzo di un Sistema di autenticazione informatica (User-ID e password) e di un sistema di autorizzazione (profili "utente" con potere di accesso);
- adozione di procedure per la custodia di copie di backup;
- installazione e aggiornamento di software (firewall) per prevenire vulnerabilità rispetto ad attacchi esterni;
- installazione di software antivirus e loro aggiornamento, almeno ogni tre mesi, per il trattamento di dati sensibili, e ogni sei mesi per gli altri dati;
- adozione di tecniche di cifratura o codici identificativi per dati sensibili, trattati con strumenti elettronici.

# 4. MISURE ORGANIZZATIVE COMUNI A TUTTI I TIPI DI TRATTAMENTO

## 4.1 Disposizioni generali per il trattamento dei dati personali

Ogni trattamento di dati personali è consentito alla Provincia, in quanto soggetto pubblico, qualora sussistano i presupposti previsti dall'articolo 18 del Codice in materia di protezione dei dati personali. Esso deve svolgersi nel rispetto delle seguenti indicazioni:

- va privilegiato, ove possibile, il trattamento di dati anonimi;
- se non è possibile perseguire le finalità istituzionali, mediante il trattamento di dati anonimi, va comunque garantita l'osservanza dei principi di necessità, pertinenza e non eccedenza rispetto alle finalità del trattamento medesimo, ai sensi degli artt. 3 e 11 del Codice in materia di protezione dei dati personali (stretta coerenza con la natura dei compiti da svolgere, minimo utilizzo dei dati personali, adozione di modalità di trattamento meno lesive possibile);
- i soggetti pubblici, per il trattamento dei dati, non devono chiedere il consenso dell'interessato, salvo quanto previsto (nella Parte II del D. Lgs. n. 196/2003) per gli esercenti le professioni sanitarie e gli organismi sanitari pubblici.

I dati personali, inoltre, devono essere:

- trattati in modo lecito e secondo correttezza;
- raccolti e registrati per scopi determinati, espliciti e legittimi ed in funzione dello svolgimento di compiti istituzionali, nei limiti stabiliti dalle leggi e dai regolamenti;
- esatti e, se necessario, aggiornati;
- trattati dagli Incaricati del trattamento, nominati dal Responsabile del trattamento, o eventualmente trattati dallo stesso Responsabile;
- trattati per il tempo strettamente necessario per lo svolgimento dei compiti istituzionali: per tale motivo, i documenti ed i supporti sui quali sono registrati, devono essere archiviati in luogo custodito, non appena concluso il trattamento;
- conservati in una forma che permetta l'identificazione dell'interessato solo per il tempo necessario agli scopi per i quali sono raccolti.

Ai fini della sicurezza dei dati personali:

- le riproduzioni di documenti equivalgono ai documenti stessi e, pertanto, vanno gestiti con le medesime cautele;
- qualunque prodotto dell'elaborazione di dati personali, ancorchè non costituente documento definitivo (appunti, stampe interrotte, stampe di prova, elaborazioni temporanee ecc.), va trattato con le stesse cautele che sarebbero riservate alla versione definitiva (v. misure relative ai trattamenti cartacei e informatizzati).

Le misure individuate nel presente documento **si applicano anche ai collaboratori esterni dell'Amministrazione provinciale** che, nell'ambito dei compiti loro affidati dalla Provincia, devono procedere al trattamento di dati personali in qualità di Responsabili o Incaricati del trattamento, come formalmente designati dall'Amministrazione provinciale e che utilizzino, per lo svolgimento dei propri compiti, dotazioni informatiche e non informatiche provinciali.
Per quanto attiene alle misure organizzative da applicare, in adempimento della legge ed in conformità agli orientamenti espressi dal Garante, in caso di affidamento a soggetti terzi di compiti e funzioni dell'Amministrazione provinciale (sulla base di concessioni, appalti e convenzioni), si rinvia a quanto specificato nel **paragrafo 4.5.1** ("I ruoli nel sistema della protezione dei dati personali").

**4.1.1 Diffusione di dati personali tramite pubblicazione sul B.U.R. e sul sito istituzionale della Provincia**

La pubblicazione sul B.U,R., **e sul sito istituzionale della Provincia**, di atti contenenti dati comuni, concretizza un'ipotesi di diffusione degli stessi. Tale pubblicazione è in linea con quanto disposto dall'art. 19 del Codice in materia di protezione dei dati personali, essendo espressamente prevista dalla legge provinciale n. 23 del 30 novembre 1992 (art. 31, comma 1) e dalla legge provinciale n. 16 del 27 luglio 2012 (art. 9, comma 1).

Nell'applicare le disposizioni che stabiliscono le forme e le modalità di pubblicazione, la struttura redigente deve, comunque, effettuare una verifica sulla pertinenza e sulla non eccedenza dei dati personali da inserire nell'atto, anche quando di tale atto è prevista la pubblicazione integrale (v. Provvedimento Garante "**Linee guida in materia di trattamento di dati personali contenuti anche in atti e documenti amministrativi, effettuato da soggetti pubblici per finalità di pubblicazione e diffusione sul web" – n. 88 del 2 marzo 2011**), e deve aver cura di evitare la diffusione di dati personali non necessari alla finalità di trasparenza dell'azione amministrativa, sottesa alla pubblicazione (Possibili soluzioni, che non ne escludono ulteriori, sono quelle consistenti nell'inserimento dei dati personali non strettamente pertinenti al provvedimento, ma necessari per adempimenti successivi (quali, ad es., codice fiscale, coordinate bancarie, conto corrente postale del beneficiario e simili), in un documento allegato (che non viene pubblicato) (1), oppure nella predisposizione, ai fini della pubblicazione dell'atto, di un testo nel quale tali dati siano omessi) (2) **(v. Corte di giustizia comunitaria 9/11/2010, Cause riunite C-92/09 e C-93/09; Cassazione Civile, Sezione I, nn. 2034 e 12726 del 2012**).

Non sono pubblicabili, in forma integrale, ma possono costituire oggetto di "pubblicazione per estremi, "gli atti "riservati" e cioè quelli contenenti informazioni che, pur costituendo dati personali ai sensi del Codice in materia di protezione dei dati personali, sono comprese nelle fattispecie indicate negli articoli 31, comma 2, 32, comma 4, e 32 –bis, commi 1 e 2, della legge provinciale n. 23 del 30 novembre 1992 nonché nell'articolo 24, comma 6, della legge n,. 241/1990.

**Diritto all'oblio**

La Direttiva 95/46/CE, ha disciplinato la "tutela delle persone fisiche, con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati"; l'articolo 6, paragrafo 1, lettera e) della fonte comunitaria (integralmente recepito nell'articolo 11 del D.Lgs. n. 196/2003) ha stabilito che i dati devono essere "…conservati in modo da consentire l'identificazione delle persone interessate per un arco di tempo non superiore a quello necessario al conseguimento delle finalità per le quali sono rilevati o sono successivamente trattati".

Il Garante per la protezione dei dati personali, con il già richiamato provvedimento n. 88/2011 ("Linee guida in materia di trattamento di dati personali contenuti anche in atti e documenti amministrativi, effettuato da soggetti pubblici per finalità di pubblicazione e diffusione su web") ha definito alcune regole per garantire il diritto all'oblio degli interessati (**v. anche Cassazione Civile, Sezione III, n. 5525/2012**), nei casi in cui la norma non preveda un termine che delimiti gli effetti della pubblicazione.

A tal proposito, ha evidenziato la necessità di prevedere meccanismi (e/o procedure) che impediscano la indiscriminata permanenza, dei vari atti (e, di conseguenza, delle informazioni e dei dati in essi contenuti), sui siti istituzionali dei soggetti pubblici.

Il Garante, nel provvedimento citato, ha individuato alcune modalità di trattamento ritenute idonee a limitare l'ingiustificata esposizione pubblica dei dati:

- privilegiare motori di ricerca interni al sito istituzionale dell'Amministrazione, in modo da garantire una selezione degli accessi;

- stabilire i tempi di permanenza degli atti sul sito. Tale durata, nei casi in cui non sia già prevista dalla legge, potrebbe essere garantita 1) dalla rimozione, dal sito web, dopo il decorso stabilito; 2) dalla permanenza dei documenti, nel sito web, ma oscurando gli elementi di identificazione dell'interessato; 3) dall'inserimento dei documenti in aree riservate ad accesso selezionato;

- utilizzare firewall, o filtri di rete, per evitare duplicazioni massive di files, e, dunque, di dati e anomale riproduzioni;

- adottare misure per ridurre, o eliminare, il rischio di cancellazioni, modifiche, alterazioni o decontestualizzazioni, al fine di garantire che i dati diffusi siano, in ogni caso, esatti ed aggiornati.

**I Dirigenti/Responsabili del trattamento sono tenuti, coordinandosi con le Strutture provinciali competenti in materia di informatica, semplificazione e privacy, a promuovere, valutare e proporre le soluzioni ritenute più idonee, con particolare riguardo ai tempi di pubblicazione dei dati, in modo tale che la Giunta provinciale, qualora lo ritenga opportuno, possa adottare un Regolamento.**

### 4.1.2 Trattamenti di dati personali per scopi storici, statistici e di ricerca scientifica

Sono di rilevante interesse pubblico le finalità riguardanti i trattamenti di dati personali per scopi storici o effettuati nell'ambito del Sistema statistico nazionale (Sistan) o per scopi scientifici (art. 98 Codice). Con riferimento ai criteri generali per il trattamento dei dati personali, l'art. 99 del Codice precisa che il trattamento di dati personali per scopi storici, di ricerca scientifica o di statistica è compatibile con gli scopi per i quali i dati sono raccolti, o successivamente trattati, e può essere effettuato anche oltre il periodo necessario a questi ultimi scopi. Questa possibilità deve essere espressamente indicata nell'informativa fornita all'interessato al momento della raccolta dei dati.

Anche in caso di cessazione del trattamento originario, i dati in oggetto possono essere conservati, o ceduti ad altro Titolare, per scopi storici, di ricerca scientifica e di statistica, in conformità alla legge, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e di buona condotta sottoscritti ai sensi dell'art. 12 del Codice.

#### 4.1.2.1 Trattamento di dati personali per scopi storici

È considerato un trattamento di "rilevante interesse pubblico" quello effettuato da soggetti pubblici per scopi storici, concernente "finalità di studio, indagine, ricerca e documentazione di figure, fatti e circostanze del passato" (art. 101 Codice). I dati personali, raccolti a tal fine, non possono essere usati per adottare provvedimenti contro l'interessato, né per fini diversi. I dati contenuti in documenti storici possono essere utilizzati solo a fini storici e diffusi quando si riferiscono a circostanze o a fatti resi noti direttamente dall'interessato o attraverso suoi comportamenti in pubblico.

La consultazione dei documenti conservati negli Archivi è soggetta alle disposizioni di cui al decreto legislativo 29 ottobre 1999, n. 490. In base a questa norma esistono limiti alla consultabilità dei documenti riservati. Sono quindi esclusi, dalla consultazione, per 50 anni, in relazione alla data del documento, i documenti "relativi alla politica estera o interna dello Stato" e, per 70 anni, quelli "relativi a situazioni puramente private di persone". Un limite di 70 anni alla consultabilità è posto anche per "i documenti dei processi penali", in relazione alla data della conclusione del procedimento.

#### 4.1.2.2 Trattamento di dati raccolti per scopi statistici e di ricerca scientifica

Gli scopi statistici e di ricerca scientifica devono essere chiaramente determinati e resi noti, all'interessato, nell'informativa di cui all'art. 13 del Codice. I dati personali trattati per scopi statistici e di ricerca scientifica non possono essere utilizzati per prendere decisioni o provvedimenti

relativamente all'interessato, né per trattamenti finalizzati a scopi di altra natura. I dati personali trattati per scopi statistici sono conservati separatamente da ogni altro dato personale trattato per finalità che non richiedano il loro utilizzo. I dati identificativi, qualora possano essere conservati, sono abbinabili ad altri dati, sempre che l'abbinamento sia temporaneo ed essenziale per i propri trattamenti statistici. Le disposizioni, relative al segreto statistico e alla riservatezza dei dati personali, non si applicano ai dati provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque.

**4.1.2.2.1 Codici di deontologia e di buona condotta**

In attuazione della normativa sono stati approvati dal Garante:

- Provvedimento 31 luglio 2002 n. 13 "Codice di deontologia e di buona condotta per i trattamenti di dati personali a scopi statistici e di ricerca scientifica effettuati nell'ambito del Sistema statistico nazionale"
- Provvedimento 16 giugno 2004 n. 2 "Codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici e scientifici" .

Tali codici hanno lo scopo di assicurare l'equilibrio tra diritto alla privacy, necessità della ricerca scientifica e ragioni che ne sono alla base: il principio della libertà della ricerca, costituzionalmente garantito, e le esigenze del relativo sviluppo per migliorare le condizioni della società. Inoltre, i codici completano il quadro delle regole del D.Lgs. 196/03 secondo i principi di necessità e non eccedenza, in base ai quali devono essere utilizzati i dati anonimi quando siano sufficienti per gli scopi di una ricerca.

Nei due Codici deontologici sono individuati fra l'altro:

- i presupposti e i procedimenti per documentare e verificare che i trattamenti, fuori dai casi previsti dal decreto legislativo 322/89, siano svolti per idonei ed effettivi scopi statistici e di ricerca scientifica;
- le regole di correttezza da osservare nella raccolta dei dati e le istruzioni che i Responsabili del trattamento devono da impartire al personale incaricato;
- le misure di sicurezza da adottare per favorire il rispetto dei principi di pertinenza e non eccedenza dei dati e delle misure di sicurezza di cui all'art. 33 del Codice.

**4.1.2.2.2 Trattamento di dati personali per fini statistici nell'ambito del programma statistico provinciale e nazionale.**

I soggetti che fanno parte del Sistema Statistico Nazionale (SISTAN) possono raccogliere, ed ulteriormente trattare, i dati personali necessari per perseguire gli scopi statistici previsti dal decreto legislativo 322/89, dalla legge o dalla normativa comunitaria, qualora il trattamento di dati anonimi non permetta di raggiungere i medesimi scopi.

La fattispecie di cui sopra si concretizza, relativamente alla Provincia di Trento, nei trattamenti effettuati per fini statistici, dalla Struttura competente in materia di statistica, nonché dalle altre strutture provinciali limitatamente alle attività previste dal Programma Statistico Nazionale.

I dati personali raccolti per uno specifico scopo statistico (così come quelli raccolti per altri scopi) possono essere trattati, dai soggetti sopra indicati, per altri scopi statistici di interesse pubblico, se ciò è previsto dal D.Lgs.322/89, dalla legge, dalla normativa comunitaria o da un regolamento. Gli ulteriori scopi statistici devono essere chiaramente determinati e di limitata durata.

**4.1.2.2.3 Trattamento di dati personali per fini statistici e di ricerca**

L'attività statistica e di ricerca, al di fuori del SISTAN, è disciplinata, oltre che dal Codice, dal citato "Codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici e scientifici", che si applica a un'università o altro ente di ricerca o società scientifica, o singolo ricercatore che operi in un'università o ente di ricerca o socio di una società scientifica.

Per quanto riguarda l’ambito provinciale, il Codice deontologico si applica agli enti provinciali di ricerca. La Provincia autonoma di Trento svolge, inoltre, attività di ricerca applicata (vedi la scheda relativa ai Trattamenti per scopi scientifici, diversi da quelli medici, biomedici ed epidemiologici del Regolamento dati sensibili e giudiziari della Provincia, adottato dalla Provincia).

Il codice deontologico non si applica ai trattamenti per scopi statistici e scientifici connessi con attività di tutela della salute svolte da esercenti professioni sanitarie od organismi sanitari.

**4.2 Disposizioni speciali per il trattamento dei dati personali sensibili e giudiziari**

Il trattamento dei dati sensibili e giudiziari, da parte della pubblica amministrazione, è soggetto ad una disciplina speciale, individuata, in particolare, dagli articoli 20, 21 e 22 del Codice in materia di protezione dei dati personali.

**Il trattamento dei dati sensibili e giudiziari:**

**è consentito solo se autorizzato da un'espressa disposizione di legge**, nella quale siano specificati i dati che possono essere trattati, le operazioni eseguibili e le rilevanti finalità di interesse pubblico perseguite (art. 20, comma 1, D. Lgs. n. 196/2003);

se il trattamento non è previsto da un'espressa disposizione di legge, i soggetti pubblici **possono richiedere, al Garante, l'individuazione delle attività,** tra quelle demandate dalla legge ai medesimi soggetti, che perseguono finalità di rilevante interesse pubblico e per le quali è conseguentemente autorizzato il trattamento dei dati sensibili; il trattamento è consentito solo se il soggetto pubblico provvede, altresì, a identificare e rendere pubblici i tipi di dati e di operazioni con atto di natura regolamentare, adottato in conformità al parere espresso dal Garante (art. 20, comma 3, D. Lgs. n. 196/2003);

nei casi in cui la legge specifichi la finalità di rilevante interesse pubblico, ma non i tipi di dati e le operazioni eseguibili, **il trattamento è consentito solo** in riferimento ai tipi di dati e di operazioni identificati e resi pubblici a cura dei soggetti che ne effettuano il trattamento, in relazione alle specifiche finalità perseguite nei singoli casi e nel rispetto dei principi di cui all'articolo 22 del Codice, **con atto di natura regolamentare** adottato in conformità al parere espresso dal Garante (art. 20, comma 2, D. Lgs. n. 196/2003).

L'articolo **22** del D. Lgs. n. 196/2003 individua i principi applicabili al trattamento dei dati sensibili e giudiziari:

- la pubblica amministrazione è autorizzata a trattare, esclusivamente, **i dati sensibili e giudiziari indispensabili** per lo svolgimento di quelle attività istituzionali che non possono essere adempiute mediante il trattamento di dati anonimi o di dati personali non sensibili. Essa può svolgere **le sole operazioni di trattamento indispensabili** al perseguimento delle finalità per le quali il trattamento è consentito (principi di pertinenza e non eccedenza) (art. 22, commi 3 e 9, D. Lgs. n. 196/2003);
- nell'**informativa** di cui all'art. 13 del Codice in materia di protezione dei dati personali, l'Amministrazione è tenuta ad informare, espressamente, l'interessato cui i dati sensibili e giudiziari si riferiscono, in merito alle disposizioni legislative in relazione alle quali deve essere eseguito il trattamento e le finalità per le quali i dati sono raccolti (art. 22, comma 2, D. Lgs. n. 196/2003);
- i dati sensibili e giudiziari possono essere **comunicati o diffusi** limitatamente a quanto previsto da disposizioni di **legge** o dai provvedimenti assunti ai sensi dell'articolo 20, con atto di natura regolamentare mirante a identificare e rendere pubblici i tipi di dati e di operazioni consentite;
- i dati sensibili relativi alla salute **non possono essere oggetto di diffusione** (art. 22, comma 8, D. Lgs. n. 196/2003);
- i dati relativi allo stato di salute ed alla vita sessuale sono soggetti **all'obbligo di custodia separata,** rispetto agli altri dati trattati per finalità che non richiedono il loro utilizzo (art. 22, comma 7, D. Lgs. n.196/2003);

- per il trattamento dei dati sensibili e giudiziari sono previste misure di sicurezza particolarmente rigide.

### 4.2.1 Cifratura o separazione dei dati sensibili e giudiziari

I dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di mezzi elettronici o comunque automatizzati, nonché i dati idonei a rivelare lo stato di salute e la vita sessuale, indipendentemente dalle modalità di trattamento, devono essere trattati con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altri sistemi che, considerato il numero e la natura dei dati trattati, permettono di identificare gli interessati solo in caso di necessità (art. 22, commi 6 e 7, Codice in materia di protezione dei dati personali).
I dati sensibili e giudiziari non possono essere trattati nell'ambito di test psico-attitudinali volti a definire il profilo o la personalità dell'interessato. Le operazioni di raffronto fra dati sensibili e/o dati giudiziari possono essere effettuate solo con l'indicazione scritta dei motivi. Quando si utilizzano banche dati di diversi titolari, l' interconnessione o raffronto sono ammessi, in relazione ai citati test, solo se previsti da espressa disposizione di legge (art. 22, commi 10 e 11, Codice in materia di protezione dei dati personali).

### 4.2.2 Diffusione dei dati sensibili e dei dati giudiziari sul B.U.R. e sul sito istituzionale della Provincia

**La diffusione dei dati sensibili e giudiziari è ammessa solo se prevista da espressa e specifica disposizione di legge** (art. 22, comma 11, Codice in materia di protezione dei dati personali); nell'ipotesi in cui il contesto normativo autorizzi la diffusione di tali dati, è, in ogni caso, necessario conformarsi alle prescrizioni contenute nel paragrafo **4.1.1.** .

**Diffusione dei dati relativi allo stato di salute**
**La diffusione dei dati idonei a rivelare lo stato di salute è sempre vietata**; pertanto gli atti amministrativi provinciali che contengono tali dati devono essere pubblicati per estremi (art. 22, comma 8, Codice in materia di protezione dei dati personali).

## 4.3 Adempimenti

### 4.3.1 Informativa

L'informativa deve essere comunicata, all'interessato cui i dati si riferiscono, secondo le modalità indicate all'art. 13 del Codice. E' atto che deve essere emanato prima dell'inizio del trattamento (art. 13, comma 1, D. Lgs. n. 196/03), ferme restando le eventuali deroghe previste dal Codice stesso (art. 13, commi 4 e 5).

L'**informativa** deve essere completa e contenere, sia pure in modo sintetico, tutte le notizie previste dal Codice:
- le finalità del trattamento;
- le modalità del trattamento (strumenti elettronici o manuali, modalità di organizzazione o di raffronto ed elaborazione particolari, creazione di profili per età, professione o altro);
- se il conferimento dei dati richiesti è obbligatorio o facoltativo relativamente agli scopi dichiarati;
- le conseguenze di un eventuale rifiuto a fornire i dati;
- se i dati possono essere ceduti a terzi, in tal caso identificandoli o quanto meno individuando le categorie dei soggetti destinatari;

- i soggetti, o le 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;
- i diritti di cui all'articolo 7 del Codice;
- i dati identificativi del Titolare del trattamento;
- i dati identificativi del Responsabile del trattamento.

Nel caso di trattamento di dati sensibili, l'informativa deve, inoltre, fare espresso riferimento alla normativa che prevede gli obblighi o i compiti in base ai quali è effettuato il trattamento.
Ai sensi dell'art. 48 del D.P.R. 28 dicembre 2000, n. 445 (Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa), è obbligatorio inserire l'informativa nella modulistica per la presentazione delle dichiarazioni sostitutive di certificazione e di atto notorio.
E' opportuno comunque inserire l'informativa, in via generale, nella modulistica relativa alle istanze da presentare all'Amministrazione provinciale.
Se i dati personali non sono raccolti presso l'interessato, l'informativa è data, al medesimo, all'atto della registrazione dei dati o, in ogni caso, non oltre la prima comunicazione ad altri soggetti, se prevista (art. 13, comma 4 del Codice), eccetto che nei seguenti casi:

1. quando sono trattati in base ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria;
2. quando sono trattati per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trattati solo per tale finalità e per il periodo necessario al loro perseguimento;
3. quando l'informativa comporta un impiego di mezzi che il Garante ha dichiarato sproporzionato rispetto al diritto tutelato.

### 4.3.2 Notifica dei trattamenti

Mentre per la normativa precedente la notificazione, salvo le eccezioni previste, era sempre obbligatoria, secondo il nuovo Codice in materia di protezione dei dati personali il Titolare deve notificare, al Garante, il trattamento di dati personali cui intende procedere, solo se il trattamento riguarda (art. 37, comma 1, del Codice):

a) dati genetici, biometrici o dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica;
b) dati idonei a rivelare lo stato di salute e la vita sessuale, trattati a fini di procreazione assistita, prestazione di servizi sanitari per via telematica relativi a banche di dati o alla fornitura di beni, indagini epidemiologiche, rilevazione di malattie mentali, infettive e diffusive, sieropositività, trapianto di organi e tessuti e monitoraggio della spesa sanitaria;
c) dati idonei a rivelare la vita sessuale o la sfera psichica trattati da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale;
d) dati trattati con l'ausilio di strumenti elettronici volti a definire il profilo o la personalità dell'interessato, o ad analizzare abitudini o scelte di consumo, ovvero a monitorare l'utilizzo di servizi di comunicazione elettronica, con esclusione dei trattamenti tecnicamente indispensabili per fornire i servizi medesimi agli utenti;
e) dati sensibili registrati in banche di dati a fini di selezione del personale per conto terzi, nonché dati sensibili utilizzati per sondaggi di opinione, ricerche di mercato e altre ricerche campionarie;
f) dati registrati in apposite banche di dati gestite con strumenti elettronici e relative al rischio sulla solvibilità economica, alla situazione patrimoniale, al corretto adempimento di obbligazioni, a comportamenti illeciti o fraudolenti.

Poiché l'organizzazione della Provincia è particolarmente complessa, i Responsabili dei trattamenti (Dirigenti delle strutture) devono verificare se i trattamenti, che si svolgono sotto la loro responsabilità, appartengono ad una delle categorie soggette a notifica, predisporre l'atto di notifica, e, dopo l'istruttoria del Dirigente competente in materia di privacy, trasmetterlo al Garante.

### 4.3.3 Comunicazione al Garante

Secondo quanto previsto dall'articolo 39, comma 1, lett. a) del Codice, quando il Titolare, Provincia autonoma di Trento – Giunta provinciale, per lo svolgimento di funzioni istituzionali, deve trasmettere, ad altro soggetto pubblico, dei dati personali, ma ciò non sia previsto da norma di legge o di regolamento, occorre effettuare una comunicazione al Garante.
Come nel caso della notificazione, la struttura provinciale competente invia la "comunicazione al Garante", a seguito dell'istruttoria espletata dalla Struttura competente in materia di privacy, e solo dopo il decorso di 45 giorni, senza aver ricevuto diversa determinazione da parte del Garante medesimo, può dar luogo alla trasmissione dei dati richiesti al soggetto pubblico.
Occorre tenere presente che il Garante può opporsi, anche successivamente, interrompendo anche un flusso di dati eventualmente in corso.

## 4.4 Rapporti tra normativa privacy e diritto d'accesso

### 4.4.1 Accesso agli atti amministrativi

La legge provinciale 30 novembre 1992, n. 23 "**Principi per la democratizzazione, la semplificazione e la partecipazione all'azione amministrativa provinciale e norme in materia di procedimento amministrativo**", in attuazione dello Statuto e del principio di massima trasparenza e pubblicità dell'azione amministrativa, detta, al Capo VI, specifiche disposizioni in merito all'accesso agli atti amministrativi dell'Amministrazione provinciale, raccordandosi sia con la legge n. 241/1990 che con il D. Lgs. n. 196/2003.

Il diritto di accesso previsto dalla L.P. n. 23/92 (e dalla L. n. 241/90):

• assicura la trasparenza dell'attività amministrativa
• riguarda il documento amministrativo
• prevale, nel caso in cui sia strumentale alla cura o tutela di interessi giuridici.

Il diritto alla riservatezza previsto dal Codice in materia di protezione dei dati personali (D.Lgs. n. 196/2003):

• garantisce il rispetto dei diritti, delle libertà fondamentali e della dignità dell'individuo
• riguarda il dato personale
• recede, nel caso in cui si debba garantire l'accesso per la cura o tutela di di interessi giuridici.

Entrambi i diritti (accesso/riservatezza) sono costituzionalmente garantiti e solo apparentemente in antitesi, poichè la normativa in materia di protezione dei dati personali si pone come fattore delimitativo, sotto il profilo delle modalità tecniche di esercizio, ma non preclusivo dell'esercizio dell'accesso.
L'articolo 59 del Codice stabilisce che i presupposti, le modalità e i limiti del diritto di accesso restano disciplinati dalla Legge n. 241/90, e che le relative norme si considerano di rilevante interesse pubblico. Viene, pertanto, affermato che l'accesso è la regola dell'azione amministrativa e la tutela della riservatezza è l'eccezione, in linea, tra l'altro, con la consolidata e prevalente giurisprudenza civile ed amministrativa.

La disciplina da applicare in concreto, con riferimento ai singoli casi, si distingue in base al tipo di dati personali contenuti nel documento oggetto della richiesta di accesso:

- documento contenente **dati comuni**: si applicano gli artt. 32 e 32–bis della legge provinciale n. 23/92 nonché gli artt. 22 (principi per l'accesso) e 24 (esclusione dell'accesso) della L. 241/90 in virtù dei quali deve comunque essere garantito l'accesso ai documenti la cui conoscenza sia necessaria per curare o difendere i propri interessi giuridici;

- documento contenente **dati sensibili e giudiziari**: si applica l'art. 32-bis, comma 2, della legge provinciale n. 23/92 (e l'art. 24, comma 7, della L. n. 241/90) in base al quale l'accesso è consentito nei limiti in cui sia strettamente indispensabile per curare o difendere i propri interessi giuridici. La richiesta di accesso deve contenere la motivazione della indispensabilità;

- documento contenente "**dati supersensibili**" (relativi allo stato di salute e alla vita sessuale): si applica l'art. 60 del D. Lgs. n. 196/2003 (e l'art. 32-bis, comma 2, della legge provinciale n. 23/92) in base al quale "il trattamento è consentito se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso è di rango almeno pari ai diritti dell'interessato, ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile". La norma pone, dunque, in capo alla PA l'onere di un doppio giudizio discrezionale relativo sia all'indispensabilità dell'accesso che alla comparazione degli interessi da tutelare. In tale specifica valutazione, l'Amministrazione è aiutata dalla casistica redatta dal Garante (es. Dati sanitari - Provvedimento generale sui diritti di pari rango del 09.07.2003)

.

Il Garante ha stabilito che, nel valutare il "rango" del diritto di un terzo, si deve utilizzare come parametro di raffronto non il "diritto di azione e difesa", che pure è costituzionalmente garantito, quanto il diritto sottostante che il terzo intende tutelare in giudizio sulla base del documento che chiede di conoscere.

#### 4.4.1.1 Diritto di accesso dei consiglieri provinciali

I Consiglieri provinciali hanno diritto di ottenere tutte le notizie e le informazioni (articolo 147 Deliberazione del Consiglio provinciale n. 3/1991), in possesso degli uffici, che siano utili all'espletamento del proprio mandato.

La concreta individuazione, da parte degli uffici, delle notizie e delle informazioni che possono essere comunicate, deve quindi tenere conto di tutto ciò che può essere funzionale allo svolgimento del mandato stesso, e quindi consentire ai Consiglieri di valutare con piena cognizione di causa l'operato dell'Amministrazione, di esprimere un voto consapevole sulle questioni sottoposte all'organo consiliare e di promuovere le iniziative di competenza. In ogni caso, i dati acquisiti dai Consiglieri devono essere utilizzati per le sole finalità realmente pertinenti il mandato.

## 4.5 Disposizioni organizzative

### 4.5.1 I ruoli nel sistema della protezione dei dati personali

Nell'ambito della pubblica amministrazione, l'applicazione delle norme del Codice in materia di protezione dei dati personali comporta l'attribuzione di compiti e responsabilità in capo alle seguenti figure:
- Titolare del trattamento (art. 4, comma 1, lett. f, e art. 28 del Codice);
- Responsabile del trattamento (art. 4, comma 1, lett. g, e art. 29 del Codice);
- Incaricato del trattamento (art. 4, comma 1, lett. h, e art. 30 del Codice);

#### 4.5.1.1 Titolare

> Il **Titolare,** secondo la definizione del Codice in materia di protezione dei dati personali, è il soggetto (persona fisica, giuridica, pubblica amministrazione ecc.) investito del potere decisionale in relazione alle attività di trattamento dei dati personali, cui competono, anche unitamente ad altro Titolare, **le decisioni in ordine alle finalità, modalità del trattamento di dati personali e strumenti utilizzati, ivi compreso il profilo della sicurezza**.

La Giunta provinciale, già con deliberazione n. 3216 del 23 dicembre 2002 (ora revocata), ha dato atto che **la Provincia autonoma di Trento (come persona giuridica) è Titolare del trattamento** dei dati personali strumentali all'esercizio delle proprie funzioni istituzionali.
La nozione di Titolare fa riferimento all'Amministrazione provinciale unitariamente considerata e non alle competenze dei singoli organi o di chi ne abbia la rappresentanza o ne esprima la volontà (Presidente, Giunta, Dirigenti), in conformità a quanto previsto dall'articolo 28 del Codice, il quale dispone che, quando il trattamento è effettuato da una persona giuridica, da una pubblica amministrazione o da un qualsiasi altro ente, associazione od organismo, **Titolare del trattamento è l'entità nel suo complesso** o l'unità od organismo periferico che esercita un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento, ivi compreso il profilo della sicurezza.
Nell'esercizio delle funzioni di Titolare del trattamento, la Provincia opererà, in concreto, attraverso gli **organi** ed i soggetti di volta in volta competenti in base alle disposizioni ordinamentali (**Presidente**, con particolare riferimento al potere di adozione degli atti di natura regolamentare, **Giunta provinciale** per quanto riguarda la competenza ad adottare atti generali di carattere organizzativo e procedurale o direttive, **Dirigenti,** nella particolare ipotesi in cui agiranno, in nome e per conto del Titolare, svolgendo compiti di stretta pertinenza di quest'ultimo).

In particolare:

**Spetta al Presidente della Provincia:**
- l'adozione e l'aggiornamento, conformemente ai principi stabiliti dall'art. 20 del Codice in materia di protezione dei dati personali, dell'atto, di natura regolamentare, che specifica e autorizza il trattamento dei tipi di dati e delle operazioni relativi a dati sensibili e/o giudiziari.

**Spetta alla Giunta provinciale:**
- la definizione dell'impianto organizzativo provinciale in materia di privacy;
- la definizione di linee strategiche per il trattamento;
- la pianificazione degli interventi di adeguamento;
- l'adozione delle decisioni in ordine alle finalità e modalità del trattamento, costituenti le istruzioni impartite dal Titolare al Responsabile del trattamento;

- la nomina dei Responsabili del trattamento. La presente deliberazione, all'Allegato A) (punti 3 e 4), nomina Responsabili, per i trattamenti di dati personali relativi alle materie di rispettiva competenza, i Dirigenti generali e i Dirigenti, ivi compresi i Dirigenti delle Agenzie, nonché Informatica Trentina s.p.a., relativamente alla gestione dei trattamenti della Provincia affidati alla medesima società. Eventuali ulteriori Responsabili esterni verranno nominati, per conto del Titolare (Giunta provinciale), dai Dirigenti/Responsabili del trattamento;
- la determinazione delle misure generali di sicurezza per il trattamento dei dati personali, in conformità con quanto disposto dal Titolo V del Codice (vedi il presente Allegato; lo stesso demanda, invece, al Dirigente del servizio competente in materia di informatica, l'individuazione di misure integrative di sicurezza);
- vigilare, anche tramite verifiche periodiche, sulla puntuale osservanza delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza, e sul rispetto delle proprie istruzioni. Tali verifiche saranno effettuate tramite i Dirigenti/Responsabili dei trattamenti, nell'ambito dell'attività connessa all'esercizio delle funzioni di direzione, coordinamento e controllo delle strutture dirette, e, in relazione ai controlli sull'applicazione delle misure di sicurezza informatica previsti nel capitolo 13, tramite il Responsabile della Struttura provinciale competente in materia di informatica, che potrà avvalersi anche di soggetti esterni.

**Affidamento all'esterno di trattamenti**

Quando la Provincia si avvale della collaborazione di soggetti esterni alla propria struttura (sulla base di concessioni, appalti, contratti convenzioni, consulenze, collaborazioni, tirocini), nell'ambito del correlativo rapporto accade spesso che vi sia comunicazione, ai soggetti esterni, di dati personali in possesso della Provincia. **Si tratta di una comunicazione,** ai sensi del Codice in materia di protezione dei dati personali, **anche se vi è una semplice autorizzazione all'accesso alle banche dati**.

Per gestire, al meglio, la situazione descritta, è necessario che, nell'ambito delle convenzioni o degli atti che disciplinano il rapporto di collaborazione, venga individuato, in relazione al trattamento dei dati, il **ruolo** del soggetto esterno. Quest'ultimo può essere qualificato:

autonomo Titolare

Responsabile

Incaricato.

Se si intende garantire, al soggetto esterno, ampia autonomia in ordine al trattamento dei dati personali, è opportuno, **qualora se ne riscontrassero le condizioni**, considerarlo quale autonomo **Titolare** del trattamento. In tal caso, la cessione di dati personali al collaboratore esterno, da parte della Provincia, anche nella forma dell'accesso alle proprie banche dati, configura **comunicazione** di dati ed è legittimata solo nelle ipotesi di cui all'art. 19 del Codice in materia di protezione dei dati personali (cioè se è prevista da norma di legge o di regolamento). Il collaboratore deve adottare, nel trattamento dei dati personali, le misure e le cautele previste dal Codice.

Tuttavia, nella maggior parte dei casi, è ravvisabile la necessità che la Provincia conservi il potere di decidere in ordine alle finalità e modalità del trattamento. Nelle ipotesi specificate, si dovrà procedere all'individuazione, in forma espressa, del soggetto esterno quale **Responsabile** o **Incaricato** del trattamento (in relazione al grado di autonomia decisionale e di responsabilità che al medesimo si vuole demandare) ed impartire allo stesso **le necessarie istruzioni/direttive**. **Si ricorda che le persone giuridiche possono essere nominate Responsabili ma non Incaricati e che gli Incaricati possono essere solo persone fisiche**.

**Nel caso, quindi, che il collaboratore esterno sia nominato Responsabile o Incaricato, la cessione di dati personali** da parte della Provincia, anche nella forma dell'accesso alle proprie banche dati, **non configura comunicazione di dati personali**. Il collaboratore esterno, considerato in tal caso alla stregua di un'articolazione organizzativa della Provincia per il trattamento dei dati personali, è soggetto alle regole previste, dal Codice, per i soggetti pubblici e deve applicare tutte le disposizioni organizzative in vigore per le strutture provinciali.

Dal punto di vista operativo, e per motivi di semplificazione, la nomina dei Responsabili esterni, ad esclusione di quelle già effettuate (Informatica Trentina, TSM ecc.), sarà effettuata, per conto del Titolare, dal Dirigente/Responsabile del trattamento; stesse modalità dovranno essere seguite per la nomina di eventuali Incaricati esterni del trattamento.

#### 4.5.1.2 Responsabile del trattamento- Adempimenti in materia di misure di sicurezza

Il Responsabile del trattamento, ai sensi del Codice, è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo **preposti dal Titolare al trattamento di dati personali** (art. 29 D. Lgs. n. 196/2003)**.**

La nomina di un Responsabile**,** pur non essendo necessaria (art. 29, comma 1, D. Lgs. n. 196/2003), è tuttavia auspicabile nelle organizzazioni complesse quali sono le pubbliche amministrazioni.
Il Responsabile viene designato, dal Titolare, tra coloro che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza (art. 29, comma 2, D. Lgs. n. 196/2003).
Spettano ai Dirigenti, in via esclusiva, le funzioni che hanno a che fare con decisioni e scelte attinenti all'attività gestionale.
Il Responsabile:
procede al trattamento **attenendosi alle istruzioni** impartite dal Titolare, il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni in materia di trattamento e delle proprie istruzioni (art. 29, comma 5, D. L.gs. n. 196/2003);
**non svolge meri compiti esecutivi** (come quelli spettanti all'Incaricato), ma traduce in istruzioni operative le scelte strategiche e le direttive generali impartite dal Titolare, puntualizzandole e adattandole agli specifici contesti lavorativi e di trattamento.
Con la presente deliberazione, che conferma quanto già disposto con deliberazione della Giunta provinciale 23 dicembre 2002, n. 3216 (ora revocata), sono nominati Responsabili, per i trattamenti di dati personali relativi alle materie di rispettiva competenza e alle funzioni di gestione amministrativa, finanziaria e tecnica:
**i Dirigenti generali**, laddove gestiscano a titolo esclusivo determinati trattamenti;
**i Dirigenti**, ivi compresi i Dirigenti delle Agenzie comunque denominati;
la Società "**Informatica Trentina s.p.a.**", relativamente ai trattamenti della Provincia affidati alla gestione della medesima società, ai sensi della legge provinciale 6 maggio 1980, n. 10, nell'ambito delle prestazioni stabilite dalla convenzione prevista dall'articolo 5, comma 1, della medesima legge.
La funzione di Responsabile non può essere delegata in nessun caso.
E' sempre possibile la nomina di un Responsabile del trattamento (persona fisica o giuridica)**,** esterno alla Provincia, nei casi - prospettati al paragrafo 4.5.1.1 - relativi a collaborazioni di soggetti esterni (concessioni, appalti, contratti, convenzioni, consulenze, collaborazioni, tirocini, ecc.) per l'espletamento dei compiti d'istituto, qualora la richiamata esternalizzazione comporti, come prestazione principale o accessoria, un trattamento di dati.

Un'apposita clausola, deI contratto di affidamento del servizio, dovrà prevedere l'impegno del soggetto esterno ad assumere il ruolo di Responsabile del trattamento, le indicazioni sulle modalità di gestione del trattamento e le misure di sicurezza da adottare. In tal modo, i soggetti esterni si assumono l'onere di operare conformemente alle regole previste dal Codice e alle disposizioni impartite dalla Provincia autonoma di Trento.

**Successivamente, il Dirigente/Responsabile del trattamento provvederà a nominare uno o più Responsabili esterni, specificando di effettuare tale nomina per conto del Titolare.**

Al fine di garantire omogeneità di comportamento, le strutture provinciali che stipulano contratti o convenzioni con strutture e/o soggetti esterni, sono tenute a raccordarsi con il Dirigente competente in materia di privacy, per concordare il testo dell'atto di nomina del Responsabile esterno, qualora non fosse sufficiente servirsi della modulistica allegata alla presente deliberazione.

Si precisa che è anche possibile che l'assunzione del ruolo di Responsabile esterno, ove ritenuto opportuno, possa avvenire, esclusivamente, nell'ambito degli accordi contrattuali, purchè i relativi obblighi, e le conseguenti responsabilità, siano definiti con estrema chiarezza e puntualità.

**Adempimenti del Responsabile del trattamento (Dirigente) in materia di misure di sicurezza**

Il Dirigente Responsabile del trattamento deve, in via generale, provvedere ai seguenti adempimenti:

*a) verifica dei trattamenti*

I Responsabili devono provvedere al trattamento dei dati personali nel rispetto delle vigenti norme e delle disposizioni impartite dal Titolare.

Pertanto, per qualsiasi trattamento, il Responsabile deve verificare:

- che il trattamento sia connesso con l'esercizio delle funzioni istituzionali e che le stesse finalità non siano perseguibili attraverso il trattamento di dati anonimi (principio di pertinenza e principio di necessità);
- che le modalità del trattamento garantiscano il diritto alla riservatezza dei terzi (principio di non eccedenza);
- che il trattamento, ed in particolare le modalità adottate, non siano difformi dalle norme di legge e di regolamento;
- che vengano adottate le misure di sicurezza.

Ogni Responsabile deve verificare, periodicamente, la sussistenza di tali requisiti nelle diverse fasi del trattamento, rispetto alle finalità perseguite nei singoli casi, anche con riferimento ai dati che l'interessato fornisce di propria iniziativa.

Nel caso in cui l'interessato fornisca, spontaneamente, dati in eccedenza rispetto a quelli strettamente indispensabili per lo svolgimento delle attività di competenza provinciale, i dati eccedenti possono essere distrutti, o conservati senza essere utilizzati, sulla base della valutazione discrezionale del Responsabile del trattamento.

Fra i requisiti di ogni trattamento, infatti, assumono particolare rilevanza quelli della pertinenza e della non eccedenza delle informazioni rispetto alle finalità per le quali i dati personali sono raccolti o trattati. Il trattamento di alcune informazioni, ad esempio, può essere necessario per la fase istruttoria del procedimento amministrativo, ma la loro conoscenza può risultare non motivata da parte di soggetti diversi da quelli preposti allo svolgimento di compiti specifici. Tale verifica deve comportare, se necessario, la revisione delle modalità organizzative degli uffici e l'adozione di idonee misure di sicurezza.

Più specificamente, il Responsabile deve:

- verificare che i trattamenti in corso, o da intraprendere presso la struttura, siano rispondenti a quanto disposto dal Codice: il trattamento, ove difforme dalla norma, deve essere adeguato o cessare;
- comunicare tempestivamente, alla Struttura competente in materia di privacy, ai fini dell'istruttoria, l'intenzione di avviare nuovi trattamenti, non compresi nell'elenco provinciale dei

trattamenti di dati personali, la modifica degli elementi essenziali dei trattamenti in atto, nonché l'eventuale cessazione di trattamenti in atto e notificare, al Garante, il corrispondente trattamento qualora risultino integrate le condizioni di cui all'art. 37 del Codice;
- effettuare al Garante le comunicazioni relative ai trattamenti contenenti dati particolari (art. 39 Codice privacy);
- provvedere al censimento dei trattamenti presenti nella propria struttura, ed inserire i medesimi nell'elenco provinciale informatizzato dei trattamenti, reperibile all'indirizzo **web http://trattamenti.provincia.tn.it;**
- aggiornare, costantemente, l'elenco provinciale informatizzato dei trattamenti;
- predisporre l'informativa, di cui all'art. 13 del Codice, e verificare che siano adottate le modalità operative necessarie perché la stessa sia effettivamente portata a conoscenza degli interessati;
- provvedere, anche tramite gli Incaricati, a dare riscontro alle istanze degli interessati per l'esercizio del diritto di accesso.

*b) verifica della adeguatezza delle abilitazioni di accesso*

Il Responsabile deve:
- individuare i soggetti abilitati all'accesso alle risorse di rete protette, in relazione ai compiti svolti dal personale;
- verificare - d'intesa con l'Amministratore di sistema - che la configurazione e l'utilizzo delle risorse presenti sul server di rete della propria struttura (unità logiche, cartelle) sia conforme a quanto stabilito nel Capitolo 7 (*Misure di sicurezza relative alle risorse di rete e dei PC*), al fine di garantire la riservatezza e l'accesso selezionato alle banche dati contenenti dati personali; la verifica può essere effettuata sulla base delle informazioni che deve comunicare l'Amministratore di sistema sulla composizione dei gruppi di utenti e sulle restrizioni di accesso assegnate alle cartelle di lavoro sul server.

*c) nomina degli Incaricati del trattamento di dati personali*

Il Responsabile deve:
- provvedere alla nomina degli Incaricati di ciascun trattamento (con ordine di servizio, a meno che gli Incaricati non siano esterni);
- impartire agli Incaricati, all'atto della loro nomina, con atto scritto, le necessarie istruzioni operative e vigilare sulle stesse.

A tale scopo, l'atto di nomina è integrato con le istruzioni per il trattamento, che devono essere coerenti con i compiti da svolgere e devono indicare, nel rispetto del principio di pertinenza e non eccedenza nel trattamento dei dati personali, le tipologie di dati da trattare, le banche dati in cui essi sono contenuti, le modalità di trattamento e di conservazione dei dati, gli eventuali limiti del trattamento, l'autorizzazione ad accedere a banche dati gestite da altre strutture o da altri soggetti (nei limiti di legge o regolamento e previo accordo tra i rispettivi Responsabili del trattamento), l'autorizzazione all'accesso a banche dati gestite in comune tra più strutture (ad es. SAP; per quest'ultimo aspetto si rinvia alle specificazioni riportate sub paragrafo b). Tale atto deve, in particolare, prescrivere espressamente che l'Incaricato abbia accesso ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere i compiti assegnati. Lo stesso atto deve, inoltre, sottolineare l'obbligo di archiviare, secondo le modalità più avanti specificate, i documenti e i supporti sui quali sono registrati i dati personali non appena concluso il trattamento; a tale scopo, si adotta il modello contenuto nell'Allegato B, da redigere in duplice originale, uno dei quali viene restituito dall'Incaricato, al Dirigente che conferisce l'incarico, sottoscritto per presa visione.

Il Decreto legislativo n. 196/2003 consente, sulla base di quanto specificato dall'articolo 30, comma 2, una modalità di nomina "semplificata", consistente nella documentata preposizione della persona fisica ad una unità per la quale è individuato, per iscritto, l'ambito del trattamento consentito agli

addetti all'unità medesima. Un atto di tale portata è considerato, dalla disposizione citata, equipollente alla nomina.

Al fine di utilizzare correttamente tale specifica modalità, il Responsabile del trattamento/Dirigente può, nell'atto di nomina, rinviare, per quanto riguarda l'ambito del trattamento consentito, alle informazioni contenute nell'elenco informatizzato dei trattamenti, alla imprescindibile condizione che il richiamato elenco, completo in ogni sua parte, sia costantemente aggiornato. Se così non fosse, la nomina risulterebbe priva di significato sostanziale, con il fondato rischio che Provincia, e Dirigente, possano essere assoggettati a sanzioni di vario tipo.

L'atto con cui il Responsabile del trattamento/Dirigente nomina l'Incaricato del trattamento, impartendo allo stesso le istruzioni necessarie, non va considerato come mero adempimento cui assolvere una tantum, bensì comporta l'impegno del Dirigente ad un aggiornamento delle disposizioni, con cadenza annuale, coerente con i mutamenti organizzativi e di assegnazione degli incarichi al personale.

*c.1)* *nomina degli Incaricati del trattamento di dati personali contenuti in banche dati e sistemi gestiti contemporaneamente da più strutture*

Nel caso in cui l'Incaricato, per lo svolgimento delle operazioni proprie del trattamento, abbia accesso o possa operare su dati contenuti in banche dati o sistemi gestiti in comune da più strutture (ad es. mediante appositi programmi applicativi, come SAP ecc.), è necessario che lo stesso sia dotato delle prescritte abilitazioni, che vengono concesse secondo le procedure prescritte. Il Responsabile del trattamento/Dirigente, che rimane responsabile della corretta attribuzione delle abilitazioni messe a disposizione della struttura e al personale ad essa assegnato, è tenuto a disciplinare i limiti di accesso ai dati, le modalità di trattamento degli stessi e quant'altro necessario per garantire il rispetto della riservatezza e del principio di non eccedenza nel trattamento, nell'ambito dell'atto di conferimento dell'incarico al trattamento ovvero separatamente.
A tal fine, il Dirigente deve aggiornare, o rinnovare, con cadenza annuale (punto 15 dell'Allegato B del Codice), le istruzioni per il trattamento dei dati personali impartite all'Incaricato all'atto dell'incarico, prevedendo che:
la visione dei dati personali, contenuti nel sistema o nella banca dati cogestita da più strutture, esclude comunque qualsiasi forma di comunicazione e diffusione degli stessi, che non sia strettamente necessaria ai fini dello svolgimento dei compiti istituzionali; se necessaria, comunque, la comunicazione deve svolgersi nei limiti stabiliti dalle leggi e dai regolamenti;
la visualizzazione occasionale, di dati non pertinenti all'esercizio dei propri specifici compiti, non ne legittima ulteriori forme di trattamento. (ad es. comunicazione e diffusione).

*d)* *autorizzazione al trattamento dei dati sensibili e giudiziari*

1) Il Responsabile del trattamento deve rilasciare specifica autorizzazione agli Incaricati del trattamento di dati sensibili; detta autorizzazione può trovare collocazione nell'atto di conferimento dell'incarico al trattamento.
2) Il Responsabile del trattamento deve concorrere all'aggiornamento del Regolamento per il trattamento dei dati sensibili e giudiziari, con specifico riferimento all'elenco dei trattamenti di dati sensibili e/o giudiziari della struttura di riferimento, secondo le direttive impartite dal Titolare.

In attuazione di tale compito, deve verificare, con riferimento al trattamento di dati sensibili (art. 20 D. Lgs. n. 196/2003) e giudiziari (art. 21 D. Lgs. n. 196/2003), se il trattamento stesso è autorizzato da espressa disposizione di legge, nella quale sono specificati i tipi di dati che possono essere trattati, le operazioni eseguibili e le rilevanti finalità di interesse pubblico perseguite.

Qualora il Responsabile del trattamento verifichi che il Codice, o la legge, individuino espressamente le rilevanti finalità di interesse pubblico, ma non i tipi di dati e le operazioni eseguibili, deve provvedere a:

a) identificare i tipi di dati e di operazioni strettamente pertinenti e necessari in relazione alle finalità perseguite;
b) comunicare tali informazioni, alla Struttura competente in materia di privacy, ai fini degli adempimenti di cui agli artt. 20 –21 del Codice.

Qualora, invece, il Responsabile verifichi che le finalità del trattamento non sono previste tra quelle specificate dal Codice, né da espressa disposizione di legge, deve tempestivamente darne comunicazione, alla Struttura competente in materia di privacy che, dopo aver svolto adeguata istruttoria, provvederà a chiedere, al Garante, il riconoscimento del rilevante interesse pubblico delle finalità del trattamento in oggetto.

*e) osservanza delle misure di sicurezza*

Il Responsabile deve:

- garantire che il trattamento, la comunicazione e la diffusione dei dati avvengano nel rispetto delle vigenti disposizioni, ivi comprese quelle relative alla sicurezza, anche evitando l'ingiustificata e prolungata permanenza dei dati personali sui siti istituzionali della Provincia;
- rispettare le direttive e le misure generali, impartite dalla Giunta provinciale, in materia di trattamento dei dati personali e di sicurezza e curare gli adempimenti da essa stabiliti;
- ottemperare alle istruzioni operative integrative, approvate dal Dirigente della Struttura competente in materia di informatica, ai sensi di quanto disposto dalla presente deliberazione, adottando, nell'ambito della struttura di competenza, le misure organizzative necessarie;
- segnalare, alle strutture provinciali competenti, le necessità di acquisizione, o di adeguamento, delle dotazioni della struttura ovvero la necessità di potenziare i servizi di portineria, al fine del rispetto delle disposizioni in materia di sicurezza dei dati personali, concorrendo alla definizione delle priorità nell'ambito della programmazione degli interventi;
- adottare, in aggiunta alle misure di sicurezza stabilite dalla Giunta provinciale e previa intesa con il Dirigente competente in materia di informatica, ulteriori misure di sicurezza, sulla base delle specifiche peculiarità dei trattamenti di competenza della struttura di appartenenza, idonee ad evitare rischi di distruzione o perdita anche accidentale dei dati, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità della raccolta;
- rispettare le misure di sicurezza per le banche dati informatizzate contenenti dati personali;
- vigilare, per conto del Titolare ed anche tramite verifiche periodiche, sulla puntuale osservanza delle vigenti disposizioni in materia di trattamento, ivi incluso il profilo della sicurezza, di quelle impartite dal Titolare nonchè sul rispetto delle proprie istruzioni;

f) nomina Amministratori di sistema

- nominare, con riferimento agli elaboratori ed agli applicativi non gestiti da Informatica Trentina, gli Amministratori di sistema, valutandone esperienza, capacità, affidabilità; -
- indicare, puntualmente, nell'atto di nomina, l'ambito di operatività dell'Amministratore;
- verificare, con cadenza annuale, l'operato degli Amministratori di sistema;
- inserire i nominativi degli Amministratori di sistema, le funzioni attribuite e l'ambito di operatività nell'elenco informatizzato dei trattamenti;
- conservare, per un periodo minimo di sei mesi, gli accessi logici effettuati dagli Amministratori di sistema.

**Spetta al Dirigente del servizio competente in materia di informatica:**

- individuare le istruzioni operative ad integrazione, specificazione e chiarimento delle indicazioni recate nel presente Allegato, o da eventuali ulteriori disposizioni della Giunta provinciale; coordinare ed assistere i Responsabili dei trattamenti nell'attuazione dei relativi adempimenti;

- individuare e proporre preventive ed idonee misure informatiche di sicurezza, da osservare nell'esecuzione dei trattamenti dei dati, in relazione all'evoluzione della tecnica, della normativa e dell'esperienza;
- svolgere, per conto del Titolare, i controlli e le funzioni specificati nel **capitolo 13 (Verifiche di sicurezza)del presente Allegato**, avvalendosi, ove ritenuto opportuno, di soggetti esterni, e vigilare sul rispetto delle misure di sicurezza informatica, segnalando eventuali problemi rilevati, in prima istanza, ai Responsabili dei trattamenti dei dati e, in ultima istanza, al Titolare;
- raccogliere e conservare, ai fini di eventuali verifiche, le attestazioni di conformità alle disposizioni dell'Allegato B (punto 25) del D.l.gs n. 196/2003.

### 4.5.1.3 Incaricato - Cautele da adottare nell'acquisizione, nella produzione e nel rilascio di documenti contenenti dati personali

> Ai sensi del Codice in materia di protezione dei dati personali (art. 4, comma 1, lettera h)), Incaricato del trattamento è la persona fisica autorizzata dal Titolare, o dal Responsabile, a compiere le operazioni di trattamento di dati personali, attenendosi alle istruzioni impartite dal Titolare e dal Responsabile. La designazione è effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito.
> Si considera tale anche la documentata preposizione della persona fisica ad una unità per la quale è individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima (art. 30, comma 2, del Codice).

**Possono essere designati Incaricati solo e soltanto persone fisiche.**
Gli Incaricati del trattamento sono nominati, dal Responsabile del trattamento/Dirigente, con le modalità indicate nella presente deliberazione.
E' sempre possibile la nomina di un Incaricato del trattamento, esterno alla Provincia (persona fisica), nei casi - prospettati al paragrafo 4.5.1.1 - riguardanti collaborazioni di soggetti esterni per l'espletamento dei compiti istituzionali (concessioni, appalti, convenzioni, consulenze, collaborazioni, tirocini, ecc.). Va ribadito che possono essere nominati Incaricati solo persone fisiche e solo coloro che operano sotto la diretta autorità del Titolare o del Responsabile, attenendosi alle istruzioni impartite (art. 30 del Codice).
**La conoscenza dei dati personali, da parte di chi sia stato nominato Incaricato, non è considerata comunicazione**.

> L'Incaricato procede al trattamento, sotto la diretta autorità del Titolare o del Responsabile, che devono impartirgli istruzioni e vigilare sul suo operato; svolge, nell'ambito del trattamento, meri compiti esecutivi sulla base delle istruzioni operative impartite dal Titolare o dal Responsabile.

**Adempimenti dell'Incaricato del trattamento**
I compiti dell'Incaricato devono essere analiticamente specificati nel relativo atto di nomina.
In via generale, l'Incaricato del trattamento deve provvedere ai seguenti adempimenti:

**Regole generali per tutti i trattamenti**
Nello svolgimento del trattamento devono essere seguite le norme di legge e di regolamento in materia di tutela della riservatezza dei dati personali e devono essere applicate le misure di sicurezza previste nel presente **Allegato B .**

Il trattamento dei dati, ai sensi dell'art. 11 del Codice, deve rispettare il principio **di pertinenza e non eccedenza** rispetto alle finalità del medesimo: l'accesso è consentito ai soli dati personali la cui conoscenza sia strettamente indispensabile per adempiere ai compiti affidati.
I dati devono essere trattati in modo **lecito e secondo correttezza ed** essere **esatti ed aggiornati**.
L'Incaricato, in particolare, nello svolgimento del trattamento, è tenuto a:

- **accertare** che l'**informativa, completa in tutte le sue parti,** venga comunicata agli interessati, ai sensi dell'art. 13 del Codice in materia di dati personali, e verificare che ciascuna operazione di comunicazione e diffusione dei dati sia conforme alle disposizioni di legge e regolamento;
- **consentire l'esercizio dei diritti e delle facoltà** previste dall'art. 7 del D.lgs. n. 196/2003 (e cioè fornire conferma, all'interessato, dell'esistenza o meno dei dati che lo riguardano; indicare le finalità e modalità del trattamento ed ogni altra attività connessa allo stesso; provvedere, previa espressa richiesta informale e scritta dell'interessato, all'aggiornamento dei dati nonché alla loro rettificazione, integrazione, cancellazione, trasformazione in forma anonima o al blocco qualora trattati in violazione della legge);
- **collaborare, con gli altri Incaricati del medesimo trattamento**, esclusivamente per i fini dello stesso e nel rispetto delle indicazioni fornite;
- **non trasmettere, a soggetti terzi, informazioni** circa dati personali trattati. La comunicazione è ammessa soltanto se funzionale allo svolgimento dei compiti affidati, previa autorizzazione del Responsabile del trattamento;
- **accertarsi dell'identità del diretto interessato**, prima di fornire informazioni circa i dati personali o il trattamento effettuato;
- **riporre in archivio,** al termine del periodo di trattamento, i supporti o i documenti, ancorchè non definitivi, contenenti i dati personali;
- **conservare i dati** trattati per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono raccolti e successivamente trattati.

Devono essere rispettate tutte le istruzioni impartite dal Titolare, nonché le istruzioni e direttive impartite dallo scrivente, in qualità di Responsabile del trattamento.
L'Incaricato, per il corretto e puntuale svolgimento del trattamento, dovrà: 1) procedere all'acquisizione, sul sito istituzionale della Provincia, delle deliberazioni della Giunta provinciale in tema di privacy (**presente deliberazione**, n. 2643/2008, n. 1037/2010 ecc.) e rispettare le prescrizioni in esse contenute; 2) visionare, nell'elenco informatizzato, il contenuto dei trattamenti assegnati.

**Nel caso di presenza di ospiti o personale di servizio sarà necessario**

- **far attendere le persone** in luoghi in cui non sono presenti informazioni riservate o dati personali;
- **evitare di allontanarsi dalla scrivania** in presenza di ospiti o riporre i documenti e attivare il salvaschermo del PC;
- **non rivelare o far digitare la password** al personale di assistenza tecnica;
- **non rivelare le password al telefono**, ne inviarle via fax; nessuno è autorizzato a chiederle;
- **segnalare** qualsiasi anomalia e stranezza al Responsabile.

**Trattamenti concernenti dati sensibili e giudiziari**

L'Incaricato è autorizzato al trattamento dei dati sensibili e giudiziari (articoli 20, 21 e 22 del Codice) indicati nell'elenco informatizzato dei trattamenti ad esso assegnati.

- **Modalità di trattamento dei dati sensibili/giudiziari.**

Ferma restando l'applicazione delle disposizioni vigenti in materia di trattamento dei dati sensibili e giudiziari e delle istruzioni impartite dal Titolare e dal Responsabile del trattamento, si riportano alcune specifiche misure da applicarsi in caso di trattamento dei predetti dati:

- **non fornire** dati o informazioni, di carattere sensibile, per telefono, qualora non si abbia certezza assoluta sull'identità del destinatario;
- **evitare** di inviare, per fax, documenti in chiaro contenenti dati sensibili: si suggerisce, in tal caso, di inviare la documentazione, senza alcun esplicito riferimento all'interessato (ad esempio, contrassegnando i documenti semplicemente con un codice);
- i documenti, ancorchè non definitivi, ed i supporti recanti dati sensibili o giudiziari, devono essere conservati, anche in corso di trattamento, in elementi di arredo muniti di serratura e non devono essere lasciati incustoditi in assenza dell'Incaricato;

*(nel caso di trattamenti di dati inerenti la salute)*
- i supporti ed i documenti, recanti dati relativi alla salute e alla vita sessuale, devono essere conservati nei predetti contenitori muniti di serratura, separatamente da ogni altro documento;
- per la redazione, la pubblicazione, la comunicazione ed il rilascio degli atti recanti dati idonei a rivelare lo stato di salute, devono essere osservate, in aggiunta alle norme di legge e di regolamento, le prescrizioni contenute nel presente Allegato .

**Trattamenti con strumenti elettronici**

Per quanto riguarda, in particolare, le elaborazioni e le altre fasi dei trattamenti effettuate attraverso strumenti informatici, ciascun Incaricato disporrà di una parola chiave per l'accesso ai dati e di un codice identificativo personale.
Gli Incaricati avranno cura di:
- **non condividere il proprio codice identificativo personale** con altri utenti, salvo i casi espressamente previsti;
- **non cedere a terzi la propria parola chiave** di autenticazione;
- **non accedere a servizi non consentiti**;
- **non caricare ed eseguire software di rete o di comunicazione**, senza previa verifica dello stesso da parte del proprio Referente informatico, che opera in stretto rapporto con il Servizio Supporto Amministrativo e Informatica;
- **non tentare di acquisire i privilegi di Amministratore di sistema**;
- **verificare l'assenza di virus** nei supporti utilizzati;
- **non collegare dispositivi** che consentano un accesso, non controllabile, ad apparati della rete della Provincia;
- **memorizzare i dati di interesse lavorativo sui dischi U e Y**, ove disponibili; in caso contrario, effettuare il backup periodico per i trattamenti non gestiti da Informatica Trentina;
- **procedere alla cancellazione dei supporti magnetici od ottici contenenti dati personali**, prima che i medesimi siano riutilizzati. Se ciò non è possibile, essi devono esser distrutti;
- **attenersi alle istruzioni specificate nelle "Prescrizioni in tema di Misure di Sicurezza", contenute nel presente Allegato B (pag. n. 89).**

**Banche dati**

La visione dei dati, contenuti nelle banche dati, esclude comunque qualsiasi forma di comunicazione, diffusione e trattamento degli stessi che non sia strettamente funzionale all'espletamento dei compiti d'istituto e che non si svolga nei limiti stabiliti da leggi e regolamenti.

**Trattamenti senza strumenti elettronici**

Per quanto riguarda la eventuale documentazione cartacea, compresi i supporti non informatici contenenti la riproduzione di informazioni relative al trattamento di dati personali, gli atti e i documenti contenenti i dati devono essere conservati, dagli Incaricati, per la durata del trattamento e successivamente riposti in archivi ad accesso controllato, secondo quanto sarà indicato di volta in volta, al fine di escludere l'accesso, agli stessi, da parte di persone non incaricate al trattamento.
Nel caso di trattamento di dati sensibili o di dati giudiziari, gli atti e i documenti, contenenti i dati

affidati agli Incaricati del trattamento, devono essere conservati in contenitori muniti di serratura, al fine di escludere l'acquisizione, degli stessi, da parte di persone non incaricate del trattamento.
Qualora sia necessario distruggere i documenti contenenti dati personali, utilizzare gli appositi apparecchi "distruggi documenti"; in assenza di tali strumenti, i documenti devono essere sminuzzati in modo da non essere più ricomponibili;
Gli Incaricati sono tenuti a segnalare le eventuali necessità di dotazioni e arredi, in modo da poter adempiere a quanto prescritto.
Analogamente, per quanto riguarda i flussi di documenti cartacei all'interno degli uffici provinciali, devono essere adottate idonee misure organizzative per salvaguardare la riservatezza dei dati personali (es. trasmissione dei documenti in buste chiuse).

**Cautele da adottare, da parte dell'Incaricato, nell'acquisizione, nella produzione e nel rilascio di documenti contenenti dati personali**

**Documenti in input**

Per "documenti in input", si intendono i documenti, o i supporti, contenenti dati personali acquisiti dalla struttura, ai fini di un loro impiego in trattamento.

Relativamente al trattamento dei documenti in input, è necessario adottare le cautele seguenti:

- i documenti in input devono essere utilizzati, soltanto, da chi sia Incaricato al trattamento o dal Responsabile;
- l'Incaricato verifica:
  - la provenienza dei documenti;
  - che tali documenti siano effettivamente necessari al trattamento in questione;
  - la tipologia dei dati contenuti (comuni, sensibili, giudiziari o altri dati particolari), al fine di individuare le modalità, legittime ed idonee, per il trattamento e le misure di sicurezza da attuare;
  - che siano osservati il principio di pertinenza e non eccedenza rispetto alle finalità del trattamento, la completezza, la correttezza e l'aggiornamento dei dati;
- per la conservazione dei documenti in input presso di sé, gli Incaricati del trattamento devono porre in essere le misure indicate nel paragrafo (n. 8.5) "Misure di sicurezza relative ai supporti di memorizzazione" e nel capitolo (n. 9) "Trattamento di dati su supporti non informatici" ed ogni ulteriore precauzione a garanzia della sicurezza.

La permanenza di atti e documenti presso l'Incaricato o il Responsabile del trattamento, in particolare, deve essere limitata al tempo strettamente necessario per eseguire le operazioni di trattamento; al termine dell'attività, la documentazione deve essere riposta nel rispettivo archivio.
Limitatamente ai supporti magnetici in input, utilizzati per l'elaborazione, è fatto inoltre obbligo all'Incaricato, o al Responsabile del trattamento dei dati, di **verificare l'assenza di virus**, ove questo sia tecnicamente possibile, prima di procedere all'elaborazione dei dati.

**Documenti in output**

Per "documenti in output", si intendono i documenti, o i supporti, contenenti dati personali prodotti e rilasciati dalla struttura a soggetti esterni alla struttura stessa.

L'Incaricato del trattamento deve trattare qualunque prodotto dell'elaborazione di dati personali, ancorchè non costituente documento definitivo, (appunti, stampe interrotte, stampe di prova, stampe elaborazioni temporanee ecc.) **con le stesse cautele che sarebbero riservate alla versione definitiva** (v. misure relative ai trattamenti cartacei e informatizzati).

Nell'ipotesi di documenti in output, è necessario, all'atto della consegna o dell'invio, verificare che la persona che riceve il documento sia legittimata al ritiro e all'utilizzo.

#### 4.5.1.4 Sistema organizzativo provinciale per la protezione dei dati personali

Per "Sistema organizzativo per la protezione dei dati personali" si intende il processo organizzativo determinato dall'insieme di modalità, attività e relazioni che attengono al trattamento e alla protezione dei dati personali e che coinvolgono la Provincia autonoma di Trento, sia nei rapporti interni, che nei rapporti che intercorrono con il sistema degli Enti, delle Agenzie, e con gli altri soggetti della P.A. (per le funzioni delegate dalla stessa Provincia).
I soggetti principalmente coinvolti nei processi organizzativi descritti, oltre a Titolare, Responsabili e Incaricati del trattamento, sono la Struttura provinciale competente in materia di privacy ed il Referente privacy.

**I.D. privacy provinciale**

Per Struttura competente in materia di protezione dei dati personali, si intende l'insieme di funzioni, facenti capo al Dirigente che si occupa di protezione dei dati personali, svolte all'interno della organizzazione provinciale.

Il Dirigente competente in materia di privacy:
- **fornisce** indirizzi, linee guida, e supporto alle strutture provinciali,
- cura i rapporti con l'Ufficio del Garante per la protezione dei dati personali,
- **fornisce** supporto**,** per conto del Titolare Provincia autonoma di Trento – Giunta provinciale, ai Responsabili del trattamento, sui quali gravano, in via esclusiva, le responsabilità connesse ai trattamenti di loro competenza, in relazione agli adempimenti generali previsti dal Codice ed in particolare alla comunicazione e alla notificazione al Garante, curandone in particolare l'istruttoria;
- **coordina** la redazione e l'aggiornamento del Regolamento per il trattamento dei dati sensibili e giudiziari;
- **coordina** l'aggiornamento dell'archivio provinciale informatizzato dei trattamenti dei dati personali.

Nell'esercizio delle competenze di cui ai punti precedenti, l'I.D. privacy si avvale della collaborazione dei Referenti privacy.

**Referente privacy**

Il Referente privacy è nominato, presso ciascuna articolazione organizzativa provinciale (intendendosi per tale ogni Dipartimento, Servizio, Progetto speciale, Incarico dirigenziale, Agenzia), con ordine di servizio del Dirigente **e si occupa, specificamente, anche di privacy**, operando in stretto raccordo con il Dirigente competente in materia di privacy.
Laddove ritenuto più opportuno, anche in relazione alle dimensioni ed alle competenze delle varie strutture, è facoltà dei Dirigenti individuare un unico Referente privacy per tutte le strutture che fanno capo ad un Dipartimento, tenendo in debita considerazione, però, che la protezione dei dati personali deve poter dispiegare i propri effetti su ogni singolo trattamento; ragion per cui il Referente privacy deve essere una figura in grado di conoscere e valutare, analiticamente, i trattamenti facenti capo ad ogni articolazione organizzativa inclusa nei vari Dipartimenti.
Ove possibile, dovrebbe essere individuato, quale Referente privacy, personale con la qualifica di funzionario, che sia, inoltre, sufficientemente competente in problematiche giuridico-amministrative.
Il Referente è figura determinante del sistema organizzativo provinciale poiché, senza il suo apporto professionale, diventa impossibile, od in ogni caso estremamente difficoltoso, adempiere, in modo adeguato, agli obblighi previsti dalla normativa vigente.

Il Referente privacy svolge le seguenti funzioni:
- **assicura l'assistenza interna alla/e struttura/e di appartenenza**, per il corretto adempimento della normativa;
- **collabora con il Responsabile del trattamento** per formulare richieste di parere al Dirigente competente in materia di privacy;
- **supporta i Responsabili del trattamento nell'aggiornamento** dell'Archivio provinciale informatizzato dei trattamenti **e del Regolamento dei dati sensibili e giudiziari;**
- **effettua il monitoraggio dello stato di attuazione delle misure di sicurezza**, in collaborazione con la Struttura competente in materia di informatica, con i Responsabili del trattamento, e con i Referente informatici della struttura di appartenenza.

E' tenuto, inoltre, a segnalare, alla Struttura competente in materia di privacy, i casi in cui presso la struttura di appartenenza occorra:
- **aggiornare** il Regolamento provinciale per il trattamento dei dati sensibili e giudiziari con ulteriori trattamenti;
- **valutare** la necessità di procedere alla **notificazione di un trattamento** al Garante ex art 37 del Codice;
- **valutare** la necessità di procedere alla **comunicazione al Garante**, ex art. 39 del Codice, nel caso in cui vi sia una richiesta di trasmissione di dati comuni da parte di soggetti pubblici non prevista dalla legge.

#### 4.5.1.5 Amministratore di sistema

L'**Amministratore di sistema** è il soggetto cui è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di base dati e di consentirne l'utilizzazione.

Sono funzioni tipiche degli Amministratori di sistema:

1. l'organizzazione dei flussi di rete
2. la manutenzione hardware
3. la realizzazione di copie di sicurezza
4. la custodia delle credenziali di autenticazione
5. la gestione dei sistemi di autenticazione e autorizzazione
6. la gestione dei supporti di memorizzazione.

La Giunta provinciale, con il presente provvedimento (e recependo quanto già stabilito con deliberazione n. 3217 di data 23 dicembre 2002, ora revocata), ha demandato, ai sottoindicati soggetti, il compito di nominare gli Amministratori di sistema:
1. **Informatica Trentina s.p.a.** per i sistemi operativi presenti su elaboratori in uso presso le strutture provinciali e affidati alla gestione della Società medesima;
2. **i Dirigenti/Responsabili del trattamento,** per i sistemi operativi non gestiti da Informatica Trentina s.p.a. .

L'Amministratore di sistema, nel generale ambito del trattamento dati, rappresenta una figura tanto strategica quanto delicata, pur non essendo espressamente qualificata in sede legislativa.
Per tale motivo, l'Autorità Garante per la protezione dei dati personali, con provvedimenti a carattere generale del 27/11/2008 e del 25 giugno 2009, ha prescritto, con riferimento all'attività dell'Amministratore di sistema, una serie di puntuali obblighi.
Pertanto, il Dirigente/Responsabile del trattamento, all'atto della nomina, deve:

- valutare l'esperienza, capacità e affidabilità del soggetto designato, nonché la predisposizione al rispetto della normativa;
- indicare, puntualmente, gli ambiti di operatività dell'Amministratore;
- rendere edotti i lavoratori circa l'identità degli Amministratori, se questi ultimi trattano dati e/o informazioni riguardanti i medesimi.

A nomina effettuata, invece, il Dirigente/Responsabile del trattamento deve:
- verificare, con cadenza almeno annuale, l'operato degli Amministratori;
- conservare l'elenco di coloro che sono adibiti ad Amministratori, se il Responsabile del trattamento è esterno;
- inserire, nel caso di Amministratori di sistema interni, nel database dei trattamenti provinciali, i nominativi degli Amministratori di sistema, le funzioni, dagli stessi svolte, nonché aggiornare costantemente le informazioni richieste dallo specifico applicativo. L'elenco informatizzato è conservato dall' Ufficio informatica, articolazione organizzativa del Servizio di supporto amministrativo e informatica;
- garantire che siano registrati, e conservati per un periodo comunque non inferiore a sei mesi, gli accessi logici effettuati, ad opera degli Amministratori, ai sistemi di elaborazione e agli archivi elettronici.

### 4.5.1.6 Interessato

L'**Interessato** è la persona fisica cui si riferiscono i dati personali (art. 4, lettera i, del Codice, riformulato ai sensi del D.L. n. 201/2011 convertito con legge n. 214/2011**). E' il soggetto tutelato dalla normativa in materia di privacy.**

Per i trattamenti effettuati dalla pubblica amministrazione, l'interessato non è tenuto ad esprimere alcun consenso, purché sussistano i presupposti per il trattamento previsti dagli articoli 18 e 19 del Codice.

Ai sensi del Codice, sono riconosciuti all'interessato i seguenti diritti:
diritto di informativa al momento della raccolta dei dati (art. 13; si veda paragrafo 4.3.1);
diritto di accesso (art. 7);
diritto di essere informato circa l'esistenza, presso l'Amministrazione, di dati che lo riguardano (art. 7, comma 1, D. Lgs. n. 196/2003);
diritto di essere informato circa i dati identificativi del Titolare e del Responsabile del trattamento, nonché in merito alle modalità e alle finalità del trattamento (art. 7, comma 2, lett. b) e d) D. Lgs. n. 196/2003);
diritto ad ottenere la cancellazione, la trasformazione in forma anonima, il blocco dei dati raccolti illegittimamente, l'aggiornamento, la rettifica o l'integrazione dei dati inesatti (art. 7, comma 3, lett. b) D. Lgs. n. 196/2003);
diritto di opporsi al trattamento dei dati ai fini di informazione commerciale, pubblicitaria, di vendita diretta o ricerche di mercato (art. 7, comma 4, lett. b) D. Lgs. n. 196/2003);
diritto al risarcimento del danno cagionato per l'effetto del trattamento di dati personali (art. 15 D. Lgs. n. 196/2003);
diritto di ricorrere al Garante per far valere i diritti sopra elencati (art. 145 D. Lgs. n. 196/2003).

**Esercizio dei diritti dell'Interessato**
La richiesta di accesso, ai dati personali che lo riguardano, può essere inoltrata dall'interessato al Titolare o al Responsabile senza formalità, anche verbalmente. Tuttavia il Garante ha predisposto un modello di richiesta informazioni, che si può scaricare dal sito internet www.garanteprivacy.it. .

Se l’interessato non ottiene risposta, potrà far valere il proprio diritto con ricorso all’Autorità giudiziaria o al Garante. Il ricorso al Garante non può essere proposto qualora, per il medesimo oggetto e tra le stesse parti, sia stata già adita l'Autorità giudiziaria.
Ai fini dell’esercizio dei diritti, l’interessato può conferire, per iscritto, delega o procura a persone fisiche o ad associazioni.
I diritti riferiti a dati personali di persone decedute, possono essere esercitati da chi ha un interesse proprio ad agire o agisce a tutela della persona deceduta o per ragioni familiari meritevoli di protezione.
L’identificazione dell’interessato è verificata sulla base di idonei elementi. La persona che agisce per conto dell’interessato, esibisce, o allega, copia della procura o della delega sottoscritta e presentata unitamente a copia fotostatica non autenticata di un documento di riconoscimento proprio e dell’interessato.
I dati sono estratti a cura dell’Incaricato e, ove sia possibile, la richiesta presentata dall'interessato viene soddisfatta in via informale e immediata, con comunicazione anche orale ovvero offerta in visione mediante strumenti elettronici. Se richiesto, si provvede alla trasposizione dei dati su supporto cartaceo o informatico ovvero alla trasmissione per via telematica.
Qualora non sia possibile l'accoglimento immediato dell'istanza, il Responsabile del trattamento deve provvedere nel minor tempo possibile, dandone comunicazione scritta all'interessato, e comunque non oltre 30 giorni dalla data di ricevimento della richiesta, come previsto dall’articolo 146, comma 3, del Codice.
Quando l’estrazione dei dati risulta particolarmente difficoltosa, il riscontro può avvenire mediante esibizione o consegna, in copia, di atti e documenti contenenti i dati personali richiesti.
La comunicazione è effettuata in forma intelligibile, anche attraverso l’utilizzo di una grafia comprensibile. In caso di codici o sigle sono forniti elementi per la comprensione del significato.
L’accesso ai dati personali è gratuito. Qualora, a seguito della richiesta di cui all’articolo 7, commi 1 e 2 del Codice, non risulti confermata l’esistenza di dati che riguardano l’interessato, può essere chiesto un contributo spese, non eccedente i costi effettivamente sopportati per la ricerca effettuata nel caso specifico.

## 5. MISURE DI SICUREZZA RELATIVE AI SERVER

I dati personali per cui la legge richiede la tutela con misure minime e idonee, vengono memorizzati, nella maggior parte dei casi, sui server di rete. Per questo motivo una particolare attenzione deve essere rivolta alle misure di sicurezza e di protezione relative ai server.

### 5.1 Misure di sicurezza organizzative

Il **Responsabile del trattamento/Dirigente** - d'intesa con l'Amministratore di sistema - **verifica** che la configurazione e l'utilizzo delle risorse presenti sul server di rete della propria struttura (unità logiche, cartelle) sia funzionale alle **esigenze di riservatezza** delle banche dati contenenti dati personali.
In particolare, verifica che la configurazione e l'utilizzo delle risorse di rete sia conforme all'impostazione di cui al Capitolo 7 *Misure di sicurezza relative alle risorse di rete e dei PC*, disponendo, in particolare, l'accesso differenziato, in base ad abilitazioni personali o per gruppi di lavoro e in relazione ai compiti svolti dal personale.

### 5.2 Misure di sicurezza logistiche

Per un'adeguata collocazione dei server, devono essere adottate le misure logistiche illustrate nei seguenti paragrafi, idonee a garantire la protezione delle apparecchiature rispetto ai seguenti rischi:
accesso fisico non autorizzato;
distruzione o perdita dei dati dovuta ad eventi fisici.

> L'Amministratore di sistema e i tecnici che hanno accesso ai locali del server devono informare il Dirigente/Responsabile del trattamento nel caso in cui riscontrino il mancato rispetto delle misure di sicurezza logistiche qui elencate (ad esempio locali server lasciati aperti o mancata custodia delle chiavi degli stessi).

#### 5.2.1 Protezione del server da accesso fisico non autorizzato

Per tutelare la riservatezza dei dati personali accessibili sul server e per proteggere l'efficienza delle apparecchiature, l'accesso ai locali in cui vi sono uno o più sistemi server è limitato nel seguente modo:

- le apparecchiature server devono essere poste in apposite stanze, destinate a contenere soltanto il server stesso ed eventualmente le apparecchiature di rete;
- ove sia logisticamente difficoltosa l'ubicazione del server in un apposito locale e per le strutture esistenti che non rispondono ai requisiti di cui al punto precedente, vanno cercate soluzioni organizzative alternative (es. armadi chiusi e appositamente allestiti) che offrano le medesime garanzie di sicurezza;
- l'accesso ai locali server è protetto tramite la chiusura a chiave del locale;
- la chiave è custodita da personale incaricato della custodia dal Responsabile del trattamento/Dirigente;
- il personale incaricato della custodia delle chiavi è tenuto a riporle in un luogo non agevolmente accessibile da altri;
- in sede di progettazione e di realizzazione di nuove strutture adibite ad uffici provinciali ovvero in sede di ristrutturazione di edifici esistenti, vanno tenute presenti le esigenze di tutela dei dati personali;
- se il locale è situato in una posizione tale da rendere agevole un'intrusione dall'esterno è opportuno munirlo della protezione adeguata, quale ad esempio l'apposizione di barre anti intrusione alle finestre;

In sede di progettazione di nuovi uffici, va tenuto presente che utilizzando, per la chiusura della stanza, dispositivi tecnici quali chiavi di tipo *badge* o chiavi di accesso in grado di consentire il rilevamento degli ingressi, è possibile assolvere, in via contemporanea, all'adempimento del controllo dell'accesso fisico al server ed al locale ed a quello relativo alla compilazione del registro degli accessi, che, in tal caso, non sarebbe richiesta.

**Accesso di personale interno della struttura**

Possono accedere ai locali in cui sono presenti uno o più sistemi server solo:
- il Dirigente/Responsabile del trattamento;
- l'Amministratore del sistema;
- il custode delle chiavi;
- il personale della struttura che deve accedervi per l'espletamento dei compiti propri, per le necessità di gestione e manutenzione dei sistemi (ad es. il personale preposto al cambio giornaliero delle cassette di backup), dei locali e degli impianti, nonché per attività di pulizia ed affini ed altre attività comunque indispensabili.

**Accesso di personale esterno alla struttura**

Gli interventi di manutenzione o adeguamento sui server, sui locali che li contengono e sui relativi impianti, sono richiesti, o comunque autorizzati, dal Dirigente/Responsabile del trattamento. Quando, per l'espletamento di compiti di servizio e per altre attività, è necessario consentire l'accesso a personale esterno o a personale dipendente della Provincia non appartenente alla struttura, vanno osservate le seguenti misure:
- il locale viene aperto dal personale custode delle chiavi;
- ciascun intervento è annotato su un apposito registro conservato nella stanza del server recante data e orario dell'intervento (inizio-fine), tipo di intervento, nome, cognome del tecnico intervenuto/Ditta o struttura, firma;
- al termine dell'intervento, l'incaricato della custodia della chiave provvede alla chiusura dei locali;
- nessun soggetto estraneo può accedere ai sistemi server se non accompagnato dal personale indicato nel paragrafo "Accesso del personale interno della struttura".

**Accesso di personale esterno alla struttura per servizi di pulizie o simili**

- Non sussiste la necessità di effettuare quotidianamente le operazioni di pulizia nella stanza contenente il server: le giornate in cui il personale addetto alle pulizie accede alla medesima sono programmate, anche al fine dell'apertura del locale;
- è preferibile che le operazioni di pulizia si svolgano quando è presente il personale addetto alla custodia della chiave, che provvede personalmente all'apertura;
- ove non sia possibile la presenza del personale addetto alla custodia della chiave, in quanto l'intervento di pulizia si svolge al di fuori dell'orario di servizio per altre cause ostative, in via eccezionale, il locale rimane aperto al fine di consentire l'ingresso del personale addetto, limitatamente ai periodi in cui è stato programmato l'intervento di pulizia;
- gli accessi sono registrati nell'apposito registro di cui sopra.

### 5.2.2 Protezione dei dati dal rischio di perdita dovuta ad eventi fisici

Tra gli eventi fisici, che possono portare alla perdita dei dati per distruzione delle apparecchiature, vengono considerati incendio, surriscaldamento delle apparecchiature, anomalie di alimentazione elettrica e altri eventi (allagamenti, crolli ecc.).

**Contromisure per il rischio di incendio**

Contro l'eventualità che un incendio, nei locali in cui sono custoditi i sistemi server, possa causare danni irreversibili ai dati sono necessarie le seguenti misure di sicurezza:
- in prossimità del server deve essere installato un dispositivo antincendio; in sede di progettazione e di realizzazione di nuove strutture adibite ad uffici provinciali ovvero in sede di ristrutturazione

di edifici esistenti, vanno tenute presenti le esigenze di sicurezza, ad es. dotando i locali di impianti di spegnimento automatico degli incendi;
- **le cassette di backup devono essere conservate in un armadio ignifugo, chiuso a chiave, dislocato in un locale diverso da quello che ospita il server.**

**Contromisure per le anomalie nell'alimentazione elettrica**

Contro l'eventualità che anomalie dell'alimentazione elettrica dei sistemi server possano danneggiare i dati, è necessario predisporre un collegamento ad un gruppo statico di continuità.

**Contromisure per altri eventi (allagamenti, crolli ecc.)**

In sede di progettazione e di realizzazione di nuove strutture adibite ad uffici provinciali ovvero in sede di ristrutturazione di edifici esistenti, vanno tenute presenti le esigenze di sicurezza evitando ad es. la collocazione dei locali contenenti i server in scantinati o piani seminterrati (a rischio allagamenti).

### 5.3 Misure di sicurezza tecniche, informatiche e procedurali

La sicurezza dei server deve essere tutelata con le misure tecniche, informatiche e procedurali illustrate nei seguenti paragrafi, idonee a garantire la protezione delle apparecchiature rispetto ai seguenti rischi:
- accesso logico non autorizzato o non conforme alle regole;
- distruzione o perdita dei dati dovuta ad attacchi esterni (es.: virus);
- distruzione o perdita dei dati dovuta ad attacchi di malintenzionati;
- perdita accidentale dei dati.

#### 5.3.1 Protezione da accessi logici non autorizzati

> Per **accesso logico**, nel contesto di questo documento, si intende l'accesso ai dati contenuti sul server attraverso l'utilizzo di un computer connesso in rete. Si tratta, cioè, dell'accesso e dell'utilizzo dei dati personali tramite i PC, collegati alla rete, a cui è connesso il server o dell'accesso ai dati dalla console del server stesso. L'accesso logico è permesso a chi digita la corretta combinazione di identificativo utente (user-id) e parola chiave (password).

I sistemi operativi consentono di:
- regolare l'accesso, disponendo di caratteristiche personalizzabili in grado di implementare vari gradi di sicurezza, garantendo contro il rischio di utilizzo dei dati da parte di persone non autorizzate;
- mantenere una traccia di tutti gli accessi (*log*), e quindi conoscere quando e che utente si è connesso al sistema e quali utenti hanno cercato di accedere a risorse non autorizzate.
- Per quanto riguarda le misure di sicurezza da adottare e i comportamenti che devono tenere gli utenti, si rinvia alle indicazioni riportate nel capitolo 7 *Misure di sicurezza relative alle risorse di rete e dei PC* e al capitolo 8 *Misure di sicurezza relative alle postazioni di lavoro*.

**Protezione all'accesso via RAS (Remote Access Server)**

RAS è un sistema che permette di accedere ad un server attraverso la linea telefonica. Nella struttura in cui sono presenti gli accessi via RAS, le misure minime da adottare sono le seguenti:
- assegnazione di identificativo (user-id) univoco ad ogni utente che deve accedere alla rete, associato ad una parola chiave criptata;
- definizione di utenti, o gruppi, con caratteristiche d'accesso differenti;
- registrazione di tutti gli accessi, per permettere la ricostruzione delle connessioni alla rete locale della struttura.

Le misure tecniche dovranno essere prese dall'Amministratore di sistema d'intesa con il Dirigente/Responsabile del trattamento dei dati.

### 5.3.2 Protezione dai virus

I virus sono particolari programmi, predisposti per essere eseguiti all'insaputa dell'utente, che possono causare danni ai dati memorizzati sul computer o al sistema operativo del computer stesso. Sui sistemi server l'Amministratore di sistema installa e provvede a mantenere un software antivirus, con aggiornamento periodico automatico via Internet, che garantisce una protezione idonea ad evitare il verificarsi di danni ai dati causati dai virus informatici.

### 5.3.3 Protezione da malintenzionati

> Ogni computer collegato in rete può essere oggetto di tentativi di connessione effettuati da soggetti che utilizzano altri computer collegati alla rete. Quando il computer è collegato a Internet, le intrusioni possono teoricamente essere effettuate da computer connessi a Internet situati in una qualsiasi parte del mondo.

Per fare fronte a questo rischio, i posti di lavoro ed i server della struttura sono collegati alla rete Internet attraverso la rete Telpat, per cui la protezione dalla distruzione o perdita dei dati, dovuta ad attacchi di malintenzionati che agiscono collegandosi dall'esterno, via Internet, è garantita dai sistemi *firewall* gestiti da Informatica Trentina s.p.a. .
**La difesa, dagli attacchi di questo tipo, è comunque assicurata solo se viene data puntuale applicazione a tutto il complesso delle regole di sicurezza comprese nel presente documento.**

### 5.3.4 Protezione dal rischio di perdita accidentale dei dati

Per ovviare al rischio di perdita accidentale dei dati, sui server è presente un sistema di salvataggio automatico degli stessi mediante copia automatica (backup).
Il salvataggio automatico:

- garantisce il recupero dei dati a fronte di guasti hardware o software, limitando i disagi connessi con la discontinuità del servizio;
- consente di recuperare dati o file accidentalmente eliminati o erroneamente modificati.

Per le politiche di back-up, occorre distinguere tra le risorse in gestione ad I.T. (e non connesse con il sistema di back-up centralizzato) e quelle in gestione a terzi.

**Politica dei backup e adempimenti dell'Incaricato:**

La maggior parte delle risorse in gestione ad I.T. sono connesse con il sistema centralizzato di back-up situato nel datacenter dell'azienda. Per queste, non è necessario nessun intervento locale ed il periodico salvataggio dei dati viene eseguito in maniera completamente automatizzata.
Il backup è gestito in automatico dal sistema server durante la notte (tra le 21:30 e le 24:00 di ogni giorno lavorativo);
a livello della struttura, nel caso di sistemi non connessi al sistema centralizzato di backup, sono presenti cinque cassette magnetiche (DAT, DLT o AIT), una per ogni giorno della settimana (da lunedì a venerdì), etichettate con il nome del giorno.
Il **referente informatico** della struttura, o altra persona incaricata dal Dirigente/Responsabile del trattamento, deve eseguire giornalmente le seguenti operazioni:
controllare, ogni mattina, l'esito del backup giornaliero (l'esito negativo del backup viene comunicato tramite e-mail al referente informatico della struttura): il file di log contiene il rapporto dettagliato di tutte le operazioni che il backup ha effettuato;
contattare, in caso di esito negativo del backup, l'Amministratore di sistema;

Nel caso di sistemi non connessi al sistema di backup centralizzato, è necessario ottemperare anche agli adempimenti seguenti:
sostituire, ogni mattina, sul sistema server, la cassetta magnetica contenete i dati di backup del giorno precedente con quella etichettata con il nome del giorno in corso;
collocare la cassetta contenente i dati di backup del giorno precedente, in un locale diverso da quello in cui è dislocato il sistema server, in armadi ignifughi chiusi a chiave; l'accesso agli armadi è consentito al solo personale autorizzato e deve essere protetto con misure di sicurezza fisiche non minori di quelle adottate per il server (in quanto le cassette contengono copia di tutti i dati presenti sul server);
provvedere alla manutenzione dell'unità nastro: utilizzare la cassetta di pulizia per mantenere sempre in buona condizione di funzionamento il lettore.

> E' consigliabile conservare per un anno la cassetta relativa all'ultimo backup di ogni mese; le cassette vanno sostituite dopo circa 50 cicli di utilizzo e/o comunque seguendo le istruzioni del costruttore.

**Sistemi server non gestiti da Informatica Trentina s.p.a.**

La politica di backup va concordata con il Dirigente del servizio competente in materia di informatica e deve assicurare almeno le medesime garanzie di efficienza e sicurezza fornite dal sistema di cui sopra e comunque il rispetto delle misure minime di sicurezza previste nell'Allegato B del Codice privacy.
La responsabilità, del rispetto delle misure di sicurezza, grava sul Dirigente della struttura che utilizza il server non gestito da Informatica Trentina.

# 6. MISURE DI SICUREZZA RELATIVE ALLA RETE DI INTERCONNESSIONE (Telpat)

## 6.1 Misure logistiche

Per un'adeguata collocazione delle apparecchiature di rete della Provincia, devono essere adottate, in quanto compatibili, le misure logistiche già illustrate nel capitolo 5 sui Server. Va ricordato, infatti, che la sicurezza dell'intera rete può essere messa a rischio se un malintenzionato ottiene l'accesso fisico, per un tempo sufficiente, ad una o più apparecchiature di rete.

## 6.2 Regole per connettersi alla rete Telpat (rivolto agli enti ai quali la Provincia mette a disposizione la rete)

La rete Telpat, negli anni, ha subìto significativi mutamenti, sia relativamente alla infrastruttura tecnologica che alla sua funzione. E' passata, infatti, da uno stato di "Rete chiusa", che ha caratterizzato l'inizio della sua storia, con lo specifico scopo di condividere informazioni con altri soggetti della Provincia, a rete connessa con Internet, fino alla situazione attuale nella quale, di fatto, è un network, di vaste dimensioni, a cui possono accedere tutti i soggetti della amministrazione pubblica locale della Provincia di Trento, per usufruire di servizi informativi centralizzati.

Il ruolo acquisito ha, necessariamente, innalzato il livello di criticità della disponibilità del servizio di connettività, riducendo drasticamente il controllo che la Provincia può esercitare sui siti periferici interconnessi. Infatti, se risulta chiaramente evidente che un non corretto funzionamento della rete può causare gravi disservizi (un esempio per tutti la posta elettronica), non è altrettanto chiaro che la Provincia, ovvero il soggetto che mette a disposizione di tutta la pubblica amministrazione locale questo fondamentale servizio, non ha, di fatto, la possibilità di controllare che le reti locali collegate rispettino un set minimo di misure di sicurezza che, oltre ad essere in gran parte previste dalla normativa vigente, riduca notevolmente il rischio di compromettere la rete provinciale.

Lo scopo di questo paragrafo è definire degli standard minimi di misure di sicurezza per tutti gli enti della pubblica amministrazione locale che si interconnettono con la rete provinciale. Gli standard sono stati elaborati per minimizzare l'esposizione della rete provinciale ai pericoli derivanti da reti, scarsamente protette, che fungono quali teste di ponte per virus, intrusioni informatiche, spyware etc..

I pericoli che si intendono evitare sono la perdita di dati, il danneggiamento o malfunzionamento dei sistemi e/o della rete provinciale, etc..

### 6.2.1 Misure minime di sicurezza per l'utilizzo della rete Telpat

Gli enti, che si interconnettono con la Telpat, devono garantire, per la loro struttura informatica, l'applicazione delle misure minime di sicurezza specificate nell'Allegato "B" del D.Lgs. 196/03 ed in particolare che:

- gli apparati informatici siano provvisti di una procedura che prevede l'autenticazione univoca dell'operatore;
- agli operatori siano impartite idonee istruzioni, sull'adozione delle necessarie cautele, per assicurare la riservatezza delle informazioni ed il corretto funzionamento dei sistemi, con l'obiettivo di non causare malfunzionamenti nella rete;
- vengano disattivate le credenziali di autenticazione degli operatori non più in servizio;
- agli operatori siano impartite istruzioni per non lasciare incustodito e accessibile lo strumento elettronico;
- venga effettuata una verifica periodica degli operatori abilitati;
- gli strumenti informatici siano dotati di software antivirus con aggiornamenti periodici.

In aggiunta a quanto previsto dalla succitata normativa (D.Lvo 196/2003), sarà cura dell'ente garantire che la propria rete locale non abbia altre connessioni di rete con l'esterno, ad eccezione del collegamento con Telpat salvo i casi di cui al successivo paragrafo.

### 6.2.2 Ulteriori misure

Nel caso in cui, per improrogabili necessità operative, l'ente sia dotato di un ulteriore collegamento geografico (es. connessione ad Internet con un operatore pubblico), ovvero si trovi nella necessità di dover garantire, a terzi, accessi remoti, alla propria rete, non verificabili dalla Provincia, (es. per ragioni di assistenza tecnica o di connettività ad Internet), dovrà darne immediata comunicazione all'Ufficio Sicurezza di Informatica Trentina affinché venga installata un idoneo apparato hardware (firewall) per garantire la difesa perimetrale

## 7. MISURE DI SICUREZZA RELATIVE ALLE RISORSE DI RETE E DEI PC

L’operatore, tramite la procedura di accesso logico, che prevede l’utilizzo di un identificativo utente (user-id) e di una password, può accedere ad una stazione di lavoro (PC) connessa alla rete della struttura. In questo modo l'operatore può:

accedere alle risorse presenti fisicamente sulla macchina stessa (dischi fissi);
accedere alle risorse di rete (cartelle del disco fisso del server su cui l'utente ha diritto di accesso);
condividere con altri utenti risorse quali file, cartelle (ad es. dischi U e T) e stampanti;
condividere con altri utenti applicazioni;
usufruire della centralizzazione delle operazioni di backup (nel caso in cui i dati siano salvati sul server) e di aggiornamento software.

### 7.1 Descrizione della configurazione standard delle stazioni di lavoro

Le unità logiche disponibili, in base alle configurazioni standard dei server amministrati da Informatica Trentina , sono in sintesi le seguenti:

**A) Unità locali del computer**

**C:\ D:\ (individuata anche con lettere diverse)** = Unità logiche/dischi installati fisicamente sul PC, altrimenti detti dischi fissi o locali.
**Unità escluse dalla garanzia del salvataggio automatico dei dati (backup notturno) attiva sul server.** Da ciò derivano rischi per la sicurezza dei dati e la loro conservazione, se non vi è un accorto utilizzo del computer e un salvataggio coscienzioso dei dati. L'utente deve evitare di conservare i dati di cui va garantita la sicurezza su queste unità. Infatti è sempre possibile che il danneggiamento del computer porti alla perdita dei dati. In secondo luogo, per quanto difficile, non è del tutto impossibile che vi sia un accesso fisico alla macchina in assenza dell'utente anche da parte estranei. Per il malintenzionato che ottiene l'accesso fisico alla macchina, l'accesso ai dati presenti sulla macchina stessa non presenta particolare difficoltà.

**B) Unità di rete individuale**

**Y:** = L’Unità logica/Disco Y è la cartella individuale dell'utente sul server di rete. L’accesso è, cioè, consentito all'utente che si è correttamente autenticato all'atto di accedere al PC locale collegato in rete. Questo disco deve essere usato per memorizzare dati che non necessitano di essere condivisi con altri utenti (quelli per cui gli altri non hanno l’incarico al trattamento o dati riservati).
*Ogni utente può vedere sempre e solo la propria cartella personale, e non quelle degli altri utenti. Per contro, l'Amministratore di sistema può vedere e modificare le cartelle e i dati di tutti.* Gli utenti hanno accesso in lettura e scrittura al proprio disco Y. Per l'unità Y è garantito il salvataggio automatico dei dati (backup notturno).
*Tale disco logico ha una capacità standard di base per ogni*

*utente, ampliabile su richiesta motivata.*

Nota Bene: se si accede alla rete della struttura utilizzando il proprio identificativo utente e la propria password da un **qualsiasi PC** connesso si avrà accesso al **proprio disco Y**. In altre parole, in caso di malfunzionamento o arresto momentaneo della propria stazione di lavoro, l'utente può servirsi della stazione di lavoro di un collega per accedere ai propri dati conservati sul disco Y (Solo per i pc della stessa struttura).

**C) Unità di rete comuni**

**T:** = Unità logica/Disco di Transito utilizzabile per il passaggio di dati tra utenti. Unità **esclusa** dalla garanzia del salvataggio automatico dei dati (backup notturno). Infatti il disco T non rientra nel backup giornaliero.
**Tutti gli utenti hanno accesso a T:\ in lettura e scrittura, anche sui file di altri utenti**.
NB: tale disco deve essere assolutamente **utilizzato solo come transito** di dati e programmi da un utente all'altro; ogni fine settimana, infatti, il disco T:\ viene cancellato per recupero spazio.
I dati pertanto vanno spostati su altro disco di rete e cancellati dal disco T:\ dopo il loro utilizzo.
Nel caso di server centralizzati, il disco T:\ è comune per tutti gli utenti della Provincia

**U:** = Unità logica/Disco dati degli utenti. Unità garantita dal **salvataggio automatico dei dati** (backup notturno). Questa Unità logica/Disco, all'inizio accessibile a tutti gli utenti sia in lettura sia in scrittura**, consente una personalizzazione dei diritti di accesso**. Questa personalizzazione di norma va richiesta all'Amministratore di sistema che può creare dei gruppi di utenti secondo le esigenze della struttura. Può anche essere operata dagli stessi utenti all'atto della creazione di una nuova directory. In questo caso l'utente che ha creato la directory mantiene anche la possibilità di cambiare le regole di accesso degli altri utenti a quella particolare directory. Ogni directory può possedere delle restrizioni che permettano l'accesso personalizzato solo a determinati utenti, individuati a seconda del gruppo di lavoro cui appartengono o delle specifiche competenze/esigenze del singolo utente. Tali diritti di accesso personalizzato (ad es. sola lettura, lettura e modifica, cancellazione su singoli file o directory), sono connessi all'account dell'utente già esistente e non richiedono pertanto la creazione di nuovi identificativi di utente. L'unità U:\ deve essere utilizzato per i documenti che devono essere condivisi tra più persone della struttura e che devono essere salvati sul backup giornaliero.

Il disco pertanto va organizzato, di norma, creando delle directory protette, tenendo conto dei gruppi di lavoro esistenti all'interno dei servizi.

A fronte di particolari esigenze nella configurazione della rete e dei PC, le Unità logiche/dischi potrebbero essere individuate da lettere diverse rispetto a quelle sopra indicate. In questo caso è necessario contattare l'Amministratore di sistema al fine di censire la situazione della propria struttura.

### 7.2 Misure di sicurezza informatiche

In base alla configurazione appena descritta vanno adottate le seguenti misure:
va privilegiato per la memorizzazione dei dati l'utilizzo delle risorse di rete (Y e U) evitando l'uso delle unità logiche presenti fisicamente sul PC (dischi fissi/locali C e D);
in ogni caso le elaborazioni riguardanti dati personali vanno memorizzate sui dischi di rete U e Y;
anche se alcuni programmi applicativi consentono la protezione dei singoli file mediante l'apposizione di specifiche password tale pratica va evitata.

**Cartelle con accesso per gruppi di lavoro sull'unità U**

Per un ottimale utilizzo delle risorse di rete, sono predisposti sul disco U cartelle con accesso limitato per gruppo di lavoro (alcuni in scrittura, altri in lettura)**.**
È così possibile usare cartelle a supporto della divisione del lavoro per gruppi (chi svolge le medesime attività può condividere i dati con i colleghi) senza sacrificare la sicurezza dei dati, in quanto l'accesso è limitato solo a chi, nell'ambito della struttura, è effettivamente Incaricato del trattamento dei dati. L'uso del disco U non richiede la creazione di ulteriori user-id e password, in quanto i gruppi di utenti vengono creati sulla base degli utenti già esistenti.

> L'organizzazione del disco U per gruppi di lavoro richiede un'analisi delle esigenze organizzative della struttura, per individuare la configurazione adatta e la creazione da parte dell'Amministratore di sistema di gruppi di abilitazione, nei quali gli utenti saranno inseriti a seconda delle attività cui sono preposti.

Ciascun utente, con l'user-id e la password di accesso alla rete è contemporaneamente abilitato all'accesso alle sole cartelle protette del disco U riservate ai gruppi di lavoro a cui appartiene.
Il responsabile della struttura deve segnalare la variazione della composizione dei gruppi all'Amministratore di sistema per l'adeguamento delle abilitazioni; l'Amministratore deve configurare i permessi sul disco U e la composizione dei gruppi di lavoro. L'eventuale presenza sul disco U di cartelle denominate secondo la comune identificazione dei gruppi di lavoro (ad esempio "segreteria del Dirigente"), su cui non vengono applicate limitazioni coerenti con la denominazione stessa (cioè accesso non limitato al solo gruppo ma indifferenziato per tutti gli utenti della struttura), ***costituisce una falla nella sicurezza perché può indurre gli utenti a ritenere protetta la memorizzazione nella cartella stessa***.

> Per questo motivo l'Amministratore di sistema e il responsabile della struttura si devono attivare al fine di verificare la correttezza delle limitazioni di accesso sul disco U. A tal fine l'Amministratore di sistema deve segnalare periodicamente al referente informatico e al responsabile della struttura quali utenti fanno parte dei gruppi di lavoro che hanno accesso alle cartelle della directory principale dell'unità U.

**Trattamento dei dati di responsabilità di un unico Incaricato**

Per la memorizzazione dei dati che devono rimanere riservati e visibili al solo utente Incaricato del trattamento, va data priorità all'utilizzo del disco Y anziché dei dischi fissi/locali. Infatti, come si è

visto sopra le esigenze di riservatezza e sicurezza sono garantite solo memorizzando i dati sul server.

**Uso dei dischi fissi/locali (C:\ e altri)**

L’utilizzo dei dischi fissi/locali, presenta inconvenienti sotto il profilo della sicurezza dei dati. Pertanto, se non è possibile usare le unità di rete (Y e U), è responsabilità dell’utente effettuare backup periodici.

## 8. MISURE DI SICUREZZA RELATIVE ALLE POSTAZIONI DI LAVORO

Per postazione di lavoro si intende il complesso delle apparecchiature che il datore di lavoro (Provincia) mette a disposizione dei dipendenti (utenti).

### 8.1 Misure di sicurezza logistiche

Una adeguata protezione dei **luoghi di lavoro** serve a garantire la sicurezza dei dati personali custoditi al loro interno. Per garantire questa sicurezza vanno adottate misure logistiche idonee ad assicurare la protezione di documenti, supporti informatici e apparecchiature rispetto al rischio di:
- accesso fisico non autorizzato;
- distruzione o perdita dei dati dovuta ad eventi fisici.

#### 8.1.1 Protezione delle postazioni da accesso fisico non autorizzato

Per accesso fisico s'intende l'accesso ai locali in cui vi sono uno o più postazioni di lavoro dotate di PC. Le misure di sicurezza devono eliminare o ridurre il rischio di accesso fisico ai locali o intrusione da parte di persone non autorizzate. L'accesso fisico alla postazione di lavoro collegata in rete, da parte di estranei non identificati, rappresenta comunque un potenziale rischio per la sicurezza dei dati custoditi sul server della rete, anche se la persona non può conoscere le password. Per evitare questo rischio, si devono adottare le seguenti misure di sicurezza:

##### 8.1.1.1 personale interno alla struttura

- le postazioni di lavoro sono accessibili solo da quanti ne hanno titolo, in qualità di Responsabili o Incaricati del trattamento, di Amministratori del sistema, o altro, nei soli limiti in cui ciò sia funzionale allo svolgimento dei compiti della struttura o per lo svolgimento di attività di manutenzione, di pulizia e affini, nonché per altre attività comunque indispensabili;
- l'accesso fisico ai luoghi di lavoro è protetto tramite la presenza di personale di portineria ovvero tramite la chiusura delle vie di accesso;
- in ogni caso, gli uffici aperti al pubblico devono essere presidiati da personale di portineria; negli orari diversi da quelle di servizio, ove non vi sia comunque un presidio, la porta di accesso all'edificio deve rimanere chiusa.

##### 8.1.1.2 personale esterno alla struttura

- la persona esterna può accedere ai locali solo quando è presente qualche addetto;
- la persona esterna deve farsi riconoscere dal personale di portineria e seguire le regole stabilite dal responsabile per l'accesso del pubblico alla struttura;

##### 8.1.1.3 Interventi di assistenza e manutenzione

###### 8.1.1.3.1 Assistenza in remoto

Gli interventi di assistenza, installazione e aggiornamento dei software e, in generale, quelli volti a fronteggiare guasti o temporanei black-out nel funzionamento delle postazioni di lavoro, sono di norma effettuati da Informatica Trentina tramite il servizio di assistenza e amministrazione remota sui PC e sui server di rete denominato *System Management*, senza la necessità dell'intervento di un tecnico informatico presso la postazione di lavoro. In caso di guasto, o malfunzionamento, del proprio PC, l'utente può attivare l'intervento di assistenza remota, contattando telefonicamente il Customer service Desk di Informatica Trentina.

###### 8.1.1.3.2 Assistenza con intervento locale del tecnico

Se invece sono necessari interventi di manutenzione sulla macchina o di assistenza, adeguamento, ecc. presso la postazione di lavoro, è necessario che l'utente o il referente informatico o, in loro assenza, altro dipendente della struttura, assista alle operazioni di manutenzione.
La segreteria deve trattenere e conservare copia del rapporto di intervento rilasciato dalla ditta intervenuta. Tale rapporto deve contenere data e orario dell'intervento (inizio e fine), descrizione

sintetica del tipo di intervento, nome e cognome del tecnico intervenuto e della ditta, firma del tecnico e dell'utente che assiste all'intervento. Ove non già presenti nello schema, tali dati devono essere apposti dal personale di segreteria in presenza del tecnico intervenuto. **La descrizione dell'intervento non può contenere codifiche dal significato non immediatamente comprensibile per l'utente che sottoscrive il rapporto.**

### 8.1.2 Protezione dei dati dal rischio di distruzione o perdita a causa di eventi fisici

Gli eventi fisici, che possono costituire fonte di rischio per le postazioni di lavoro, sono quelli indicati nel paragrafo relativo ai server.
Al fine di ridurre al minimo i rischi di distruzione o perdita di dati, è consigliabile:
prediligere il lavoro sui dischi di rete, la cui protezione è assicurata dalle misure di sicurezza e di salvataggio automatico adottate per i server;
in caso di utilizzo dei dischi installati fisicamente sul PC (C e D), vanno effettuati periodici backup dei dati su supporti magnetici, da conservare secondo quanto disposto nell'apposito paragrafo.
Si ribadisce che, in quest'ultimo caso, la responsabilità di effettuare backup periodici è a carico dell'utente.

## 8.2 Misure di sicurezza tecniche, informatiche e procedurali

### 8.2.1 Protezione da accessi logici non autorizzati

L'accesso logico alle postazioni di lavoro è consentito attraverso l'utilizzo combinato di una parola chiave (password) e di un identificativo utente (user-id) che autentica l'utente sul server della rete. In assenza dell'autenticazione, la postazione non è immediatamente utilizzabile. A ciascun utente, all'assegnazione della dotazione informatica, viene attribuito un identificativo utente (user-id) univoco ed immutabile ed una password personale, segreta e sostituibile dall'utente stesso. La password e il codice identificativo sono personali.
Pertanto vanno osservate le seguenti misure di sicurezza:
evitare di rendere note le password. E', in primo luogo, interesse dell'utente evitare che altri utilizzino la sua password d'accesso: infatti, dalla registrazione dell'attività effettuata dal sistema, risulterebbe a lui attribuito il trattamento effettuato da altri, con connessa responsabilità in caso di trattamenti scorretti o non autorizzati o illeciti;
evitare di trascrivere le password su supporti agevolmente accessibili da parte di terzi;
evitare di utilizzare codici di accesso di personale nel frattempo cessato, assente per lungo periodo o che è stato assegnato ad altra struttura o attività.

> Il Dirigente è tenuto - in caso di entrata in servizio, cessazione, mobilità o cambio di mansioni del personale assegnatario di dotazioni informatiche - a provvedere alla richiesta dei relativi nuovi inserimenti, delle cancellazioni o delle modifiche alle abilitazioni utente che si rendano necessarie secondo le modalità individuate con la procedura operativa per la gestione delle richieste di attività IMAC, nell'ambito del servizio di Change Management.

L'accesso ai dati, per ragioni di lavoro, da parte dei colleghi dell'Incaricato assente, può essere facilmente ottenuto utilizzando le cartelle del disco U per tutte le attività che prevedono la collaborazione di più utenti. Nel caso invece di trattamenti di dati con un singolo Incaricato, se il Responsabile del trattamento deve accedere ai dati in sua assenza, può fare richiesta all'Amministratore del sistema di venire, transitoriamente, abilitato ad accedere alla cartella che li contiene. Si ricorda che **l'Amministratore di sistema non ha modo di conoscere le password degli altri utenti** (che sono conservate sul server in forma cifrata), tuttavia l'utente amministratore ha sempre accesso diretto e immediato a tutti i dati e può abilitare a questo accesso anche altri

utenti. **I dati quindi sono sempre reperibili anche in assenza della persona che conosce la password.**
L'utente è tenuto a:
sostituire la password ad intervalli regolari; il sistema consente la sostituzione della password da parte dell'utente; il sistema consente anche di impostare, per tutta la rete, un vincolo che impone a tutti gli utenti di cambiare le password entro periodi prestabiliti. La password deve essere cambiata dall'utente al primo utilizzo e, successivamente, ogni sei mesi. La parola chiave deve essere composta da almeno otto caratteri oppure, nel caso di sistemi che non lo prevedono, dal numero di caratteri massimo consentito**;**
rendere inaccessibile il sistema dalla propria postazione di lavoro ogni volta che si assenta; ciò si ottiene utilizzando la funzione di blocco *workstation* del sistema (che viene attivata premendo contemporaneamente i tasti Ctrl/Alt/Canc e cliccando sul bottone "blocca computer");
impostare uno *screen saver* automatico protetto da password con tempo di attivazione inferiore ai 10 minuti di inattività della macchina;
se accede alla rete da una postazione di lavoro non assegnatagli, usare il proprio identificativo utente e la propria password e non chiedere di utilizzare la password del collega.

### 8.2.2 Protezione da accessi logici non autorizzati a PC non connessi alla rete

Per l'accesso logico ai PC stand-alone, cioè PC non connessi al server di rete della struttura, bisogna adottare, prima dell'inizio del trattamento dei dati personali, le seguenti misure:
se il sistema operativo lo consente, impostare password e user-id per l'accesso logico al PC, che vanno fornite a ciascun Incaricato del trattamento di dati personali;

### 8.2.3 Protezione da accessi logici, non autorizzati, agli applicativi

L'accesso logico alla posta elettronica, e ad altri programmi applicativi, può essere protetto da parola chiave, associata o meno ad un user-id. Per quanto riguarda gli applicativi, vanno osservate le seguenti disposizioni:
le applicazioni che trattano dati personali, devono essere protette con una specifica password di accesso all'applicazione stessa, oltre alla parola chiave di accesso al sistema;
la password e l'eventuale codice identificativo sono personali; pertanto devono essere adottate le cautele previste nel paragrafo 8.2;
se necessario, la creazione, la modificazione e la cancellazione delle abilitazioni vengono richieste dal Dirigente/Responsabile del trattamento secondo le modalità individuate con la procedura operativa per la gestione delle richieste di attività IMAC, nell'ambito del servizio di Change Management.

### 8.2.4 Protezione dai virus

I PC connessi in rete sono protetti da un prodotto antivirus, installato e connesso ai sistemi server, con aggiornamento periodico automatico a carico dell'Amministratore di sistema.
Sui PC stand alone è invece necessario installare un prodotto antivirus ad hoc che, per risultare efficace nel tempo, dovrà essere aggiornato periodicamente secondo le modalità richieste dal prodotto stesso. L'aggiornamento è a carico dell'Amministratore di sistema (cioè Informatica Trentina nel caso dei PC registrati nell'inventario centralizzato).
Per maggiori dettagli sui virus, e sulle loro caratteristiche, vedi il capitolo relativo alla protezione dei server al punto 5.3.2.

### 8.2.5 Protezione dai malintenzionati

I posti di lavoro ed i server delle strutture provinciali sono collegati alla rete Telpat; la protezione in relazione alla possibile distruzione o perdita dati dovuta ad attacchi esterni da parte di malintenzionati, via Internet, è effettuata dal *firewall* gestito da Informatica Trentina s.p.a.. **Si ricorda comunque che la difesa, dagli attacchi di questo tipo, è assicurata solo se viene data**

**puntuale applicazione a tutto il complesso delle regole di sicurezza comprese nel presente documento.**

### 8.2.6 Protezione dal rischio di perdita accidentale dei dati

Per i dati contenuti nei dischi di rete, viene effettuato un *backup*, programmato in automatico dal sistema server durante la notte, su apposite, cassette da sostituire giornalmente.
Per i dati contenuti nei dischi installati fisicamente sul PC (C:\ e D:\) è necessario, invece, che ciascun operatore provveda a periodici backup dei dati su supporti magnetici e alla conservazione dei supporti stessi nel rispetto delle disposizioni individuate al paragrafo 8.5 *Misure di sicurezza relative ai supporti di memorizzazione*.
Si consiglia, comunque, di utilizzare i dischi del PC come sistema di memorizzazione dei dati solo quando non sono disponibili unità di rete, mentre la memorizzazione sulle unità di rete messe a disposizione dal server **deve rappresentare la regola**.

### 8.2.7 Accesso ai dati in assenza dell'Incaricato

Qualora, in caso di assenza dell'Incaricato assegnatario della dotazione informatica, ovvero della casella di posta elettronica, si renda necessario, per ragioni improrogabili, l'utilizzo di dati accessibili in via esclusiva con i suoi codici di accesso, si devono rispettare le seguenti regole:

**Procedura operativa per l'accesso, in assenza dell'Incaricato, a dati presenti su server, PC o casella di posta elettronica**

**A. Premessa**
In merito all'accesso a dati memorizzati sul server si ricorda che:
**(a1)** per salvataggio dei dati/documenti comuni della struttura, che devono essere accessibili a più utenti, è opportuno che vengano utilizzate cartelle collocate su dischi di rete sul server dipartimentale, opportunamente condivise e protette, e accessibili a più di un soggetto.
**(a2)** allo stesso modo, per quanto riguarda le caselle di posta elettronica, si consiglia la creazione e l'utilizzo di caselle di posta di struttura, opportunamente condivise e protette, e accessibili a più di un soggetto per le comunicazioni di lavoro che possono necessitare di una consultazione da parte di più utenti.

**B. Regole per l'accesso ai dati di un utente**
Qualora si possa prevedere con anticipo l'assenza di un Incaricato, la quale, a sua volta, impedisca l'accesso a dati, o e-mail, di interesse per la struttura, è possibile seguire procedure preventive che permettano l'accesso alle informazioni anche nel caso di irreperibilità dell'Incaricato.
Di norma, nei dischi in locale (es. disco C: o D:), non dovrebbero transitare dati; nel caso in cui sulle unità C o D si trovino dei dati, i medesimi devono essere copiati, su una cartella, in un disco di rete accessibile a più utenti autorizzati.
Per l'accesso alla casella di posta, l'Incaricato ha la possibilità di effettuare una "delega", per l'accesso alla propria casella e-mail da parte di altri utenti Lotus. La delega deve essere impostata, direttamente, dall'utente titolare della casella.

**C. Caso residuale: come fare se si deve comunque accedere a dati di un utente in sua assenza**
Premesso che non è consentito l'utilizzo dei codici di accesso di personale assente, cessato o assegnato ad altra struttura, qualora, malgrado gli accorgimenti sopra descritti, ci si trovi nelle condizioni di dover accedere ai dati in assenza dell'Incaricato, è possibile adottare la procedura descritta più avanti. Si ricorda che l'accesso è consentito solo se sussistono le seguenti condizioni: improrogabile necessità di accedere ai dati, per ragioni di servizio; accertata impossibilità, o notevole difficoltà, di raggiungere l'utente; comunicazione, al dipendente assente, da parte del Dirigente/Responsabile del trattamento, dell'accesso alle sue risorse.

**C1. Accesso a dati presenti su server, o PC, in assenza dell'Incaricato, unico titolare del permesso di accedere alla cartella.**

1. Qualora si presenti la necessità di accedere a dati contenuti in una cartella protetta, presente sul server, e gli Incaricati abilitati all'accesso a tale cartella siano irreperibili, il Responsabile del trattamento (Dirigente) può chiedere che il proprio account e/o quello di altri Incaricati siano abilitati all'accesso a tale cartella.
2. Qualora i dati a cui si intende accedere, siano contenuti su una porzione di disco privato di un utente (es disco Y:\ o cartella "Documenti" in locale sul PC) e l'utente abilitato all'accesso sia irreperibile, il Responsabile del trattamento (Dirigente) può chiedere che i dati di interesse siano copiati in una cartella sul server e che il proprio account e/o quello di altri Incaricati siano abilitati all'accesso a tale cartella.

La richiesta deve essere inoltrata al CSD.

**C2. Accesso, in assenza dell'Incaricato, a casella di posta elettronica presente sul server.**

Qualora si presenti la necessità di accedere a dati contenuti in una casella di posta elettronica, e l'Incaricato (titolare della casella) abilitato all'accesso a tale cartella sia irreperibile, il Responsabile del trattamento (Dirigente) può chiedere che il proprio account e/o quello di altri Incaricati siano abilitati all'accesso a tale casella.

La richiesta deve essere inoltrata al CSD.

Le attività possono essere eseguite da remoto.

### 8.2.8 Procedura di ripristino password

Premessa

**La procedura di seguito descritta entrerà in vigore nel momento in cui sarà realizzato il relativo software; fino a tale termine, si applicherà la procedura di ripristino password disciplinata nella deliberazione della Giunta provinciale n. 232/2007 – Allegato B, che, di conseguenza, continuerà, per la parte specificata, ad esplicare i suoi effetti. Informatica Trentina è tenuta a sostituire la procedura in vigore entro e non oltre 4 mesi dalla data di pubblicazione della presente deliberazione.**

**Gli accessi alle applicazioni informatiche, della Provincia autonoma di Trento, sono protetti da password. Per garantire un adeguato livello di sicurezza, le credenziali di accesso sono protette nei modi seguenti: a) dopo 6 mesi di mancato utilizzo, scadono; b) dopo 7 tentativi errati, vengono bloccate per un'ora.**

**Al fine di ripristinare l'accesso alle applicazioni, nelle ipotesi in cui le credenziali siano scadute, bloccate o smarrite, è utilizzabile una procedura di riattivazione che, conformemente alla normativa vigente in materia di sicurezza, risulti caratterizzata da tempi minimi di ripristino.**

**La procedura assicura che la password sia consegnata esclusivamente all'utente, e che venga, sempre, notificato, sulla casella di posta elettronica istituzionale personale, l'avvio della procedura di ripristino.**

Ciascuna applicazione informatica, al primo accesso con la password fornita dal processo di ripristino, richiede, all'utente, di inserirne una nuova. L'applicazione verifica anche che siano rispettati i requisiti minimi di complessità, conformi a quanto previsto al punto 5 dell'allegato B del D. l.gs. 196/2003.

Il processo di ripristino password parte da una richiesta, dell'utente, che riporta il proprio codice fiscale e l'applicazione interessata.

Il procedimento, le basi dati, gli operatori e quanto necessario per soddisfare la richiesta di ripristino, verranno di seguito indicati come “sistema”.

**Portale ripristino password**

La procedura descritta sarà attivabile, **all’indirizzo web: http://password.provincia.tn.it.**, quando sarà realizzato il propedeutico e necessario software.

**Il portale permette agli utenti di:**

1. richiedere il ripristino della password;
2. controllare la correttezza dei dati personali, e di ambiente, oltrechè inoltrare le eventuali richieste di modifica;
3. controllare il registro dei ripristini password e delle modifiche dei dati inseriti.

Di seguito, il portale del ripristino password verrà indicato come “portale”.

**Dati archiviati**

Nel portale, a cura dell’utente o del sistema, vengono memorizzate le seguenti informazioni:

a) Codice fiscale;
b) Nome e Cognome;
c) Matricola;
d) Indirizzo della casella di posta elettronica personale istituzionale (nome.cognome@provincia.tn.it);
e) Indirizzo postale del luogo di lavoro;
f) Indirizzo postale della segreteria di riferimento;
g) Numero di cellulare di servizio (se disponibile);
h) Indirizzo della casella di posta personale (facoltativo, a discrezione dell’utente);
i) Numero di cellulare personale (facoltativo, a discrezione dell’utente);

**Aggiornamento dei dati da parte dell’utente**

Per accedere alle funzioni di aggiornamento dei dati del portale, l’utente deve essere autenticato: l’autenticazione avviene attraverso l’accesso alla propria postazione di lavoro o tramite apposita procedura.

I dati personali, relativi all’indirizzo della casella di posta elettronica e al numero di cellulare, possono essere inseriti ed aggiornati dall’utente. Gli altri dati sono inseriti e aggiornabili, attraverso il sistema, automaticamente o su richiesta dell’utente.

Ad ogni inserimento ed aggiornamento di dati, da parte dell’utente, il sistema ne controlla e ne verifica la correttezza e la validità, inviando messaggi di test agli indirizzi ed ai numeri specificati con la richiesta di risposte di conferma.

**I dati sono modificabili dall’utente, direttamente o tramite richiesta al sistema, solamente se non vi sono richieste di ripristino password pendenti.**

Le modifiche dei dati, e le richieste di ripristino password, vengono notificate all’utente, riportando le informazioni indicate nel registro degli accessi sul portale descritto di seguito.

**Obbligo di aggiornamento dei dati da parte dell’utente**

È fatto obbligo, a ciascun utente, di mantenere aggiornate tutte le informazioni che lo riguardano: correggendo, direttamente, i dati sui quali è autorizzato ad apportare modifiche o segnalando al sistema gli altri dati, utilizzando l’apposita funzione “Segnalazione dati errati”.

Nel caso tale obbligo non venisse rispettato e il sistema non reperisse informazioni relative all'utente che ha richiesto il ripristino, la segnalazione va inoltrata al CSD di Informatica Trentina, che provvederà a comunicare la password ripristinata, in busta chiusa, all'indirizzo postale della segreteria di riferimento, segnalando l'evento al Dirigente competente, per valutare gli effetti sull'attività lavorativa e gli eventuali disservizi determinati.

**Registro delle attività nel portale delle password**

Il portale, previa autenticazione, consente di controllare gli accessi effettuati, sia per le modifiche dei dati che per le richieste di ripristino password.
Il registro, per ogni richiesta di ripristino password e ogni richiesta di aggiornamento dei dati, contiene la data e l'ora della richiesta, l'indirizzo IP dal quale è stata inoltrata, gli estremi dell'utente richiedente, la tipologia, l'applicazione di riferimento.
Il registro è visualizzabile, e scaricabile.
A seconda del ruolo dell'utente, le registrazioni possono essere visibili a diversi livelli (ad esempio relative al solo utente, alla/e struttura/e organizzativa/e alla/e quale/i è abilitato o a tutte le strutture provinciali).

**Richiesta di ripristino della password**

La richiesta di ripristino della password avviene attraverso il portale, o telefonicamente, e non richiede alcuna autenticazione: è sufficiente comunicare il codice fiscale e l'applicazione informatica alla quale la password si riferisce. Attraverso il registro delle attività, e la notifica all'utente delle richieste, è possibile verificare gli eventuali abusi.

La richiesta di ripristino della password prevede, tra utente e sistema, la seguente sequenza di comunicazioni:

1. **richiesta,** da parte dell'utente, al sistema;
2. **conferma della ricezione** della richiesta, da parte del sistema;
3. **comunicazione, all'utente, della password** da parte del sistema.

**Richiesta da parte dell'utente**

Le informazioni che l'utente deve comunicare, per il ripristino password, sono:

a) il codice fiscale;
b) il codice e la definizione dell'applicativo per il quale si chiede l'intervento (opportunamente facilitato dalle istruzioni fornite dal portale o dal colloquio con un operatore).

La comunicazione della richiesta può avvenire:

A. tramite il portale;
B. per telefono al numero 800-260 (o, eventualmente, ad altro numero che verrà indicato) - solo se l'utente è impossibilitato ad accedere al portale.

**Conferma ricezione della richiesta da parte del sistema**

Le informazioni che il sistema restituisce, immediatamente, al fine di confermare l'avvenuta ricezione della richiesta sono:

a) il nome dell'applicativo per il quale si richiede il ripristino;
b) gli indirizzi a cui verrà recapitata la nuova password;
c) la data e l'ora entro cui verrà inviata la password.

La conferma della ricezione della richiesta viene fornita, contestualmente alla ricezione della richiesta stessa, attraverso lo stesso canale usato dall'utente per la richiesta, e in ogni caso inviando un'email sulla casella istituzionale personale dell'utente.

**Comunicazione della password da parte del sistema**

La comunicazione della password all'utente, da parte del sistema, contiene le seguenti informazioni:

a) l’identificativo dell’utente, relativo all’applicazione richiesta;
b) la password provvisoria, da cambiare al primo accesso;
c) l’indicazione che la password andrà cambiata, al primo successivo accesso, e le policy sulla complessità della password previste dall’applicazione;
d) i nomi degli applicativi sui quali il ripristino password ha effetto;

Le modalità della comunicazione della password vengono precisate nel seguente paragrafo.

**Modalità per la comunicazione della password**

I recapiti, per la comunicazione all’utente della nuova password, sono recuperati dai dati a disposizione del sistema, precedentemente inseriti nel portale delle password.
In nessun modo i recapiti potranno essere comunicati, o modificati, nella fase di richiesta di ripristino della password.
La comunicazione verrà sempre inviata alla casella istituzionale personale**,** anche se l’utente in quel momento non può accedervi.
Nel caso di richieste di ripristino, che riguardano: a) l’accesso alla postazione di lavoro; b) l’accesso alla casella di posta personale istituzionale; c) i casi in cui il sistema rileva che la casella non è raggiungibile (perché piena, perché non esistente, ecc.), la comunicazione della nuova password viene trasmessa tramite:

A. sms al numero di cellulare di servizio;
B. sms al numero di cellulare personale;
C. e-mail all’indirizzo casella di posta personale;
D. Indirizzo postale del luogo di lavoro;
E. Indirizzo postale della segreteria di riferimento.

La sequenza della procedura descritta non rappresenta una mera formalità, ma serve a implementare la sicurezza, in quanto predisposta per garantire, all'Amministratore di sistema, che la richiesta di ripristino password proviene da chi è effettivamente legittimato al trattamento dei dati. Si sono, infatti, verificati casi in cui le violazioni di sistemi protetti sono state ottenute da malintenzionati che si spacciavano per altre persone (dichiarando al telefono di aver smarrito la password e ottenendone il ripristino).

## 8.3 Modalità e procedure, relative alla salvaguardia dei dati personali memorizzati sui pc, in caso di dismissione e/o sostituzione delle apparecchiature

### 8.3.1 Introduzione

I tradizionali supporti di memorizzazione (hard disk, floppy, supporti USB), utilizzati nella quotidiana attività lavorativa, contengono un’enorme quantità di dati riservati.

I frequenti refresh tecnologici, favoriti da un sempre minor costo dell’hardware, richiedono che sia gli strumenti di memorizzazione (es. gli hard disk) che qualunque oggetto li contenga (es. i PC), vengano movimentati, con la dovuta cautela, soprattutto quando vengono ceduti per un qualsiasi motivo.

Gli utenti, normalmente, danno per scontato che i dati cancellati tramite sistema operativo, o contenuti su supporti danneggiati, non siano più disponibili per successivi utilizzi. La rapida evoluzione tecnologica degli ultimi anni ha permesso, purtroppo, lo sviluppo di strumenti software che consentono un agevole recupero dei dati, siano questi cancellati in maniera tradizionale o memorizzati su supporti danneggiati, anche da parte di utenti non particolarmente esperti e con costi molto contenuti.

Il metodo più efficace, per preservare la riservatezza delle informazioni memorizzate su supporti, è la distruzione fisica degli stessi. Tale metodo è particolarmente indicato per gli strumenti che, per loro natura, non possono essere riutilizzati (es. CD e/o DVD), mentre, con riferimento ai supporti riutilizzabili (es. hard disk, supporti esterni, chiavette USB, nastri di backup etc.), è necessario considerare l'elevato costo di un approccio di questo tipo.

L'alternativa più frequentemente utilizzata, rispetto alla distruzione fisica dei supporti, è quella della completa riscrittura mediante l'utilizzo di appositi software. Attraverso tale operazione, infatti, i dati precedentemente memorizzati non potranno essere più reperibili.

### 8.3.2 Dismissione della postazione di lavoro

Nell'ipotesi in cui venga sostituita la postazione di lavoro, il disco rigido verrà formattato dai tecnici incaricati da Informatica Trentina, con un processo che garantisce l'irrecuperabilità dei dati precedentemente memorizzati.

Sulla base di quanto sopra esposto, costituisce responsabilità dell'utente assegnatario provvedere a copiare tutti i dati che devono essere salvaguardati, nei percorsi standard (cartella Documenti), affinché il tecnico incaricato possa provvedere al loro riversamento sulla nuova postazione.

I dati non riversati non potranno in alcun modo essere recuperati.

### 8.3.3 Sostituzione dell'hard disk

Nel caso di sostituzione del disco rigido della postazione di lavoro, da parte dei tecnici incaricati da Informatica Trentina, il contenuto sarà cancellato mediante un processo che garantisce l'irrecuperabilità dei dati precedentemente memorizzati. Oppure, nel caso non se ne preveda il riutilizzo, l'hard disk verrà distrutto fisicamente.

Per eventuali postazioni, non direttamente gestite da Informatica Trentina, per le quali la sostituzione dell'hard disk non viene effettuata da personale incaricato dalla stessa, sarà necessario richiedere un intervento congiunto, per garantire la cancellazione irreversibile di tutti i dati, prima che il disco sostituito venga consegnato al tecnico esterno.

Sulla base di quanto specificato, costituisce precisa responsabilità dell'utente assegnatario provvedere ad indicare, al tecnico incaricato, tutti i dati che devono essere copiati sul nuovo supporto affinché il medesimo possa provvedere al loro riversamento.

I dati non riversati non potranno in alcun modo essere recuperati.

## 8.4 Misure di sicurezza relative ai pc portatili

### 8.4.1 Misure di sicurezza logistiche

#### 8.4.1.1 Protezione da accesso fisico non autorizzato e dal furto

Il personale che ha in consegna un PC portatile è tenuto a:
- evitare di lasciare incustodito il portatile per evitare il rischio di furto;
- custodire i portatili negli armadi muniti di serratura;
- escludere l'accesso ai dati da parte di soggetti non autorizzati al trattamento, evitando, così, che tali dati giungano a conoscenza di terzi;
- evitare, ove non strettamente necessario per lo svolgimento dei compiti affidati, la connessione del portatile a reti che non siano quella provinciale.

### 8.4.2 Misure di sicurezza tecniche, informatiche e procedurali

#### 8.4.2.1 Protezione da accesso logico non autorizzato

Si richiamano, in quanto compatibili con le caratteristiche tecniche del PC portatile e con le esigenze organizzative, le misure previste per l'accesso logico alle postazioni di lavoro fisse (user-id, password, comunicazione della password al custode, screen saver…).

#### 8.4.2.2 Protezione dai virus

Per ridurre al minimo il pericolo di perdite di dati a causa di virus informatici, è necessario verificare che sia installato un prodotto antivirus ad hoc: per risultare efficace nel tempo, deve essere aggiornato, periodicamente, secondo le modalità richieste dal prodotto stesso.

#### 8.4.2.3 Protezione dai malintenzionati

I PC portatili, quando collegati a rete diversa da Telpat, o connessi a Internet, tramite un provider diverso da Informatica Trentina s.p.a., non usufruiscono della protezione effettuata tramite *firewall* gestito da Informatica Trentina stessa.
Pertanto, a fronte del pericolo di attacchi esterni dei malintenzionati, vanno adottate le seguenti cautele:
- evitare, ove non strettamente necessario per lo svolgimento dei compiti affidati, la connessione del portatile a reti che non siano quella provinciale
- ove sia necessario collegarsi a reti, concordare idonee misure di protezione con il Servizio competente in materia di informatica.

#### 8.4.2.4 Protezione dal rischio di perdita accidentale dei dati

Nel caso non sia possibile connettere il portatile alla rete dell'ufficio, il personale che lo ha in uso è tenuto a:
- provvedere a periodici backup dei dati contenuti nel disco fisso del portatile su supporti magnetici;
- custodire i supporti di backup con le precauzioni individuate nel paragrafo 8.5 "Misure di sicurezza relative ai supporti di memorizzazione".

## 8.5 Misure di sicurezza relative ai supporti di memorizzazione

### 8.5.1 Misure di sicurezza logistiche

Nell'uso e nella conservazione dei supporti di memorizzazione si devono porre in essere le misure necessarie a ridurre al minimo i rischi di:
- accesso fisico non autorizzato;
- furto e manomissione dei dati da parte di malintenzionati;
- distruzione o perdita dei dati dovuta ad eventi fisici;
- perdita accidentale dei dati.

Sono necessari, inoltre, gli ulteriori accorgimenti, di seguito riportati, derivanti dalle specifiche caratteristiche di tali supporti.

#### Reimpiego

Ai sensi del punto 22, del Disciplinare tecnico in materia di misure minime di sicurezza (allegato B del Codice privacy), i supporti rimovibili contenenti dati sensibili o giudiziari, se non utilizzati, sono distrutti, o resi inutilizzabili, ovvero possono essere riutilizzati da altri Incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.
Si riportano, di seguito, le indicazioni operative da seguire, relative ad alcuni supporti, nel caso in cui gli stessi siano consegnati a terzi:

- floppy disk e dvd/cd-rom riscrivibili e altri supporti rimovibili: prima di essere consegnati a terzi, debbono essere sottoposti ad una operazione di cancellazione delle informazioni precedentemente contenute, con l'apposito comando di formattazione completa del supporto;
- hard disk: prima di essere consegnato a terzi, deve essere sottoposto ad una operazione di cancellazione delle informazioni precedentemente contenute, con l'apposita procedura;
  nel caso in cui, a seguito di intervento tecnico, si ravvisi la necessità di sostituire l'hard disk, è necessario procedere alla cancellazione dei dati dall'hard disk sostituito; si ricorda che l'hard disk potrebbe costituire un mezzo di esportazione illegittima di dati personali, qualora gli stessi fossero recuperati da personale non autorizzato;
- nel caso in cui i supporti contenenti dati personali non siano destinati al riutilizzo, essi debbono essere fisicamente distrutti mediante rottura.

### 8.6. Regole per l'utilizzo delle dotazioni informatiche

#### 8.6.1. Uso corretto

L'entrata in vigore del D.Lgs. 30 giugno 2003 n. 196 ha introdotto rilevanti obblighi, a carico della Provincia, sanzionati sia civilmente che penalmente, imponendo di trattare i dati personali nel rispetto del diritto di riservatezza degli interessati, e prescrivendo un trattamento lecito e corretto. Tale provvedimento normativo, inoltre, ha demandato al Titolare (Giunta provinciale), ovvero al/ai Responsabile/i del trattamento (per la Provincia autonoma di Trento i Dirigenti Generali, che gestiscono, in via esclusiva, determinati trattamenti e i Dirigenti in base alla presente deliberazione della Giunta provinciale), la responsabilità di controllare il corretto impiego degli strumenti informatici e di dettare le disposizioni per il corretto utilizzo degli stessi.

Tutti i beni che la Provincia autonoma di Trento mette a disposizione, per lo svolgimento dell'attività lavorativa, restano nella disponibilità esclusiva della stessa. Pertanto, devono essere utilizzati, da parte di coloro che vi operano a qualunque livello e con qualsiasi rapporto, in maniera adeguata, anche al fine di evitare comportamenti potenzialmente pericolosi per la sicurezza del sistema informativo, derivanti da conoscenza non adeguata o incompleta, ed in conformità alle mansioni attribuite, dal contratto di lavoro, all'utente. Tutti gli utenti, che accedono alle reti LAN della Provincia, vengono automaticamente abilitati all'utilizzo di Internet ed è facoltà dei Responsabili delle strutture di appartenenza chiedere di limitare l'accesso a determinati utenti e a determinate categorie di siti.

Tutti i soggetti, che utilizzano gli strumenti informatici messi a disposizione dalla Provincia per lo svolgimento dell'attività lavorativa, devono:

a) adottare, nello svolgimento della propria attività lavorativa, le necessarie cautele per assicurare la confidenzialità dei dati personali e di quelli che possono fornire indicazioni utili ad un eventuale attaccante dei sistemi informativi (per es. dati relativi ad incidenti di sicurezza pregressi, alla tipologia di rete, alla configurazione dei software, all'ubicazione dell'hardware, al personale preposto alla gestione ed alla sicurezza dei sistemi);

b) utilizzare, sulle postazioni di lavoro, esclusivamente il software autorizzato e fornito dalla Provincia: richiedere eventuale software aggiuntivo, rispetto all'installazione standard, al proprio referente informatico;

c) in caso di telelavoro, durante l'attività lavorativa, utilizzare la postazione di lavoro fornita esclusivamente per motivi inerenti all'attività lavorativa, senza manomettere, in alcun modo, gli apparati e la configurazione della postazione stessa, nel rispetto delle esigenze di funzionalità e di sicurezza della rete e dei sistemi. Internet può, comunque, essere utilizzato, anche per motivi personali, purchè nei limiti specificati dal Disciplinare approvato con delibera della Giunta provinciale n. 1037/2010. Se si utilizzano dispositivi mobili per il telelavoro, collegare gli stessi,

alla LAN della Provincia, almeno una volta ogni 30 giorni per l'aggiornamento automatico delle patch di sicurezza;

d) utilizzare gli strumenti di telefonia, sia fissa che mobile, per lo svolgimento dell'attività lavorativa ed in modo pertinente alle specifiche finalità della propria attività, nel rispetto delle esigenze di funzionalità e sicurezza dei sistemi informativi. Per tutto quanto non specificato, ci si dovrà attenere al Disciplinare, approvato con deliberazione della Giunta provinciale n. 1037/2010.

### 8.6.2. Uso non consentito delle dotazioni informatiche e telefoniche

Le seguenti attività sono proibite:

a) inviare messaggi di posta elettronica contenenti segnalazioni del virus ad altri utenti. Tali segnalazioni vanno inviate solo all'assistenza tecnica, all'indirizzo sicurezza@infotn.it

b) rimuovere il programma antivirus installato sulla postazione di lavoro;

c) lasciare incustoditi i dispositivi mobili;

d) aprire allegati di posta elettronica~~,~~ dal mittente e/o dall'oggetto sospetti, per prevenire i rischi causati da software nocivi (per es. virus, worm, spyware, ecc. In tal caso cancellare immediatamente tali messaggi e, in caso di dubbio, contattare l'indirizzo di posta dedicato alle problematiche di sicurezza **(sicurezza@infotn.it))**;

e) effettuare copie non autorizzate, di materiale coperto da copyright, compresi, ma non limitati a, digitalizzazione e distribuzione di foto da riviste, libri o altre fonti protette da copyright; musica coperta da copyright;

f) eseguire attività di Port Scanning o Security Scanning;

g) eseguire qualsiasi forma di monitoraggio della rete che permetta di catturare dati non espressamente inviati all'host dell'utente;

h) aggirare le procedure di autenticazione o la sicurezza di qualunque host, rete o account;

i) interferire o bloccare l'operatività di qualunque utente (es. Denial of Service Attack) ivi compreso l'utilizzo di qualunque programma/script/comando o l'invio di un messaggio, sia localmente sia via Internet/Intranet/Extranet, con l'intento di interferire o disabilitare una qualunque connessione di altri utenti;

j) inviare messaggi di posta elettronica non desiderati, o richiesti, ivi inclusa la spedizione di qualunque informazione pubblicitaria, a soggetti che non abbiano specificatamente richiesto tali informazioni o l'inoltro di email appartenenti a catene o similari (Spam);

k) utilizzare intestazioni delle email non autorizzate.

La lista sopra riportata non deve essere considerata esaustiva, ma intende fornire un quadro di massima delle attività che ricadono nella categoria di utilizzo non accettabile.

### 8.6.3. Eccezioni agli usi non consentiti

Gli utenti possono essere dispensati, da una o più delle restrizioni previste dal Disciplinare approvato con deliberazione della Giunta provinciale n.1037/2010, nel caso in cui tali limiti compromettano lo svolgimento di attività che rientrino tra quelle previste, esplicitamente, dalle loro mansioni lavorative, e siano pertanto ufficialmente autorizzate dai loro responsabili di struttura.

## 8.7. Regole per la configurazione delle postazioni di lavoro della Provincia

### 8.7.1. Premessa

Il contenuto del presente paragrafo è giustificato dal fatto che alcuni utenti sono Amministratori del proprio posto di lavoro e, quindi, sono in grado di modificare la configurazione standard di seguito descritta e fornita da Informatica Trentina.

Nel momento in cui le postazioni di lavoro sono messe in rete, le medesime divengono, automaticamente, vulnerabili ad un attacco, ai virus, agli errori umani (accidentali o dolosi) etc.. A causa di tale circostanza, un utente sufficientemente motivato, e con adeguate conoscenze tecniche, è in grado di individuare eventuali errori e/o dimenticanze, nella configurazione di un sistema, e metterne a rischio la riservatezza dei dati contenuti, nel caso migliore, o addirittura le funzionalità dello stesso.

**La sicurezza di un sistema non può essere, dunque, un'attività occasionale, ma deve essere parte del modo di lavorare, poichè, in ogni istante, occorre cercare di mantenere al riparo dalle minacce esistenti utenti, dati, transazioni, ecc..**

Per tale motivo, all'atto della configurazione di un sistema in rete, è compito dell'Amministratore implementare, con ragionevoli misure di sicurezza, la difesa dello stesso: la loro applicazione limiterà l'esposizione del sistema ai rischi esistenti ovvero ne ridurrà la vulnerabilità.

### 8.7.2 Configurazione Standard

Il sistema operativo, autorizzato sulle postazioni di lavoro in dotazione ai dipendenti della Provincia, è la versione più aggiornata di Microsoft Windows, ovvero il sistema operativo più adeguato allo svolgimento delle attività lavorative.
Nel caso di postazioni di lavoro con sistema operativo Microsoft Windows, tutti i files del sistema operativo, e tutti i programmi, durante il processo di installazione e configurazione, dovranno essere memorizzati sulla partizione principale "*c*"; le informazioni personali degli utenti utilizzatori dovranno essere allocate, nella apposita cartella utente, all'interno della cartella Documents and settings.

### 8.7.3. Regole per gli utenti amministratori della propria postazione di lavoro

Gi utenti, su richiesta del proprio responsabile di struttura, possono divenire Amministratori del proprio posto di lavoro. Si ricorda ai Responsabili, cui compete tale concessione, che l'opportunità di essere Amministratore del proprio PC, da un lato, permettendo di operare sulla configurazione della propria macchina, aumenta la cultura informatica del personale, dall'altro, però, comporta un aumento dei costi di manutenzione dovuti ad errori di utenti non professionali. Si raccomanda, quindi, ai Responsabili di struttura, di valutare attentamente le caratteristiche individuali degli utenti ai quali si decide di concedere i privilegi di Amministratore della propria postazione di lavoro.

Gli utenti, cui è stato concesso di essere Amministratore della propria postazione di lavoro, sono comunque tenuti a rispettare le seguenti regole:

- non istallare software non regolarmente licenziati;
- non disabilitare il sistema di antivirus;
- non bloccare gli aggiornamenti di sicurezza del software installato;
- nel caso di interventi tecnici, segnalare l'installazione di software licenziati non previsti dalla configurazione standard.

## 9. TRATTAMENTO DI DATI SU SUPPORTI NON INFORMATICI

Nel caso di trattamento dei dati effettuato con strumenti diversi da quelli elettronici o comunque automatizzati (supporto cartaceo o altri supporti quali fotografie, fiche, slides, diapositive, ecc.), si applica quanto previsto dall'articolo 35 del Codice, che prevede alcune misure minime di sicurezza.

Si richiama quanto previsto nel capitolo 4. *Misure organizzative comuni a tutti i trattamenti* (censimento delle banche dati, verifica della legittimità del trattamento, nomina degli Incaricati ed autorizzazione al trattamento di dati sensibili).

### 9.1 Misure logistiche

Il personale, addetto al trattamento di dati personali, deve porre in essere le misure necessarie a ridurre al minimo i rischi di:
- accesso fisico non autorizzato;
- furto o manomissione dei dati da parte di malintenzionati;
- distruzione o perdita dei dati dovuta ad eventi fisici;
- perdita accidentale dei dati.

#### 9.1.1 Protezione dall'accesso fisico non autorizzato o dalla manomissione dei dati

Le misure idonee ad evitare l'accesso fisico non autorizzato o la manomissione dei dati, da parte di malintenzionati, sono le seguenti:

**Dati personali comuni**

I documenti contenenti dati personali comuni sono conservati in archivi ad accesso selezionato: pertanto, l’accesso ai dati è consentito ai soli Incaricati del trattamento (ivi compreso il Direttore o Responsabile del settore cui il trattamento si riferisce), al Dirigente/Responsabile del trattamento, nonché al personale che deve accedervi per l’espletamento di compiti comunque connessi con il trattamento.

I documenti possono essere estratti dall’archivio, e affidati alla custodia dell’Incaricato del trattamento, per il tempo strettamente necessario al trattamento medesimo: egli ha cura di garantirne la riservatezza e provvede al deposito in archivio al termine delle operazioni; tale disposizione va precisata nelle istruzioni formalmente fornite all’Incaricato stesso nell’atto di nomina.
La struttura che custodisce dati personali su supporto fisico, deve dotarsi di arredi (cassettiere, armadi ecc.) muniti di meccanismi di serratura adatta a garantire la sicurezza, da destinare ad archivio di documenti contenenti dati personali; solo così si possono avere garanzie di sicurezza.

**Dati sensibili e giudiziari**

L'accesso ai dati è limitato agli Incaricati del trattamento (ivi compresi i Direttori o Responsabili di settore) e al Dirigente/Responsabile del trattamento, nonché al personale che deve accedervi per l’espletamento di compiti comunque connessi con il trattamento. L’accesso agli archivi deve essere selezionato e controllato: i documenti contenenti dati personali sensibili devono essere conservati in elementi di arredo (armadi o cassettiere) muniti di serratura a chiave (o altro sistema che offra pari garanzie di sicurezza); la chiusura a chiave garantisce sia la selezione del personale autorizzato ad accedere, quanto il controllo sugli accessi medesimi.

Si devono, inoltre, osservare le seguenti misure:
la chiave deve essere custodita da personale incaricato della custodia dal Dirigente/Responsabile (di norma presso la segreteria della struttura);
il personale incaricato della custodia delle chiavi è tenuto a riporle in un luogo non agevolmente accessibile da altri;

l’archivio viene aperto e chiuso dal personale custode delle chiavi;
i soggetti ammessi all’archivio, dopo l’orario di servizio, devono essere identificati e registrati;
i documenti, anche quando estratti dall’archivio per essere affidati agli Incaricati per uno specifico trattamento, devono essere comunque custoditi in arredi muniti di serratura e depositati in archivio al termine del trattamento; pertanto, quando l’Incaricato abbandona la propria postazione di lavoro, i documenti devono essere riposti e conservati sotto chiave; questa disposizione va precisata nelle istruzioni formalmente fornite all’Incaricato stesso nell’atto di nomina (Allegato B, punto 27 Codice privacy).

### 9.1.2 Protezione dei locali archivio contenenti dati personali sensibili

Poiché è obbligatorio archiviare i documenti contenenti dati personali sensibili in arredi (armadi o cassettiere) chiusi a chiave, l’accesso ai locali che contengono i documenti può non essere soggetto a particolari restrizioni. Resta fermo l’obbligo per l'Incaricato, e per il Responsabile/del trattamento, di verificare che gli elementi di arredo siano sempre chiusi e che vengano rispettate le misure sopra riportate, relative alla custodia delle chiavi e all’apertura degli archivi.
Se non c'è immediata disponibilità di arredi muniti di serratura per l’archiviazione dei documenti contenenti dati personali sensibili, gli archivi devono, in ogni caso, essere ubicati in appositi locali chiusi a chiave e, se appare agevole l’intrusione dall’esterno, muniti di sbarre.
Una apposita stanza-archivio, chiusa a chiave, può essere una soluzione adatta anche nel caso di armadi con serratura, in quanto aumenta il livello di protezione dei dati stessi.
Il personale diverso dagli Incaricati del trattamento, che accede a questi locali, deve essere accompagnato da uno dei soggetti Incaricati del trattamento o dal custode delle chiavi che deve verificare che non vi sia un accesso ai dati sensibili contenuti nei documenti (es: apertura e consultazione dei fascicoli).

**Adempimenti relativi ai fornitori che possono venire a conoscenza di dati personali**

Il Titolare Provincia autonoma di Trento, per garantire che il personale di ditte fornitrici che si trovi ad intervenire presso l’Amministrazione provinciale operi nel rispetto delle vigenti disposizioni in materia di protezione dei dati personali, adotta le seguenti idonee misure:
**1.** in base a quanto disposto dal D.Lgs. 196/2003 – Allegato B, punto 25 “Il Titolare che adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere alla esecuzione, riceve dall’installatore una descrizione scritta dell’intervento effettuato che ne attesta la conformità alle disposizioni del presente disciplinare tecnico.” Deve quindi essere fatta esplicita e formale richiesta, al fornitore esterno, di idoneo rapporto di intervento, da redigere in modalità conforme alla vigente normativa, che dovrà essere controfirmato da un rappresentante del Settore oggetto dell’intervento;
**2.** In base a quanto previsto ai punti 1, 2, 3, 4, 6 dell’Allegato B del D.Lgs. 196/2003, è indispensabile nominare Incaricati tutti quei soggetti che hanno accesso, al patrimonio informativo provinciale, a fini manutentivi, o più in generale per erogare il servizio oggetto di fornitura, o che, in ogni caso, trattino dati personali che ricadono sotto le competenze del Titolare Provincia autonoma di Trento – Giunta provinciale. A tal fine, il fornitore deve essere nominato Responsabile esterno del trattamento, e, a sua volta, deve individuare il personale coinvolto nel trattamento e procedere a formale incarico, con l’individuazione dei compiti specifici che tale personale dovrà svolgere presso le sedi provinciali. Qualora i soggetti interessati cessino di svolgere, definitivamente o comunque per un periodo superiore a sei mesi, le funzioni per le quali hanno ricevuto l’incarico, dovrà esserne data tempestiva comunicazione alla struttura provinciale interessata, che provvederà a revocare i diritti di accesso ai locali e ai sistemi.

### 9.1.3 Protezione dal rischio di perdita dei dati dovuta ad eventi fisici

Un archivio è sottoposto al rischio di svariati tipi di eventi, che possono provocare la distruzione o il danneggiamento dei documenti. Per ridurre al minimo questo rischio, le principali misure da prendere sono le seguenti:
-in sede di progettazione e di realizzazione di nuove strutture adibite a sede di uffici provinciali ovvero in sede di ristrutturazione degli edifici esistenti, va tenuta presente la necessità di collocare i locali adibiti ad archivio in luoghi sicuri, evitando ad esempio scantinati e piani seminterrati che sono a rischio di allagamenti;
-nelle strutture devono essere presenti idonei dispositivi antincendio.

### 9.1.4 Misure per prevenire lo smarrimento accidentale dei documenti

Al fine di evitare lo smarrimento accidentale dei documenti, l'Incaricato del trattamento deve aver cura di depositare i documenti negli appositi archivi non appena cessate le operazioni di trattamento.

## 10. MISURE DI SICUREZZA RELATIVE ALLE AULE CORSI

Le aule dove si tengono corsi di formazione, nelle quali siano presenti postazioni informatiche connesse al server di una struttura, oppure archivi cartacei contenenti dati personali, vanno protette con adeguate misure di sicurezza. Le misure logistiche e quelle di difesa da attacchi virus vanno applicate, in generale, a tutte le aule corsi nelle quali siano presenti dotazioni informatiche, anche non connesse al server di una struttura (ad es. stazioni stand-alone o stazioni collegate in rete tra loro o ad un server riservato alla sola aula).

### 10.1 Misure di sicurezza logistiche

#### 10.1.1 Protezione dall'accesso fisico non autorizzato

In primo luogo, devono essere adottate le seguenti misure:

- le aule corsi, quando non utilizzate, anche durante la pausa pranzo, devono essere chiuse a chiave;
- le chiavi delle aule corsi sono depositate presso il personale incaricato della custodia dal Dirigente della struttura competente per la gestione dell'aula;
- le aule vengono aperte e chiuse da personale dell'Amministrazione provinciale: non è ammessa la consegna di chiavi a personale esterno;
- il docente, o eventuale altro personale di sorveglianza, deve essere sempre presente in aula in modo da poter contrastare eventuali tentativi di danneggiamento delle dotazioni informatiche;
- l'accesso alle aule, da parte di personale esterno all'Amministrazione, deve essere autorizzato.

### 10.2 Misure di sicurezza tecniche, informatiche e procedurali

#### 10.2.1 Protezione dall'accesso logico al sistema non autorizzato

Il docente, o eventuale altro personale di sorveglianza, deve essere sempre presente in aula, in modo da poter contrastare eventuali tentativi, non autorizzati, di accesso logico ai sistemi. Conseguentemente, devono essere adottate le seguenti misure:
ove il software di sistema lo consenta, è fatto obbligo di attivare la funzione di screen saver con parola chiave (con tempo di attivazione inferiore ai 5 minuti) per evitare possibili accessi non autorizzati alla rete.

#### 10.2.2. Protezione dai virus

Le postazioni informatiche dell'aula, connesse in rete, sono protette da un prodotto antivirus installato sul server, con aggiornamento periodico automatico via Internet a carico dell'Amministratore di sistema.
Sulle postazioni non connesse, al fine di evitare la propagazione dei virus, deve essere installato un prodotto antivirus ad hoc, da aggiornarsi periodicamente, secondo le modalità richieste dal prodotto stesso. L'aggiornamento è a carico dell'Amministratore di sistema (cioè Informatica Trentina nel caso dei PC registrati nell'inventario centralizzato).

#### 10.2.3 Protezione dai malintenzionati

Le postazioni di lavoro delle aule corsi, collegate alla rete Telpat, sono protette tramite *firewall* gestito da Informatica Trentina s.p.a.. La difesa dagli attacchi di questo tipo è comunque assicurata solo se viene data puntuale applicazione a tutto il complesso delle regole di sicurezza comprese nel presente documento.

## 11. MISURE DI SICUREZZA RELATIVE A INTERNET

### 11.1 Premessa

L'utilizzo di una connessione ad Internet, attraverso un *provider* diverso da Informatica Trentina, espone il PC utilizzato ai rischi normalmente presenti nel corso di una connessione ad Internet in assenza della protezione garantita da un *firewall*.
Inoltre:

- l'eventuale attacco alla macchina, nel corso della navigazione non protetta, diventa un fattore di rischio per l'intera rete provinciale;
- sia l'accesso a siti "impropri" che lo scaricamento di file non autorizzati, in alcuni casi possono essere illegali e puniti dalla legge penale (oltre ad essere in contrasto con il codice di disciplina del dipendente provinciale);
- l'utilizzo della connessione Internet della Provincia, per finalità non riconducibili all'attività di lavoro, anche se non produce un costo diretto, **può diventare causa di sovraccarico della linea** e può portare a un deterioramento della velocità della connessione per tutti gli utenti;
- le informazioni presenti su siti Internet non connessi a istituzioni ben conosciute, possono essere **non accurate**, **non valide o deliberatamente false**: ogni decisione basata su di esse deve essere valutata adeguatamente;
- qualora il collegamento alla rete Internet avvenga al di fuori di Telpat (ad es. tramite PC portatile), ogni macchina che può accedere a Internet (o il server, se gli elaboratori sono in rete) va protetta da un antivirus aggiornato: non aggiornarlo, può essere più pericoloso che non averlo: si crea una falsa sicurezza.

> I messaggi di posta elettronica, di cui non si conosce il mittente, vanno trattati con la massima circospezione; **non bisogna mai cliccare sugli eventuali allegati senza riflettere**; si tenga presente che i danni, per virus ricevuti attraverso la posta elettronica, rappresentano, da soli, la grande maggioranza delle cause di eventi dannosi per virus informatico all'interno delle reti aziendali.

Anche in presenza di un utente conosciuto, è meglio riflettere sul contesto del messaggio per verificare se l'allegato è, in qualche modo, connesso con il proprio lavoro (e quindi viene effettivamente dal mittente indicato).

### 11.2 Regole per l'utilizzo della rete Internet

Non è pensabile, al giorno d'oggi, lavorare senza l'ausilio di Internet, ma, allo stesso tempo, occorre evitare, e prevenire, comportamenti anomali ovvero garantire un uso appropriato dello strumento. La rete, infatti, permette di accedere a moltissimi siti, contenenti informazioni più o meno lecite, che possono anche contenere virus e/o software malevoli, creati per interrompere, distruggere e/o limitare il funzionamento degli applicativi, degli apparati hardware o delle comunicazioni di rete. Purtroppo, anche a fronte di una semplice ed innocua ricerca in Internet, non è sempre facile evitare di imbattersi, almeno una volta, in siti web non conformi o contenenti informazioni inadeguate.

La delibera del Garante Privacy n. 13/2007, emanata in data 01/03/2007, ha disposto una serie di prescrizioni ed adempimenti, relativamente all'accesso ai dati del personale dipendente da parte del datore di lavoro, riferendosi specificatamente anche alle informazioni desumibili dall'analisi dei log del traffico web effettuato dalle postazioni aziendali.

Nello specifico, pur dettando delle linee guida molto stringenti a protezione dei dati personali dei dipendenti, il Garante della Privacy ha altresì riconosciuto la necessità del datore di lavoro, ovvero del Titolare del trattamento, di adottare opportune misure, per ridurre il rischio di usi impropri della connessione aziendale ad Internet. Ciò al fine di ridurre i controlli successivi sui lavoratori, e di

predisporre le opportune procedure per disciplinare l'accesso alle informazioni del dipendente (limitatamente alla casella di posta elettronica di lavoro e alle risorse di rete) in caso di improvvisa e/o prolungata assenza dell'Incaricato.

Le condizioni dettate dal Garante per riconoscere la liceità del trattamento, prevedono, tra l'altro, l'adozione e la pubblicazione di un disciplinare interno, definito coinvolgendo anche le rappresentanze sindacali, nel quale siano chiaramente indicate le regole per l'uso di Internet e della posta elettronica e l'adozione delle necessarie misure, di tipo organizzativo e tecnologico, per offrire, all'utente Incaricato, delle soluzioni alternative.

E', inoltre, compito del datore di lavoro informare il personale dipendente, con chiarezza e in modo dettagliato, sulla possibilità che vengano effettuati controlli e con quali modalità.

**La Provincia autonoma di Trento ha provveduto a definire le modalità d'uso di Internet e posta elettronica con deliberazione della Giunta provinciale n. 1037 del 2010, attraverso la quale è stato adottato il "Disciplinare per l'utilizzo della rete internet, della posta elettronica, delle attrezzature informatiche e telefoniche."**

### 11.2.1 Disposizioni per l'accesso a Internet

Onde limitare la necessità di controlli successivi ed in conformità a quanto disposto dal Garante Privacy, sono definite le seguenti linee guida, relativamente alla navigazione in Internet:

- le richieste di accesso a siti Internet interdetti, provenienti da dipendenti della Provincia, devono essere verificate e autorizzate dall'infrastruttura cui compete l'attività di filtro degli indirizzi Internet;
- è facoltà dei Dirigenti chiedere ulteriori restrizioni, o particolari concessioni, per gli utenti sotto le dirette dipendenze; tutti gli utenti che accedono alle reti LAN della Provincia, infatti, vengono automaticamente abilitati all'utilizzo di Internet, ma è facoltà dei Responsabili delle strutture di appartenenza chiedere che l'accesso venga circoscritto a determinati utenti e a determinate categorie di siti;
- per gli apparati di infrastruttura (server, apparati di rete etc) per i quali si renda necessario consentire un accesso ad Internet (p.e. per l'aggiornamento del software), verranno applicate le stesse restrizioni, secondo quanto riportato nel paragrafo 11.3.1 (Categorie interdette alla navigazione), e verranno identificati tramite il loro indirizzo IP.

### 11.3 Disposizioni generali per la navigazione in Internet

Gli utenti che accedono ad Internet, tramite la rete provinciale Telpat, sono tenuti a rispettare alcune norme comportamentali per un uso etico e legale della rete.

Ad integrazione di quanto riportato nel paragrafo 8.6 del presente Allegato, vengono di seguito specificati ulteriori comportamenti da evitare, poiché si pongono in contrasto con la normativa vigente:

- creare, trasmettere, pubblicare e/o archiviare qualsiasi tipo di materiale:
    - che infranga le leggi sul diritto d'autore e la proprietà intellettuale;
    - che includa contenuti che siano dannosi, minatori, molesti, offensivi, calunniosi o volgari;
    - che violi la legge sulla privacy;
    - che incoraggi il compiersi di azioni criminali;
    - che, in generale, possa arrecare danno alla Provincia;
- partecipare a forum, chat e simili se ciò non è richiesto dall'attività lavorativa;

- rimanere collegati a siti musicali, anche se contestualmente si continua la propria attività lavorativa, in particolare per periodi di tempo prolungati, in quanto ciò appesantisce il traffico della rete.

### 11.3.1 Categorie interdette alla navigazione

Nella prospettiva della prevenzione di comportamenti illegittimi, la Provincia ha adottato una soluzione tecnologica volta a bloccare l'accesso a determinati siti, a contenuto estraneo alla normale attività istituzionale.
L'intervento sul traffico Internet, con modalità automatiche di filtro e inibizione, non comporta un controllo diretto o indiretto sull'attività individuale, ma semplicemente impedisce l'accesso a determinati siti non pertinenti all'attività istituzionale, così come previsto anche dal provvedimento del Garante per la Privacy n. 13 del 1° marzo 2007.

Per gli utenti Telpat è inibita la navigazione verso i siti che rientrano nelle seguenti macro categorie, poichè non correlate o correlabili con la normale attività lavorativa:

- Siti che trattano argomenti illeciti;
- Siti contenenti argomenti di cattivo gusto;
- Siti che trattano armi e armamenti in generale;
- Siti che permettono la chat via Web;
- Siti legati al gioco (giochi online, gioco d'azzardo, recensione giochi);
- Siti inerenti il file sharing in generale e il peer-to-peer in particolare, salvo le eccezioni di cui punti 8A e 8C del disciplinare per l'utilizzo della rete Internet, della posta elettronica, delle attrezzature informatiche e telefoniche (Deliberazione Giunta provinciale n. 1037 del 2010);
- Siti che riconoscono un corrispettivo economico legato alla navigazione;
- Siti di intermediazione finanziaria e trading online;
- Siti che trattano file musicali (MP3) o, più in generale, forniscono illecitamente materiale coperto dal diritto d'autore;
- Siti contenenti materiale per adulti, nudità o comunque con contenuti legati al sesso (fanno eccezione i siti di natura medica e scientifica);
- Siti che permettono di eludere i sistemi di controllo della navigazione, tramite l'utilizzo di proxy o l'occultamento dell'URL di destinazione/provenienza;
- Siti riguardanti Hacking o pirateria informatica;
- Siti collegati alle violazioni della sicurezza informatica;
- Siti per lo streaming audio e video (solo per quanto riguarda siti che violano i diritti di autore);
- Siti legati al razzismo, al fanatismo e all'estremismo;
- Siti con contenuti violenti;
- Siti che si occupano esclusivamente di pubblicità.

### 11.3.2 Eccezioni agli usi non consentiti

Gli utenti possono essere dispensati da una o più delle precedenti restrizioni, nel caso in cui gli accessi vietati siano pertinenti alle loro mansioni lavorative, e siano pertanto ufficialmente autorizzati.

Con riferimento alle linee telefoniche, alla posta elettronica, a Internet e agli altri beni telematici, gli utenti devono utilizzare tali strumenti nei limiti specificati dal disciplinare approvato con delibera della Giunta provinciale n.1037 del 7/5/2010.

### 11.4 Conservazione dei log

I log, del traffico Internet (ora e data, ip del client, userid, indirizzo o url di destinazione e protocollo) effettuato, sono registrati e conservati da Informatica Trentina s.p.a., fornitore del servizio, come richiesto dall'articolo 132 del D. L.gs n. 196/2003 e rispettando le modalità previste nel Provvedimento del Garante della Privacy "Sicurezza dei dati di traffico telefonico e telematico" del 17 gennaio 2008, per quanto concerne i tempi di ritenzione e le modalità di conservazione e di consultazione,.
I dati di traffico potranno essere consultati esclusivamente durante le attività di verifica e controllo, per motivi di sicurezza interna, o su richiesta dell'Autorità Giudiziaria. In alcun modo potranno essere utilizzati per effettuare la profilazione delle abitudini di traffico degli utenti.

# 12. MODALITA' E PROCEDURE RELATIVE ALLA FORMAZIONE DEL PERSONALE IN AMBITO PRIVACY E SECURITY

## 12.1 Introduzione

Il continuo aggiornamento dei soggetti coinvolti nel trattamento dei dati, pur essendo venuto meno come obbligo, rimane lo strumento più efficace per aumentare la consapevolezza del personale dipendente in merito a quanto previsto dalla normativa e, conseguentemente, innalzare il livello di sicurezza delle informazioni. Inoltre, anche in considerazione delle diverse responsabilità correlate al ruolo ricoperto, è opportuno pianificare interventi formativi differenziati per categoria (Responsabili, Incaricati, Amministratori di sistema, Referenti privacy).

Per tale motivo, è opportuno istituire cicli periodici di formazione, con l'obiettivo di illustrare le problematiche della privacy, della sicurezza delle informazioni, delle misure minime di sicurezza previste dal D.Lgs. 196/03, e di quanto attuato dalla Provincia in tale specifica materia.

## 12.2 Tipologia degli eventi formativi

Per realizzare una formazione efficiente ed efficace, è opportuno che questa sia caratterizzata da riferimenti concreti con l'attività quotidiana degli interessati. Sulla base di un simile obiettivo, l'attività formativa viene suddivisa in due moduli.

Il primo, comune a tutti i dipendenti, è caratterizzato dall'esposizione generale dell'attuale disciplina della privacy, delle misure di sicurezza previste e dei provvedimenti del Garante per la Privacy.

Il secondo modulo, invece, dal carattere più mirato, viene elaborato in relazione alle diverse tipologie omogenee di utenti, in modo da analizzare aspetti più vicini all'operatività quotidiana.

La formazione può, inoltre, rappresentare una opportunità di confronto sui temi della privacy, della sicurezza informatica e sull'efficacia delle misure adottate, costituendo l'occasione per raccogliere proposte, suggerimenti e contributi da parte dei soggetti protagonisti del trattamento, favorendone, al contempo, il coinvolgimento personale, elemento essenziale per perseguire una effettiva e concreta politica di sicurezza.

I gruppi omogenei di utenti individuati sono i seguenti:

- Responsabili e Direttori;
- Referenti Informatici e Referenti Privacy;
- Utenti generici.

Sarà cura dei singoli Dirigenti segnalare l'eventuale necessità di formazione specifica per il personale alle loro dipendenze.

## 13. VERIFICHE DI SICUREZZA

### 13.1 Premessa

Le verifiche previste in questo paragrafo consentono di monitorare la concreta attuazione delle misure di sicurezza informatica adottate dall'Amministrazione, e di effettuare un loro costante aggiornamento e adeguamento; ciò risponde all'obbligo, posto in capo a ciascun Titolare di trattamenti di dati personali, di mettere in atto sia le misure minime, previste dagli articoli 33-36 e dall'Allegato B del D. Lgs. n. 196/03, che le misure idonee di cui all' articolo 31 del predetto Codice, in modo da ridurre, al minimo, i rischi di distruzione e di perdita, anche accidentale, dei dati personali, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta. Pertanto, tali verifiche costituiscono esse stesse una misura di sicurezza, che, in quanto tale, è obbligatoria per la Provincia autonoma di Trento, nella sua qualità di Titolare del trattamento di dati personali.

E' bene ricordare che la sicurezza di un sistema è strettamente connessa alla sicurezza del suo anello più debole, e che l'interconnettività e interdipendenza fra le componenti di un sistema informativo, implicano che i problemi di sicurezza, su una sola di esse, propaghino i loro effetti incidendo gravemente sulla sicurezza del sistema nel suo complesso.

**Le verifiche di sicurezza** oggetto del presente capitolo **sono effettuate su tutti i sistemi attinenti ai trattamenti di competenza della Provincia.**

A tale fine, i Responsabili di sistemi differenti da quello della Provincia, e connessi col medesimo, dovranno sottoscrivere appositi protocolli di intesa in cui si precisa che le verifiche di sicurezza sulle strumentazioni verranno effettuate con le modalità e le procedure stabilite dal presente capitolo.

### 13.2 Finalità

Il presente capitolo fornisce **le prescrizioni per lo svolgimento delle verifiche e dei controlli** finalizzati ad individuare, e possibilmente prevenire, il rischio di utilizzo improprio del Sistema informativo che gestisce i trattamenti provinciali.

Le prescrizioni in tema di controlli mirano a:

- preservare la riservatezza, l'integrità e la disponibilità dei dati e delle informazioni;
- garantire il rispetto di leggi e regolamenti in materia di protezione dei dati personali, in particolare dei requisiti minimi di sicurezza previsti dalla normativa vigente;
- proteggere la Provincia autonoma di Trento, ed i suoi utenti, da attività irresponsabili o illegali e preservarne la reputazione e l'immagine nei confronti dei cittadini;
- ridurre la spesa pubblica, sia rilevando eventuali danni già posti in essere, sia adottando procedure che fungano da deterrente rispetto a comportamenti impropri e potenzialmente dannosi; il mancato accertamento dei quali potrebbe comportare responsabilità patrimoniali dirette a carico dell'Amministrazione;
- ridurre i rischi di coinvolgimento dell'Amministrazione, per concorso, nel caso di illeciti, civili e penali, commessi mediante un utilizzo improprio dei beni messi a disposizione dall'Amministrazione stessa;
- verificare la coerenza del funzionamento dei sistemi informativi con le politiche di sicurezza adottate, con gli standard nazionali e/o internazionali e le normative vigenti in materia;
- individuare gli incidenti di sicurezza (comportamenti che infrangono le politiche di sicurezza) per garantire l'affidabilità e la sicurezza della rete e dei servizi erogati e/o

approfondire tutte le circostanze, che emergono in seguito a segnalazioni di incidenti, in modo da evidenziare eventuali rischi ed orientare la successiva attività di prevenzione;

- proporre eventuali modifiche o nuove implementazioni ai sistemi di sicurezza sulla base delle verifiche effettuate.

### 13.3 Ambito di applicazione

Il presente capitolo si rivolge a tutti coloro ai quali la Provincia, per la gestione dei trattamenti di competenza, concede l'accesso al proprio Sistema Informativo Elettronico, siano essi legati all'Amministrazione provinciale da un rapporto di lavoro subordinato, di prestazione d'opera occasionale, di rapporti di collaborazione a progetto, di lavoro interinale, collaborazioni occasionali (d'ora in avanti: il contratto di lavoro; i lavoratori), sia che prestino il proprio lavoro, o la propria opera, nelle sedi dell'ente (compresi i cantieri mobili), o in un luogo diverso dalla sede di lavoro per il mezzo della tecnologia informatica (telelavoro nelle forme dell'ufficio satellite, del telelavoro mobile, del telelavoro a domicilio, ....).

### 13.4 Competenza e responsabilità

#### 13.4.1 Responsabilità del Servizio provinciale competente in materia di Informatica

**I controlli previsti nel presente provvedimento sono di pertinenza della Struttura provinciale competente in materia di informatica, che potrà, ove ritenuto necessario od opportuno, affidarli ad altri soggetti esterni.**

Qualora si renda necessario l'ausilio di persone non appartenenti alla predetta struttura, tali operatori dovranno essere, dalla stessa, preventivamente autorizzati.

Nel caso in cui l'esecuzione delle verifiche comprenda il trattamento di dati personali, non strettamente connessi alla struttura che effettua i controlli, gli addetti dovranno essere preventivamente individuati quali Incaricati del trattamento dati in questione.

## 13.5 Procedure per lo svolgimento dei controlli

### 13.5.1 Principi

Le verifiche consistono in un'attività di monitoraggio sulla conformità dei sistemi informativi, e dei comportamenti dei soggetti che, a vario titolo, li utilizzano, alle prescrizioni normative e alle regole comportamentali disposte dalla Giunta provinciale, mirando a realizzare un modello fortemente improntato alla prevenzione di disfunzioni nelle procedure che implicano un trattamento di dati personali.

Le verifiche effettuate, dall'ente, devono in ogni caso rispettare i seguenti principi:

a) **necessità**: i dati trattati durante l'attività di controllo devono essere sempre e soltanto quelli strettamente necessari a perseguire le finalità di cui al paragrafo 13.2 e conservati per il tempo strettamente necessario;

b) **proporzionalità**: i controlli devono sempre essere effettuati con modalità tali da garantire, nei singoli casi, la pertinenza e non eccedenza delle informazioni rilevate rispetto alle finalità perseguite e specificate al paragrafo 13.2;

c) **imparzialità**: i controlli devono essere effettuati su tutte le strumentazioni informatiche messe a disposizione dall'Amministrazione provinciale e, conseguentemente, possono coinvolgere gli utilizzatori delle stesse, a qualunque titolo ne abbiano la detenzione. L'imparzialità, inoltre, deve essere garantita mediante sistemi automatici di estrazione casuale per l'effettuazione dei controlli a campione, ed in nessun caso possono essere effettuati controlli mirati, e ripetuti, nei confronti di soggetti specifici, con finalità discriminatorie o persecutorie o volutamente sanzionatorie. I controlli puntuali possono essere effettuati soltanto sulla base di specifiche, oggettive e circostanziate segnalazioni, come esplicitato al paragrafo 13.5.3.2;

d) **trasparenza**: in base a tale principio l'Amministrazione deve mettere in atto tutte le azioni necessarie per garantire la preventiva conoscenza, da parte di tutti i soggetti potenzialmente sottoposti ai controlli del presente disciplinare, della possibilità di verifiche da parte del Titolare. Devono, pertanto, essere informati dei possibili controlli i soggetti che operano, a qualunque titolo e con qualunque rapporto, per la Provincia, tra cui, in particolare, quelli che intrattengono, con lo stesso, un rapporto di lavoro (subordinato (di qualsiasi tipologia) o autonomo). A tal fine, l'Amministrazione deve, in particolare, consegnare l'informativa, ex art. 13 del Codice per la protezione dei dati personali, all'atto della sottoscrizione del contratto e tale informativa deve contenere espresso riferimento ai controlli previsti nel presente capitolo;

e) **protezione dei dati personali**: i controlli devono essere effettuati, in ogni caso, rispettando la dignità e la libertà personale dei soggetti che ne risulteranno assoggettati, garantendo la riservatezza dei dati personali raccolti durante la procedura di controllo. I dati devono essere conosciuti soltanto dai soggetti preventivamente designati quali Responsabili e Incaricati del trattamento, tra i quali, in particolare, il Responsabile della Struttura provinciale competente in materia di informatica.

### 13.5.2 Modalità

Il Codice impone, in particolare al Titolo V, numerosi obblighi in materia di sicurezza dei dati e dei sistemi.

In ragione della complessità organizzativa della Provincia autonoma di Trento e della peculiarità della materia, che richiede particolari competenze professionali di carattere spiccatamente tecnico, si reputa opportuno individuare **un'articolazione organizzativa** (Struttura provinciale competente in materia di informatica o eventuale soggetto esterno) **con la specifica responsabilità di**

**sensibilizzare, coordinare, vigilare e dare attuazione a tali obblighi**, nei modi di seguito specificati:

- definire idonee misure di sicurezza informatica da adottare, anche nei modi previsti dal disciplinare tecnico (all. B al d.lgs. 196/2003), nel trattamento di dati personali, sensibili e giudiziari effettuato tramite l'impiego di strumenti elettronici;

- definire un'architettura di sicurezza che soddisfi i requisiti di cui sopra, con particolare riferimento alla armonizzazione delle misure di sicurezza con le architetture informatiche esistenti od in corso di implementazione;

- collaborare, con il Titolare, per definire Linee guida in materia di protezione dei dati personali relativamente alla sicurezza informatica;

- individuare le misure idonee, da osservare nell'esecuzione dei trattamenti dei dati personali, aggiornandole in relazione all'evoluzione della tecnica, della normativa e dell'esperienza, segnalando eventuali problemi rilevati, in prima istanza, ai Responsabili dei trattamenti di dati personali e, in ultima istanza, al Titolare;

- curare la redazione dei disciplinari tecnici, ivi comprese eventuali forme di controllo, in materia di Sistemi informativi, promuovendone anche l'aggiornamento ogni qualvolta l'evoluzione tecnica o normativa lo renda opportuno;

- ogni qualvolta venga avvertito un problema di sicurezza informatica, attivarsi per:
  - verificare il rispetto delle misure minime di sicurezza informatica;
  - individuare, se necessario, altre misure idonee al miglioramento della sicurezza informatica dei trattamenti dei dati personali;
  - inviare opportuna segnalazione, in prima istanza, ai Responsabili dei trattamenti e, in ultima istanza, al Titolare, affinché pongano in essere le misure necessarie per garantire la sicurezza dei dati trattati con strumenti elettronici;

- vigilare, per conto del Titolare ed avvalendosi ove ritenuto necessario di soggetti esterni, sulla puntuale osservanza delle vigenti disposizioni (e delle istruzioni fornite dal Titolare) in materia di trattamento, relativamente al profilo della sicurezza informatica, segnalando eventuali problemi rilevati, in prima istanza, ai Responsabili dei trattamenti di dati personali e, in ultima istanza, al Titolare;

- raccogliere e conservare, ai fini di eventuali verifiche, le attestazioni di conformità alle disposizioni della misura 25 dell'Allegato B del Codice.

### 13.5.3 Tipologie di verifiche

Le verifiche di sicurezza possono essere di quattro tipi:

a) ***puntuali preventive***: attività di verifica effettuate precedentemente all'implementazione, o modifica sostanziale, di un sistema o processo per verificarne la rispondenza alle politiche di sicurezza;

b) ***puntuali a posteriori***: attività di verifica effettuate a seguito del verificarsi di incidenti di sicurezza;

c) ***periodiche*:** attività di verifica, manuali o automatizzate, per contrastare minacce incombenti o potenziali, effettuate con cadenza periodica programmata;

d) ***a campione***: attività di verifica effettuate su campioni scelti secondo criteri prestabiliti e ad intervalli di tempo non fissi.

e)

**13.5.3.1-Verifiche puntuali preventive**

Prima della messa in produzione di un sistema (hardware o software), o di modifiche sostanziali di sistemi già in produzione, devono essere effettuate le verifiche necessarie per assicurare il rispetto delle politiche di sicurezza della Provincia e, nel caso il sistema preveda il trattamento di dati personali, delle misure minime di sicurezza di cui all'Allegato "B" del D.Lgs. 196/03 e dei provvedimenti del Garante per la Privacy che lo interessano.

Le verifiche sono effettuate dal personale della Struttura provinciale competente in materia di informatica o del soggetto esterno eventualmente incaricato, coadiuvato dal Responsabile o referente del sistema.

Le verifiche sono condotte seguendo il "Piano di test" preventivamente concordato fra i soggetti interessati.

Al termine delle verifiche, è redatto il "Verbale di test" (vedi Modello a pag. 110) secondo lo schema del "Piano di test". Il verbale è conservato agli atti della Struttura provinciale competente in materia di informatica anche nel caso in cui i controlli siano affidati a soggetto esterno.

Il sistema può essere messo in produzione solo se le verifiche hanno dato esito positivo. In caso contrario, nel "Verbale di test" sono indicati gli adeguamenti necessari.

**13.5.3.2- Verifiche puntuali a posteriori**

La verifica puntuale può essere avviata a seguito di:

a) segnalazione di un soggetto terzo;

b) verifica di sicurezza, periodica o a campione.

Relativamente alle segnalazioni di cui alla lettera a):

- non sono tenute in considerazione quelle anonime;
- devono essere rivolte, per iscritto, alla Struttura provinciale competente in materia di informatica, anche nel caso in cui i controlli siano affidati a soggetto esterno.

Allorché si verifichi un evento di sicurezza (lettera b)), il fattore decisivo è la capacità di rispondere in modo veloce ed efficace: la rapidità con cui un'organizzazione è in grado di riconoscere un incidente, o un attacco, e successivamente analizzarlo e contrastarlo, incide sul danno, inferto o potenziale, ed abbassa i costi di ripristino.

Per questo è fondamentale che, a seguito di un "evento di sicurezza" (una violazione, o minaccia di imminente violazione, delle norme di sicurezza), il soggetto competente allo svolgimento dei controlli avvii un processo di verifica al fine di:

a) accertare se si tratta di un incidente di sicurezza;

b) adoperarsi per contenere gli effetti dannosi provocati dall'incidente, isolando il sistema o i sistemi colpiti;

c) dare disposizioni affinché siano conservati i dati necessari da mettere eventualmente a disposizione delle autorità giudiziarie;

d) adoperarsi per ripristinare il sistema o i sistemi coinvolti;

e) effettuare un'analisi delle cause dell'incidente;

f) effettuare, nell'ipotesi in cui si riscontrino elementi che inducano ad ipotizzare un utilizzo improprio degli strumenti, le ulteriori verifiche necessarie ad acquisire i dati, anche personali, strettamente necessari da comunicare ai soggetti di cui alla lettera g);

g) redigere il "Rapporto incidente di sicurezza". (vedi Modello a pag. 112) Tale rapporto è integrato dalle prove raccolte, affinché i Responsabili dei sistemi coinvolti possano effettuare le ulteriori valutazioni e adottare le azioni conseguenti. Il Rapporto di incidente deve essere conservato agli atti, a cura della Struttura provinciale competente in materia di informatica, anche nel caso in cui i controlli siano affidati a soggetto esterno.

h) inviare, in forma riservata, il Rapporto incidente di sicurezza ai Responsabili coinvolti (ad esempio Responsabili del trattamento di dati personali, Responsabili della sicurezza o Responsabili dei Sistemi Informativi di altri enti, Responsabili dai quali il soggetto che ha provocato l'incidente dipende funzionalmente) o ad altri Titolari del trattamento di dati personali.

Relativamente ai log di navigazione è possibile, qualora sia riscontrato un incidente di sicurezza, verificare il contenuto dei siti visitati soltanto nel caso in cui le relative informazioni siano indispensabili al fine di accertare se vi sia stato un utilizzo proprio, o improprio, degli strumenti messi a disposizione dall'Amministrazione. Le ulteriori verifiche, inoltre, qualora sia necessario, possono essere effettuate sui dati relativi a più giornate lavorative, anche consecutive, con un limite massimo di 20 giornate lavorative.

Qualora, anche a seguito delle ulteriori verifiche effettuate, il soggetto competente allo svolgimento dei controlli riscontri elementi che confermino un possibile uso improprio delle strumentazioni messe a disposizione dalla Provincia, associa il nominativo dell'utilizzatore alla postazione client e successivamente procede come di seguito disciplinato:

- ✓ trasmette, al Dirigente di riferimento del soggetto coinvolto nel controllo, il Rapporto incidente di sicurezza affinché anch'egli possa effettuare le valutazioni di competenza, con particolare riferimento ad una verifica relativa alla pertinenza (o stretta attinenza) o meno dei dati di navigazione con l'attività lavorativa;
- ✓ contestualmente comunica, al soggetto coinvolto, la verifica in corso.

Sarà cura del Dirigente convocare il soggetto interessato per una tempestiva audizione, affinché possa fornire chiarimenti, motivazioni ed osservazioni a proposito di quanto rilevato. All'audizione può essere presente, su richiesta del Dirigente e/o del soggetto coinvolto, il Responsabile della Struttura provinciale competente in tema di informatica (o altro tecnico addetto alla sicurezza individuato dal Responsabile della Struttura provinciale competente in tema di informatica).

### 13.5.3.3- Verifiche periodiche

**I sistemi informativi sono soggetti a verifica costante (come desumibile chiaramente dagli articoli 31 e 33 nonchè dall'Allegato B del D.Lgs. n. 196/2003).**

Tali verifiche devono essere opportunamente documentate, da parte del personale che le effettua, e la documentazione deve essere conservata anche agli atti della Struttura provinciale competente in materia di informatica, pure nel caso in cui i controlli siano affidati a soggetto esterno.

Nell'ipotesi in cui si riscontri un incidente di sicurezza, si deve procedere come specificato al paragrafo 13.5.3.2;

I controlli devono essere effettuati, con cadenza periodica, e precedentemente pianificati. A seconda della frequenza con cui vengono svolti, si distinguono due ulteriori tipologie.

**13.5.3.3.1- Verifiche periodiche effettuate con cadenza inferiore ai 15 giorni**

Tali verifiche mirano al controllo della sicurezza dei trattamenti di dati personali effettuati; tutti gli utenti del Sistema informativo che gestisce i trattamenti della Provincia devono essere resi edotti di tali iniziative.

Esempi di tali attività sono:

a) verifiche giornaliere sui log del sistema firewall;
b) verifiche dei software installati sui sistemi server e client;
c) verifiche sul traffico di rete;
d) verifiche sull'efficienza dei sistemi proxy;
e) verifiche sui sistemi antivirus;
f) verifiche sull'efficacia dei filtri antispam.

**13.5.3.3.2-Verifiche periodiche effettuate con cadenza superiore ai 15 giorni**

Tali verifiche mirano al controllo sulla corretta applicazione e sull'efficiente funzionamento delle misure di sicurezza nell'ambito del Sistema informativo che gestisce i trattamenti della Provincia, e devono essere pianificate dal soggetto competente allo svolgimento dei controlli utilizzando il "Piano di Test" e condividendolo, preventivamente, con i soggetti interessati.

A titolo esemplificativo, rientrano in tale categoria le seguenti iniziative:

a) verifiche sull'avvenuta adozione e sul contenuto degli atti di designazione dei Responsabili esterni o degli Incaricati dei trattamenti di dati personali;
b) verifiche sui trattamenti della Provincia e sul loro continuo aggiornamento;
c) verifiche sulla corretta applicazione delle procedure di controllo degli accessi presso le portinerie;
d) verifiche sulle configurazioni dei sistemi server e client;
e) verifiche su sviluppo, configurazione e deployment delle applicazioni informatiche;
f) verifiche sugli accessi remoti alla rete provinciale (VPN, dial-up, ecc.);
g) verifiche sugli apparati di rete e sui sistemi (vulnerability scan, penetration test, ecc.);
h) verifiche sulla corretta applicazione delle misure di sicurezza previste nell'Allegato B del D.Lgs. n. 196/2003 nonché quelle consistenti nel rispetto dei comportamenti specificati nella Deliberazione della Giunta provinciale n. 1037/2010.

**13.5.3.4-Verifiche a campione**

Limitatamente ai dipendenti della Provincia, la Struttura provinciale competente in tema di sicurezza informatica (o l'eventuale affidatario esterno) può eseguire le medesime verifiche, esemplificate al paragrafo 13.5.3.3.2, anche a campione, con estrazione casuale e con cadenza trimestrale.

L'estrazione è pubblica: tramite un avviso sul sito intranet provinciale (http://verifichesicurezza.provincia.tn.it), vengono comunicati luogo e modalità dell'estrazione almeno 15 giorni prima della stessa.

Il campione controllato è costituito, in via alternativa:

a) da una percentuale pari allo 0,5% del totale delle postazioni client;

b) da tutte le postazioni client di una determinata struttura organizzativa.

Nell'ipotesi di cui alla lettera a), sono estratte a sorte, con un generatore di numeri casuali, le singole postazioni client fino al raggiungimento della percentuale sopra determinata.

Nell'ipotesi di cui alla lettera b), è estratta a sorte, con un generatore di numeri casuali, una struttura organizzativa, tra tutte quelle della Provincia, e sono sottoposte a controllo tutte le postazioni client assegnate alla struttura estratta.

L'identificativo univoco delle postazioni client è il numero di inventario della postazione stessa. Nel caso in cui la verifica coinvolga il controllo dei log di navigazione, l'indirizzo IP preso in considerazione è quello associato alla postazione di lavoro estratta e saranno considerati i log relativi alla giornata estratta e ai 4 giorni lavorativi successivi.
Relativamente allo svolgimento dell'attività, si applicano le stesse modalità delle verifiche programmate di cui al paragrafo 13.5.3.3.2.

Nel caso in cui, a seguito delle verifiche, si riscontri un incidente di sicurezza, il Responsabile della Struttura competente in tema di informatica (o l'eventuale affidatario esterno) deve procedere come specificato al paragrafo 13.5.3.2.

## 14. PRESCRIZIONI IN TEMA DI MISURE DI SICUREZZA

1. **UTILIZZATE LE CHIAVI**
Il primo livello di protezione di qualunque sistema è quello fisico; è vero che un armadio chiuso a chiave può in molti casi non costituire una protezione sufficiente, ma è anche vero che pone se non altro un primo ostacolo, e richiede comunque uno sforzo volontario, non banale, per aprirlo. Quando vi allontanate dal vostro ufficio, chiudete i documenti a chiave nei cassetti e/o negli armadi. Quando i documenti riservati sono conservati in armadi a vetri, è sempre meglio oscurarli, apponendo alle ante fogli di carta montati all'interno.

2. **CONSERVATE I SUPPORTI ESTRAIBILI (CDROM, CHIAVI USB, ETC.) IN UN LUOGO SICURO** Per i supporti estraibili si applicano gli stessi criteri stabiliti per i documenti cartacei, dovendo, però, considerare l'ulteriore rischio che il loro smarrimento (che può anche essere dovuto a un furto) può passare più facilmente inosservato. A meno che non siate sicuri che non contengano dati personali, riponeteli sotto chiave non appena avete finito di usarli.

3. **UTILIZZATE LE PASSWORD**
Vi sono svariate categorie di password, ognuna con il proprio ruolo preciso.
- La password di accesso al computer impedisce l'utilizzo, improprio, della vostra postazione, quando per un motivo o per l'altro non vi trovate in ufficio.
- La password di accesso, alla rete, impedisce che l'eventuale accesso non autorizzato a una postazione renda disponibili tutte le risorse dell'Ufficio.
- La password dei programmi specifici permette di restringere l'accesso ai dati al solo personale autorizzato.
- La password del salva-schermo, infine, impedisce che una vostra assenza momentanea permetta, a una persona non autorizzata, di accedere alle risorse del vostro computer.

4. **COME DEVE ESSERE SCELTA LA PASSWORD**
La parola chiave per l'accesso al sistema deve essere composta da almeno otto caratteri e, nel caso il sistema non lo consenta, da un numero di caratteri massimo consentito; la parola chiave non deve contenere caratteri riconducibili ad informazioni personali e/o di lavoro (ad esempio matricola, data di nascita) dell'Incaricato, ed è modificata al primo utilizzo e successivamente ogni sei mesi; per il trattamento dei dati sensibili e giudiziari la parola chiave deve essere modificata ogni tre mesi.
L'Amministrazione, ove possibile, adotterà meccanismi di obbligo del cambio password con le modalità e gli obblighi ritenuti opportuni od imposti dalla legge.

5. **NON FATEVI SPIARE QUANDO STATE DIGITANDO LE PASSWORD**
Anche se molti programmi non ripetono in chiaro la password sullo schermo, quando digitate la vostra password, questa potrebbe essere letta guardando i tasti che state battendo, anche se avete buone capacità di dattiloscrittura.

6. **CUSTODITE LE PASSWORD IN UN LUOGO SICURO**
Non scrivete la vostra password, meno che mai vicino alla vostra postazione di lavoro. Se avete necessità di conservare traccia delle password per scritto, non lasciate in giro i fogli utilizzati.

7. **PER EVITARE LA IDENTIFICAZIONE DELLA PASSWORD**
a) non comunicate, a nessuno, la Vostra password. Ricordate che lo scopo principale per cui usate una password è assicurare che nessun altro possa utilizzare le Vostre risorse o possa farlo a Vostro nome.

b) non scrivete la password da nessuna parte che possa essere letta facilmente, soprattutto vicino al computer.
c) quando immettete la password, non permettete, a nessuno, di vedere quello che state battendo sulla tastiera.
d) non scegliete password che si possano trovare nei dizionari delle lingue più diffuse ( ad esempio inglese, francese, spagnolo) oltre a quello italiano. Su alcuni sistemi è possibile "provare" tutte le password contenute in un dizionario, per verificare quale sia quella giusta.
e) non crediate che utilizzare parole straniere renderà più difficile il lavoro di scoperta; infatti, chi vuole scovare una password è dotato di molti dizionari delle più svariate lingue.
f) non usate il Vostro nome utente. È la password più semplice da indovinare.
g) non usate password che possano in qualche modo essere legate a Voi come, ad esempio, il Vostro nome, quello di Vostra moglie/marito, dei figli, del cane, date di nascita, numeri di telefono etc..
h) Una frode molto diffusa, che fa uso della posta elettronica, è il phishing. Si tratta di una metodologia di attacco informatico che si po' riassumere nelle seguenti fasi:
1. il phisher spedisce, al malcapitato e ignaro utente, un messaggio email che simula, nella grafica e nel contenuto, quello di una istituzione nota al destinatario (per esempio la sua banca, il suo provider web, un sito di aste online a cui è iscritto).
2. l'e-mail contiene quasi sempre avvisi concernenti particolari situazioni o problemi verificatisi con il proprio conto corrente/account (ad esempio un addebito enorme, la scadenza dell'account, ecc.) oppure un'offerta di denaro.
3. l'e-mail invita il destinatario a seguire un link, presente nel messaggio, per evitare l'addebito e/o per regolarizzare la sua posizione con l'ente o la società dei quali il messaggio simula la grafica e l'impostazione.
4. il link fornito, tuttavia, non porta, in realtà, ad alcun sito web ufficiale, ma a una copia fittizia, apparentemente simile al sito ufficiale, situata su un server controllato dal phisher, allo scopo di richiedere e ottenere dal destinatario dati personali particolari, normalmente con la scusa di una conferma o della necessità di effettuare una autenticazione al sistema; queste informazioni vengono memorizzate, dal server gestito dal phisher, e quindi finiscono nella disponibilità del malintenzionato.
5. il phisher utilizza questi dati per acquistare beni, trasferire somme di denaro o anche solo come "ponte" per ulteriori attacchi.

Si consiglia, quindi, di fare molta attenzione all'autenticità di e-mail che rimandano a siti che richiedono l'introduzione di dati personali, in modo tale da utilizzare in sicurezza le apparecchiature informatiche messe a disposizione dal datore di lavoro. In caso di dubbio, contattare l'indirizzo di posta dedicato alle problematiche di sicurezza **(sicurezza@infotn.it).**

## 8. ATTENZIONE ALLE STAMPE DI DOCUMENTI RISERVATI

Non lasciate accedere, alle stampe persone non autorizzate; se la stampante non si trova sulla vostra scrivania, recatevi quanto prima a ritirare le stampe. Distruggete, personalmente, le stampe quando non servono più. Se una stampante si blocca, assicuratevi (eventualmente coinvolgendo il referente informatico) che non restino dati importanti, o riservati, nella memoria della stampante, che potrebbero essere di nuovo inviati in stampa una volta che le funzionalità della stampante sono state ripristinate.

## 9. NON LASCIATE TRACCIA DEI DATI RISERVATI

Quando rimuovete un file, i dati non vengono effettivamente cancellati ma soltanto marcati come non utilizzati, e sono facilmente recuperabili. Neanche la formattazione assicura l'eliminazione dei dati; solo l'utilizzo di un programma apposito, garantisce che sul supporto estraibile non resti traccia dei dati precedenti. Nel dubbio, è sempre meglio usare un nuovo supporto estraibile.

10. **PRESTATE ATTENZIONE ALL'UTILIZZO DEI PC PORTATILI**
I PC portatili sono un facile bersaglio, per i ladri, anche fuori dalla sede di lavoro. Se avete necessità di gestire dati riservati su un portatile, fatevi installare un buon programma di cifratura del disco rigido, e utilizzate una procedura di backup periodico.

11. **NON FATE USARE IL VOSTRO COMPUTER A PERSONALE ESTERNO, A MENO DI NON ESSERE SICURI DELLA LORO IDENTITÁ**
Personale esterno può avere bisogno di installare un nuovo software/hardware nel vostro computer. Assicuratevi dell'identità della persona e delle autorizzazioni ad operare sul vostro PC.

12**. NON UTILIZZATE APPARECCHI NON AUTORIZZATI**
L'utilizzo di modem, su postazioni di lavoro collegate in rete, offre una porta d'accesso, dall'esterno, non solo al vostro computer, ma a tutta la Rete, ed è quindi vietato. Per l'utilizzo di altri apparecchi, consultatevi con il Responsabile del trattamento dati del vostro ufficio e con il referente informatico.

13. **NON INSTALLATE PROGRAMMI NON AUTORIZZATI**
Solo i programmi istituzionali, o acquistati dall'Amministrazione con regolare licenza, sono autorizzati. Se il vostro lavoro richiede l'utilizzo di programmi specifici, consultatevi con il Responsabile del trattamento dati e con il referente informatico.

14. **PER GARANTIRE IL RIPRISTINO DEI DATI EFFETTUARE DEI BACKUP PERIODICI.**
memorizzare i dati di interesse lavorativo sui dischi U e Y, ove disponibili; in caso contrario, effettuare il backup periodico per i trattamenti non gestiti da Informatica Trentina.

15. **APPLICATE CON CURA LE LINEE GUIDA PER LA PREVENZIONE DA INFEZIONI DI VIRUS**
La prevenzione dalle infezioni da virus, sul vostro computer, è molto più facile e comporta uno spreco di tempo molto minore della correzione degli effetti di un virus; tra l'altro, potreste incorrere nella perdita irreparabile dei dati.

***CHE COS'È UN VIRUS:***
Un virus è un programma in grado di trasmettersi autonomamente e che può causare effetti dannosi. Alcuni virus si limitano a riprodursi, senza ulteriori effetti; altri, si limitano alla semplice visualizzazione di messaggi sul video; i più dannosi arrivano a distruggere tutto o parte del contenuto del disco rigido.

***COME SI TRASMETTE UN VIRUS****:*
1. Attraverso programmi;
2. Attraverso le macro dei programmi di automazione d'ufficio;
3. Attraverso supporti esterni (ad esempio chiavi usb), contenenti file non controllati da antivirus.

***COME NON SI TRASMETTE UN VIRUS****:*
1. Attraverso file di dati non in grado di contenere macro (file di testo, html, pdf, ecc.);
2. Attraverso mail non contenenti allegati.

***QUANDO IL RISCHIO DA VIRUS SI FA SERIO***:
1. Quando si aprono messaggi di posta elettronica da mittenti sconosciuti contenenti allegati o collegamenti a siti internet;
2. Quando si copiano dati da supporti di memorizzazione;

3. Quando si scaricano dati o programmi da Internet.

***ALCUNI EFFETTI PROVOCATI DA VIRUS**:*
1. Effetti sonori e messaggi sconosciuti appaiono sul video;
2. Nei menù appaiono funzioni extra finora non disponibili;
3. Lo spazio disco residuo si riduce inspiegabilmente;
4. Rallentamenti inspiegabili del PC
5. Diffusione del virus su altre stazioni collegate al network aziendale.

***COME PREVENIRE I VIRUS:***
**1.Usate soltanto programmi provenienti da fonti fidate**
Copie sospette di programmi possono contenere virus o altro software dannoso. Ogni programma deve essere sottoposto alla scansione prima di essere installato. Non utilizzate programmi non autorizzati, con particolare riferimento ai videogiochi, che sono spesso utilizzati per veicolare virus.
**2. Assicuratevi di non far partire accidentalmente il vostro computer da supporto estraibile**
Infatti se il supporto estraibile fosse infettato, il virus si trasferirebbe nella memoria RAM, e potrebbe espandersi ad altri file.
**3. Assicuratevi che il vostro software antivirus sia aggiornato**
La tempestività nell'azione di bonifica è essenziale per limitare i danni che un virus può causare; inoltre è vitale che il programma antivirus conosca gli ultimi aggiornamenti sui nuovi virus in circolazione. (Attualmente, per le macchine collegate in rete, tutti i sistemi antivirus della Provincia vengono gestiti da Informatica Trentina, tramite un sistema di controllo, che provvede a segnalare, al presidio di assistenza delle postazioni di lavoro, le macchine che non sono aggiornate; per le macchine non collegate in rete l'aggiornamento è affidato al software antivirus che si aggiorna appena si collegano ad internet**)**

***COME EVITARE DI DIFFONDERE I VIRUS*:**
**4. Non diffondete messaggi di provenienza dubbia**
Se ricevete messaggi che avvisano di un nuovo virus pericolosissimo, ignorateli: le e-mail di questo tipo sono qualificate, con terminologia anglosassone, hoax (termine spesso tradotto in italiano con "bufala"), l'equivalente delle "leggende metropolitane" della rete. Questo è vero anche se il messaggio proviene dal vostro migliore amico, dal vostro capo, da un vostro parente o da un tecnico informatico. È vero anche, e soprattutto, se si fa riferimento a "una notizia proveniente dalla Microsoft" oppure dall'IBM (sono gli hoax più diffusi).
5. **Non partecipate a "catene di S. Antonio" e simili**
Analogamente, tutti i messaggi che vi invitano a "diffondere la notizia quanto più possibile", sono hoax.
Anche se parlano della fame nel mondo, della situazione delle donne negli stati arabi, di una bambina in fin di vita, se promettono guadagni miracolosi o grande fortuna, sono tutti hoax aventi spesso scopi molto simili a quelli dei virus, cioè utilizzare indebitamente le risorse informatiche.

## 16. POSTA ELETTRONICA/INTERNET
L'uso della Posta elettronica e di Internet deve essere improntato a quanto previsto nell'apposito disciplinare, adottato dalla Giunta provinciale con deliberazione n. 1037/2010.

## SEZIONE III: VIDEOSORVEGLIANZA

## 15. DOCUMENTO COORDINATO IN TEMA DI VIDEOSORVEGLIANZA

### 15.1. Deliberazione n. 2643/2008

A titolo di mero coordinamento, e per favorire una migliore gestione delle procedure di sicurezza delle informazioni, si riporta il contenuto della deliberazione della Giunta provinciale n. 2643/2008 (**Procedure operative di sicurezza delle informazioni attuate dalle strutture organizzative dipendenti dalla Giunta provinciale: approvazione del documento "Procedura operativa per la gestione dei dispositivi di videosorveglianza"**). In aggiunta alle prescrizioni della citata deliberazione, ancora attuali ed in vigore, sono evidenziati alcuni precetti, introdotti dal Garante per la protezione dei dati personali successivamente alla data del provvedimento provinciale.

**Deliberazione della Giunta provinciale n. 2643/2008**

“ll Relatore comunica:

con il presente provvedimento viene approvato il documento “Procedura operativa per la gestione dei dispositivi di videosorveglianza” la cui articolazione permette l’integrazione di questo insieme di disposizioni in un contesto più ampio nel rispetto di quanto previsto dalle metodologie internazionali di pianificazione della sicurezza delle informazioni che dispongono l’approvazione di documenti di dettaglio denominati procedure operative, regole standard o linee guida.
La presente “Procedura operativa per la gestione dei dispositivi di videosorveglianza”, pertanto, si affianca alle altre già esistenti in considerazione del fatto che la sicurezza nella gestione delle informazioni può essere garantita, esclusivamente, attraverso un sistema comune di disposizioni e misure nel quale la valenza di ogni singolo settore disciplinato dipende dal rispetto dal complesso di regole e contromisure contenute anche nelle altre singole procedure.
Altro scopo della “Procedura operativa per la gestione dei dispositivi di videosorveglianza” è altresì quello teso alla formalizzazione e alla documentazione di misure già adottate in materia di videosorveglianza dalle competenti strutture della Provincia Autonoma di Trento.
Nella documentazione vengono anche evidenziati mediante rappresentazione grafica il numero e la collocazione dei dispositivi di videosorveglianza attivati presso gli edifici ospitanti le strutture provinciali alla data di approvazione del presente documento. Gli eventuali aggiornamenti verranno inseriti nella apposita banca dati informatizzata a cura degli uffici competenti.
La procedura operativa è stata messa a punto grazie ad un lavoro comune delle strutture organizzative provinciali competenti in materia di informatica e in materia di logistica, con il supporto della struttura competente in materia di autonomie locali che si è avvalsa dell’esperienza acquisita su questo tema nel corso della collaborazione con il centro interuniversitario Transcrime - Università degli studi di Trento e Università Cattolica del S. Cuore di Milano per l'implementazione dell'Osservatorio sulla sicurezza in Trentino e del Sistema integrato di sicurezza il cui contributo si è concretizzato in uno studio generale che inquadra dal punto di vista giuridico la tematica della videosorveglianza e che viene allegato al presente provvedimento.
Tutto ciò premesso, il Relatore propone di approvare la “Procedura operativa per la gestione dei dispositivi di videosorveglianza”, assieme allo studio di Transcrime “Installare un sistema di videosorveglianza per ragioni di sicurezza ovvero tutela del patrimonio” e alla mappatura dei dispositivi di videosorveglianza installati nelle strutture provinciali alla data del presente provvedimento .

Tutto ciò premesso,

LA GIUNTA PROVINCIALE

- udito il Relatore;

- visto il Decreto legislativo n. 196/2003;
- vista la propria deliberazione n. 3372 di data 30 dicembre 2003;
- vista la propria deliberazione n. 232 di data 09 febbraio 2007;

a voti unanimi, espressi nelle forme di legge,

d e l i b e r a

1. di approvare l'allegato "A", parte integrante del presente provvedimento, dal titolo "Procedura operativa per la gestione dei dispositivi di videosorveglianza" dando atto che la disciplina in materia coinvolge competenze sia della struttura organizzativa competente in materia di logistica che della struttura organizzativa competente in materia di informatica;
2. di dare atto che quanto previsto nell'allegato "A" tiene conto dei risultati dello studio di Transcrime dal titolo "Installare un sistema di videosorveglianza per ragioni di sicurezza ovvero tutela del patrimonio gli adempimenti da seguire per un soggetto pubblico" contenuto nell'allegato "B" allegato al presente provvedimento a titolo di documentazione;
3. di dare atto che i dispositivi di videosorveglianza, installati negli edifici che ospitano strutture provinciali alla data del presente provvedimento, sono evidenziati a titolo di documentazione nell'allegato "C" del medesimo provvedimento, che riporta la mappatura delle telecamere contenuta nella banca dati del cui aggiornamento viene incaricata la struttura competente in materia di logistica.

**Allegato parte integrante**
Allegato A

**Procedura operativa per gestione dei dispositivi di videosorveglianza**

**Indice generale**

**1. <u>Premessa</u>**

I sistemi di videosorveglianza trattano dati personali. La voce e l'immagine, infatti, sono da considerarsi, in base alla Direttiva 95/46/CE ed alla normativa italiana, informazioni riferite ad una persona identificata o identificabile. Per questo motivo il Garante è intervenuto per individuare un punto di equilibrio tra esigenze di sicurezza, prevenzione e repressione dei reati, e diritto alla riservatezza e libertà delle persone. Come in tutti gli altri casi anche il trattamento dei dati attraverso sistemi di videosorveglianza da parte della Provincia è possibile solo se è fondato sul presupposto di liceità che il Codice prevede per gli organi pubblici (svolgimento di funzioni istituzionali: artt. 18-22). La videosorveglianza deve avvenire nel rispetto, oltre che della disciplina in materia di protezione dei dati, di quanto prescritto da altre disposizioni di legge da osservare in caso di installazione di apparecchi audiovisivi. Vanno richiamate al riguardo le vigenti norme dell'ordinamento civile e penale in materia di interferenze illecite nella vita privata, di tutela della dignità, dell'immagine, del domicilio e degli altri luoghi cui è riconosciuta analoga tutela (toilette, stanze d'albergo, cabine, spogliatoi, ecc.). Vanno tenute presenti, inoltre, le norme riguardanti la tutela dei lavoratori, con particolare riferimento alla legge 300/1970 (Statuto dei lavoratori). Specifici limiti possono derivare da altre speciali disposizioni di legge o di regolamento.

## 2. Scopo del presente documento

Scopo del presente documento è la formalizzazione e la documentazione delle misure già adottate in materia di videosorveglianza dagli uffici competenti della Provincia Autonoma di Trento. Vengono anche evidenziate in allegato anche mediante rappresentazione grafica il numero e la collocazione dei dispositivi di videosorveglianza attivati presso le strutture provinciali alla data di approvazione del presente documento. Gli eventuali aggiornamenti verranno inseriti a cura delle strutture competenti nella apposita banca dati informatizzata attivata dal Servizio organizzazione e Informatica.

## 3. Ruoli di titolare, responsabile e incaricato del trattamento

Come per tutti gli altri trattamenti in atto titolare del trattamento, ai sensi di quanto previsto dal Dlgs. 196/2003, è la Provincia Autonoma di Trento. Per quanto riguarda il caso specifico della videosorveglianza vanno individuati tre casi distinti per la determinazione del responsabile del trattamento.

### 3.1 Dispositivi di videosorveglianza senza registrazione dei dati

Nei casi cui i dispositivi di videosorveglianza non effettuano la registrazione delle immagini e sono utilizzati solo per la sorveglianza a vista, va considerato responsabile del trattamento il dirigente della struttura competente per la gestione del personale di sorveglianza che a sua volta assume il ruolo di incaricato del trattamento.

### 3.2 Dispositivi di videosorveglianza con registrazione dei dati senza sorveglianza a vista

Nei casi cui i dispositivi di videosorveglianza effettuano la registrazione delle immagini senza essere utilizzati per la sorveglianza a vista, va considerato responsabile del trattamento il dirigente della struttura competente per la gestione dei dispositivi stessi sia nel caso di dispositivi gestiti direttamente dalla struttura che nel caso di dispositivi con gestione appaltata all'esterno. Il personale incaricato dal responsabile del recupero delle immagini in caso di bisogno assume il ruolo di incaricato del trattamento.

### 3.3 Dispositivi di videosorveglianza con registrazione dei dati e sorveglianza a vista

Nei casi in cui i dispositivi di videosorveglianza effettuano la registrazione delle immagini e contemporaneamente vengono utilizzati per la sorveglianza a vista, va considerato responsabile del trattamento sia il dirigente della struttura competente per la gestione dei dispositivi stessi che il dirigente della struttura cui è assegnata la gestione del personale addetto alla sorveglianza a vista. Il personale di sorveglianza assume il ruolo di incaricato del trattamento. Il personale incaricato dal responsabile del recupero delle immagini in caso di bisogno assume il ruolo di Incaricato del trattamento.

## 4. Limiti di utilizzo delle immagini

Le immagini acquisite attraverso i dispositivi di cui al punto 3 possono essere utilizzate esclusivamente dal responsabile del trattamento e su suo ordine dagli incaricati del trattamento per le finalità assegnate all'attività di videosorveglianza.

## 5. Procedura di accesso alle immagini registrate

Per alcuni siti, l'accesso alle immagini registrate può avvenire sia sul posto che da remoto. L'accesso da remoto avviene su un unico PC, collocato presso il Servizio Edilizia Pubblica e

Logistica, mediante apposito software e password di accesso. Negli altri casi il recupero delle immagini registrate può avvenire solo dalla postazione centrale dislocata presso l'edificio coperto dalla videosorveglianza.
Nel caso di manutenzione dei dispositivi di videosorveglianza il personale addetto sarà accompagnato dal personale incaricato dal dirigente competente.
La richiesta di accesso può essere presentata dall'interessato e/o da altro soggetto legittimato (autorità giudiziaria, forze dell'ordine) al Servizio Edilizia Pubblica e Logistica. Il Dirigente provvederà a dare le opportune autorizzazioni e impartire disposizioni al personale del Servizio o al responsabile della ditta manutentrice dell'impianto, responsabili del recupero delle immagini, che potranno, se richiesto, essere riversate su apposito supporto informatico".

**15.2. Precetti nuovi introdotti dal Garante (punto specifico da coordinare con la deliberazione 2643/2008)**

Nelle strutture dove sono attivati sistemi di videosorveglianza, finalizzati alla protezione dei dipendenti, dei visitatori e del patrimonio, deve essere affissa apposita informativa che informi il pubblico della presenza degli impianti e delle finalità perseguite attraverso la videosorveglianza. I pannelli devono essere affissi in prossimità degli ingressi ed essere visibili a chi vi accede.
Nella gestione dei sistemi di videosorveglianza, inoltre, è necessario rispettare i seguenti principi:
a) limitazione delle modalità di ripresa delle immagini (memorizzazione, angolo visuale delle telecamere e limitazione della possibilità di ingrandimento dell'immagine), avendo attenzione alla individuazione del livello di dettaglio della ripresa dei tratti somatici delle persone, in ordine alla pertinenza e non eccedenza dei dati rispetto agli scopi perseguiti;
b) limitazione dei tempi di conservazione delle immagini (nel caso specifico in cui il trattamento dati sia effettuato mediante sistemi di videosorveglianza, la conservazione deve essere limitata, al massimo, alle ventiquattrore successive alla rilevazione, fatte salve alcune specifiche ipotesi (festività o chiusura uffici; richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria). In ulteriori e peculiari casi, per esigenze tecniche (mezzi di trasporto) o per la pericolosità dell'attività esercitata dal Titolare del trattamento (es. banca), la conservazione dei dati può essere assoggettata ad un termine più lungo, che non potrà, in ogni caso, superare la settimana);
c) individuazione dei soggetti legittimati ad accedere alle registrazioni;
d) indicazione del soggetto e della struttura cui l'interessato può rivolgersi e dei diritti che può esercitare.
Per tutto quanto non previsto nella presente deliberazione, si rinvia al Provvedimento a carattere generale, del Garante, dell'8 aprile 2010.

## SEZIONE IV - “MODULISTICA”

## *1.* MODELLO DI ISTANZA ESERCIZIO DIRITTI

**ai sensi dell'art. 7 del Codice in materia di protezione dei dati personali**
*(l'utilizzo di tale modello non è obbligatorio, ma le strutture possono metterlo a disposizione dei soggetti interessati al trattamento che intendano esercitare i diritti di cui all'art. 7 del Codice)*

[indirizzo del Responsabile del trattamento]

**OGGETTO**: istanza ai sensi dell'art. 7 del Codice in materia di protezione dei dati personali

Il sottoscritto _____ nato a _____ il _____, residente a _____, con la presente istanza si rivolge alla Provincia autonoma di Trento, nella persona del Responsabile del trattamento dei dati personali/Dirigente del Servizio _____ /Dipartimento _____, per l'esercizio dei diritti di cui all'art. 7 del Codice in materia di protezione dei dati personali ed in particolare:

- per avere conferma dell'esistenza di propri dati personali e per ottenerne la comunicazione in forma intelligibile;
- per conoscere l'origine dei dati medesimi;
- per conoscere le finalità e la logica su cui si basa il trattamento.
- ...

*(indicare la o le richieste che interessano)*

Si segnala che, in caso di mancato o inidoneo riscontro alla presente istanza, il sottoscritto si riserva di rivolgersi all'autorità giudiziaria o di presentare ricorso al Garante per la protezione dei dati personali.

FIRMA dell'interessato
*(cioè del soggetto cui si riferiscono i dati richiesti)*

**Avvertenze:**

1. *Il modello di istanza di accesso ai dati personali di cui sopra può essere utilizzato, con le opportune modifiche, anche per esercitare gli altri diritti tutelati dal medesimo art. 7 del Codice ed in particolare:*
   - *per chiedere l'aggiornamento, la rettificazione o l'integrazione dei propri dati personali eventualmente raccolti e trattati in modo incompleto o inesatto;*
   - *per chiedere la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge;*
   - *per opporsi in tutto o in parte, per motivi legittimi, al trattamento dei dati personali che lo riguardano.*
2. *Si consiglia di inviare l'istanza di esercizio dei diritti mediante raccomandata con avviso di ricevimento, allo scopo di avere prova della data di spedizione e di ricezione della stessa (specie in vista dell'eventuale presentazione di un ricorso in merito).*

## *2*. Modello di nomina ad Incaricato interno del trattamento

**Ordine di servizio**

**…….…….**

**Numero …….. del ……**

**Oggetto: Codice in materia di protezione dei dati personali - nomina ad incaricato.**

- Visto il Codice in materia di protezione dei dati personali;
- Considerato che la Provincia autonoma di Trento è Titolare dei trattamenti di dati personali funzionali all'esercizio delle proprie competenze istituzionali, ai sensi di quanto disposto con la deliberazione della Giunta provinciale n. del (**indicare estremi della deliberazione della Giunta provinciale che ha approvato il presente modello)**;
- Appurato che l'articolo 30, comma 1, del Codice in materia di protezione dei dati personali prevede che il trattamento dei dati possa essere effettuato solo da Incaricati che operano sotto la diretta autorità del Titolare o del Responsabile, attenendosi alle loro istruzioni;
- Constatato che l'articolo 30, comma 2, del Codice in materia di protezione dei dati personali impone che la designazione degli Incaricati sia effettuata, per iscritto, e specifichi, con precisione, l'ambito del trattamento consentito;
- Considerato che il medesimo articolo 30, comma 2, considera valida designazione anche la documentata preposizione della persona fisica ad unità per la quale è individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità organizzativa;
- Constatato che la Provincia autonoma di Trento si è dotata di un elenco informatizzato dei trattamenti (raggiungibile all'indirizzo http://**trattamenti.provincia.tn.it**);
- Appurato che nel richiamato elenco viene analiticamente individuato il contenuto dei trattamenti di ogni struttura provinciale;
- Considerato che, come puntualmente specificato nell'Allegato B della **deliberazione** della Giunta provinciale **n. del (indicare estremi della deliberazione della Giunta provinciale che ha approvato il presente modello)**, la designazione è valida solo se il correlativo elenco informatizzato dei trattamenti provinciali è costantemente aggiornato;

**il sottoscritto**

in qualità di **Dirigente** del **Servizio/Dipartimento _____**

- nominato, ai sensi dell'art. 29 del Codice, **Responsabile per i trattamenti di dati personali** relativi alle materie di competenza del citato Servizio/Dipartimento, con deliberazione della Giunta provinciale n… del (**indicare estremi della deliberazione della Giunta provinciale che ha approvato il presente modello)**;

**NOMINA**

**Incaricato/i dei trattamenti dei dati personali,** di pertinenza della struttura (incluse le relative banche dati), così come individuati nell'elenco informatizzato dei trattamenti provinciali (raggiungibile all'indirizzo http://**trattamenti.provincia.tn.it**):

**1) Elenco incaricati come specificato nell'elenco informatizzato**

**2) Si riportano di seguito le PRINCIPALI ISTRUZIONI per il trattamento:**

**Regole generali per tutti i trattamenti**

Nello svolgimento del trattamento devono essere osservate le norme di legge e di regolamento in materia di tutela della riservatezza dei dati personali e devono essere applicate le misure di sicurezza previste nell'**Allegato B della deliberazione** della Giunta provinciale **n…del… (indicare estremi della deliberazione della Giunta provinciale che ha approvato il presente modello).**
Il trattamento dei dati, ai sensi dell'art. 11 del Codice, deve rispettare il principio **di pertinenza e non eccedenza** rispetto alle finalità del medesimo: è consentito l'accesso ai soli dati personali la cui conoscenza sia strettamente indispensabile per adempiere i compiti affidati.
I dati devono essere trattati in modo **lecito e secondo correttezza ed** essere **esatti ed aggiornati**.
L'Incaricato, in particolare, nello svolgimento del trattamento, è tenuto a:

- **accertare** che l'**informativa, completa in tutte le sue parti,** venga comunicata agli interessati, ai sensi dell'art. 13 del Codice in materia di dati personali, e verificare che ciascuna operazione di comunicazione e diffusione dei dati sia conforme alle disposizioni di legge e regolamento;
- **consentire** l'esercizio dei diritti e delle facoltà previste dall'art. 7 del D.lgs. n. 196/2003 (e cioè fornire conferma, all'interessato, dell'esistenza o meno dei dati che lo riguardano; indicare le finalità e modalità del trattamento ed ogni altra attività connessa allo stesso; provvedere, previa espressa richiesta informale e scritta dell'interessato, all'aggiornamento dei dati nonché alla loro rettificazione, integrazione, cancellazione, trasformazione in forma anonima o al blocco qualora trattati in violazione della legge);
- **collaborare**, con gli altri incaricati del medesimo trattamento, esclusivamente per i fini dello stesso e nel rispetto delle indicazioni fornite;
- **non trasmettere**, a soggetti terzi, informazioni circa dati personali trattati. La comunicazione è ammessa soltanto se funzionale allo svolgimento dei compiti affidati, previa autorizzazione del Responsabile del trattamento;
- **accertarsi** dell'identità del diretto interessato, prima di fornire informazioni circa i dati personali o il trattamento effettuato;
- **riporre in archivio,** al termine del periodo di trattamento, i supporti o i documenti, ancorchè non definitivi, contenenti i dati personali;
- **conservare i dati** trattati per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono raccolti e successivamente trattati.

Devono essere rispettate tutte le istruzioni impartite dal Titolare, nonché le istruzioni e direttive impartite dallo scrivente, in qualità di Responsabile del trattamento.

L'Incaricato, per il corretto e puntuale svolgimento del trattamento, dovrà: 1) procedere all'acquisizione, sul sito istituzionale della Provincia, delle deliberazioni della Giunta provinciale in tema di privacy (**deliberazione n…del… (indicare estremi della deliberazione della Giunta provinciale che ha approvato il presente modello)**, n. 2643/2008, n. 1037/2010 ecc.) e rispettare le prescrizioni in esse contenute; 2) visionare, nell'elenco informatizzato, il contenuto dei trattamenti assegnati.

**Nel caso di presenza di ospiti o personale di servizio sarà necessario:**

- **fare attendere** in luoghi in cui non sono presenti informazioni riservate o dati personali;
- **evitare di allontanarsi** dalla scrivania in presenza di ospiti o riporre i documenti e attivare il salvaschermo del PC;
- **non rivelare** o far digitare la password al personale di assistenza tecnica;
- **non rivelare** le password al telefono ne inviarle via fax ; nessuno è autorizzato a chiederle;
- **segnalare** qualsiasi anomalia e stranezza al Responsabile.

**Trattamenti concernenti dati sensibili e giudiziari**

L'Incaricato è autorizzato al trattamento dei dati sensibili e giudiziari (articoli 20, 21 e 22 del Codice) indicati nell'elenco informatizzato dei trattamenti ad esso assegnati.

**Modalità di trattamento dei dati sensibili/giudiziari.**

Ferma restando l'applicazione delle disposizioni vigenti in materia di trattamento dei dati sensibili e giudiziari e delle istruzioni impartite dal Titolare e dal Responsabile del trattamento, si riportano alcune specifiche misure da applicarsi in caso di trattamento dei predetti dati:

- **non fornire** dati o informazioni di carattere sensibile per telefono, qualora non si abbia certezza assoluta sull'identità del destinatario;
- **evitare di inviare**, per fax, documenti in chiaro contenenti dati sensibili: si suggerisce, in tal caso, di inviare la documentazione, senza alcun esplicito riferimento all'interessato (ad esempio, contrassegnando i documenti semplicemente con un codice);
- i documenti, ancorchè non definitivi, ed i supporti recanti dati sensibili o giudiziari, devono essere conservati, anche in corso di trattamento, in elementi di arredo muniti di serratura e non devono essere lasciati incustoditi in assenza dell'Incaricato;

*(nel caso di trattamenti di dati inerenti la salute)*

- i supporti ed i documenti, recanti dati relativi alla salute e alla vita sessuale, devono essere conservati nei predetti contenitori muniti di serratura, separatamente da ogni altro documento;
- per la redazione, la pubblicazione, la comunicazione ed il rilascio degli atti recanti dati idonei a rivelare lo stato di salute, devono essere osservate, in aggiunta alle norme di legge e di regolamento, le prescrizioni contenute nella deliberazione della Giunta provinciale n…del… (**indicare estremi della deliberazione della Giunta provinciale che ha approvato il presente modello).**

**Trattamenti con strumenti elettronici**

Per quanto riguarda, in particolare, le elaborazioni e le altre fasi dei trattamenti effettuate attraverso strumenti informatici, ciascun Incaricato disporrà di una parola chiave per l'accesso ai dati e di un codice identificativo personale.

Gli Incaricati avranno cura di:

- **non condividere** il proprio codice identificativo personale con altri utenti, salvo i casi espressamente previsti;
- **non cedere a terzi** la propria parola chiave di autenticazione;
- **non accedere** a servizi non consentiti;
- **non caricare** ed eseguire software di rete o di comunicazione, senza previa verifica dello stesso da parte del proprio Referente informatico, che opera in stretto rapporto con il Servizio Supporto Amministrativo e Informatica**;**
- **non tentare** di acquisire i privilegi di Amministratore di sistema;
- **verificare** l'assenza di virus nei supporti utilizzati;
- **non collegare** dispositivi che consentano un accesso, non controllabile, ad apparati della rete della Provincia;
- **memorizzare** i dati di interesse lavorativo sui dischi U e Y, ove disponibili; in caso contrario, effettuare il backup periodico per i trattamenti non gestiti da Informatica Trentina;
- **procedere alla cancellazione** dei supporti magnetici od ottici contenenti dati personali, prima che i medesimi siano riutilizzati. Se ciò non è possibile, essi devono esser distrutti;
- **attenersi alle istruzioni** specificate nel capitolo 14 **("Prescrizioni in tema di Misure di Sicurezza**") dell'Allegato B) della deliberazione della Giunta provinciale n… del.. **(indicare estremi della deliberazione della Giunta provinciale che ha approvato il presente modello)**.

**Banche dati**

La visione dei dati, contenuti nelle banche dati, esclude comunque qualsiasi forma di comunicazione, diffusione e trattamento degli stessi che non sia strettamente funzionale all'espletamento dei compiti d'istituto e che non si svolga nei limiti stabiliti da leggi e regolamenti.

**Trattamenti senza strumenti elettronici**

Per quanto riguarda la eventuale documentazione cartacea, compresi i supporti non informatici contenenti la riproduzione di informazioni relative al trattamento di dati personali, gli atti e i documenti contenenti i dati devono essere conservati, dagli Incaricati, per la durata del trattamento e successivamente riposti in archivi ad accesso controllato, secondo quanto sarà indicato di volta in volta, al fine di escludere l'accesso, agli stessi, da parte di persone non incaricate al trattamento.

Nel caso di trattamento di dati sensibili o di dati giudiziari, gli atti e i documenti, contenenti i dati affidati agli Incaricati del trattamento, devono essere conservati in contenitori muniti di serratura, al fine di escludere l'acquisizione, degli stessi, da parte di persone non incaricate del trattamento.

Qualora sia necessario distruggere i documenti contenenti dati personali, utilizzare gli appositi apparecchi "distruggi documenti"; in assenza di tali strumenti, i documenti devono essere sminuzzati in modo da non essere più ricomponibili;

Gli incaricati sono tenuti a segnalare le eventuali necessità di dotazioni e arredi, in modo da poter adempiere a quanto prescritto.

Analogamente, per quanto riguarda i flussi di documenti cartacei all'interno degli uffici provinciali, devono essere adottate idonee misure organizzative per salvaguardare la riservatezza dei dati personali (es. trasmissione dei documenti in buste chiuse).

Nel caso di trasferimento, anche temporaneo, ad altra struttura/ufficio, o nell'ipotesi di cessazione del rapporto di lavoro, l'Incaricato perde i privilegi di accesso ai dati personali attribuiti all'ufficio di provenienza; la nomina si intenderà revocata con la cancellazione dell'Incaricato dall'elenco informatizzato dei trattamenti.

Data _____

| | |
|---|---|
| Firma<br>del DIRIGENTE/RESPONSABILE DEL TRATTAMENTO | Firma, per presa visione,<br>dell'INCARICATO DEL TRATTAMENTO |

## 3. Modello di nomina ad Incaricato esterno del trattamento

Oggetto: Nomina a Incaricato esterno del trattamento di dati personali ai sensi dell'art. 30 del D. Lgs. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali".

L'art. 30 del D.Lgs. 30 giugno 2003, n. 196 "Codice in materia di trattamento dei dati personali (di seguito, "Codice"), relativo alla tutela delle persone rispetto al trattamento dei dati personali, impone che i soggetti che effettuano il trattamento di dati personali, per conto del Titolare dei dati medesimi, assumano il ruolo di Incaricato del trattamento. Tale individuazione è inoltre prevista da diversi articoli (1, 13, 14, e 15) dell'Allegato B del Codice (Disciplinare tecnico in materia di misure minime di sicurezza).

Ai sensi e per gli effetti delle citate disposizioni normative, nello svolgimento del proprio incarico, Lei assume il ruolo di Incaricato del trattamento dei soli dati personali della Provincia autonoma di Trento, la cui conoscenza sia strettamente necessaria per adempiere ai compiti previsti nell'incarico di collaborazione a Lei affidato dalla Provincia autonoma di Trento.

Nello svolgimento delle operazioni di trattamento dei dati, Lei dovrà rispettare la massima riservatezza e discrezione, ponendo in essere ogni attività necessaria ad evitare i rischi di perdita o distruzione, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alla finalità per cui i dati sono stati raccolti, in osservanza delle disposizioni previste dal Codice e dalle relative norme di attuazione.

In qualità di Incaricato, inoltre, Lei dovrà rispettare le istruzioni e le procedure in materia di privacy adottate dalla Provincia (e riportate nella deliberazione della Giunta provinciale n. del e ss. mm. (**indicare estremi della deliberazione della Giunta provinciale che ha approvato il presente modello**). In particolare, e a titolo meramente esemplificativo, Lei dovrà:

1. in caso di trattamento di dati personali sensibili su elaboratore non collegato alla rete informatica provinciale, salvare i files con password di protezione di almeno otto caratteri e non agevolmente identificabile;
2. in caso di accesso alle risorse di rete e agli applicativi della Provincia, rispettare le regole di composizione delle password di accesso richieste dal sistema informatico provinciale;
3. non lasciare incustodito, e accessibile, lo strumento elettronico durante una sessione di trattamento;
4. conservare, con massimo riserbo, e riporre negli archivi di origine, i documenti contenenti dati personali al termine delle operazioni affidate;
5. conservare accuratamente i documenti, fino alla restituzione;
6. procurarsi e rispettare le istruzioni riportate nella deliberazione della Giunta provinciale n. del (**indicare estremi della deliberazione della Giunta provinciale che ha approvato il presente modello**).

La presente nomina ha durata pari alla durata del contratto e si intenderà revocata all'atto della conclusione del contratto stesso, per qualsiasi causa ciò avvenga. Al termine del rapporto contrattuale, l'Incaricato dovrà restituire tutti i dati personali, appartenenti alla Provincia di Trento, di cui fosse in possesso, e provvedere ad eliminarli, definitivamente, dal proprio sistema informativo e dai propri archivi cartacei, dandone conferma per iscritto all'ente titolare del trattamento.

Distinti saluti.

Trento, _____

firma Dirigente/Responsabile del trattamento

## *4.* Modello di nomina a Responsabile esterno del trattamento

Il/la sottoscritto/a Dirigente del Servizio/Dipartimento……, in nome e per conto della Provincia autonoma di Trento - Titolare del trattamento di dati personali relativi alle attività istituzionali di competenza;

preso atto che l'affidamento del servizio di ……. con contratto (o altro titolo giuridico) n…… in data ……., comporta anche il trattamento di dati personali, ed è quindi soggetto alla normativa in materia di protezione dei dati personali, emanata con il decreto legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali);

vista la deliberazione della Giunta provinciale n…… del …. (**indicare estremi della deliberazione della Giunta provinciale che ha approvato il presente modello**) con la quale il sottoscritto è stato nominato Responsabile del trattamento, in relazione ai trattamenti di dati personali, svolti nell'ambito della struttura dirigenziale di competenza;

ai sensi dell'articolo 29 (Responsabile del trattamento) del d.lgs. 196/2003;

**NOMINA**

Il/la (**indicare persona fisica, persona giuridica ecc**.), nella persona del sig……, legale rappresentante della stessa (specificazione necessaria nei soli casi di persone giuridiche), Responsabile esterno del trattamento dei dati personali, utilizzati per lo svolgimento del servizio affidatogli con il citato contratto, nel rispetto di tutte le norme relative all'applicazione del d.lgs 196/2003.

In particolare, il Responsabile esterno del trattamento dovrà:

a) garantire la riservatezza delle informazioni, dei documenti e degli atti amministrativi, dei quali venga a conoscenza durante l'esecuzione della prestazione;
b) utilizzare i dati solo per le finalità connesse allo svolgimento dell'attività oggetto del contratto, con divieto di qualsiasi altra diversa utilizzazione. Il Responsabile esterno non produce copie dei dati personali e non esegue nessun altro tipo di trattamento che non sia attinente allo scopo dei servizi offerti; non potrà, inoltre, diffondere, né comunicare, dati oltre ai casi previsti nel contratto o necessari per l'adempimento dello stesso. In nessun caso il Responsabile esterno acquisisce la proprietà intellettuale di dati e informazioni trattati nell'ambito di svolgimento del contratto;
c) adottare preventive misure di sicurezza atte ad eliminare o, comunque, a ridurre al minimo, qualsiasi rischio di distruzione o perdita, anche accidentale, dei dati personali trattati, di accesso non autorizzato o di trattamento non consentito o non conforme, nel rispetto delle disposizioni contenute nell'articolo 31 del d.lgs. 196/2003;
d) adottare e rispettare tutte le misure di sicurezza previste dagli articoli 33, 34, 35 e 36 del d.lgs. 196/2003, che configurano il livello minimo di protezione richiesto in relazione ai rischi indicati all'articolo 31, e analiticamente specificate nell'allegato B ("Disciplinare tecnico in materia di misure minime di sicurezza") del citato decreto. Qualora, ai sensi delle norme concernenti le misure minime di sicurezza, risulti necessario un adeguamento delle stesse, il Responsabile esterno provvede, nei termini di legge, al relativo adeguamento, senza alcun costo aggiuntivo per la Provincia;
e) individuare, per iscritto, le persone Incaricate del trattamento e fornire loro le istruzioni relative alle operazioni da compiere, affinché il trattamento avvenga in conformità alla legge, per gli scopi e le finalità previste in contratto e nel rispetto delle misure minime 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, previste dal Codice, e

delle disposizioni impartite dal Titolare. Vigilare sulla corretta osservanza delle istruzioni impartite;

f) rispettare le istruzioni e le procedure in materia di privacy, adottate dalla Provincia **(e riportate nella deliberazione della Giunta provinciale (n. del ) (indicare estremi) che ha approvato il presente modello)** per garantire la sicurezza dei dati personali; in particolare, qualora gli Incaricati del Responsabile esterno accedano, per esigenze di servizio, alle sedi o al sistema informativo del Titolare. Il Responsabile esterno risponderà di eventuali violazioni ai sensi dell'art. 2049 del codice civile;

g) provvedere alla formazione degli incaricati;

h) verificare annualmente lo stato di applicazione del d.lgs. 196/2003

i) adempiere agli obblighi relativi alla riservatezza, alla comunicazione ed alla diffusione dei dati personali anche dopo che l'incarico è stato portato a termine o revocato;

j) comunicare, tempestivamente, al sottoscritto, responsabile del Settore ……., le eventuali richieste degli interessati all'accesso, alla rettifica, all'integrazione, alla cancellazione dei propri dati, ai sensi dell'articolo 7 (diritto di accesso ai dati personali ed altri diritti) del d.lgs. 196/2003;

k) avvisare, tempestivamente, il Titolare qualora ricevesse ispezioni o richieste di informazioni, documenti od altro, da parte del Garante, in merito ai trattamenti effettuati per la Provincia autonoma di Trento;

l) fornire al Titolare, a semplice richiesta e secondo le modalità indicate da quest'ultimo, i dati e le informazioni necessari per consentire, allo stesso, di svolgere una tempestiva difesa in eventuali procedure instaurate davanti al Garante o all'Autorità Giudiziaria e relative al trattamento dei dati personali connessi all'esecuzione del contratto in vigore tra le parti;

m) consentire che il Titolare – come imposto dalla normativa – effettui verifiche periodiche in relazione al rispetto delle presenti disposizioni.

Si precisa che tale nomina sarà valida per il tempo necessario ad eseguire le operazioni affidate dal Titolare e si considererà revocata a completamento dell'incarico. All'atto della cessazione delle operazioni di trattamento, il Responsabile esterno dovrà restituire tutti i dati personali del Titolare, a quest'ultimo, e provvedere ad eliminare definitivamente dal proprio sistema informativo, e dagli archivi cartacei, i medesimi dati o copie degli stessi, dandone conferma per iscritto al Titolare.
Il Titolare e il Responsabile esterno si mantengono vicendevolmente indenni per qualsiasi danno, incluse le spese legali, che possa derivare da pretese, avanzate nei rispettivi confronti a seguito dell'eventuale illiceità o non correttezza delle operazioni di trattamento che siano imputabili a fatto, comportamento od omissione dell'altro.

per la Provincia autonoma di Trento
Il Responsabile – Dirigente

## *5.* Modello di nomina ad Amministratore di Sistema

**OGGETTO: Nomina ad "Amministratore di Sistema", ai sensi del provvedimento a carattere generale del Garante per la protezione dei dati personali del 27 novembre 2008 (G.U. n. 300 24/12/2008).**

La Provincia autonoma di Trento, Titolare del trattamento dei dati personali ai sensi dell'art. 4, comma 1, lett. f), del D. Lgs n.196/2003, nella persona del Responsabile del trattamento dei dati, Dr. _____, nominato con Deliberazione della Giunta provinciale numero……del….. (**indicare estremi deliberazione della Giunta provinciale che ha approvato il presente modello**), considerato:
-il rapporto di lavoro con Lei in vigore, la sua qualifica e la documentata preposizione alla unità operativa di appartenenza;
-che le prestazioni da lei effettuate, in via ordinaria, forniscono idonea garanzia del pieno rispetto delle caratteristiche di esperienza, capacità e affidabilità, nonché delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza;

La nomina, con la presente, incaricato con funzioni di "**Amministratore di sistema**" per i trattamenti svolti per conto della Provincia, con riguardo agli ambiti e ai compiti riportati, a titolo esemplificativo, nello schema seguente (quale "*elencazione analitica*" degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato):

| Descrizione | Dati elettronici | Ambito | Operatività |
|---|---|---|---|
| *tipo di Amministratore* | *dati in oggetto* | *data base* | *attività dell'Amministratore* |
| *Esempio: Amministratore di sistema software* | *Software, informazioni gestite da applicativi e servizi* | *DB-ABC* | *Installazione e gestione delle singole postazioni e aree di lavoro, di software di base, aggiornamenti, backup; Manutenzione e configurazione server di produzione* |

Specificatamente e limitatamente a tale contesto, l'Amministratore di sistema deve assicurare il corretto funzionamento e utilizzo del sistema informatico oggetto dell'incarico.

Con l'occasione La informo, altresì, che:

- ai sensi del punto 2, lett. c), del provvedimento del Garante per la protezione dei dati personali del 27/11/2008, il titolare del trattamento, per finalità di trasparenza interna all'organizzazione potrebbe essere tenuto, a tutela dei lavoratori, ad instaurare un regime di conoscibilità dell'identità degli Amministratori di sistema;
- ai sensi del punto 2, lett. e), del provvedimento del Garante per la protezione dei dati personali del 27/11/2008, l'operato degli Amministratori di sistema deve essere oggetto, da parte del titolare del trattamento o dei responsabili, di una attività di verifica, con cadenza

almeno annuale, sull'attività svolta in modo da controllare la rispondenza alle misure organizzative, tecniche e di sicurezza previste dalle norme vigenti;

- ai sensi del punto 2, lett. f), del provvedimento del Garante per la protezione dei dati personali del 27/11/2008, devono essere registrati gli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli Amministratori di sistema.

…….....

*  *  *

Il sottoscritto dichiara di accettare la nomina ad Amministratore di sistema con riguardo agli ambiti e ai compiti sopra descritti, dichiarandosi, altresì, disponibile e competente per la piena attuazione di quanto ivi disposto.

**PER ACCETTAZIONE**

## 6) Modello di verbale di test

### Introduzione

### Obiettivo

- L'obiettivo delle attività di test è la verifica dell'efficacia delle singole misure di continuità, tecnologiche ed organizzative che lo compongono.
- Obbiettivo secondario di tali attività è la formazione e l'addestramento del personale coinvolto, in quanto l'adeguatezza delle singole misure di continuità dipende in larga misura dalla capacità dello stesso di porre in essere, correttamente e tempestivamente, in caso di necessità, quanto predisposto.
- Lo scopo del presente documento è di descrivere tutte le attività necessarie per la corretta pianificazione, e successiva esecuzione, del test programmato per data del test relativo alla verifica *elementi da verificare*.

### Perimetro

*Perimetro di applicazione del test.*

### INFORMAZIONI GENERALI

### Tipologie di verifiche

*Tipologie delle verifiche da effettuare.*

### Responsabile dei Test

*Identificazione del responsabile del test*

### Risorse Umane coinvolte

*Individuazione puntuale delle risorse umane, interne ed esterne, coinvolte.*

### Asset coinvolti

*Individuazione puntale degli asset coinvolti nel test.*

### Pianificazione dell'attività

*Pianificazione dettagliata delle attività programmate.*

### Obiettivi delle verifiche

*Descrizione degli obiettivi delle verifiche.*

### Risultati attesi ed elementi da verificare

### Punti di criticità

*Punti di criticità che hanno suggerito l'effettuazione del test.*

**procedure di emergenza e di rollback**

*Procedure di emergenza previste.*

**stima dei costi del test**

*Stima dei costi del test*

Relativamente alle risorse interne è previsto un costo aziendale come nella seguente tabella:

| Tipologia di costo | Quantità |
|---|---|
| Ore “Personale” | |

valorizzate a costo standard con le maggiorazioni del caso per il personale vigenti (circa xxxx Euro).

## 7) Modello di rapporto sull'incidente di sicurezza

DENOMINAZIONE INCIDENTE

## DATA INCIDENTE

## INTRODUZIONE

### Premessa

Gli incidenti di sicurezza possono essere seri, come una violazione che compromette le operazioni cruciali o il guasto di un apparato o il verificarsi di un evento naturale, o minori, come una mancanza di rispetto per una procedura a causa di un errore. Investire tempo e risorse nello sviluppo delle politiche e delle procedure, usando i controlli di sicurezza per le reti, le applicazioni e le operazioni di revisioni e di monitoraggio, non ci garantisce che gli incidenti non avvengano.
Una progettazione attenta della governance della Sicurezza delle Informazioni richiede anche le procedure per una risposta agli incidenti.
Le procedure per rispondere a un incidente dovrebbero chiaramente definire cosa si intende per incidente, le persone responsabili per le risposte, le persone e le strutture che occorre informare degli incidenti, i passi per minimizzare le minacce, le procedure per il ripristino e le revisioni e le analisi ex post.
Gli incidenti sono delle minacce alle organizzazioni, ma sono anche delle occasioni per valutare i limiti delle procedure e le operazioni esistenti. Occorre eseguire una revisione ex post dopo ogni incidente per capire come l'evento è avvenuto all'interno dell'infrastruttura di sicurezza esistente e si richiedono cambiamenti tali da evitare un incidente simile nel futuro.

### Scopo

La gestione degli incidenti è un complesso processo che comincia dalla segnalazione di un evento, procedendo poi con la gestione e l'analisi dell'evento stesso e terminando con delle azioni di risposta e propositive.

Il presente documento ha lo scopo di illustrare i passi percorsi per analizzare l'incidente rilevato il giorno **.**.****, riportando anche le conclusioni del lavoro svolto.

### scenario di analisi

### scenario dell'incidente di sicurezza

*Descrizione dello scenario dell'incidente (*R*ete, desktop, ambiente).*

### descrizione dell'incidente di sicurezza

*Descrizione cronologica degli eventi e di eventuali misure intraprese*

### Evidenze

*Elencazione delle evidenze raccolte (log, configurazioni, testimonianze).*

### Passi dell'indagine effettuata

*Descrizione delle attività di indagine svolte***.**

**Cause dell'Incidente**

*Descrizione delle cause che hanno generato l'incidente se individuate.*

**Conclusioni**

*Conclusioni sull'accaduto.*

**Azioni correttive**

*Descrizione delle azioni correttive intraprese o da intraprendere individuate durante la fase di gestione dell'incidente.*