DOCUMENTO PROGRAMMATICO sulla SICUREZZA

Progettato e Redatto dalla G.E.N.I. S.r.l.

Stato delle Revisioni del Documento Programmatico sulla Sicurezza

Data di Revisione	Capitolo / Sezione	Motivazioni
17/03/10	L'intero DPsS	1° Stesura
24/03/11	L'intero DPsS	2° Stesura

Lista di Distribuzione del Documento Programmatico sulla Sicurezza		
N.	**SOCIETA' / Settore / Persona Fisica**	**FIRMA**

Indice

0.1 NOTE GENERALI

Ragione sociale: Comune Di Marsala

Sede Centrale: Via Garibaldi, 5 – 91025 Marsala

Sedi distaccate: relative ai vari settori distaccati

Telefono: 0923-993111

Fax: 0923-953402

http: www.comune.marsala.tp.it

0.2 DESCRIZIONE

Il Comune di Marsala rappresenta la comunità di coloro che vivono nel territorio comunale, ne cura gli interessi, ne promuove lo sviluppo, armonizzando le proprie finalità con quelle degli altri Comuni della provincia di Trapani e delle altre province alle quali è legato da affinità storico-culturali ed etniche.

In tale Documento Programmatico sulla Sicurezza saranno quindi indicate linee guida e/o moduli e/o documenti cui far riferimento per l'effettuazione di quanto utile alla gestione dei dati, dei trattamenti e delle responsabilità secondo il Decreto Legislativo n. 196 del 30 giugno 2003.

1. SCOPO E CAMPO DI APPLICAZIONE

1.1 Scopo

Il presente Documento Programmatico sulla Sicurezza è adottato, ai sensi dell'Allegato B del D. Lgs. n. 196/2003, allo scopo di:

- definire le politiche di sicurezza in materia di trattamento di dati personali
- stabilire le misure di sicurezza organizzative, fisiche e logiche da adottare affinché siano rispettati gli obblighi, in materia di sicurezza, previsti dal D. Lgs. n. 196/2003.

In particolare nel Documento Programmatico sulla Sicurezza vengono descritti:

a) i criteri tecnici organizzativi per la protezione delle aree e dei locali interessati dalle misure di sicurezza, nonché le procedure per controllare l'accesso delle persone autorizzate ai medesimi locali;
b) i criteri tecnici organizzativi e le procedure per assicurare l'integrità dei dati;
c) i criteri tecnici organizzativi e le procedure per la sicurezza della trasmissione dei dati, ivi compresi quelli per le redazioni di accesso per via telematica;
d) i criteri tecnici organizzativi per l'elaborazione di un piano di formazione per rendere edotti gli incaricati del trattamento dei rischi individuati e dei modi per prevenire i danni;
e) i criteri tecnici organizzativi per fornire agli incaricati del trattamento una panoramica sulle responsabilità loro spettanti, rispetto alla gestione ed allo sviluppo della sicurezza dell'informazione.

Il D. Lgs. 196/03 stabilisce le regole fondamentali cui devono sottostare i soggetti pubblici nel trattamento di qualunque tipologia di informazioni personali.

Viene ribadito il fondamentale "principio di finalità" ai sensi del quale il trattamento in ambito pubblico è consentito univocamente per lo svolgimento delle funzioni istituzionali, nei limiti stabiliti dallo steso Codice in relazione alla specifica natura dei dati, nonché dalla legge e dai regolamenti.

Viene altresì enunciato esplicitamente il principio secondo il quale gli Enti Pubblici, a differenza dei soggetti privati, non operano in base al consenso degli interessati, che è comunque richiesto nel caso in cui il trattamento venga effettuato dagli esercenti le professioni sanitarie e dagli organismi sanitari pubblici, mentre si precisa che sussiste comunque il divieto di comunicazione e di diffusione dei dati in alcuni casi specifici.

Ci si riferisce, a quest'ultimo proposito, al caso in cui ne sia stata ordinata la cancellazione, sia decorso un periodo di tempo non superiore a quello necessario agli scopi per i quali sono stati raccolti o successivamente trattati, o se si intende utilizzarli per finalità diverse da quelle previste, nel rispetto della legge. Resta tuttavia fermo l'obbligo della trasmissione, ove richiesti, alle forze di polizia, all'autorità giudiziaria ovvero ad organismi d'informazione e sicurezza per finalità di difesa o di sicurezza dello Stato, nonché di prevenzione, accertamento o repressione dei reati.

Le Amministrazioni Pubbliche possono effettuare solo i trattamenti di dati connessi all'esercizio delle proprie funzioni istituzionali e rispondenti, in caso di comunicazioni ad altri Enti Pubblici, a puntuali previsioni di legge o di regolamento. Rimane in generale vietata la divulgazione ovvero il flusso di dati verso un soggetto privato, quando ciò non sia previsto da una norma di legge o di regolamento.

Nell'ambito informatico, il termine "sicurezza" si riferisce a tre aspetti distinti:

- **Riservatezza:** Prevenzione contro l'accesso non autorizzato alle informazioni;
- **Integrità:** Le informazioni non devono essere alterabili da incidenti o abusi;

- **Disponibilità:** Il sistema deve essere protetto da interruzioni impreviste.

Il raggiungimento di questi obiettivi richiede non solo l'utilizzo di appropriati strumenti tecnologici, ma anche gli opportuni meccanismi organizzativi; misure soltanto tecniche, per quanto possano essere sofisticate, non saranno efficienti se non usate propriamente.

Le misure organizzative hanno il fine di fare in modo che l'intera struttura adotti comportamenti conformi ai principi della sicurezza e, più in generale, della privacy, quindi evitando carenze organizzative.

In particolare, le precauzioni di tipo tecnico possono proteggere le informazioni durante il loro transito attraverso i sistemi, o anche quando queste rimangono inutilizzate su un disco di un computer; nel momento in cui esse raggiungono l'utente finale, la loro protezione dipende esclusivamente da quest'ultimo, e nessuno strumento tecnologico può sostituirsi al suo senso di responsabilità e al rispetto delle norme.

A nulla serve essere estremamente scrupolosi nel trattamento dei dati, inviando informative, acquisendo consensi ed autorizzazioni, aggiornandoli con maniacale puntualità se si lasciano poi i supporti contenenti i dati incustoditi sulla scrivania, alla mercè di chiunque possa entrare nell'ufficio.

L'Ente si adopera per ridurre al minimo per quanto tecnologicamente ed organizzativamente possibile e nell'ottica del miglioramento continuo. A tal'uopo la sicurezza non si intende solo come protezione da eventi negativi, accidentali o internazionali, ma anche come limitazione degli effetti causati dall'eventuale verificarsi di tali eventi.

Lo scopo del DPsS è di fornire una fotografia reale della filosofia che l'Ente adotta per garantire la protezione, l'integrità, la conservazione, la tutela dei dati personali trattati.

Nel seguito termini come Titolare, Responsabile, Incaricato, Trattamento e Dato personale saranno usati in conformità alle definizioni del D. Lgs. n. 196/2003. L'Ente, in qualità di Titolare del trattamento, ha provveduto a redigere, in tutte le sue parti, il seguente Documento Programmatico sulla Sicurezza.

La verifica di congruità del Documento Programmatico sulla Sicurezza ai requisiti del Decreto Legislativo di riferimento è effettuata dal Titolare del trattamento. L'approvazione del Documento Programmatico sulla Sicurezza nel complesso è effettuata dal Titolare e/o dal Responsabile per il trattamento (che ne fa le veci) che provvede a firmarlo in calce e/o con atto deliberativo. L'emissione del Documento Programmatico sulla Sicurezza, da parte del Titolare e/o dal Responsabile del trattamento, avviene in maniera controllata.

1.2 Campo di applicazione

Il Documento Programmatico sulla Sicurezza, in accordo con il Regolamento di attuazione delle norme sulla tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali, adottato dall'Ente, e del quale si richiamano tutte le definizioni e disposizioni, definisce le politiche e gli standard di sicurezza in merito al trattamento dei dati personali.

Il Documento Programmatico sulla Sicurezza deve essere applicato da tutta la struttura (in quanto interconnessa) al trattamento di tutti i dati personali per mezzo di:

strumenti elettronici di elaborazione

altri strumenti di elaborazione (es. cartacei, etc.)

L'Ente, in qualità di Titolare assicurerà che il programma di sicurezza sia adeguatamente sviluppato, realizzato e mantenuto aggiornato e conforme alla legge sulla privacy e alle prescrizioni del presente documento.

1. Scopo e Campo di Applicazione

Il complesso normativo disciplinante il trattamento dei dati personali si configura, infatti, in modo del tutto peculiare nei confronti dei soggetti pubblici e, più in generale, nei riguardi dell'attività amministrativa.

Come è noto, in tale ambito si è affermato il fondamentale principio della trasparenza, sancito dalle leggi amministrative, quale evidente espressione dei canoni costituzionali dell'imparzialità e del buon andamento, che devono permeare l'azione della pubblica amministrazione. A fronte di tali norme si situa, in posizione in parte antitetica, il principio della tutela della riservatezza, anch'esso annoverato tra i diritti di rango costituzionale, in quanto espressione dei diritti e delle libertà inviolabili di ogni essere umano.

Il trattamento dei dati personali nel settore pubblico assume delle caratteristiche peculiari, sia sotto il profilo qualitativo che quantitativo: l'ingente quantità di informazioni sul singolo in possesso delle pubbliche amministrazioni rischia di rappresentare la fonte più ricorrente di diffusione dei dati personali.

Peraltro, la mancanza di consenso dell'interessato al trattamento dei propri dati personali potrebbe generare abusi nella conseguente fase operativa da parte del soggetto pubblico: come ha avuto modo di sottolineare il Garante per la protezione dei dati personali, è di tutta evidenza l'importanza delle disposizioni che regolano la materia nel settore pubblico, le quali devono contenere già in se quel bilanciamento di valori perseguiti e interessi tutelati che, nei rapporti fra privati, scaturisce dal confronto intersoggettivo alla base della manifestazione del consenso.

A tal'uopo il presente Documento sarà uno strumento, nell'ambito applicativo dell'Ente, perchè esso operi in modo da:

- minimizzare la probabilità di appropriazione, danneggiamento o distruzione anche non voluta di apparecchiature informatiche o archivi informatici o cartacei contenenti dati personali, minimizzare la probabilità di accesso, comunicazione o modifiche non autorizzate alle informazioni personali,
- minimizzare la probabilità che i trattamenti dei dati personali siano modificati senza autorizzazione.

Il Documento Programmatico sulla Sicurezza con i suoi contenuti deve essere divulgato e spiegato a tutti gli incaricati ed applicato da tutte le risorse lavoranti per l'Ente, secondo le proprie competenze.

La parte che riguarda i dipendenti deve essere divulgata e spiegata a cura del Titolare e/o dei diretti Responsabili (qualora designati) e/o di soggetti specializzati.

Eventuali situazioni di deviazione accertate rispetto a quanto precisato nel presente documento dovranno essere analizzate e gestite in maniera da valutarne il peso e, a seconda dello stesso, rimuoverle nel più breve tempo possibile.

2. RIFERIMENTI NORMATIVI

Il presente Documento Programmatico sulla Sicurezza ha come riferimento la seguente documentazione:

- *Decreto Legislativo n. 196 del 30.06.2003: "Codice in materia di protezione dei dati personali" e s.m.i.*
- *Documenti prodotti dal Garante a fronte dell'evoluzione nel settore della privacy e/o per approfondimento, quali Provvedimenti, Newsletter, Comunicati Stampa, Dossier etc.*

Tali Decreti e/o Leggi possono essere archiviati da parte del Titolare e/o Responsabile del trattamento e/o loro incaricato, che è responsabile del controllo, aggiornamento ed eventuale distribuzione delle relative copie controllate all'interno dell'Ente e/o consultabili presso il sito del Garante.

3. TIPOLOGIA DI DATI E LORO TRATTAMENTO

3.1 Individuazione delle banche di dati oggetto del trattamento

Al Titolare e/o al Responsabile del trattamento dei dati è affidato il compito di redigere e di aggiornare ad ogni variazione l'elenco delle tipologie di trattamenti effettuati. Ogni banca di dati o archivio deve essere classificato in relazione alle informazioni in essa contenute indicando se si tratta di:

- dati personali comuni
- dati personali sensibili
- dati personali giudiziari

Per l'individuazione degli archivi dei dati oggetto del trattamento deve essere utilizzato apposito modulo, che deve essere conservato a cura del Titolare e/o Responsabile del trattamento e/o loro incaricato in luogo apposito.

Elenco dei dati personali

L'Ente ad oggi tratta i seguenti dati:

- dati comuni dei fornitori o di terzi ricavati da albi, elenchi pubblici, eventuali visure camerali;
- dati comuni del personale dipendente, quali quelli necessari al rapporto di lavoro, alla reperibilità ed alla corrispondenza con gli stessi o richiesti ai fini fiscali e previdenziali o dati di natura bancaria;
- dati comuni dei cittadini;
- dati comuni dei fornitori concernenti la reperibilità e la corrispondenza con gli stessi, nonché inerenti ai fini fiscali o dati di natura bancaria strettamente necessari ai rapporti contrattuali;
- dati comuni del personale dipendente e professionisti cui l'Ente affida eventualmente incarichi o si rivolge per consulenze, quali quelli concernenti la reperibilità e la corrispondenza con gli stessi, nonché inerenti a finalità fiscali o dati di natura bancaria strettamente necessari ai rapporti contrattuali;
- dati comuni di terzi forniti dagli utenti per l'espletamento degli incarichi affidati all'Ente;
- dati per istruzione pratiche di patrocinio, atti di liquidazione, etc.;
- dati per contratti d'appalto e gare, contabilità, atti amministrativi, determine, derivanti da atti notarili, etc.;
- dati inerenti pubblicità e affissioni;
- dati inerenti tasse per occupazioni spazi e aree pubbliche e quanto ad essi correlato;
- dati inerenti la TARSU sia per le attività commerciali che per le civili abitazioni, notifiche, sgravi e accertamenti, contenziosi tributati TARSU, e quanto ad essi correlato;
- dati inerenti tributi, cartelle esattoriali, cartelle ICI, contenziosi tributati ICI e quanto ad essi correlato;
- dati inerenti il patrimonio di beni mobili e immobili, dell'economato e quanto ad essi correlato;
- dati relativi a pratiche legali, giudiziari, atti difensivi, atti amministrativi e quanto ad essi correlato;
- dati relativi allo stato civile, documentazione anagrafica e liste elettorali;
- dati del personale dipendente, conseguenti al rapporto di lavoro, ovvero inerenti i rapporti con gli enti previdenziali ed assistenziali: gestione amministrativa del personale (dall'instaurazione alla cessazione del rapporto di lavoro), gestione informatica di rilevazione presenze del personale di ruolo (ferie, malattie, lavoro straordinario, riposo compensativo);
- dati del personale che presta servizio presso l'Ente;

- dati sensibili del personale dipendente idonei a rivelare lo stato di salute;
- dati sensibili dei cittadini idonei a rivelare lo stato di salute;
- dati sensibili dei cittadini idonei a rivelare l'origine razziale o etnica;
- dati sensibili dei cittadini idonei a rivelare l'adesione a partiti, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale;
- dati sensibili dei dipendenti e/o del personale che presta servizio per conto dell'Ente idonei a rivelare l'adesione a partiti, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale;
- dati giudiziari dei cittadini e/o fornitori;
- dati relativi alla viabilità, alle contravvenzioni e quanto ad essi connesso;
- dati relativi alle concessioni edilizie, all'ecologia ambiente e quanto ad essi connesso;
- dati relativi ai settori cimiteriale, sportivo, manutenzione strade, spettacoli mercati, caccia e quanto ad essi connesso.

Il codice disciplinante il trattamento nel settore pubblico, individua una serie di rilevante finalità di interesse pubblico per il cui perseguimento è consentito il trattamento di dati sensibili o afferenti a provvedimenti giudiziari, specificando i tipi di dati trattabili nonché di operazioni eseguibili. L'elencazione di cui sopra opera una ricognizione delle più diffuse e rilevanti finalità di interesse pubblico che legittimano le operazioni di trattamento di alcune specifiche tipologie di dati sensibili e giudiziari: essa, tuttavia, non deve essere considerata una puntualizzazione esaustiva né tassativa.

Non si può escludere, infatti la configurabilità di ulteriori trattamenti di dati sensibili e giudiziari da parte dei soggetti pubblici che siano effettuati o in base ad altre disposizioni legislative che stabiliscano finalità di interesse pubblico, nonché i tipi di informazione trattate e le operazioni eseguibili.

In ogni caso da un lato i soggetti pubblici vengono esplicitamente autorizzati ad effettuare determinati trattamenti e dall'altro si produce un significativo potenziamento della tutela della riservatezza degli interessati nei confronti dei trattamenti operati dalle pubbliche amministrazioni.

A tal fine il legislatore ha individuato i seguenti settori:

- *cittadinanza, immigrazione e condizione dello straniero*, nel cui ambito si rinviene in particolare il trattamento dei dati indispensabili per l'emissione di autorizzazioni o permessi, per il riconoscimento di particolari situazioni (ad esempio diritto di asilo, status di rifugiato), o per l'applicazione della legislazione in materia di lavoro, istruzione e alloggio, ferma restando l'inapplicabilità della disciplina con riferimento ai trattamenti effettuati in esecuzione degli accordi di Schengen e della Convenzione Europol ovvero per esigenze di difesa, sicurezza dello Stato, prevenzione, accertamento o repressione dei reati.
- *Diritti politici e pubblicità dell'attività di organi:* all'interno di tale campo si individua una serie di attività connesse con l'esercizio dei diritti di elettorato attivo e passivo e di altri diritti politici, nonché di tenuta degli elenchi dei giudici popolari; nella norma sono compresi, fra gli altri, gli adempimenti per lo svolgimento delle consultazioni elettorali e referendarie, per la verifica dei requisiti per l'esercizio dei diritti (come le sottoscrizioni di liste, la presentazione di candidature, le cariche istituzionali, l'accertamento di cause di ineleggibilità o incompatibilità, l'esame di segnalazioni e petizioni, la designazione di rappresentanti in commissioni e enti).

Poiché in tali ipotesi la trasparenza può assumere rilievo preminente, la norma autorizza altresì il trattamento dei dati contenuti nei verbali delle assemblee rappresentative e quelli necessari all'esercizio delle funzioni di controllo, indirizzo politico, e sindacato ispettivi, nonché la pubblicità e la diffusione dei dati indispensabili per assicurare il rispetto della pubblicità dell'attività istituzionale.

- *Materia tributaria e doganale*, ove vengono incluse le attività dei soggetti pubblici diretta all'applicazione anche tramite loro concessionari della disciplina in materia (ivi compresa la repressione delle violazioni), nonché il controllo e l'esecuzione forzata dell'esatto adempimento dei relativi obblighi di legge;
- *Attività di controllo e ispettive*, volte a verificare che l'azione amministrativa si svolga nel rispetto dei noti principi di legittimità, buon andamento, imparzialità, economicità, efficienza ed efficacia; in tale sfera sono altresì ricompresi gli accertamenti di dati relativi ad esposti e petizioni ed, infine, gli atti di controllo o sindacato ispettivo per l'espletamento del mandato elettivo;
- *Benefici economici ed abilitazioni con riferimento alla relativa concessione, liquidazione, revoca o modifica:* in questo ambito vi rientrano anche i trattamenti della normativa antimafia e antiracket, per il conferimento delle pensioni di guerra, di invalidità civile, per la formazione professionale, per l'elargizione dei contributi previsti dalla legge anche in favore di associazioni e fondazioni, per il riconoscimento di esoneri, agevolazioni tariffarie o rilascio di concessioni radiotelevisive;
- *Onorificenze, ricompense e riconoscimenti* attinenti a tutte quelle attività volte all'attribuzione della personalità giuridica ed associazioni, fondazioni ed enti nonché all'accertamento dei requisiti di onorabilità e professionalità, volontariato e obiezione di coscienza, segnatamente per quanto riguarda l'elargizione di contributi per il sostegno e la tenuta di registri generali delle organizzazioni impegnate nelle varie forme di assistenza sociale;
- *Attività sanzionatorie e di tutela*, con riferimento alle quali da un lato, è stata inserita la previsione che, nell'ambito delle finalità volte a far valere il diritto di difesa in sede amministrativa o giudiziaria, rientrano anche le attività effettuate per consentire l'acquisizione da parte del difensore di documenti in possesso della pubblica amministrazione, nonché quelle connesse alla disciplina in materia di violazione del termine ragionevole del processo e, dall'altro lato, è stato disciplinato il principio della pari ordinazione dei diritti coinvolti nel caso in cui vengano in rilievo dati idonei a rivelare lo stato di salute o la vita sessuale;
- *Rapporti con enti di culto*, che riguardano unicamente e relazioni istituzionali che possano intercorrere tra la pubblica amministrazione e gli organismi di carattere religioso, essendo perciò esclusi dalla norma i trattamenti relativi agli aderenti alle confessioni religiose ed ai soggetti che, con riferimento a finalità di natura esclusivamente religiosa, hanno dei legami con le medesime conf4essioni, che trovano invece compiuta regolamentazione nel Codice;
- *Altre finalità in ambito amministrativo e sociale*: come previsto dal Codice si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, nell'ambito delle attività che la legge demanda ad un soggetto pubblico, le finalità socio-assistenziali, con particolare riferimento a:
  1. interventi di sostegno psico-sociale e di formazione in favore di giovani o di altri soggetti che versano in condizioni di disagio sociale, economico o familiare;
  2. interventi anche di rilievo sanitario in favore di soggetti bisognosi o non autosufficienti o incapaci, ivi compresi i servizi di assistenza economica o domiciliare, di telesoccorso, accompagnamento e trasporto;

3. assistenza nei confronti di minori, anche in relazione a vicende giudiziarie;
4. indagini psico-sociali relative a provvedimenti di adozione anche internazionale;
5. compiti di vigilanza per affidamenti temporanei;
6. iniziative di vigilanza e di sostegno in riferimento al soggiorno di nomadi;
7. interventi in tema di barriere architettoniche.
8. di gestione di asili nido;
9. concernenti la gestione di mense scolastiche o la fornitura di sussidi, contributi e materiale didattico;
10. ricreative o di promozione della cultura e dello sport, con particolare riferimento all'organizzazione di soggiorni, mostre, conferenze e manifestazioni sportive o all'uso di beni immobili o all'occupazione di suolo pubblico;
11. assegnazione di alloggi di edilizia residenziale pubblica;
12. leva militare;
13. polizia amministrativa anche locale, salvo quanto previsto dall'articolo 53, con particolare riferimento ai servizi di igiene, di polizia mortuaria e ai controlli in materia di ambiente, tutela delle risorse idriche e difesa del suolo;
14. uffici per le relazioni con il pubblico;
15. protezione civile;
16. supporto al collocamento e all'avviamento al lavoro, in particolare a cura di centri di iniziativa locale per l'occupazione e di sportelli-lavoro;
17. difensori civici regionali e locali.

I dati relativi agli utenti e/o fornitori sono trattati allo scopo di raggiungere l'obiettivo dell'erogazione dei servizi offerti dall'Ente.

I dati sensibili relativi agli utenti sono trattati ai sensi dell'*Autorizzazione n. 2/2009 al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale* del 16 dicembre 2009 del Garante della Privacy, pubblicata in G.U. n. 13 del 18 gennaio 2010, suppl. ord. N. 12.

I dati giudiziari relativi agli utenti sono trattati ai sensi dell'*Autorizzazione n. 7/2009 al trattamento dei dati a carattere giudiziario da parte di privati, di enti pubblici economici e di soggetti pubblici* del 16 dicembre 2009 del Garante della Privacy, pubblicata in G.U. n. 13 del 18 gennaio 2010, suppl. ord. N. 12.

I dati relativi ai dipendenti sono trattati ai sensi dell'*Autorizzazione n. 1/2009 al trattamento dei dati sensibili nei rapporti di lavoro* del 16 dicembre 2009 del Garante della Privacy, pubblicata in G.U. n. 13 del 18 gennaio 2010, suppl. ord. N. 12.

I dati non pubblici vengono acquisiti previa informativa predisposta secondo le modalità indicate nel presente DPsS. Questi dati vengono trattati e conservati in contenitori dotati di chiusura e/o trattati tramite computer in rete in locali protetti e con accesso ad internet, e archiviati al termine del trattamento.

La tempistica di archiviazione deve rispettare i termini di legge al termine dei quali l'Ente provvederà alla distruzione dei dati.

3.2 Inventario delle sedi in cui vengono trattati i dati

L'Ente presenta una sede centrale, sita in Via Garibaldi 5, in quel di Marsala per i seguenti settori:

- Settore Staff - Ufficio di Gabinetto;
- Settore Staff – Ufficio Legale;
- Settore Affari Generali e Risorse Umane;
- Settore Risorse Finanziarie;
- Settore Servizi al Cittadino;
- Settore Attività Produttive, SUAP, Sport, Turismo e Attività Culturali.

Altre unità sono dislocate presso i seguenti siti:

- Via Garibaldi 1, per le attività svolte dal Settore Attività Produttive, SUAP, Sport, Turismo e Attività Culturali.
- Via XI maggio, per le attività svolte dai Settori Staff, dal Settore Attività Produttive, SUAP, Sport, Turismo e Attività Culturali e dal Settore Territorio e Ambiente;
- Piazza del Popolo, per le attività svolte dai Settori Staff, dal Settore Attività Produttive, SUAP, Sport, Turismo e Attività Culturali;
- Via Garibaldi, Palazzo VII Aprile, per le attività svolte dal Settore Affari Generali e Risorse Umane e dal Settore Risorse Finanziarie;
- Via Damiani, per le attività svolte dal Settore Affari Generali e Risorse Umane e dal Settore Risorse Finanziarie;
- Via Sant'Agostino, per le attività svolte dal Settore Lavori Pubblici;
- Piazza Ugo Foscolo, per le attività svolte dal Settore Lavori Pubblici;
- Via Salemi, per le attività svolte dal Settore Lavori Pubblici (Acquedotto);
- Via Correale, per le attività svolte dal Settore Attività Produttive, SUAP, Sport, Turismo e Attività Culturali;
- Piazza della Vittoria, per le attività svolte dal Settore Attività Produttive, SUAP, Sport, Turismo e Attività Culturali;
- Via Sappusi, per le attività svolte dal Settore Servizi al Cittadino;
- Via Trapani, per le attività svolte dal Settore Servizi al Cittadino;
- Largo di Girolamo, per le attività svolte dal Settore Territorio e Ambiente;
- Via Prof. Ernesto del Giudice, per le attività svolte dal Settore Polizia Municipale (Comando centrale) e dal Settore Settore Attività Produttive, SUAP, Sport, Turismo e Attività Culturali;
- Contrada San Leonardo, per le attività svolte dal Settore Servizi al Cittadino;
- Contrada Strasatti, per le attività svolte dal Settore Servizi al Cittadino e dal Settore Polizia Municipale (distretto n. 1);
- Contrada Bosco, per le attività svolte dal Settore Servizi al Cittadino e dal Settore Polizia Municipale (distretto n. 2);
- Distretto n. 3 Amabilina, per le attività svolte dal Settore Polizia Municipale;
- Contrada Dicerbato, per le attività svolte dal Settore Servizi al Cittadino;
- Contrada Paolini, per le attività svolte dal Settore Servizi al Cittadino;

- Contrada Pontefiumarella, per le attività svolte dal Settore Servizi al Cittadino e del Settore Servizi Pubblici Locali;
- Zona Favara, per le attività svolte dal Settore Servizi Pubblici Locali;
- Archivio Storico, per le attività svolte dal Settore Attività Produttive, SUAP, Sport, Turismo e Attività Culturali;
- Ente Mostra di Pittura, Pinacoteca Comunale, per le attività svolte dal Settore Attività Produttive, SUAP, Sport, Turismo e Attività Culturali.

Ad oggi, i dati inerenti i servizi erogati dall'Ente risiedono nelle strutture sopra riportate.

Quanto eventualmente dato in outsourcing, come gestione dei dati forniti dall'Ente per finalità specifiche, viene effettuato secondo quanto previsto nel paragrafo apposito e secondo quanto riportato nel presente Documento Programmatico.

Per l'archiviazione dei documenti cartacei, a seconda del peso degli stessi, sono utilizzati contenitori dotati di serratura, e/o posizionati in luoghi muniti di chiusura cui l'eventuale accesso di estranei avviene in presenza del Titolare e/o Responsabile e/o loro incaricato.

Gli uffici sono dotati di reti interne che collegano i servers alle singole postazioni operative e la connessione verso la rete Internet avviene mediante linee ADSL, HDSL, e/o ISDN a seconda delle strutture.

Tutti i dati sotto forma informatica sono conservati su computer e/o server appositi, e tutti i dati sotto forma cartacea vengono conservati negli appositi contenitori e/o locali dotati di serratura.

3.3 Inventario dei settori in cui vengono trattati i dati

La struttura organizzativa del Comune di Marsala viene articolata in "Settori", cui sono preposti dipendenti in possesso di qualifica dirigenziale. I Settori sono le strutture preposte alla produzione ed erogazione di specifiche prestazioni.

Il settore può essere ulteriormente articolato in strutture inferiori a livello di area delle posizioni organizzative e/o di alta professionalità. I Settori e le Aree delle posizioni organizzative costituiscono quindi la struttura organizzativa portante del Comune.

La struttura organizzativa è supportata dagli uffici di staff in quanto strutture organizzative le cui attività svolte sono riconducibili a funzioni di supporto e di assistenza agli organi politici e alle strutture organizzative dell'Ente.

I Settori e le Aree individuati dal Comune di Marsala sono di seguito riportati:

1. Settore Staff - Ufficio di Gabinetto:
   - Ufficio di Gabinetto
   - Ufficio Stampa e Informazione
2. Settore Staff – Ufficio Legale:
   - Ufficio Legale;
3. Settore Affari Generali e Risorse Umane:
   - Affari generali e Istituzionali
   - Risorse Umane e Organizzative
   - Servizi di supporto al Nucleo di valutazione

- Servizio contabile del personale (stipendi e pensioni)
- Servizi Informatici – CED

4. Settore Risorse Finanziarie:
   - Ragioneria – Bilancio
   - Controllo di Gestione
   - Provveditorato ed economato
   - Ufficio tributi
   - Patrimonio
   - Ufficio Contratti
5. Settore Servizi al Cittadino:
   - Servizi demografici
   - Servizi Sociali / Ufficio solidarietà sociale
6. Settore Attività Produttive, SUAP, Sport, Turismo e Attività Culturali:
   - Attività produttive
   - Servizio unico attività produttive
   - Servizio suolo pubblico
   - Sport
   - Turismo
   - Servizi culturali
   - Ufficio contenitori culturali
7. Settore Territorio e Ambiente:
   - Urbanistica, Servizio sviluppo locale e politiche comunitarie
   - Edilizia Residenziale – Condono – Abusivismo
   - Ambiente e riqualificazione urbana – SITR
   - Gestione Amministrativa del settore
8. Settore Lavori Pubblici:
   - Ufficio tecnico
   - Ufficio protezione civile
9. Settore Polizia Municipale:
   - Controllo del territorio e vigilanza Palazzo PP.UU.
   - Polizia giudiziaria e formazione del personale
10. Settore Servizi Pubblici Locali:
    - Servizio ecologia ed ambiente
    - Autoparco comunale
    - Servizio idrico integrato
    - S.M.A.

3.4 Inventario dei sistemi di elaborazione

Al Titolare e/o Responsabile del trattamento e/o loro incaricato, in collaborazione con l'Amministratore di sistema, se diverso dallo stesso, è affidato il compito di redigere ed aggiornare, ad ogni variazione, l'elenco dei sistemi di elaborazione con cui viene effettuato il trattamento dei dati.

Per ogni sistema debbono essere descritte le caratteristiche e, ad esempio, se si tratta di sistema di elaborazione:

- non accessibile da altri elaboratori (stand-alone);
- in rete non accessibile al pubblico;
- in rete accessibile al pubblico.

Per ogni sistema deve essere specificato il nome dell'incaricato o degli incaricati che lo utilizzano nonché del Custode delle passwords.

Per l'inventario dei sistemi di elaborazione deve essere utilizzato apposito modulo e/o carta intestata dell'Ente che deve essere conservato, a cura del Titolare e/o Responsabile del trattamento e/o loro incaricato, in luogo apposito.

3.5. Modalità di trattamento dei dati

Ogni incaricato al trattamento dei dati può accedervi, per quanto pratico e ragionevole, mediante proprie username e/o password che gli sono stati attribuiti. Il Titolare e/o il Responsabile, con le medesime modalità, impartisce agli incaricati le necessarie istruzioni per il corretto trattamento.

3.5.1 Trattamento con strumenti informatici

Il soggetto Responsabile della gestione delle abilitazioni provvede ai propri compiti con le seguenti modalità:

a) a ciascun incaricato che, per esigenze di servizio, deve poter utilizzare una procedura informatizzata ed accedere di conseguenza alle informazioni contenute negli archivi della stessa, è assegnato (per quanto pratico e ragionevole) un "codice personale utente" ed una "parola chiave" segreta (password) individuale e riservata (per quanto pratico e ragionevole) in modo esclusivo.
b) ciascun incaricato, per mezzo di detto codice di accesso, è abilitato all'utilizzo delle funzionalità necessarie allo svolgimento delle attività allo stesso assegnate e può contemporaneamente accedere ai soli dati strettamente necessari allo scopo.

Ciascuna procedura informatizzata deve essere strutturata in modo da consentire di:

a) segmentare (per quanto pratico e ragionevole) le abilitazioni di accesso ed utilizzo in base alle necessità dell'unità operativa;
b) individuare a posteriori (per quanto pratico e ragionevole) l'autore di ciascuna operazione effettuata sui dati trattati. Il rispetto dei requisiti, di cui al presente punto, deve essere garantito anche dal fornitore o dal produttore di ciascuna procedura informatizzata.

E' fatto obbligo a ciascun incaricato (per quanto pratico e ragionevole), di non comunicare ad altri il proprio codice identificativo personale, né la parola chiave (password) segreta, di non lasciare la stazione di lavoro situata al proprio posto di lavoro collegata ed incustodita e di non utilizzare i dati per fini non strettamente attinenti alle esigenze di servizio.

3.5.1.1 Archivi Elettronici

L'Ente, ad oggi, ha delineato i seguenti Archivi Elettronici:

- CED;
- Comando Polizia Municipale.

In essi vengono gestiti i seguenti database, correlati ai dati trattati dall'Ente:

- Fornitori;
- Indirizzi di posta elettronica;
- Dipendenti e affini;
- Utenti;
- Utenti con indicazione dei dati ed informazioni ad essi riferiti;
- Atti Amminstrativi.

3.5.2 Trattamento senza l'ausilio di strumenti informatici

Il Titolare e/o i Responsabili (qualora designati) nel designare per iscritto gli incaricati e nell'impartire le istruzioni, devono prescrivere che i soggetti designati abbiano accesso ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere i compiti loro assegnati.

Gli atti e i documenti contenenti i dati personali devono essere conservati in archivi ad accesso selezionato a seconda del loro peso specifico e, se affidati agli incaricati del trattamento, devono essere da questi ultimi conservati e restituiti al termine delle operazioni eseguite.

Le medesime modalità di cui al presente articolo si applicano alla conservazione anche dei supporti informatici (es. floppy disk, Compact Disk, etc.).

Nel caso di dati personali di tipo "sensibile", oltre alle misure di cui sopra, al fine di provvedere al controllo ed alla custodia in modo tale che non possano accedere persone prive di autorizzazione, devono essere osservate le seguenti modalità:

a) se affidati agli incaricati, gli atti e i documenti concernenti i dati vanno conservati, sino alla restituzione, in contenitori muniti di serratura e/o in armadi chiudibili a chiave e/o in locali adibiti ad archivio chiudibili a chiave nei quali devono riporsi i documenti, contenenti i dati sensibili, prima di assentarsi dal posto di lavoro, anche temporaneamente. In tali dispositivi (armadi e/o cassetti) i documenti possono essere riposti anche al termine della giornata di lavoro, qualora l'incaricato debba continuare ad utilizzarli nei giorni a seguire;
b) l'accesso agli archivi va controllato e devono essere identificati e registrati i soggetti qualora vi accedano dopo l'orario di chiusura degli archivi stessi.

3.5.2.1 Archivi Cartacei

L' Ente, ad oggi, ha delineato i seguenti data base, trattati senza l'ausilio degli strumenti elettronici:

- Copia Cedolini paga;
- Autorizzazioni a prelievi per contributi sindacali;
- Elenchi di Concessioni Edilizie ed Autorizzazioni;

- Copia dei certificati malattia ed altri dati sensibili;
- Documenti di lavoro;
- Documenti necessari perché previsti da leggi cogenti;
- Atti Amministrativi;
- Agende di vario tipo e contenuto.

3.5.3 Controllo e/o registrazione degli accessi

L'Ente ha sedi generalmente dotate di portierato tramite cui viene controllato l'accesso alle strutture stesse. Per quanto riguarda i dipendenti/lavoratori, sono dotati di badges, utili per la gestione della retribuzione tramite il relativo rilevatore di presenze. Tutti i lavoratori, al loro arrivo in Ente, sono tenuti a registrare la propria presenza utilizzando il rilevatore di presenze elettronico predisposto ed il badge personale.

Per i calcoli relativi alla retribuzione di ciascun lavoratore, gli orari di lavoro (normale e/o straordinario) saranno forniti dall'orologio del rilevatore di presenze.

Per quanto concerne gli utenti che si recano presso le sedi dell'Ente, non viene effettuata alcuna registrazione degli accessi. Al contrario per le risorse che vogliano accedere al CED, è prevista la registrazione degli accessi.

3.5.4 Videosorveglianza

3.5.4.1 Videosorveglianza dei locali dell'Ente

Ad oggi, l'Ente, al fine di proteggere i beni di sua proprietà, nonchè delle risorse ivi lavoranti, usufruisce di alcuni sistemi di videosorveglianza, in alcune aree ritenute più a rischio:

- CED;
- Comando Centrale della Polizia Municipale;
- Settore Servizi Pubblici Locali;
- Settore Lavori Pubblici.

Le immagini che vengono acquisite vengono gestite dall'Ente, effettuando una registrazione nell'arco di 24 ore, al termine delle quali viene custodita per un tempo non superiore a 7 giorni, salvo eventuale diversa tempistica ritenuta necessaria e motivata dall'Ente.

Gli impianti sono congegnati in maniera da evitare, per quanto possibile di riprendere persone al di fuori dell'area aziendale (ivi comprensiva l'area antistante le entrate) e nell'area designata deve essere affisso manifesto con l'informativa in merito alla videosorveglianza, come richiesto dalla normativa in vigore.

Nell'esercitare attività di videosorveglianza, l'Ente rispetta il principio di proporzionalità tra i mezzi impiegati ed i fini perseguiti, in particolare si precisa che:

il trattamento dei dati avviene secondo correttezza e per scopi determinati, espliciti e legittimi;

l'attività viene svolta per la prevenzione di un pericolo concreto o di specifici reati e solo le autorità competenti sono legittimate ad accedere alle informazioni raccolte, qualora necessario.

Inoltre l'attività di videosorveglianza è esercitata osservando le seguenti indicazioni:

- deve essere scrupolosamente rispettato il divieto di controllo a distanza dei lavoratori;

- devono essere fornite alle persone che possono essere riprese, indicazioni chiare, anche se sintetiche, circa la presenza di impianti di videosorveglianza;
- sono visionate le immagini strettamente necessarie per il raggiungimento delle finalità perseguite, limitando l'angolo di visuale delle riprese, evitando, quando non indispensabili, immagini dettagliate, ingrandite o con particolari non rilevanti;

L'Ente, ad oggi, è esonerato dall'obbligo di notifica al garante, in virtù del fatto che i dati relativi ad immagini o suoni servono per esclusive finalità di sicurezza o di tutela delle persone e/o del patrimonio non sono neanche conservati oltre il tempo necessario alle necessità.

3.5.4.2 Eventuale rilevazione degli accessi dei veicoli nei centri storici o nelle zone a traffico limitato

Una particolare notazione è dedicata al trattamento dei dati raccolti mediante impianti per la rilevazione degli accessi di veicoli a centri storici ed alle zone a traffico limitato. Il regolamento recante norme per l'autorizzazione all'installazione ed all'esercizio di impianti per la rilevazione degli accessi di veicoli ai centri storici ed alle zone a traffico limitato, disciplina le procedure di installazione e l'utilizzo dei dispositivi o mezzi tecnici di controllo del traffico che permettono il rilevamento a distanza di infrazioni, prevedendo l'obbligo di munirsi di un'autorizzazione rilasciata, ai comuni richiedenti, dal Ministero dei lavori pubblici, Ispettorato generale per la circolazione e la sicurezza stradale. Il predetto regolamento stabilisce esplicitamente che gli impianti si limitino a raccogliere dati relativi al traffico o all'accesso alle zone a traffico limitato, consentendo la rilevazione di immagini solamente in caso di infrazione.

È altresì previsto che la documentazione con immagini sia utilizzata per le sole finalità di applicazione del regolamento medesimo e conservata unicamente per il periodo necessario alla contestazione dell'infrazione, alla corresponsione della sanzione ed alla definizione dell'eventuale contenzioso, restando i dati accessibili esclusivamente per fini di polizia giudiziaria o di indagine penale.

A completamento della cornice normativa relativa all'installazione di telecamere in luoghi pubblici e privati, si sottolinea che il garante (anche in ragione della particolare sensibilità manifestata al riguardo dai cittadini ed alle numerose richieste di parere preventivo proveniente dagli enti locali) non ha mancato di richiamare l'attenzione sulla necessità che i sistemi di rilevazione vengano attivati in presenza di un articolato quadro di garanzie individuando, in un apposito decalogo sulla videosorveglianza (Provvedimento inerente la videosorveglianza nei locali ed in esterna), una serie di linee guida e di misure idonee per assicurare un utilizzo corretto dei dati da parte dei soggetti legittimati ogniqualvolta si realizzi un impianto di controllo dotato di strumenti automatizzati di rilevazione di immagini:

1. Tutti gli interessati devono determinare esattamente le finalità perseguite attraverso la videosorveglianza e verificarne la liceità in base alle norme vigenti. Se l'attività è svolta in presenza di un pericolo concreto o per la prevenzione di specifici reati, occorre rispettare le competenze che le leggi assegnano per tali fini solo a determinate amministrazioni pubbliche, prevedendo che alle informazioni raccolte possano accedere solo queste amministrazioni.
2. Il trattamento dei dati deve avvenire secondo correttezza e per scopi determinati, espliciti e legittimi.

3. Nei casi in cui la legge impone la notificazione al Garante dei trattamenti di dati personali effettuati da determinati soggetti, questi devono indicare fra le modalità di trattamento anche la raccolta di informazioni mediante apparecchiature di videosorveglianza. Non è prevista alcuna altra forma di specifica comunicazione o richiesta di autorizzazione al Garante.
4. Si devono fornire alle persone che possono essere riprese indicazioni chiare, anche se sintetiche, che avvertano della presenza di impianti di videosorveglianza, fornendo anche le informazioni necessarie ai sensi dell'art. 13 del D.Lgs. 196/03e s.m.i. Ciò è tanto più necessario quando le apparecchiature non siano immediatamente visibili.
5. Occorre rispettare scrupolosamente il divieto di controllo a distanza dei lavoratori e le precise garanzie previste al riguardo (art. 4 legge 300/1970 e s.m.i.).
6. Occorre rispettare i princìpi di pertinenza e di non eccedenza, raccogliendo solo i dati strettamente necessari per il raggiungimento delle finalità perseguite, registrando le sole immagini indispensabili, limitando l'angolo visuale delle riprese, evitando - quando non indispensabili - immagini dettagliate, ingrandite o dettagli non rilevanti, e stabilendo in modo conseguente la localizzazione delle telecamere e le modalità di ripresa.
7. Occorre determinare con precisione il periodo di eventuale conservazione delle immagini, prima della loro cancellazione, e prevedere la loro conservazione solo in relazione a illeciti che si siano verificati o a indagini delle autorità giudiziarie o di polizia.
8. Occorre designare per iscritto i soggetti - responsabili e incaricati del trattamento dei dati - che possono utilizzare gli impianti e prendere visione delle registrazioni, avendo cura che essi accedano ai soli dati personali strettamente necessari e vietando rigorosamente l'accesso di altri soggetti, salvo che si tratti di indagini giudiziarie o di polizia.
9. I dati raccolti per determinati fini (ad esempio, ragioni di sicurezza, tutela del patrimonio) non possono essere utilizzati per finalità diverse o ulteriori (ad esempio, pubblicità, analisi dei comportamenti di consumo), salvo le esigenze di polizia o di giustizia, e non possono essere diffusi o comunicati a terzi.
10. I particolari impianti per la rilevazione degli accessi dei veicoli ai centri storici e alle zone a traffico limitato devono essere conformi anche alle disposizioni contenute nel D.P.R. 250/1999 e s.m.i. E' altresì necessario che la relativa documentazione sia conservata per il solo periodo necessario per contestare le infrazioni e definire il relativo contenzioso e che ad essa si possa inoltre accedere solo a fini di indagine giudiziaria o di polizia.

3.5.4.3 Eventuale sistema di videosorveglianza ai fini della tutela della sicurezza pubblica ed al contrasto della criminalità

La videosorveglianza è divenuta sempre più uno strumento indispensabile nelle città, nei comuni piccoli e grandi per la tutela della sicurezza pubblica ed al contrasto della criminalità, potendo essere assimilata come parte integrante dell'arredo urbano come i lampioni, le panchine, i semafori.

Nel caso in cui l'Ente vorrà adottare un sistema di videosorveglianza ai fini della tutela della sicurezza pubblica e quanto ad esso correlato, si doterà di apposito regolamento, quale forma di trasparenza amministrativa nei confronti dei cittadini, indicandovi le specifiche finalità e tutte le altre attività (come ad esempio l'individuazione delle figure responsabili e degli incaricati del trattamento delle immagini, le modalità di accesso alle stesse, di conservazione dei dati, etc.) richiamati nel Provvedimento dell'8 aprile 2010 (riportato al capitolo 14 del presente documento).

3.5.5 Controllo a distanza e/o diretto

3.5.5.1 Apparecchiature preordinate al controllo a distanza

Con riguardo al principio secondo cui occorre perseguire finalità determinate, esplicite e legittime, il datore di lavoro può riservarsi di controllare (direttamente o attraverso la propria struttura) l'effettivo adempimento della prestazione lavorativa e, se necessario, il corretto utilizzo degli strumenti di lavoro.

Nell'esercizio di tale prerogativa occorre rispettare la libertà e la dignità dei lavoratori, in particolare per ciò che attiene al divieto di installare *"apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori"* , tra cui sono certamente comprese strumentazioni *hardware* e *software* mirate al controllo dell'utente di un sistema di comunicazione elettronica.

Il trattamento dei dati che ne conseguirebbe, qualora non si rispettasse la libertà e la dignità dei lavoratori, sarebbe illecito, a prescindere dall'illiceità dell'installazione stessa, anche quando i singoli lavoratori ne fossero consapevoli.

In particolare non può ritenersi consentito il trattamento effettuato mediante sistemi *hardware* e *software* preordinati al controllo a distanza, grazie ai quali sia possibile ricostruire –a volte anche minuziosamente– l'attività di lavoratori. É il caso, ad esempio:

- della lettura e della registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio *e-mail*;
- della riproduzione ed eventuale memorizzazione sistematica delle pagine *web* visualizzate dal lavoratore;
- della lettura e della registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;
- dell'analisi occulta di computer portatili affidati in uso.

Il controllo a distanza vietato dalla legge riguarda l'attività lavorativa in senso stretto e altre condotte personali poste in essere nel luogo di lavoro. A parte eventuali responsabilità civili e penali, i dati trattati illecitamente non sono utilizzabili.

3.5.5.2 Programmi che consentono controlli indiretti

Il datore di lavoro, utilizzando sistemi informativi per esigenze produttive o organizzative (ad es., per rilevare anomalie o per manutenzioni) o, comunque, quando gli stessi si rivelano necessari per la sicurezza sul lavoro, può avvalersi legittimamente, nel rispetto dello Statuto dei lavoratori, di sistemi che possano consentire indirettamente un controllo a distanza (c.d. controllo preterintenzionale) e determinare un trattamento di dati personali riferiti o riferibili ai lavoratori. Ciò, anche in presenza di attività di controllo discontinue.

Il trattamento di dati che ne consegue può risultare lecito. Resta ferma la necessità di rispettare le procedure di informazione e di consultazione delle risorse in relazione all'introduzione o alla modifica di sistemi automatizzati per la raccolta e l'utilizzazione dei dati, nonché in caso di introduzione o di modificazione di procedimenti tecnici destinati a controllare i movimenti o la produttività dei lavoratori.

In applicazione del menzionato principio di necessità il datore di lavoro è chiamato a promuovere ogni opportuna misura, organizzativa e tecnologica volta a prevenire il rischio di utilizzi impropri (da preferire rispetto all'adozione di misure "repressive") e, comunque, a "minimizzare" l'uso di dati riferibili ai lavoratori.

Dal punto di vista organizzativo è quindi opportuno che:

- si valuti attentamente l'impatto sui diritti delle risorse (prima dell'installazione di apparecchiature suscettibili di consentire il controllo a distanza e dell'eventuale trattamento);
- si individui preventivamente (anche per tipologie) a quali risorse è accordato l'utilizzo della posta elettronica e l'accesso a Internet;
- si determini quale ubicazione è riservata alle postazioni di lavoro per ridurre il rischio di un loro impiego abusivo.

Il datore di lavoro ha inoltre l'onere di adottare tutte le misure *tecnologiche* volte a minimizzare l'uso di dati identificativi. Le misure possono essere differenziate a seconda della tecnologia impiegata (ad es., posta elettronica o navigazione in Internet).

a) Internet: la navigazione web - Il datore di lavoro, per ridurre il rischio di usi impropri della navigazione in Internet (consistenti in attività non correlate alla prestazione lavorativa quali la visione di siti non pertinenti, l'*upload* o il *download* di *file*, l'uso di servizi di rete con finalità ludiche o estranee all'attività), deve adottare opportune misure che possono, così, prevenire controlli successivi sul lavoratore. Tali controlli, leciti o meno a seconda dei casi, possono determinare il trattamento di informazioni personali, anche non pertinenti o idonei a rivelare convinzioni religiose, filosofiche o di altro genere, opinioni politiche, lo stato di salute o la vita sessuale.

In particolare, il datore di lavoro può adottare una o più delle seguenti misure opportune, tenendo conto delle peculiarità proprie e dei diversi profili professionali:

- individuazione di categorie di siti considerati correlati o meno con la prestazione lavorativa;
- configurazione di sistemi o utilizzo di filtri che prevengano determinate operazioni –reputate inconferenti con l'attività lavorativa– quali l'*upload* o l'accesso a determinati siti (inseriti in una sorta di *black list*) e/o il *download* di *file* o *software* aventi particolari caratteristiche (dimensionali o di tipologia di dato);
- trattamento di dati in forma anonima o tale da precludere l'immediata identificazione di utenti mediante loro opportune aggregazioni (ad es., con riguardo ai *file* di *log* riferiti al traffico *web*, su base collettiva o per gruppi sufficientemente ampi di lavoratori);
- eventuale conservazione nel tempo dei dati strettamente limitata al perseguimento di finalità organizzative, produttive e di sicurezza.

b) Posta elettronica - Il contenuto dei messaggi di posta elettronica – come pure i dati esteriori delle comunicazioni e i *file* allegati – riguardano forme di corrispondenza assistite da garanzie di segretezza tutelate anche costituzionalmente, la cui *ratio* risiede nel proteggere il nucleo essenziale della dignità umana e il pieno sviluppo della personalità nelle formazioni sociali; un'ulteriore protezione deriva dalle norme penali a tutela dell'inviolabilità dei segreti.

Tuttavia, con specifico riferimento all'impiego della posta elettronica nel contesto lavorativo e in ragione della veste esteriore attribuita all'indirizzo di posta elettronica nei singoli casi, può risultare dubbio se il lavoratore, in qualità di destinatario o mittente, utilizzi la posta elettronica operando quale espressione dell'Ente datoriale o ne faccia un uso personale pur operando nella struttura lavorativa.

É quindi particolarmente opportuno che si adottino accorgimenti anche per prevenire eventuali trattamenti in violazione dei principi di pertinenza e non eccedenza. Si tratta di soluzioni che possono risultare utili per contemperare

le esigenze di ordinato svolgimento dell'attività lavorativa con la prevenzione di inutili intrusioni nella sfera personale dei lavoratori, nonché violazioni della disciplina sull'eventuale segretezza della corrispondenza.

In questo quadro è opportuno che:

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

3.5.5.3 Pertinenza e non eccedenza

Nell'eventualità di effettuare controlli sull'uso degli strumenti elettronici deve essere evitata un'interferenza ingiustificata sui diritti e sulle libertà fondamentali di lavoratori, come pure di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata.

L'eventuale controllo è lecito solo se sono rispettati i principi di pertinenza e non eccedenza.

Nel caso in cui un evento dannoso o una situazione di pericolo non sia stato impedito con preventivi accorgimenti tecnici, il datore di lavoro può adottare eventuali misure che consentano la verifica di comportamenti anomali. Deve essere per quanto possibile preferito un controllo preliminare su dati aggregati, riferiti all'intera struttura lavorativa o a sue aree.

L'eventuale controllo anonimo può concludersi con un avviso generalizzato relativo ad un rilevato utilizzo anomalo degli strumenti aziendali e con l'invito ad attenersi scrupolosamente a compiti assegnati e istruzioni impartite.

L'eventuale avviso può essere circoscritto a dipendenti afferenti all'area o settore in cui è stata rilevata l'anomalia. In assenza di successive anomalie non è di regola giustificato effettuare controlli su base individuale.

Va esclusa l'ammissibilità di controlli prolungati, costanti o indiscriminati.

I sistemi software dovrebbero quindi essere programmati e configurati in modo da cancellare periodicamente ed automaticamente (attraverso procedure di sovraregistrazione come, ad esempio, la cd. rotazione dei log file) i dati personali relativi agli accessi ad Internet e al traffico telematico, la cui conservazione non sia necessaria.

In assenza di particolari esigenze tecniche o di sicurezza, la conservazione temporanea dei dati relativi all'uso degli strumenti elettronici deve essere giustificata da una finalità specifica e comprovata e limitata al tempo necessario – e predeterminato– a raggiungerla (non superiore all'anno solare).

Un eventuale prolungamento dei tempi di conservazione va valutato come eccezionale e può aver luogo solo in relazione:

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

In questi casi, il trattamento dei dati personali deve essere limitato alle sole informazioni indispensabili per perseguire finalità preventivamente determinate ed essere effettuato con logiche e forme di Ente strettamente correlate agli obblighi, compiti e finalità già esplicitati.

3.5.6 Trattamento dei dati sensibili e/o giudiziari

3.5.6.1 Trattamento dei dati inerenti l'appartenenza dei dipendenti a sindacati

L'Ente ad oggi tratta informazioni che hanno attinenza con eventuale appartenenza dei dipendenti a sindacati, richiedendo preventivamente ai dipendenti l'eventuale autorizzazione al prelievo sindacale.

Il documento riportante la voce relativa ai prelievi sindacali è il cedolino paga: esso viene predisposto dal settore competente designato dall'Ente tramite strumenti informatici, i cui dati sono memorizzati presso il CED, che usufruisce anche del processo crittografico al fine di evitare la visione di tali dati a chi non ha diritto di accesso e/o di trattamento.

Cartaceamente, i cedolini dello stipendio devono essere consegnati spillati o in busta chiusa e non devono contenere informazioni lesive della riservatezza. Gli addetti alla predisposizione e/o alla consegna dei cedolini sono tenuti a tutelare la privacy dei lavoratori, limitando l'inserimento di informazioni sulla sfera privata e impedendo l'indebita conoscenza dei dati da parte di persone non autorizzate

Essi non possono essere lasciati sui tavoli dei dipendenti, nè aperti in modo da rendere accessibili a chiunque informazioni sulla sfera privata dei lavoratori. Tra le varie voci possono apparire, infatti, anche informazioni sulle coordinate bancarie, l'indicazione della sigla del su citato sindacato di appartenenza destinatario della ritenuta o, ancora, trattenute per cessioni del quinto, motivazioni di eventuali circostanze debitorie del lavoratore appartenenza a categorie protette, etc.

A tal'uopo, su indicazioni del Garante nell'elaborare i cedolini è consigliabile, laddove il software utilizzato lo permetta, configurarlo in modo da ridurre al minimo l'utilizzo di dati personali non necessari, pur assicurando il perseguimento di legittime finalità, consistenti nella corretta redazione delle voci della busta paga.

Tali configurazioni potrebbero essere ad esempio la sostituzione delle voci specifiche con descrizioni più generiche o dei codici o l'oscurazione delle stesse per permetterne la circolazione al di fuori dello stretto contesto

lavorativo come in caso di acquisti effettuati con modalità di pagamento rateali, per i quali sovente viene richiesta l'esibizione della busta-paga .

3.5.6.2 Trattamento dei dati inerenti lo stato di salute dei dipendenti

I dati relativi al servizio di medicina preventiva rientravano già nelle normative «ante privacy» quali dati riservati da trattare con riserva e protezioni adeguate.

Per quanto riguarda i dati cosiddetti ordinari, è doveroso fare attenzione al consenso al loro trattamento in funzione delle finalità. Comunicazioni a soggetti non pertinenti alle finalità del servizio di prevenzione e protezione rischi o diffusione di dati di cui è prevista la sola comunicazione potrebbero innescare reazioni a catena.

Il datore di lavoro non è legittimato a raccogliere certificati di malattia dei dipendenti con l'indicazione della diagnosi. In assenza di specifiche disposizioni, il lavoratore assente per malattia deve fornire un certificato contenente esclusivamente la prognosi con la sola indicazione dell'inizio e della durata dell'infermità.
La normativa prevede che la raccolta da parte del datore di lavoro di certificazioni mediche dei dipendenti comprensive di diagnosi è consentita solo se espressamente prevista da specifiche disposizioni.

Il servizio tratta una rilevante quantità di dati riservati dell'Ente (processi produttivi, eventuali programmi di ricerca e sviluppo, rapporti di lavoro, ec.) che non rientrano nelle categorie dei dati sensibili e/o giudiziari, ma non per questo sono privi di protezione.

I dati sensibili ad esso collegati si possono così riassumere:

- ***Schede di anamnesi mediche***: vengono fornite in busta chiusa a disposizione solo dell'interessato (una copia) del medico competente e della vigilanza;
- ***Piano sanitario***: deve contenere i nomi dei sottoposti alle visite preventive, la periodicità delle stesse, le analisi ed attività specialistiche programmate. È ovviamente conosciuto dal datore di lavoro, va comunicato al RSPP ed alle funzioni Enteli incaricate della gestione del programma;
- ***Idoneità alla mansione***, con o senza riserva: da trattare nell'ambito della gestione organizzativa dell'attività, con comunicazioni mirate ai soli interessati. Il datore di lavoro non ha l'obbligo di giustificare le decisioni assunte per applicare correttamente le eventuali limitazioni all'attività prescritte dal medico competente;
- ***Eventuali dati giudiziari da infortuni***: trattamenti strettamente riservati al datore di lavoro, agli interessati, al RSPP ed al medico competente.

Medico competente

Considerazioni ulteriori devono essere svolte in relazione a taluni specifici trattamenti che possono o devono essere effettuati all'interno dell'impresa in conformità alla disciplina in materia di sicurezza e igiene del lavoro.

Tale disciplina, che attua anche alcune direttive comunitarie e si colloca nell'ambito del più generale quadro di misure necessarie a tutelare l'integrità psico-fisica dei lavoratori, pone direttamente in capo al medico competente in materia di igiene e sicurezza dei luoghi di lavoro la sorveglianza sanitaria obbligatoria.

In quest'ambito, il medico competente effettua accertamenti preventivi e periodici sui lavoratori e istituisce (curandone l'aggiornamento) una cartella sanitaria e di rischio.

Detta cartella è custodita presso l'Ente o l'unità produttiva,"*con salvaguardia del segreto professionale",* e [consegnata in] copia al lavoratore stesso al momento della risoluzione del rapporto di lavoro, ovvero quando lo stesso ne faccia richiesta, fornendo allo stesso le informazioni necessarie relative alla conservazione della medesima; in caso di cessazione del rapporto di lavoro le cartelle vanno conservate in originale da parte del datore di lavoro, per almeno 10 anni, salvo il diverso termine previsto dalle disposizioni del D. Lgs. 81/08 e s.m.i..

In relazione a tali disposizioni, il medico competente è deputato a trattare i dati sanitari dei lavoratori, procedendo alle dovute annotazioni nelle cartelle sanitarie e di rischio, e curando le opportune misure di sicurezza per salvaguardare la segretezza delle informazioni trattate in rapporto alle finalità e modalità del trattamento stabilite. Ciò, quale che sia il titolare del trattamento effettuato dal medico.

Alle predette cartelle il datore di lavoro non può accedere, dovendo soltanto concorrere ad assicurarne un'efficace custodia nei locali dell'Ente (anche in vista di possibili accertamenti ispettivi da parte dei soggetti istituzionalmente competenti), ma, come detto, "*con salvaguardia del segreto professionale*".

Il datore di lavoro, sebbene sia tenuto, su parere del medico competente (o qualora il medico lo informi di anomalie imputabili all'esposizione a rischio), ad adottare le misure preventive e protettive per i lavoratori interessati, non può conoscere le eventuali patologie accertate, ma solo la valutazione finale circa l'idoneità del dipendente (dal punto di vista sanitario) allo svolgimento di date mansioni.

Dati sanitari

Devono essere osservate cautele particolari anche nel trattamento dei dati sensibili del lavoratore e, segnatamente, di quelli dati idonei a rivelarne lo stato di salute.

Tra questi ultimi, può rientrare l'informazione relativa all'assenza dal servizio per malattia, indipendentemente dalla circostanza della contestuale enunciazione della diagnosi.

Per tali informazioni, l'ordinamento appresta anche fuori della disciplina di protezione dei dati personali particolari accorgimenti per contenere, nei limiti dell'indispensabile, i dati dei quali il datore di lavoro può venire a conoscenza per dare esecuzione al contratto. In questo contesto, la disciplina generale contenuta nel Codice deve essere coordinata ed integrata, come si è visto, con altre regole settoriali o speciali.

Resta comunque vietata la diffusione di dati sanitari.

Assenze per ragioni di salute

Con specifico riguardo al trattamento di dati idonei a rivelare lo stato di salute dei lavoratori, la normativa di settore e le disposizioni contenute nei contratti collettivi giustificano il trattamento dei dati relativi ai casi di infermità (e talora a quelli inerenti all'esecuzione di visite specialistiche o di accertamenti clinici) che determini un'incapacità lavorativa (temporanea o definitiva, con la conseguente sospensione o risoluzione del contratto).

Non diversamente, il datore di lavoro può trattare dati relativi a invalidità o all'appartenenza a categorie protette, nei modi e per le finalità prescritte dalla vigente normativa in materia.

A tale riguardo, infatti, sussiste un quadro normativo articolato che prevede anche obblighi di comunicazione in capo al lavoratore e di successiva certificazione nei confronti del datore di lavoro e dell'ente previdenziale della condizione di malattia: obblighi funzionali non solo a giustificare i trattamenti normativi ed economici spettanti al

lavoratore, ma anche a consentire al datore di lavoro, nelle forme di legge, di verificare le reali condizioni di salute del lavoratore.

Per attuare tali obblighi viene utilizzata un'apposita modulistica, consistente in un attestato di malattia da consegnare al datore di lavoro – con la sola indicazione dell'inizio e della durata presunta dell'infermità: c.d. "prognosi" – e in un certificato di diagnosi da consegnare, a cura del lavoratore stesso, all'Istituto nazionale della previdenza sociale (Inps) o alla struttura pubblica indicata dallo stesso Istituto d'intesa con la regione, se il lavoratore ha diritto a ricevere l'indennità di malattia a carico dell'ente previdenziale.

Tuttavia, qualora dovessero essere presentati dai lavoratori certificati medici redatti su modulistica diversa da quella sopradescritta, nella quale i dati di prognosi e di diagnosi non siano separati, i datori di lavoro restano obbligati, ove possibile, ad adottare idonee misure e accorgimenti volti a prevenirne la ricezione o, in ogni caso, ad oscurali.

Denuncia all'Inail

Diversamente, per dare esecuzione ad obblighi di comunicazione relativi a dati sanitari, in taluni casi il datore di lavoro può anche venire a conoscenza delle condizioni di salute del lavoratore.

Tra le fattispecie più ricorrenti deve essere annoverata la denuncia all'Istituto assicuratore (Inail) avente ad oggetto infortuni e malattie professionali occorsi ai lavoratori; essa, infatti, per espressa previsione normativa, deve essere corredata da specifica certificazione medica.

In tali casi, pur essendo legittima la conoscenza della diagnosi da parte del datore di lavoro, resta fermo a suo carico l'obbligo di limitarsi a comunicare all'ente assistenziale esclusivamente le informazioni sanitarie relative o collegate alla patologia denunciata e non anche dati sulla salute relativi ad altre assenze che si siano verificate nel corso del rapporto di lavoro, la cui eventuale comunicazione sarebbe eccedente e non pertinente –con la conseguente loro inutilizzabilità–, trattandosi di dati non rilevanti nel caso oggetto di denuncia.

Altre informazioni relative alla salute

A tali fattispecie devono essere aggiunti altri casi nei quali può, parimenti, effettuarsi un trattamento di dati relativi alla salute del lavoratore (e finanche di suoi congiunti), anche al fine di permettergli di godere dei benefici di legge (quali, ad esempio, permessi o periodi prolungati di aspettativa con conservazione del posto di lavoro): si pensi, ad esempio, a informazioni relative a condizioni di *handicap*.

Allo stesso modo, il datore di lavoro può venire a conoscenza dello stato di tossicodipendenza del dipendente, ove questi richieda di accedere a programmi riabilitativi o terapeutici con conservazione del posto di lavoro (senza retribuzione), atteso l'onere di presentare (nei termini prescritti dai contratti collettivi) specifica documentazione medica al datore di lavoro.

Comunicazioni all'Inps

È altresì legittima la comunicazione di dati idonei a rivelare lo stato di salute dei lavoratori che il datore di lavoro faccia ai soggetti pubblici (enti previdenziali e assistenziali) tenuti a erogare le prescritte indennità in adempimento a

specifici obblighi derivanti dalla legge, da altre norme o regolamenti o da previsioni contrattuali, nei limiti delle sole informazioni indispensabili.

In particolare, il datore di lavoro può comunicare all'Istituto nazionale della previdenza sociale (Inps) i dati del dipendente assente, anche per un solo giorno, al fine di farne controllare lo stato di malattia: a tal fine deve tenere a disposizione e produrre, a richiesta, all'Inps, la documentazione in suo possesso.

Le eventuali visite di controllo sullo stato di infermità del lavoratore, ai sensi dell'art. 5 della legge 20 maggio 1970, n. 300 e s.m.i., o su richiesta dell'Inps o della struttura sanitaria pubblica da esso indicata, sono effettuate dai medici dei servizi sanitari indicati dalle regioni.

3.5.6.3 Trattamento di dati sensibili e/o giudiziari dei cittadini e/o fornitori

Per il trattamento dei dati sensibili e giudiziari si riportano di seguito i principi applicabili al trattamento degli stessi ai sensi dell'art. 22 del Codice:

1. I soggetti pubblici conformano il trattamento dei dati sensibili e giudiziari secondo modalità volte a prevenire violazioni dei diritti, delle libertà fondamentali e della dignità dell'interessato.
2. Nel fornire l'informativa di cui all'art. 13, i soggetti pubblici fanno espresso riferimento alla normativa che prevede gli obblighi o i compiti in base alla quale è effettuato il trattamento dei dati sensibili e giudiziari.
3. I soggetti pubblici possono trattare solo i dati sensibili e giudiziari indispensabili per svolgere attività istituzionali che non possono essere adempiute, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa.
4. I dati sensibili e giudiziari sono raccolti, di regola, presso l'interessato.
5. In applicazione dell'articolo 11, comma 1, lettere c), d) ed e), i soggetti pubblici verificano periodicamente l'esattezza e l'aggiornamento dei dati sensibili e giudiziari, nonché la loro pertinenza, completezza, non eccedenza e indispensabilità rispetto alle finalità perseguite nei singoli casi, anche con riferimento ai dati che l'interessato fornisce di propria iniziativa. Al fine di assicurare che i dati sensibili e giudiziari siano indispensabili rispetto agli obblighi e ai compiti loro attribuiti, i soggetti pubblici valutano specificamente il rapporto tra i dati e gli adempimenti. I dati che, anche a seguito delle verifiche, risultano eccedenti o non pertinenti o non indispensabili non possono essere utilizzati, salvo che per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene. Specifica attenzione è prestata per la verifica dell'indispensabilità dei dati sensibili e giudiziari riferiti a soggetti diversi da quelli cui si riferiscono direttamente le prestazioni o gli adempimenti.
6. I dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, sono trattati con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni che, considerato il numero e la natura dei dati trattati, li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità.
7. I dati idonei a rivelare lo stato di salute e la vita sessuale sono conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo. I medesimi dati sono trattati con le modalità di cui al comma 6 anche quando sono tenuti in elenchi, registri o banche di dati senza l'ausilio di strumenti elettronici.
8. I dati idonei a rivelare lo stato di salute non possono essere diffusi.

9. Rispetto ai dati sensibili e giudiziari indispensabili ai sensi del comma 3, i soggetti pubblici sono autorizzati ad effettuare unicamente le operazioni di trattamento indispensabili per il perseguimento delle finalità per le quali il trattamento è consentito, anche quando i dati sono raccolti nello svolgimento di compiti di vigilanza, di controllo o ispettivi.
10. 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 tra dati sensibili e giudiziari, nonché i trattamenti di dati sensibili e giudiziari ai sensi dell'articolo 14, sono effettuati solo previa annotazione scritta dei motivi.
11. In ogni caso, le operazioni e i trattamenti di cui al comma 10, se effettuati utilizzando banche di dati di diversi titolari, nonché la diffusione dei dati sensibili e giudiziari, sono ammessi solo se previsti da espressa disposizione di legge.
12. Le disposizioni di cui al presente articolo recano principi applicabili, in conformità ai rispettivi ordinamenti, ai trattamenti disciplinati dalla Presidenza della Repubblica, dalla Camera dei deputati, dal Senato della Repubblica e dalla Corte costituzionale.

3.5.7 Linee guida per la sicurezza ad uso degli incaricati

a) Utilizzare le chiavi

Il primo livello di protezione di qualunque sistema è quello fisico; è vero che una porta chiusa 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 la sua rimozione.

È fin troppo facile per un estraneo entrare in un ufficio non chiuso a chiave e sbirciare i documenti posti su una scrivania; pertanto, chiudere a chiave il proprio ufficio alla fine della giornata e chiudere i documenti a chiave nei cassetti ogni volta che si può.

b) Conservare i dischetti, cd, etc., in un luogo apposito

Per i dischetti, cd, etc. si applicano gli stessi criteri che per i documenti cartacei, con l'ulteriore pericolo che il loro smarrimento (che può anche essere dovuto a un furto) può passare più facilmente inosservato.

A meno che non si è sicuri che contengano solo informazioni non sensibili, riporli sotto chiave non appena finito di usarli.

c) Utilizzare le password

Vi sono svariate categorie di password, ognuna con il proprio ruolo preciso:

a) La password di accesso al computer impedisce l'utilizzo improprio della propria postazione, quando per un motivo o per l'altro l'incaricato non si trovi in ufficio.
b) La password di accesso alla rete impedisce che l'eventuale accesso non autorizzato a una postazione renda disponibili tutte le risorse dell'Ufficio.
c) La password dei programmi specifici permette di restringere l'accesso ai dati al solo personale autorizzato.
d) La password del salvaschermo, infine, impedisce che una assenza momentanea permetta a una persona non autorizzata di visualizzare il lavoro dell'incaricato.

Imparare a utilizzare questi quattro tipi fondamentali di password, per quanto pratico e ragionevole, e mantenere distinta almeno quella di tipo *a*, che può dover essere resa nota, almeno temporaneamente, ai tecnici incaricati dell'assistenza.

È bene provvedere, per quanto pratico e ragionevole, scegliere le passwords secondo le indicazioni della sezione apposita.

d) Attenzione alle stampe di documenti riservati

Non lasciare accedere alle stampe persone non autorizzate; se la stampante non si trova sulla propria scrivania recarsi quanto prima a ritirare le stampe. Distruggere personalmente le stampe quando non servono più.

e) Non lasciare traccia dei dati riservati

Quando si rimuove 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 dischetto non resti traccia dei dati precedenti. Nel dubbio, è sempre meglio usare un dischetto nuovo.

f) Prestare attenzione all'utilizzo di eventuali PC portatili

I PC portatili sono un facile bersaglio per i ladri. Se si ha la necessità di gestire dati riservati su un portatile, farvi installare un buon programma di cifratura del disco rigido, e utilizzare una procedura di backup periodico.

g) Non farsi spiare quando si digita le passwords

Anche se molti programmi non ripetono in chiaro la password sullo schermo, quando si digita la propria password, questa potrebbe essere letta guardando i tasti che si stanno battendo, anche se si hanno buone capacità di dattiloscrittura.

h) Custodire le passwords in un luogo apposito

Non scrivere la propria password, meno che mai vicino alla propria postazione di lavoro. L'unico affidabile dispositivo di registrazione è la propria memoria.

Se si ha necessità di conservare traccia delle password per scritto, non lasciare in giro i fogli utilizzati.

i) Non fare usare il proprio computer a personale esterno a meno di non essere sicuri della loro identità

Personale esterno può avere bisogno di installare un nuovo software/hardware nel computer del generico incaricato e/o accedere per esempio ad internet.

Assicurarsi dell'identità della persona e delle autorizzazioni ad operare sul proprio PC ed evitare, per quanto pratico e ragionevole, di lasciare solo il personale esterno in situazioni del genere.

j) Non installare programmi non autorizzati

Solo i programmi istituzionali o acquistati dall'Amministrazione con regolare licenza sono autorizzati. Se il proprio lavoro richiede l'utilizzo di programmi specifici, consultarsi con il Titolare e/o Responsabile del trattamento dati .

k) Applicare con cura le linee guida per la prevenzione da infezioni di virus

La prevenzione dalle infezioni da virus sul proprio computer è molto più facile e comporta uno spreco di tempo minore della correzione degli effetti di un virus; tra l'altro, si potrebbe incorrere in una perdita irreparabile di dati.

3.6. L'informativa all'Interessato

L' informativa rappresenta il primo obbligo a carico del titolare, che è tenuto a comunicare all'interessato (ovvero, secondo il Decreto Legislativo n. 196 del 30.06.2003, la persona fisica, la persona giuridica, l'ente o

l'associazione cui si riferiscono i dati personali), o al terzo presso cui sono raccolti dati all'interessato, oralmente o per iscritto, i seguenti argomenti:

1. ***le finalità e le modalità del trattamento cui sono destinati dati***

   È necessario informare l'interessato in modo da rendere chiaro e facilmente intelligibile lo scopo per il quale i dati sono trattati, ciò anche nei casi in cui sia l'interessato stesso a chiedere un certo tipo di servizio e, quindi, ne sia già perfettamente al corrente.

   Non sono esaustive, a tal'uopo, le indicazioni generiche che facciano riferimento alle "finalità istituzionali" o "statutarie".

   È importante altresì che l'interessato abbia l'immediata percezione del perché e in quale modo i suoi dati personali vengono trattati.

   Per quanto riguarda le modalità di trattamento si possono operare le stesse considerazioni. Non è sufficiente la semplice indicazione "trattamento informatizzato" o "cartaceo". Anche se non devono essere indicate tutte le operazioni che verranno effettuate, è necessario indicare le operazioni fondamentali (ad esempio: inserimenti in una o più banche dati, l'utilizzo di tali banche dati ecc.), nonché soggetti incaricati di svolgere dette operazioni.

2. ***la natura obbligatoria o facoltativa del conferimento dei dati***

   La norma si riferisce ai casi in cui la conoscenza di determinate informazioni è richiesta direttamente dalla legge per permettere lo svolgimento di determinate attività (ad esempio per richieste relative all'assstenza sociale). In tali casi, deve essere operata la distinzione tra le informazioni obbligatorie per legge o per contratto e quelle facoltative. Queste ultime possono configurarsi come richieste aggiuntive del titolare del trattamento, per poter fornire un servizio migliore o aggiuntivo all'interessato, il quale deve poter liberamente decidere se aderire a meno all'ulteriore richiesta di dati, valutando personalmente i vantaggi e svantaggi connessi.

3. ***le conseguenze dell'eventuale rifiuto di rispondere***

   Tale punto è in relazione con il precedente. Infatti, solo in presenza di un'espressa previsione normativa che impone la conoscenza di determinate informazioni, o a causa di impossibilità materiali di fornire il servizio richiesto, il titolare può prospettare all'interessato la circostanza che il rifiuto a fornire i dati personali può comportare la mancata esecuzione del trattamento, o la mancata prosecuzione del rapporto.

4. ***i soggetti o le categorie di soggetti ai quali dati personali possono essere comunicati che possono venire a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi***

   Anche l'indicazione dei soggetti ai quali dati possono o devono essere comunicati o diffusi dev'essere formulata in modo che l'interessato possa esprimere un consenso consapevole in ordine a tale comunicazione o diffusione. Ciò significa che è necessario indicare specificatamente l'ambito di comunicazione o diffusione, riportando, se possibile, nominalmente i soggetti o le categorie di soggetti ai quali i dati saranno comunicati. Inoltre, per dare completa esecuzione al dettato normativo, è importante indicare anche i motivi e le finalità di tale comunicazione o diffusione.

5. ***i diritti di cui all'art. 7***

I diritti, precedentemente analizzati, attribuiti all'interessato sono elencati nell'art. 7 del testo unico. Con riferimento a tali diritti, l'art. 13 del codice ripropone l'obbligo del titolare di fornire all'interessato l'elencazione di quanto disposto dall'art. 7.

Al riguardo è opportuno sottolineare che non è sufficiente un semplice richiamo al suddetto articolo ma è opportuno riportare nell'informativa l'intero testo normativo.

6. ***gli estremi identificativi del titolare e, se designati, del rappresentante nel territorio dello Stato ai sensi dell'art. 5 e del responsabile.***

L'informativa deve contenere gli estremi identificativi del titolare e, se designati, del rappresentante del territorio dello Stato sensi dell'art. 5 e del responsabile. Quando il titolare ha designato più responsabili dev'essere indicato almeno uno di essi, indicando il sito della rete di comunicazione o le modalità attraverso le quali è conoscibile in modo agevole l'elenco aggiornato dei responsabili.

Qualora il titolare abbia nominato un responsabile per le specifiche operazioni conseguenti ad eventuali richieste degli interessati, formulate nell'esercizio del loro diritti, nell'informativa preventiva resa all'interessato sarà indicato questo responsabile, mentre saranno comunque indicate le modalità per conoscere l' elenco aggiornato degli altri responsabili.

L'informativa deve essere essenziale, comunicare le sue notizie utili e evitando inutili ridondante e possono non comprendere gli elementi già noti alla persona che fornisce i dati.

3.6.1 L'informativa ai dipendenti

Il datore di lavoro è tenuto a rendere al lavoratore, prima di procedere al trattamento dei dati personali che lo riguardano (anche in relazione alle ipotesi nelle quali la legge non richieda il suo consenso), un'informativa individualizzata completa degli elementi indicati dall'art. 13 del Codice.

Con particolare riferimento a realtà produttive nelle quali, per ragioni organizzative (ad esempio, per l'articolata dislocazione sul territorio o per il ricorso consistente a forme di *out-sourcing*) o dimensionali, può risultare difficoltoso per il singolo lavoratore esercitare i propri diritti ai sensi dell'art. 7 del Codice, è opportuna la designazione di un responsabile del trattamento appositamente deputato alla trattazione di tali profili (o di responsabili esterni all'ente, che effettuino, ad esempio, l'attività di gestione degli archivi amministrativi dei dipendenti), indicandolo chiaramente nell'informativa fornita.

3.7. Il Consenso

3.7.1 Necessità del Consenso

L'interessato deve manifestare il suo consenso ad autorizzare nella fattispecie trattamenti proposti sui propri dati personali. Il trattamento dei dati personali è ammesso solo con il consenso espresso dell'interessato, il che significa che la mancanza di consenso validamente espressa equivale al diniego.

I principi di fondo sono i seguenti:

- Il trattamento è ammesso solo su espresso consenso dell'interessato;

- Il consenso può riguardare intero trattamento o singole parti (operazioni) di esso; può accadere che un trattamento di dati sia composto da diverse operazioni (ad esempio, i dati personali raccolti per scopi amministrativi possono essere utilizzati per successive promozioni di nuove attività). In questo caso l'interessato potrebbe acconsentire alle operazioni che ritiene utili per se stesso e potrebbe non acconsentire alle operazioni in cui non ripone alcun interesse;
- Il consenso è valido se espresso liberamente in riferimento ad un trattamento specifico e chiaramente individuato; tale punto chiarisce che non può essere ritenuto valido un consenso espresso in forma generica, es. "acconsento al trattamento dei miei dati personali da parte della ditta Alfa", senza alcuna specificazione preventiva delle caratteristiche essenziali di tale trattamento (finalità, modalità di svolgimento, comunicazione, diffusione, titolare, responsabile, ecc.), in pratica senza informativa resa sensi dell'articolo 13 del codice;
- Il consenso è valido se documentato in forma scritta. Non vi può essere un consenso in forma orale, come di contro per l'informativa. Di esso vi dev'essere sempre una certificazione scritta.
- Il consenso deve essere manifestato in forma scritta quando il trattamento riguarda dati sensibili. Quando il trattamento contiene dati sensibili, il codice richiede che l'interessato esprima direttamente il suo consenso in forma scritta.

3.7.2 Deroghe al Consenso

Vi sono casi in cui si può effettuare il trattamento senza consenso. Queste deroghe sono esplicitate nell'art. 24, e tale elenco è tassativo e non interpretabile in via estensiva.

Il consenso non è richiesto quando il trattamento:

- È necessario per adempiere un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria. Tale punto deve essere inteso come riferito ad obblighi propri del titolare del trattamento (es. registrazione delle fatture) e non in modo da includervi anche gli obblighi di terzi assolti attraverso la fornitura di un servizio specifico (es. società che adempie ad obblighi contabili di terzi con o senza corrispettivo).
- È necessario per eseguire obblighi derivanti da un contratto del quale è parte l'interessato o per adempiere, prima della conclusione del contratto, specifiche richieste all'interessato;
- Riguarda dati provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque;
- Riguarda dati relativi allo svolgimento di attività economiche;
- È necessario per perseguire un legittimo interesse del titolare, nei casi indicati dal garante e con esclusione dei casi di diffusione;
- È necessario per la salvaguardia della vita o dell'incolumità fisica dell'interessato o di un terzo, nel caso in cui l'interessato non può prestare il proprio consenso per impossibilità fisica, per incapacità di agire o per incapacità di intendere o di volere.

I dati comuni, come abbiamo già visto, se trattati per scopi istituzionali non richiedono il consenso dell'interessato anche se, benché la norma non lo chiarisca espressamente, è necessario fornire l'informativa in base alle regole generali.

3.7.3 Il Consenso dei dipendenti

A seguito della visione dell'informativa fornita dal datore di lavoro, il dipendente deve manifestare il suo consenso ed autorizzare nella fattispecie i trattamenti proposti sui dati personali.

Il trattamento dei dati personali è ammesso solo con il consenso espresso dal dipendente, il che significa che la mancanza di consenso validamente espressa equivale al diniego.

3.8 Comunicazione e diffusione dei dati personali

3.8.1 Comunicazione

3.8.1.1 Comunicazione dati personali dei dipendenti

La conoscenza dei dati personali relativi ad un lavoratore da parte di terzi è ammessa se l'interessato vi acconsente.

Se il datore di lavoro non può avvalersi correttamente di uno degli altri presupposti del trattamento equipollenti al consenso, non può prescindersi dal consenso stesso per comunicare dati personali (ad esempio, inerenti alla circostanza di un'avvenuta assunzione, allo *status* o alla qualifica ricoperta, all'irrogazione di sanzioni disciplinari o a trasferimenti del lavoratore) a terzi quali:

- associazioni (anche di categoria) di datori di lavoro, o di *ex* dipendenti (anche della medesima istituzione);
- conoscenti, familiari e parenti.

Fermo restando il rispetto dei principi generali sopra richiamati in materia di trattamento di dati personali, rimane impregiudicata la facoltà del datore di lavoro di disciplinare le modalità del proprio trattamento designando i soggetti, interni o esterni, incaricati o responsabili del trattamento, che possono acquisire conoscenza dei dati inerenti alla gestione del rapporto di lavoro, in relazione alle funzioni svolte e a idonee istruzioni scritte alle quali attenersi.

Ciò, ove necessario, anche mediante consegna di copia di documenti all'uopo predisposti**.**

È altresì impregiudicata la facoltà del datore di lavoro di comunicare a terzi in forma realmente anonima dati ricavati dalle informazioni relative a singoli o gruppi di lavoratori: si pensi al numero complessivo di ore di lavoro straordinario prestate o di ore non lavorate, qualifiche/livelli professionali, anche nell'ambito di singole funzioni o unità organizzative, etc.).

3.8.1.2 Comunicazione dati personali degli utenti

I principi generali che presiedono il trattamento da parte di soggetti pubblici in merito alla comunicazione dei dati sono i seguenti:

1. la comunicazione da parte di un soggetto pubblico ad altri soggetti pubblici è ammessa quando è prevista da una norma di legge o di regolamento;
2. la comunicazione da parte di un soggetto pubblico a privati o a enti pubblici economici e la diffusione da parte di un soggetto pubblico sono ammesse unicamente quando sono previste da una norma di legge o di regolamento.

3.8.2 Intranet Aziendale

Allo stesso modo, il consenso del lavoratore è necessario per pubblicare informazioni personali allo stesso riferite (quali fotografia, informazioni anagrafiche o *curricula*) nella *intranet a*ziendale (e a maggior ragione in *Internet*), non risultando tale ampia circolazione di dati personali di regola "*necessaria per eseguire obblighi derivanti dal contratto di lavoro*".

Tali obblighi possono trovare esecuzione indipendentemente da tale particolare forma di divulgazione che comunque, potendo a volte risultare pertinente (specie in realtà produttive di grandi dimensioni o ramificate sul territorio), richiede il preventivo consenso del singolo dipendente, salva specifica disposizione di legge.

3.8.3 Diffusione

3.8.3.1 Diffusione di dati relativi ai dipendenti

In assenza di specifiche disposizioni normative che impongano al datore di lavoro la diffusione di dati personali riferiti ai lavoratori o la autorizzino, o comunque di altro presupposto ai sensi dell'art. 24 del Codice, la diffusione stessa può avvenire solo se necessaria per dare esecuzione a obblighi derivanti dal contratto di lavoro. È il caso, ad esempio, dell'affissione in eventuale bacheca aziendale di ordini di servizio, di turni lavorativi o feriali, oltre che di disposizioni riguardanti l'Ente del lavoro e l'individuazione delle mansioni cui sono deputati i singoli dipendenti.

Salvo che ricorra una di queste ipotesi, non è invece di regola lecito dare diffusione a informazioni personali riferite a singoli lavoratori, anche attraverso la loro pubblicazione in bacheche aziendali o in comunicazioni interne destinate alla collettività dei lavoratori, specie se non correlate all'esecuzione di obblighi lavorativi. In tali casi la diffusione si pone anche in violazione dei principi di finalità e pertinenza, come nelle ipotesi di:

affissione relativa ad emolumenti percepiti o che fanno riferimento a particolari condizioni personali;

sanzioni disciplinari irrogate o informazioni relative a controversie giudiziarie;

assenze dal lavoro per malattia;

iscrizione e/o adesione dei singoli lavoratori ad associazioni.

3.8.3.2 Diffusione di dati relativi ai dati degli utenti

3.8.3.2.1 Il trattamento di dati contenuti in registri pubblici e negli albi professionali

Il Codice contiene una serie articolata di disposizioni normative disciplinanti il trattamento di dati personali provenienti da registri pubblici ed albi professionali. Esso ha opportunamente mantenuto inalterata la disciplina legislativa relativa al regime di pubblicità dei registri pubblici e degli albi: questi ultimi sono destinati per loro stessa natura e funzione ad un regime di piena conoscibilità che esclude la necessità di acquisire previamente il diritto degli interessati per il relativo trattamento.

Tuttavia, in armonia con quanto previsto a livello comunitario, la necessità di contemperare adeguatamente anche il diritto alla privacy dei soggetti iscritti agli albi o inseriti in elenchi pubblici ha spinto il legislatore ad istituzionalizzare l'adozione di un codice di deontologia e buona condotta "per il trattamento dei dati personali provenienti da archivi, registri, elenchi, atti o documenti tenuti da soggetti pubblici.

A questo proposito, occorre però specificare che la pubblicità di dati contenuti in elenchi o pubblici registri non può essere riferita a qualunque dato personale che sia di fatto consultabile, come ad esempio gli indirizzi di posta

elettronica lasciati in siti web o forum, ma si riferisce ai soli dati personali che sono sottoposti ad un regime giuridico di piena conoscibilità da parte di chiunque, come può ritenersi per gli elenchi telefonici.

A completamento di tale principio il Garante ha precisato che "le disposizioni della legge sulla privacy non possono, dunque, essere arbitrariamente estese e non possono essere applicate in modo da potere raccogliere ed utilizzare liberamente qualsiasi dato personale di natura non sensibile in base alla circostanza che il dato sia conoscibile di fatto, anche momentaneamente, da una pluralità di soggetti", come nel caso di chi lascia il proprio nominativo ed indirizzo e-mail in newsgroup, forum etc., solo per scopi di discussione su determinati temi.

Il legislatore ha chiarito che il trattamento dei dati personali contenuti, in particolare, negli albi professionali soggiace agli stessi principi stabiliti con riferimento alle operazioni di comunicazione e diffusione di dati da parte di soggetti pubblici, autorizzando il trattamento anche mediante reti di comunicazione elettronica, nonché la possibilità di menzionare eventuali procedimenti disciplinari o che comunque incidono sull'esercizio della professione. Ciò in quanto il regime di piena pubblicità cui sono ispirati gli albi dei liberi professionisti, così come i provvedimenti adottati dagli ordini, è stabilito anche in funzione della tutela dei diritti di coloro che a vario titolo hanno rapporti con gli iscritti e del regolare svolgimento dei procedimenti nel settore professionale di riferimento.

L'autorità ha sottolineato, infatti, che ai fini dell'applicazione della privacy, non è rilevante la modalità attraverso cui le informazioni vengono diffuse (pubblicazione cartacea o informatica), bensì il rispetto dei requisiti specifici che rendono possibile tale diffusione. Pertanto, "anche la diffusione per via telematica richiede la preventiva acquisizione del consenso degli interessati ovvero verificare che ricorra uno dei presupposti che permetta di farne a meno, ad esempio quando si tratta di adempiere un obbligo di legge o di regolamento oppure i dati provengono da pubblici registri, elenchi o atti conoscibili da chiunque"

3.8.3.2.2 Stato civile, documentazione anagrafica e liste elettorali

Il codice non si distingue, per particolari innovazioni apportate alla disciplina sulla riservatezza dei dati personali, in quanto si limita a qualificare di rilevante interesse pubblico "la tenuta degli atti e dei registri dello stato civile, delle anagrafi della popolazione residente in Italia e dei cittadini italiani residenti all'estero, e delle liste elettorali", ivi incluse le attività relative al rilascio di documenti di riconoscimento ed al cambiamento delle generalità.

Tuttavia, la disciplina codicistica non si limita a regolamentare tali materie, che trovano un opportuno completamento nelle disposizioni del codice che ha menzionato alcune disposizioni legislative per armonizzare la normativa vigente ai principi in materia di protezione dei dati personali e che, sotto certi aspetti, segna un totale capovolgimento della disciplina previgente.

Si sottolinea che i dati contenuti nei registri anagrafici, dello stato civile e nelle liste elettorali, che non sono necessariamente di carattere "sensibile", sono soggetti per loro natura ad un trattamento comprensivo dell'attività di raccolta, di comunicazione e di diffusione. In un primo luogo si segnala la possibilità, attribuita al comune, di utilizzare gli elenchi degli iscritti all'anagrafe della popolazione residente esclusivamente per l'uso di pubblica utilità, anche in applicazione della disciplina in materia di comunicazione istituzionale.

Sempre con riferimento alla materia anagrafica occorre sottolineare il fatto che la normativa sulla riservatezza non ha abrogato la relativa disciplina: l'autorità è più volte intervenuta sul tema, ricordando che l'ufficiale dell'anagrafe deve rilasciare, a chiunque ne faccia richiesta, i soli "certificati concernenti la residenza e lo stato di famiglia" degli

iscritti all'anagrafe, potendo comunicare i dati anagrafici solo se resi anonimi ed aggregati, ed esclusivamente per fini statistici e di ricerca, mentre altre informazioni desumibili dagli atti anagrafici possono essere oggetto di attestazione su ordine del sindaco, a meno che non vi ostino gravi o particolari esigenze di ordine pubblico.

Il rilascio degli elenchi degli iscritti nell'anagrafe della popolazione residente è invece previsto, per motivi di pubblica utilità, solamente verso pubbliche amministrazioni che ne facciano motivata richiesta. Stesso dicasi anche per quanto concerne le liste anagrafiche ed elettorali dei cittadini italiani residenti all'estero. Al di fuori delle sopra citare ipotesi, e fatta salva la particolare disciplina in materia di accesso ai documenti amministrativi, non è possibile comunicare o diffondere a privati i dati personali provenienti dagli archivi anagrafici.

In caso di affidamento di un attività in outsourcing, l'autorità pur riconoscendo che nello svolgimento dei propri compiti istituzionali il soggetto pubblico può ricorrere a privati affidando ad essi determinate attività anche attraverso concessioni, appalti o convenzioni, ha tuttavia ricordato che, a garanzia della tutela della riservatezza dei dati personali trattati dal soggetto privato (che si deve distinguere per gli evidenti requisiti di esperienza, capacità ed affidabilità) la convenzione deve essere stipulata con atto scritto ed essere accompagnata da precise istruzioni da parte del titolare. Ulteriori interventi effettuati dall'autorità si ricollegano a quanto disciplinato dal codice in relazione al diritto dell'anonimato della madre in occasione del parto. A tale proposito il codice in merito all'adozione ed all'affidamento dei minori, precisa in maniera più chiara ed intelligibile che è precluso all'adottato il diritto di accesso alle informazioni riguardanti la madre che abbia dichiarato di non volere essere nominata nella dichiarazione di nascita.

Il garante è altresì intervenuto a tutela dei dati personali e sanitari relativi a minori adottabili , nonché ai coniugi ed alle persone non coniugate che aspirano all'adozione (sia nazionale che internazionale).

In considerazione della rilevante particolarità delle informazioni ivi raccolte (quali i dati sanitari, le condizioni socio familiari dei singoli, i livelli di reddito e culturali, ecc.) l'autorità ha chiesto l'introduzione di maggiori garanzie e di misure di sicurezza adeguate. Il codice contiene alcune precisazioni in merito a rilascio degli estratti degli atti dello stati civile. Questa disposizione autorizza il rilascio di tali estratti unicamente nei confronti dei soggetti cui l'atto si riferisce ovvero dietro presentazione di un istanza motivata che comprovi la necessità da parte dei richiedente, di ottenete tali informazioni per il perseguimento di un interesse personale e concreto ai fini della tutela di una situazione giuridicamente rilevante, fermo restando il libero accesso a tali atti qualora siano decorsi 70 anni dalla loro formazione.

Di singolare evidenza risultano essere le modifiche apportate in materia di liste elettorali esse non indicheranno più il titolo di studio, ne la professione o il mestiere dell'elettore. Tale riformulazione è stata dettata dall'esigenza di assicurare il pieno rispetto dei noti principi di pertinenza e di non eccedenza rispetto alla finalità istituzionale relativa alla tenuta delle liste medesime, evitando l'esposizione degli interessati ad una inopportuna ed incontrollata divulgazione di informazioni riguardanti la propria persona, potendo essere assunte da chiunque acquistasse o copiasse le predette liste. In ogni caso il legislatore ha opportunamente operato un notevole ridimensionamento del regime di piena conoscibilità e pubblicità.

3.8.3.2.3 La tutela della riservatezza in alcuni settori particolari: l'uso dei contrassegni ed i sistemi di rilevazione delle infrazioni al codice della strada.

Nel quadro normativo ha trovato spazio anche la disciplina relativa ai contrassegni di veicoli e per accessi nei centri storici.

Il Codice prevede alcune cautele di base per il trattamento di dati personali ai fini della circolazione di veicoli in zone a traffico limitato o per la sosta in spazi riservati.

A garanzia della riservatezza dell'interessato, la disposizione prevede che i contrassegni che devono essere esposti sui veicoli per consentire la circolazione e la sosta dei veicoli di persone invalide,così come il transito e la soste in zone a traffico limitato, devono contenere unicamente i dati necessari ad individuare l'autorizzazione rilasciata, dovendosi omettere l'apposizione di simboli o diciture dalle quali si possa desumere la natura dell'autorizzazione per effetto della sola visione del contrassegno: in altri termini la necessità che il trattamento dei dati personali operato ai fini di cui sopra deve pur sempre avvenire nel rigoroso rispetto dei principi di pertinenza e di non eccedenza, a fronte di scopi perseguiti.

Si può ricorrere ad accorgimenti tali da ovviare la diretta visibilità delle generalità e dell'indirizzo del titolare, che potranno essere identificabili solo su richiesta di esibizione o per necessità di accertamento.

Come ha suggerito l'autorità, ciò può avvenire omettendo le generalità del beneficiario, riportandole sul lato posteriore del contrassegno, oppure celandole opportunamente all'immediata visibilità dall'esterno del veicolo, adottando dei sistemi in grado di evitare l'immediata leggibilità del titolo che attribuisce al relativo titolare il diritto alle facilitazioni. Dovrà essere indicato esclusivamente il comune competente a rilasciare il permesso ed il numero di autorizzazione, in modo tale da poter comunque risalire al titolare nel momento in cui si renda eventualmente necessario verificare la validità ed il corretto utilizzo del documento stesso.

I medesimi accorgimenti sono richiesti rispetto all'uso invalso in alcuni comuni di obbligare gli automobilisti ad esporre sui veicoli copia del libretto di circolazione o di altro documento, ipotesi che secondo l'autorità possono essere considerate lecite solo qualora sia resa nota agli interessati la possibilità di poter depennare dalle fotocopie le proprie generalità e l'indirizzo.

3.8.3.3 Linea Guida per la pubblicazione e diffusione sul web di atti e documenti adottati

L'attuale processo di innovazione e digitalizzazione della pubblica amministrazione è caratterizzato da numerose iniziative, anche legislative, volte a migliorare l'efficienza e la qualità delle prestazioni e dei servizi erogati dai soggetti pubblici mediante l'incremento dell'utilizzo delle tecnologie informatiche e telematiche.

Le disposizioni in materia di trasparenza e pubblicità dell'azione amministrativa, e di consultabilità degli atti prevedono in capo ai soggetti pubblici diversi obblighi di messa a disposizione delle relative informazioni da realizzare con modalità di divulgazione e ambiti di conoscenza di tipo differente, comportando, a seconda dei casi, operazioni di comunicazione oppure di diffusione di dati personali.

Tali obblighi si aggiungono a quelli previsti da normative previgenti in relazione ai quali il Garante si è già pronunciato in passato, rilevando che, in linea di principio, non sussiste alcuna incompatibilità di fondo tra le disposizioni in materia di protezione dati personali e determinate forme di conoscibilità di informazioni riconducibili alla trasparenza dell'azione amministrativa.

La disciplina legislativa sulla protezione dei dati personali regola la comunicazione e la diffusione delle informazioni personali in maniera tendenzialmente uniforme, indipendentemente dalle modalità tecniche utilizzate; ciò, sia nei casi in cui i dati personali siano resi noti mediante una pubblicazione cartacea, sia laddove tali informazioni siano messe a disposizione *on line* tramite una pagina *web*. Il presente paragrafo ha lo scopo di definire un quadro

unitario di misure e accorgimenti finalizzati a individuare opportune cautele che i soggetti pubblici sono tenuti ad applicare in relazione alle ipotesi in cui effettuano, in attuazione alle disposizioni normative vigenti, attività di comunicazione o diffusione di dati personali sui propri siti istituzionali per finalità di trasparenza, pubblicità dell'azione amministrativa, nonché di consultazione di atti su iniziativa di singoli soggetti.

Riscontro all'interessato in caso di accesso ai propri dati personali

Non sono presi in considerazione in questo ambito i casi in cui i soggetti pubblici sono destinatari di istanze di accesso ai dati personali, in quanto il dare conoscenza all'interessato delle proprie informazioni in possesso dell'amministrazione non configura un'operazione di comunicazione (artt. 4, comma 1, lett. l) e 7 del Codice).

3.8.3.3.1 Pubblicazione di atti, documenti e informazioni

I soggetti pubblici possono utilizzare informazioni personali per lo svolgimento delle proprie funzioni istituzionali anche in mancanza di una norma di legge o di regolamento che preveda espressamente il trattamento di dati personali e non devono richiedere il consenso dell'interessato (artt. 18, commi 2 e 4, 19, comma 1, del Codice).

Pubblicazione di dati personali anche contenuti in atti e documenti amministrativi

In relazione alle sole operazioni di comunicazione e di diffusione di dati personali, le pubbliche amministrazioni, nel mettere a disposizione, sui propri siti istituzionali, atti e documenti contenenti dati personali (in forma integrale, per estratto, ivi compresi gli allegati), devono preventivamente verificare che una norma di legge o di regolamento preveda tale possibilità (artt. 4, comma 1, lett. l) e m), 19, comma 3, 20 e 21, del Codice), fermo restando comunque il generale divieto di diffusione dei dati idonei a rivelare lo stato di salute dei singoli interessati (artt. 22, comma 8, 65, comma 5, 68, comma 3, del Codice). Quando una norma di legge o di regolamento lo disponga espressamente, l'amministrazione è tenuta a comunicare e diffondere anche il contenuto parziale o integrale degli atti o dei documenti o le informazioni che da essi si possono trarre.

Pubblicazione di informazioni personali

L'amministrazione può pubblicare sul proprio sito web informazioni che contengono dati personali, eventualmente anche tratti da atti e documenti amministrativi, qualora tale divulgazione, che deve essere sempre sorretta da una puntuale motivazione, costituisca un'operazione strettamente necessaria al perseguimento delle finalità assegnate all'amministrazione da specifiche leggi o regolamenti, e riguardi informazioni utili ai destinatari dell'attività o dei servizi prestati dall'amministrazione, fermo restando che non possono essere comunicate o diffuse informazioni riferite agli utenti se non nei casi in cui questo è esplicitamente previsto da una legge o da un regolamento.

Resta fermo che la pubblicazione di dati personali aventi natura sensibile è consentita solo se autorizzata da espressa disposizione di legge nella quale siano specificati i tipi di dati, le operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite ovvero qualora tale operazione sia identificata nel regolamento che l'amministrazione è tenuta ad adottare, previo parere conforme del Garante (art. 20, commi 1 e 2, del Codice).

Pubblicazione di informazioni alla luce della recente riforma normativa in materia di trasparenza delle pubbliche amministrazioni

L'amministrazione può, infine, disporre la pubblicazione sul proprio sito web di informazioni personali, qualora tale divulgazione sia riconducibile all'attuazione del Programma triennale per la trasparenza e l'integrità che ciascuna amministrazione è tenuta ad adottare, anche sulla base delle *"Linee guida per la predisposizione del Programma triennale per la trasparenza e l'integrità"*, adottate il 14 ottobre 2010 dalla Commissione indipendente per la valutazione, la trasparenza e l'integrità delle amministrazioni pubbliche (Civit). In tale quadro gli stessi Programmi triennali delle amministrazioni dovranno contenere un'adeguata motivazione circa l'esigenza sottesa alla scelta di pubblicazione dei dati.

Pubblicazione di informazioni personali su richiesta dell'interessato

Nell'ambito dei rapporti intercorrenti con l'amministrazione pubblica, gli interessati possono formulare specifiche richieste volte a ottenere che taluni propri dati personali siano pubblicati sul sito istituzionale dell'amministrazione.

Tali richieste possono riguardare informazioni personali che sono già nella disponibilità dell'amministrazione in quanto acquisite per lo svolgimento delle proprie funzioni istituzionali, ovvero che possono essere conferite facoltativamente dall'interessato allo specifico scopo di consentirne la diffusione (art. 13, comma 1, lett. b) del Codice).

E' facoltà dell'amministrazione valutare se prendere in esame tali richieste di pubblicazione che comunque potranno essere accolte solo all'esito di un'attenta verifica con cui si accerti che tale operazione sia compatibile con lo svolgimento delle proprie funzioni istituzionali e che i dati oggetto di diffusione *on line* risultino pertinenti e non eccedenti rispetto alle finalità perseguite. Si pensi alla possibilità per la pubblica amministrazione, nel quadro dello svolgimento delle funzioni istituzionali volte a favorire la trasparenza della propria organizzazione, di riconoscere ai propri dipendenti che ne facciano specifica e libera richiesta, di pubblicare le loro foto sul sito istituzionale, al fine di migliorare, ad esempio, il rapporto fra operatori ed utenti (allo stato, specifiche disposizioni normative prevedono a tale scopo l'obbligo dell'esibizione dei cartellini identificativi).

Sindacabilità delle scelte in ordine alla pubblicazione di dati personali

Tutte le decisioni assunte dall'amministrazione in relazione alla pubblicazione sui propri siti istituzionali di atti e documenti contenenti dati personali sono sindacabili da parte del Garante ove non siano rispettati i principi di necessità, proporzionalità e pertinenza dei dati (artt. 11, comma1, del Codice).

3.8.3.3.2 Trasparenza, pubblicità e consultabilità di atti e documenti: valutazione delle tre grandi finalità perseguibili mediante la pubblicazione *on line*

Le previsioni normative in materia di trasparenza, pubblicità e consultabilità degli atti, preordinate ad assicurare un certo grado di conoscenza dell'operato della pubblica amministrazione, non perseguono finalità analoghe.

La pubblica amministrazione, pertanto, è tenuta, in primo luogo, a valutare quali specifiche finalità sono rinvenibili dalle disposizioni legislative o regolamentari che prevedono un particolare regime di conoscibilità di informazioni, di atti e documenti amministrativi.

In particolare, occorre distinguere i casi in cui, in relazione alla attività di comunicazione o diffusione di dati personali attraverso la pubblicazione di atti e documenti amministrativi sui siti istituzionali, si perseguano finalità di:

A. Trasparenza;

B. Pubblicità;

C. Consultabilità.

Tali valutazioni devono essere effettuate dall'amministrazione pubblica nel rispetto dei principi di necessità e proporzionalità del trattamento dei dati personali (artt. 3 e 11 del Codice) in modo da garantire modalità differenziate di messa a disposizione di dati e documenti tenendo conto delle diverse finalità sopra evidenziate, delle tipologie di informazioni oggetto di divulgazione, nonché degli strumenti e dei mezzi utilizzati per assicurarne la conoscibilità, affinché siano correttamente rispettati i diritti degli interessati.

A. TRASPARENZA

Per *Trasparenza* si intende la disponibilità sui siti istituzionali delle amministrazioni di atti e documenti amministrativi, contenenti dati personali, per finalità di trasparenza è volta a garantire una conoscenza generalizzata delle informazioni concernenti aspetti dell'organizzazione dell'amministrazione al fine di assicurare un ampio controllo sulle capacità delle pubbliche amministrazioni di raggiungere gli obiettivi nonché sulle modalità adottate per la valutazione del lavoro svolto dai dipendenti pubblici.

In presenza dei presupposti legislativi o regolamentari che legittimano le operazioni di comunicazione e di diffusione, le pubbliche amministrazioni sono tenute a verificare in concreto quali siano i dati personali, ritenuti pertinenti per il corretto svolgimento delle proprie funzioni istituzionali, che devono essere resi conoscibili mediante la loro messa a disposizione sui siti istituzionali (artt. 11, 18 e 19 del Codice).

Il procedimento di selezione dei dati personali che possono essere resi conoscibili *on line* deve essere particolarmente accurato nei casi in cui tali informazioni siano di tipo sensibile o giudiziario o, in particolare, qualora riguardino dati idonei a rivelare lo stato di salute o la vita sessuale. Un quadro di garanzie particolarmente stringente protegge, infatti, i dati sensibili e giudiziari prevedendo espressamente che i soggetti pubblici possono trattare tali informazioni solo se in concreto indispensabili per svolgere le attività istituzionali che non possono essere adempiute, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa (art. 22 del Codice).

A. 1. Informazioni riferite agli addetti ad una funzione pubblica

Il legislatore ha individuato, nel corso del tempo, molteplici obblighi di pubblicazione on line di dati, dando luogo a una forte frammentazione della disciplina.

Essi rispondono all'esigenza fondamentale di garantire la trasparenza amministrativa anche le disposizioni che, novellando l'art. 19 del Codice, sono intervenute sul tema della conoscibilità delle notizie riguardanti lo svolgimento delle prestazioni e la relativa valutazione di *"chiunque sia addetto ad una funzione pubblica"*. Tali disposizioni escludono la conoscibilità, salvo nei casi previsti dalla legge, delle *"notizie concernenti la natura delle infermità e degli impedimenti personali o familiari che causino l'astensione dal lavoro, nonché le componenti della valutazione o le notizie concernenti il rapporto di lavoro tra il predetto dipendente e l'amministrazione, idonee a rivelare taluna delle informazioni di cui all'articolo 4, coma 1, lett. d)"* (v. art. 14, comma 1, lett. b) l. 4 novembre 2010, n. 183).

Specifiche disposizioni legislative fissano i limiti massimi delle retribuzioni e degli emolumenti direttamente o indirettamente erogati a carico delle pubbliche finanze per rapporti di lavoro dipendente o autonomo, le quali impongono alle amministrazioni l'obbligo di rendere noti sul proprio sito web i relativi atti di spesa con l'indicazione dei nominativi dei destinatari e dell'ammontare del compenso quale condizione indispensabile per l'attuazione dei medesimi atti di spesa (art. 3, comma da 44 a 52-bis, l. n. 244/2007).

Per quanto riguarda i *curricula* professionali di dirigenti, segretari comunali e provinciali, nonché di titolari di posizioni organizzative, di funzioni di valutazione e misurazione della *performance* e di incarichi di indirizzo politico-amministrativo, il riferimento del legislatore all'obbligo di pubblicazione del vigente modello di *curriculum* europeo non può comportare la riproduzione di tutti i suoi contenuti sui siti istituzionali dell'amministrazione, in ragione unicamente delle finalità di trasparenza perseguite (art. 11, comma 8, lett. e), f), e h), d.lg. n. 150/2009 e art. 21, comma 1, l. n. 69/2009).

Tale modello, infatti, contiene l'indicazione di dati personali eccedenti o non pertinenti rispetto alle legittime finalità di trasparenza perseguite, in quanto risponde alle diverse esigenze di favorire l'incontro tra domanda e offerta di lavoro e la valutazione di candidati. Prima di pubblicare sul sito istituzionale il *curriculum* europeo va quindi operata una selezione delle informazioni in esso contenute ritenute pertinenti in relazione agli incarichi svolti o alle funzioni pubbliche ricoperte dal personale interessato quali, ad esempio:

- informazioni personali (dati anagrafici, amministrazione di appartenenza, qualifica e/o incarico ricoperto, recapito telefonico dell'ufficio, *e-mail* istituzionale);
- dati riguardanti i titoli di studio e professionali, le esperienze lavorative (incarichi ricoperti, capacità linguistiche e nell'uso delle tecnologie, partecipazione a convegni e seminari, pubblicazioni, collaborazione a riviste, ecc.);
- ulteriori informazioni di carattere professionale indicate dall'interessato.

Dovrebbe inoltre essere garantita agli interessati la possibilità di aggiornare periodicamente il proprio *curriculum*.

Non appare giustificato riprodurre sul *web* informazioni quali i cedolini dello stipendio, dati di dettaglio risultanti dalle dichiarazioni fiscali, oppure riguardanti l'orario di entrata e di uscita di singoli dipendenti, l'indirizzo del domicilio privato, il numero di telefono e l'indirizzo di posta elettronica personale (diversi da quelli ad uso professionale), ovvero informazioni attinenti allo stato di salute di persone identificate, quali le assenze verificatesi per ragioni di salute.

Per quanto riguarda le modalità di messa a disposizione dei dati personali sulla sezione dei siti istituzionali dei soggetti pubblici dedicata appositamente a "Trasparenza, valutazione e merito", si ritiene che debbano essere privilegiati canali o modalità di ricerca interni ai medesimi siti limitando, attraverso idonei accorgimenti, l'indicizzazione da parte dei motori di ricerca esterni, nonché la creazione di copie cache presso gli stessi motori di ricerca. Resta invece ferma la possibilità di utilizzare strumenti idonei ad agevolare la reperibilità, all'interno dei siti istituzionali delle amministrazioni, delle informazioni e dei documenti oggetto di divulgazione.

A. 1.1. Trasparenza dell'attività delle pubbliche amministrazioni senza dati personali

Il perseguimento della finalità di trasparenza dell'attività delle pubbliche amministrazioni può avvenire anche senza l'utilizzo di dati personali.

In tale quadro, quindi, non si ravvisa la necessità di adottare alcuna specifica cautela qualora le pubbliche amministrazioni ritengano di pubblicare sul sito *web* informazioni non riconducibili a persone identificate o

identificabili (es. dati quantitativi aggregati per uffici riguardanti i livelli retributivi ed accessori risultanti dai contratti collettivi o da atti interni di organizzazione; tassi di assenza e di maggiore presenza del personale; l'ammontare complessivo dei premi collegati alla *performance* stanziati e di quelli effettivamente distribuiti; obiettivi assegnati agli uffici ed i relativi indicatori; dati relativi al grado di differenziazione nell'utilizzo della premialità, informazioni concernenti la dimensione della qualità dei servizi erogati, notizie circa la gestione dei pagamenti e le buone prassi).

A. 2. Situazione patrimoniale di titolari di cariche e incarichi pubblici

Uno specifico regime di conoscibilità riconducibile alle esigenze di trasparenza della pubblica amministrazione è previsto dalla legge 5 luglio 1982, n. 441 sulla pubblicità della situazione patrimoniale di coloro che ricoprono cariche pubbliche o incarichi di rilievo pubblico. Tale norma dispone espressamente che esclusivamente i *"cittadini iscritti nelle liste elettorali per le elezioni della Camera dei Deputati"* possono, mediante la messa a disposizione, consultare legittimamente il bollettino nel quale sono riportati i dati riguardanti la situazione patrimoniale di titolari di cariche elettive e di cariche direttive di alcuni enti (artt. 8 e 9).

Nell'ambito del suesposto quadro normativo deve, tuttavia, rilevarsi che una distinta modalità è prevista per la consultabilità dei dati in questione con riferimento agli enti territoriali per i quali, infatti, la legge n. 441/1982 dispone che la pubblicazione individuata dall'art. 9 sopra richiamato sia effettuata, su appositi bollettini, senza tuttavia limitare la conoscibilità di tali informazioni ai soli cittadini elettori della Camera dei Deputati. In forza della predetta specificazione normativa, le regioni e gli enti locali nel pubblicare sul proprio bollettino la situazione patrimoniale dei consiglieri e le spese sostenute per la propaganda elettorale, possono dare ampia diffusione ai propri bollettini e alle informazioni ivi riportate, anche mediante la riproduzione dei bollettini stessi sui propri siti istituzionali.

Ulteriori disposizioni prevedono che talune informazioni relative agli amministratori locali e regionali (dati anagrafici, lista o gruppo di appartenenza o di collegamento, titolo di studio e professione esercitata) vengano raccolte dal Ministero dell'interno in un'apposita anagrafe di cui chiunque ha il diritto di prendere visione ed estrarre copia, anche su supporto informatico. In considerazione dell'ampio regime di conoscibilità previsto per tali informazioni riferite agli amministratori, gli atti statutari, legislativi o regolamentari delle amministrazioni regionali e degli enti locali interessati possono autorizzarne la messa a disposizione per via telematica attraverso i propri siti istituzionali (art. 76 d.lg. n. 267/2000).

A. 3. Ruoli del personale e bollettini ufficiali

Sono parimenti riconducibili alle esigenze di trasparenza dell'apparato amministrativo anche gli obblighi posti in capo a ciascuna amministrazione dello Stato di pubblicare sul proprio sito *web* il ruolo dei dirigenti, dando avviso della pubblicazione nella Gazzetta Ufficiale. Nel ruolo, che l'amministrazione deve aver cura di tenere secondo principi di completezza e trasparenza, nonché di pertinenza e non eccedenza dei dati, vanno rese pubbliche le sole informazioni individuate nel dettaglio dalla disciplina di settore (cognome, nome, luogo e data di nascita; data di inquadramento nella fascia di appartenenza o in quella inferiore; data di primo inquadramento nell'amministrazione; incarichi conferiti ai sensi dell'articolo 19, commi 3 e 4, del d.lg. 30 marzo 2001, n. 165 con l'indicazione della decorrenza e del termine di scadenza) (artt. 1, comma 7, e 2, commi 1 e 3, D.P.R. 23 aprile 2004, n. 108).

Sono soggetti a pubblicazione obbligatoria anche i ruoli di anzianità dei dipendenti pubblici che ciascuna amministrazione è tenuta a predisporre, annualmente, in modalità cartacea, dandone avviso nel proprio bollettino ufficiale (Art. 55, comma 5, D.P.R. 10 gennaio 1957, n. 3). Dal 1° gennaio 2007, per ragioni di efficacia ed

economicità, la pubblicazione a stampa dei ruoli di anzianità delle amministrazioni statali è stata sostituita con la riproduzione in rete dei medesimi documenti.

Poiché la disciplina di settore in questione non individua nel dettaglio le informazioni che devono essere riportate nei ruoli, occorre nel caso di specie effettuare un'opportuna selezione in modo da rendere conoscibili soltanto i dati necessari a determinare l'anzianità di servizio, evitando l'inserimento di notizie non pertinenti, eccedenti o riguardanti stati, qualità o situazioni personali ovvero informazioni idonee a rivelare dati sensibili (es. mutilato o invalido civile; aspettativa per motivi di salute o distacco per motivi sindacali).

Per ciò che concerne gli atti riferiti a ciascun dipendente, la normativa di riferimento stabilisce che nei bollettini ufficiali va data notizia, in particolare, degli atti relativi alla nomina, allo stato, alla carriera, ad encomi ed onorificenze, a sanzioni disciplinari, alla responsabilità verso l'amministrazione e i terzi, nonché all'invalidità per causa di guerra o di lavoro e alle infermità contratte per causa di servizio (art. 24, commi 1 e 3, D.P.R. 3 maggio 1957, n. 686).

Anche in tale caso si ritiene opportuno suggerire che nella predisposizione di tali pubblicazioni, rese disponibili *on line*, le amministrazioni interessate riportino solo informazioni pertinenti, non eccedenti e - laddove vengano in rilievo dati sensibili o giudiziari - indispensabili, rispettando il divieto di diffondere dati idonei a rivelare lo stato di salute dei dipendenti adottando a tale fine idonei accorgimenti quali l'utilizzo di *omissis*, diciture generiche o codici numerici.

Non vi sono ostacoli, comunque, alla diffusione per via telematica degli atti generali di organizzazione e gestione del personale la cui conoscibilità risponda ad esigenze di carattere informativo diffuso (es. decreti, circolari, bandi di concorso, ecc.).

A. 4. Albo dei beneficiari di provvidenze di natura economica

Le amministrazioni dello Stato, le regioni, comprese quelle a statuto speciale, e le province autonome di Trento e Bolzano, gli enti locali e gli altri enti pubblici sono tenuti ad istituire l'albo dei soggetti, ivi comprese le persone fisiche, cui sono stati erogati in ogni esercizio finanziario contributi, sovvenzioni, crediti, sussidi e benefici di natura economica a carico dei rispettivi bilanci e devono provvedere ad aggiornarlo annualmente (D.P.R. 7 aprile 2000, n. 118).

Il previsto regime di conoscibilità, anche on line, dei medesimi albi risponde all'esigenza di rendere trasparente l'azione amministrativa, anche in ordine all'utilizzo delle risorse finanziarie da parte dei soggetti eroganti nonché all'esigenza di assicurare la partecipazione dei cittadini al procedimento amministrativo di concessione dei contributi consentendo l'accesso alle relative informazioni.

Entrambe le suesposte esigenze sono pertanto soddisfatte mediante la pubblicazione, sui siti delle pubbliche amministrazioni individuate dalla norma in esame, degli elenchi di beneficiari di provvidenze economiche e di altri atti che riconoscono agevolazioni, sussidi o altri benefici. In tali elenchi possono essere riportati i soli dati necessari all'individuazione dei soggetti interessati (nominativi e relativa data di nascita), l'esercizio finanziario relativo alla concessione del beneficio, nonché l'indicazione della *"disposizione di legge sulla base della quale hanno luogo le erogazioni"* medesime. Non risulta invece giustificato diffondere ulteriori dati non pertinenti quali l'indirizzo di abitazione, il codice fiscale, le coordinate bancarie dove sono accreditati i contributi, la ripartizione degli assegnatari secondo le fasce dell'Indicatore della situazione economica equivalente-Isee ovvero informazioni che descrivano le condizioni di indigenza in cui versa l'interessato.

Non devono inoltre essere riportate negli albi diffusi *on line* informazioni idonee a rivelare lo stato di salute degli interessati (artt. 22, comma 8, e 68, comma 3, del Codice). Si pensi, in tale caso, all'indicazione:

- dei titoli dell'erogazione dei benefici (es. attribuzione di borse di studio a "soggetto portatore di *handicap*", o riconoscimento di buono sociale a favore di "anziano non autosufficiente" o con l'indicazione, insieme al dato anagrafico, delle specifiche patologie sofferte dal beneficiario);
- dei criteri di attribuzione (es. punteggi attribuiti con l'indicazione degli "indici di autosufficienza nelle attività della vita quotidiana");
- della destinazione dei contributi erogati (es. contributo per "ricovero in struttura sanitaria oncologica").

Per quanto riguarda le modalità di messa a disposizione dei dati personali contenuti nell'*Albo dei beneficiari di provvidenze di natura economica*, che possono essere riportati nei siti istituzionali dei soggetti pubblici che erogano tali benefici, si suggerisce di privilegiare canali o modalità di ricerca interni ai medesimi siti limitando, attraverso idonei accorgimenti, l'indicizzazione da parte dei motori di ricerca esterni, nonché la creazione di copie cache presso gli stessi motori di ricerca. Resta invece ferma la possibilità di utilizzare strumenti idonei ad agevolare la reperibilità, all'interno dei siti istituzionali delle amministrazioni, delle informazioni riguardanti i beneficiari individuati nell'Albo.

B. PUBBLICITÀ DEGLI ATTI AMMINISTRATIVI

Per *Pubblicità* si intende la disponibilità on line per finalità di pubblicità è volta a garantire che atti e documenti amministrativi producano effetti legali al fine di favorire eventuali comportamenti conseguenti da parte degli interessati.

Tale pubblicità può configurarsi come uno strumento della trasparenza poiché funzionale a rendere conoscibili gli atti amministrativi.

E' necessario verificare se i dati personali contenuti in atti e documenti messi a disposizione sul sito istituzionale devono essere resi conoscibili all'intera collettività dei consociati (quindi liberamente reperibili da chiunque sul sito istituzionale), ovvero ai soli utenti che hanno richiesto un servizio, ovvero agli interessati o ai contro interessati in un procedimento amministrativo (utilizzando in tale caso regole per garantire un accessibilità selezionata).

B.1. Concorsi e selezioni pubbliche

L'ordinamento prevede particolari forme di pubblicità per gli esiti delle prove concorsuali e delle graduatorie finali di concorsi e selezioni pubbliche (es. affissione presso la sede degli esami, pubblicazione nel bollettino dell'amministrazione interessata o, per gli enti locali, all'albo pretorio). Tale regime di conoscibilità assolve principalmente alla funzione di rendere note le decisioni adottate dalla commissione esaminatrice e dall'ente pubblico procedente anche per consentire il controllo sulla regolarità delle procedure concorsuali o selettive da parte dei soggetti interessati.

Le previsioni normative che disciplinano la pubblicazione di graduatorie, esiti e giudizi concorsuali prevedono espressamente la diffusione dei relativi dati personali, anche mediante l'utilizzo del sito istituzionale dell'amministrazione di riferimento.

Al riguardo, devono ritenersi appropriate quelle modalità di diffusione *on line* di graduatorie, esiti e giudizi concorsuali che consentono di rendere conoscibili i dati personali ivi riportati consultando il sito istituzionale dell'amministrazione pubblica competente, escludendone quindi la reperibilità tramite i comuni motori di ricerca

esterni. A tale scopo è possibile, ad esempio, attribuire ai partecipanti alla procedura concorsuale credenziali di autenticazione (es. *username* o *password*, n. di protocollo o altri estremi identificativi forniti dall'ente agli aventi diritto) per consentire agli stessi di accedere agevolmente ad aree del sito istituzionale nelle quali possono essere riportate anche eventuali ulteriori informazioni rese disponibili ai soli aventi diritto sulla base della normativa in materia di accesso ai documenti amministrativi (elaborati, verbali, valutazioni, documentazione relativa a titoli anche di precedenza o preferenza, pubblicazioni, *curricula*, ecc.).

Devono ritenersi certamente pertinenti ai fini della pubblicazione *on line* gli elenchi nominativi ai quali vengano abbinati i risultati di prove intermedie, gli elenchi di ammessi a prove scritte o orali, i punteggi riferiti a singoli argomenti di esame, i punteggi totali ottenuti. Appare invece eccedente la pubblicazione di dati concernenti il recapito di telefonia fissa o mobile, l'indirizzo dell'abitazione o dell'e-mail, i titoli di studio, il codice fiscale, l'indicatore Isee, il numero di figli disabili, i risultati di test psicoattitudinali.

B. 2. Graduatorie, elenchi professionali ed altri atti riguardanti il personale

Analoghe cautele devono essere adottate in relazione alle pubblicazioni effettuate nel quadro delle ordinarie attività di gestione di rapporti di lavoro (es., graduatorie di mobilità professionale; provvedimenti relativi all'inquadramento del personale, all'assegnazione di sede, alla progressione di carriera, all'attribuzione di incarichi dirigenziali).

C. CONSULTABILITA' DI ATTI E DOCUMENTI

Per *Consultabilità* si intende la disponibilità sui siti istituzionali delle amministrazioni di atti e documenti amministrativi per finalità di consultabilità è volta a consentire la messa a disposizione degli stessi solo a soggetti determinati -anche per categorie- al fine di garantire in maniera agevole la partecipazione alle attività e ai procedimenti amministrativi.

Specifiche disposizioni normative richiedono ai soggetti pubblici di mettere a disposizione atti e documenti amministrativi a persone legittimate o che ne facciano richiesta al fine di consentire la partecipazione dei consociati all'attività amministrativa o nell'ambito dell'erogazione di servizi. Per attuare tali esigenze sottese alle previste ipotesi di consultabilità di atti e documenti su iniziativa di singoli soggetti, le amministrazioni possono parimenti avvalersi delle tecnologie telematiche, il cui utilizzo generalizzato è anche in tali casi espressamente incentivato dal legislatore allo scopo di facilitare il rapporto con i consociati e incentivare l'utilizzo dei servizi pubblici in rete.

In queste ipotesi, risultando determinabili *a priori* i soggetti o le categorie di soggetti legittimati a conoscere le informazioni detenute dalle pubbliche amministrazioni (es. destinatari del provvedimento, terzi interessati e contro interessati, ecc.), non è in linea di principio giustificato, alla luce del principio di proporzionalità consentire, al di fuori dei casi espressamente previsti, l'accesso *on line* libero e incondizionato, senza applicare criteri selettivi, alla consultazione di atti e documenti contenenti informazioni personali, specie se aventi natura sensibile.

In tale quadro occorre, quindi, privilegiare modalità di accessi dedicati ai soli aventi diritto (che ne abbiano fatto specifica richiesta) selezionando, a tal fine, anche preliminarmente, nell'ambito dei singoli atti e documenti, le sole informazioni da rendere consultabili.

Si ritiene utile evidenziare che le informazioni ritenute non pertinenti o eccedenti ai fini della loro pubblicazione *on line*, ivi comprese quelle idonee a rivelare lo stato di salute, possono naturalmente essere trattate dall'amministrazione competente per lo svolgimento dei propri compiti istituzionali ed essere oggetto di richieste di accesso da parte degli aventi diritto (es. ex l. n. 241 del 1990).

In tale prospettiva si ritiene che le informazioni personali contenute in atti e documenti da rendere consultabili possano essere, ad esempio, reperibili a partire da una sezione del sito istituzionale dell'amministrazione ad accesso selezionato (ad es. Intranet o Extranet) o attraverso l'attribuzione alle persone legittimate di una chiave personale di identificazione informatica secondo le regole stabilite in materia dal Codice dell'amministrazione digitale nel caso in cui l'accessibilità ai dati e documenti venga assicurata nell'ambito di servizi erogati in rete dall'amministrazione.(20)

C. 1. Elenchi del collocamento obbligatorio dei disabili

Il trattamento dei dati riferito alle persone disabili da parte di soggetti pubblici effettuato nell'ambito delle attività previste dalla disciplina sul collocamento mirato può ritenersi, in termini generali, lecito anche in quanto rispondente alle finalità di rilevante interesse pubblico individuate dal Codice (artt. 73, comma 2, lett. i) e 112, comma 1, lett. a)).

In tale quadro, le disposizioni di legge in materia di diritto al lavoro e di collocamento di disabili appartenenti a categorie protette e centralinisti telefonici non vedenti, nel prevedere la formazione di elenchi e graduatorie dei soggetti che hanno diritto al collocamento obbligatorio, ne stabiliscono un generico regime di pubblicità.

Il regime di conoscibilità di tali documenti, stabilito per legge, può essere assicurato anche attraverso la loro messa a disposizione *on line*, purché vengano prescelte modalità che ne impediscano la libera consultabilità in Internet, tenuto conto che gli elenchi e le graduatorie del collocamento obbligatorio contengono informazioni idonee a rivelare lo stato di salute delle persone iscritte (nominativi degli interessati associati allo stato di disabilità o all'appartenenza alle altre categorie di aventi diritto al collocamento).

Nell'utilizzare le tecnologie telematiche per attuare il previsto regime di pubblicità delle predette liste, le amministrazioni devono, pertanto, adottare idonei accorgimenti volti a impedire che vengano diffusi dati sulla salute (artt. 22, comma 8 e 68, comma 3, del Codice), rendendo conoscibili le informazioni riportate in tali elenchi ai soli soggetti richiedenti per le sole finalità previste dalla specifica normativa di riferimento o a coloro che vi abbiano interesse per la tutela di situazioni giuridicamente rilevanti (es. attribuendo a tali soggetti idonee credenziali di accesso, quali *username* o *password*, n. di protocollo o altri estremi correlati alla richiesta di iscrizione nelle liste, ovvero ancora predisponendo, nei siti istituzionali, aree ad accesso parimenti selezionato).

3.8.3.3.3 Gli accorgimenti tecnici in relazione alle finalità perseguite

A fronte della messa a disposizione *on line* di atti e documenti amministrativi contenenti dati personali, occorre individuare idonei accorgimenti volti ad assicurare forme corrette e proporzionate di conoscibilità di tali informazioni impedendo la loro indiscriminata e incondizionata reperibilità in Internet, garantendo il rispetto dei principi di qualità ed esattezza dei dati e delimitando la durata della loro disponibilità on line.

Va tenuto presente, inoltre che la diffusione indiscriminata di dati personali basata su un malinteso e dilatato principio di trasparenza può determinare conseguenze gravi e pregiudizievoli tanto della dignità delle persone quanto della stessa convivenza sociale. Pericoli questi che si dilatano ulteriormente quando la diffusione dei dati e la loro messa a disposizione avvenga *on line*.

Infatti, questo metodo di diffusione presenta pericoli e criticità specifiche che vanno dalla difficoltà di garantire che i dati siano a disposizione solo per un periodo determinato dalla normativa di settore (nei casi in cui tali norme prevedano un termine), sia che i dati siano conosciuti solo da chi abbia diritto a conoscerli (nei casi in cui il diritto non è esteso a tutti ma solo a certe categorie di cittadini) sia, infine, che i dati non possano essere manipolati o indebitamente acquisiti e archiviati da chi dovrebbe al massimo limitarsi a prenderne conoscenza (come avviene nel caso in cui non siano adottate adeguate misure di sicurezza).

Infine, deve sempre essere tenuto presente il pericolo oggettivo costituito dai motori di ricerca che "decontestualizzano il dato" estrapolandolo dal sito in cui è contenuto, e trasformandolo in una parte, non controllata e non controllabile, delle informazioni che di una persona sono date dal motore di ricerca stesso, secondo una "logica" di priorità di importanza del tutto sconosciuta e non conoscibile all'utente.

Motori di ricerca

E' necessario stabilire se i dati siano reperibili mediante motori di ricerca esterni ovvero – come appare preferibile – interni al sito. La seconda soluzione va infatti privilegiata, in linea generale, in quanto assicura accessi maggiormente selettivi e coerenti con le finalità di volta in volta sottese alla pubblicazione assicurando, nel contempo, la conoscibilità sui siti istituzionali delle informazioni che si intende mettere a disposizione.

Si pensi al caso della pubblicazione delle informazioni e di dati nell'apposita sezione del sito istituzionale dell'amministrazione denominata *"Trasparenza, valutazione e merito"* di cui si prevede, per facilitarne l'accesso e la consultazione, la raggiungibilità da un *link* posto nell'*home page* del sito stesso [D. Lgs. N. 150/09].

A tale scopo, in relazione ai dati personali di cui si intende escludere la diretta individuabilità in Internet tramite motori di ricerca generalisti, è possibile utilizzare regole di accesso convenzionali codificate all'interno di uno specifico file di testo (quali i *metatag noindex* e *noarchive* e il *file robots.txt*, quest'ultimo opportunamente configurato secondo le regole del *Robot Exclusion Protocol*).

Resta impregiudicato l'utilizzo di strumenti idonei ad agevolare la reperibilità, all'interno del sito istituzionale dell'amministrazione, delle informazioni e dei documenti oggetto di divulgazione.

Tempi proporzionati di mantenimento della diffusione dei dati

Le esigenze di trasparenza, pubblicità e consultabilità degli atti, proprio in relazione alla circostanza che i dati personali in essi contenuti sono diffusi sul *web*, devono comunque tenere anche conto dell'obbligo di individuare un congruo periodo di tempo entro il quale devono rimanere disponibili (in una forma che consenta l'identificazione dell'interessato) che non può essere superiore al periodo ritenuto, caso per caso, necessario al raggiungimento degli scopi per i quali i dati stessi sono resi pubblici.

Come detto, la diffusione illimitata e continua in Internet di dati personali relativi ad una pluralità di situazioni riferite ad un medesimo interessato, costantemente consultabili da molteplici luoghi e in qualsiasi momento, può comportare conseguenze pregiudizievoli per le persone interessate, specie se si tratta di informazioni non più aggiornate o relative ad avvenimenti risalenti nel tempo contenute anche in atti e provvedimenti amministrativi reperibili *on line* che hanno già raggiunto gli scopi per i quali si era reso necessario renderli pubblici.

In tale quadro, nelle ipotesi in cui specifiche disposizioni di settore individuino determinati periodi di tempo per la pubblicazione di atti e documenti, i soggetti pubblici sono tenuti ad assicurare il rispetto dei limiti temporali previsti, rendendoli accessibili sul proprio sito *web* solo durante il circoscritto ambito temporale individuato dalle disposizioni normative di riferimento (es., art. 124, d.lg. n. 267/2000 riguardante le deliberazioni del comune e della provincia che devono essere affisse all'albo pretorio, nella sede dell'ente, per quindici giorni consecutivi).

Nei casi in cui, invece, la disciplina di settore non stabilisce un limite temporale alla pubblicazione degli atti, vanno individuati – a cura delle amministrazioni interessate- congrui periodi di tempo entro i quali mantenerli on line.

La predetta congruità va commisurata alle esigenze sottese alle finalità di trasparenza, di pubblicità o di consultabilità di volta in volta perseguite. Più in particolare, in relazione alla finalità di trasparenza potrebbe risultare necessario individuare dei tempi ragionevoli di permanenza dei dati in rete, proprio al fine di garantire a chiunque una effettiva e immediata accessibilità alle informazioni.

Tempi più circoscritti, invece, devono riguardare la disponibilità on line dell'atto o del documento pubblicato per finalità di pubblicità, avuto anche riguardo ai termini previsti dalla legge per l'impugnazione dei provvedimenti oggetto di pubblicazione.

Trascorsi i predetti periodi di tempo specificatamente individuati, determinati documenti o sezioni del sito devono essere rimossi dal *web* ovvero, in alternativa, devono essere inseriti in un'area di archivio consultabile solo a partire dal sito stesso e non raggiungibili utilizzando i motori di ricerca esterni.

A questo scopo, è possibile utilizzare sistemi di *web publishing* e *Cms* (*Content management systems*) in grado di attribuire, anche mediante l'utilizzo di parole-chiave (meta-dati) (Vedasi anche le Linee guida per i siti web della PA del Ministro per la pubblica amministrazione e l'innovazione), un intervallo temporale di permanenza della documentazione all'interno del sito istituzionale, consentendone una sua agevole rimozione, anche in forma automatica.

In assenza di meccanismi automatizzati di gestione del termine di scadenza della medesima documentazione, andrebbero inoltre previste procedure di verifica della validità temporale e del requisito di disponibilità al pubblico delle informazioni ivi contenute, da programmare con cadenza periodica o in seguito ad un aggiornamento dell'informazione.

Duplicazione massiva dei file contenenti dati personali

Devono essere adottate opportune cautele per evitare operazioni di duplicazione massiva dei *file* contenenti dati personali, rinvenibili dagli utenti sui siti istituzionali delle amministrazioni, mediante l'utilizzo di software o programmi automatici, al fine di ridurre il rischio di riproduzione e riutilizzo dei contenuti informativi in ambiti e contesti differenti. A tale scopo si può fare ricorso a specifici accorgimenti consistenti, ad esempio, nell'utilizzo di *firewall* di rete in grado di riconoscere accessi che risultino anomali per numero rapportato all'intervallo di tempo di riferimento oppure di opportuni filtri applicativi che, a fronte delle citate anomalie, siano in grado di rallentare l'attività dell'utente e di mettere in atto adeguate contromisure. Gli accorgimenti che si intende utilizzare devono comunque essere conformi ai principi di fruibilità, di usabilità e di accessibilità dei siti istituzionali delle pubbliche amministrazioni, garantendo in particolare l'accessibilità alle informazioni riprodotte *on line* anche alle persone disabili nel rispetto delle disposizioni della l. 9 gennaio 2004, n. 4.

Dati esatti e aggiornati

Per garantire la qualità dei dati trattati, le amministrazioni pubbliche, nel procedere nei casi previsti alla divulgazione *on line* di informazioni personali, sono tenute a mettere a disposizione soltanto dati esatti, aggiornati e attendibili (art. 11, comma 1, lett. c), del Codice). In tale quadro, assume particolare rilievo l'obbligo posto in capo alle amministrazioni pubbliche di garantire *"che le informazioni contenute sui siti siano conformi e corrispondenti alle informazioni contenute nei provvedimenti amministrativi originali dei quali si fornisce comunicazione tramite il sito"* (art. 54, comma 4, d.lg. n. 82/2005, Codice dell'amministrazione digitale).

A tale fine occorre adottare idonee misure per eliminare o ridurre il rischio di cancellazioni, modifiche, alterazioni o decontestualizzazioni delle informazioni e dei documenti resi disponibili tramite Internet. Un utile accorgimento consiste, ad esempio, nell'indicazione, tra i dati di contesto riportati all'interno del contenuto informativo dei documenti, delle fonti attendibili per il reperimento dei medesimi documenti.

Un ulteriore accorgimento la cui adozione potrà essere valutata dalle amministrazioni interessate, anche in relazione a specifiche categorie di documenti, è l'utilizzo di certificati e firma digitale, in modo da assegnare una data asseverabile di creazione del documento che può essere validata con certezza e che consente, a chi faccia uso di quel documento, di verificarne l'attendibilità in qualsiasi momento.

Il rischio della decontestualizzazione è strettamente correlato alla possibilità che i contenuti informativi disponibili sul sito istituzionale siano accessibili mediante l'utilizzo di motori di ricerca esterni ovvero siano reperibili attraverso la consultazione di siti dove sono ospitate copie dei medesimi contenuti informativi.

Pertanto ogni file oggetto di pubblicazione sui siti istituzionali, potendo essere letto in un altro ambito e in un momento successivo alla sua diffusione, dovrebbe prevedere l'inserimento dei "dati di contesto" (es. data di aggiornamento, periodo di validità, amministrazione).

3.8.4 Cartellini identificativi / badges

Ad ogni dipendente è fornito un badge e/o un tesserino di riconoscimento contenente la foto, il nome e/o cognome del dipendente, eventualmente la matricola, il logo e/o il nome dell'Ente di appartenenza e i dati identificativi dell'Ente stesso e/o del settore specifico.

Il badge serve alla timbratura della presenza al lavoro. Tuttavia, in relazione al rapporto con l'utenza, nel cartellino identificativo è sempre meglio riportare il numero e l'entità di informazioni ritenute utili, per quanto pratico e ragionevole, affinché da sole siano in grado di essere d'ausilio all'identificazione univoca per l'utenza.

I lavoratori, in virtù di ciò, sono quindi tenuti ad esporre tale tessera di riconoscimento (ad esempio sull'abito o divisa fornita dall'Ente), ad averne cura e a non scambiarla con nessuno per alcun motivo.

Qualora un badge venisse smarrito, oltre a riportare l'accadimento nel documento aziendale apposito, è tenuto a comunicarlo al responsabile del proprio settore di appartenenza.

Le informazioni necessarie per l'attribuzione del badge, per la predisposizione dello stesso (con la relativa immissione dei dati consoni) sono gestite dal Titolare e/o dall'Amministratore di Sistema e/o da loro incaricato.

Le informazioni inerenti la gestione delle presenze, della busta paga e quanto ad esse connesso, sono gestite dal settore Risorse Umane.

3.8.5 Modalità di comunicazione dei dati personali dei dipendenti e/o degli utenti

Salvi i casi in cui forme e modalità di divulgazione di dati personali discendano da specifiche previsioni, il datore di lavoro deve utilizzare forme di comunicazione individualizzata con il lavoratore, adottando le misure più opportune per prevenire un'indebita comunicazione di dati personali, in particolare se sensibili, a soggetti diversi dal destinatario, ancorché incaricati di talune operazioni di trattamento (ad esempio, inoltrando le comunicazioni in plico chiuso o spillato; invitando l'interessato a ritirare personalmente la documentazione presso l'ufficio competente; ricorrendo a comunicazioni telematiche individuali).

Analoghe cautele, tenendo conto delle circostanze di fatto, devono essere adottate in relazione ad altre forme di comunicazione indirizzate al lavoratore dalle quali possano desumersi vicende personali.

I principi generali che presiedono le modalità di comunicazione dei dati personali degli utenti sono correlate alla tipologia di dati trattati secondo le norme di legge e/o regolamenti.

3.9 Esercizio dei diritti previsti dall'art. 7 del Codice e riscontro del Titolare / Datore di lavoro

3.9.1 Diritto di accesso a tutela della riservatezza

Fin dalla sua emanazione la normativa a tutela della riservatezza ha posto la necessità di ricercare una soluzione in grado di contemperare due valori altrettanto meritevoli di protezione giuridica: la salvaguardia del principio di trasparenza ed imparzialità dell'azione amministrativa, da un lato, ed il diritto alla riservatezza proprio di ciascun soggetto singolo o collettivo, dall'altro.

3.9.1.1 Diritto di accesso da parte dei lavoratori

I lavoratori interessati possono esercitare nei confronti del datore di lavoro i diritti previsti dall'art. 7 del Codice (nei modi di cui agli artt. 8 e ss.), tra cui il diritto di accedere ai dati che li riguardano (anziché, in quanto tale, all'intera documentazione che li contiene), di ottenerne l'aggiornamento, la rettificazione, l'integrazione, la cancellazione, la trasformazione in forma anonima o il blocco se trattati in violazione di legge, di opporsi al trattamento per motivi legittimi.

La richiesta di accesso che non faccia riferimento ad un particolare trattamento o a specifici dati o categorie di dati, deve ritenersi riferita a tutti i dati personali che riguardano il lavoratore comunque trattati dall'amministrazione e può riguardare anche informazioni di tipo valutativo, alle condizioni e nei limiti di cui all'art. 8, comma 5.

Tra essi non rientrano notizie di carattere contrattuale o professionale che non hanno natura di dati personali in qualche modo riferibili a persone identificate o identificabili.

3.9.1.2 L'accesso ai documenti contenenti dati personali comuni da parte dell'utenza

L'Accesso a documenti amministrativi è connesso alla Legge 241/1990 e s.m.i., quale criterio guida per stabilire "i presupposti, le modalità, i limiti dell'esercizio del diritto di accesso ai documenti amministrativi contenenti dati personali, e la relativa tutela giurisdizionale", esplicitando così la piena vigenza delle norme sulla trasparenza amministrativa.

Da parte sua, la Legge 241/1990 e s.m.i., individua, quale titolare del diritto d'accesso, "chiunque vi abbia interesse per la tutela di situazioni giuridicamente rilevanti". In tal caso la qualità delle informazioni racchiuse nel documento amministrativo, vale a dire le informazioni relative a terzi, si pone come un limite "facoltativo" o "eventuale", in quanto l'accesso viene deciso a discrezione della pubblica amministrazione.

Per converso, qualora vengano in rilievo i documenti coperti da segreto di Stato e quelli contenenti dati relativi alla sicurezza e difesa nazionale, alla politica monetaria, valutaria e d'ordine pubblico, alla prevenzione e repressione della criminalità, si configurano invece come limiti "assoluti" o "tassativi", sanciti in modo vincolante dalla legge e comportanti l'esclusione del diritto di accesso.

Viene riconosciuta una limitata prevalenza del diritto di accesso sulla riservatezza a condizione che, da un lato, la richiesta di ostensione degli atti sia finalizzata alla cura e alla difesa degli interessi giuridici del richiedente e, dall'altro, che sia circoscritta alla sola visione dei documenti.

Tali principi sono stati delineati con maggiore dovizia di particolari dal regolamento di attuazione successivamente emanato, richiedente inoltre che l'interesse sotteso alla richiesta presenti le caratteristiche della "personalità" e della "concretezza", ovvero da una parte esige la verifica di un nesso di causalità con il soggetto agente, dall'altra l'effettività e non la mera potenzialità dell'interesse.

Il bilanciamento tra il diritto di accesso degli interessati ed il diritto alla riservatezza dei terzi non è stato totalmente rimesso alla potestà regolamentare od alla discrezione delle singole amministrazioni, ma è stato compiuto direttamente dal legislatore, in quanto "l'interesse alla riservatezza tutelato dalla normativa mediante una limitazione del diritto di accesso, recede quando l'accesso stesso sia esercitato per la difesa di un interesse giuridico, nei limiti ovviamente in cui esso è necessario alla difesa di quell'interesse", venendo così ad attribuire alla privacy "il riduttivo ruolo di fattore delimitativo, sotto il profilo delle modalità tecniche di esercizio, ma non preclusivo dell'esercizio dell'accesso".

Come confermato anche dalla successiva giurisprudenza amministrativa, a fronte di una richiesta di ostensione di documenti amministrativi contenenti dati personali di terzi, l'amministrazione interpellata potrà unicamente consentire la visione, non estrapolazione di copia, dei soli documenti strettamente necessari per la difesa dell'interesse giuridico del richiedente. L'amministrazione, quindi, è chiamata a valutare attentamente i presupposti per consentire legittimamente alla richiesta: dovrà quindi verificare che il richiedente vanti un "interesse giuridico" cioè una posizione giuridica soggettiva tutelata dall'ordinamento su cui il provvedimento finale, al quale ineriscono i documenti richiesti, è in grado di incidere.

La normativa sulla riservatezza non ha abrogato la disciplina sul diritto di accesso, ma ha inteso unicamente prevedere determinate garanzie nel coinvolgimento di terzi.

3.9.1.3 L'accesso ai documenti contenenti dati personali sensibili e/o giudiziari da parte dell'utenza

Il legislatore ha mantenuto inalterata l'impostazione fondata su "un sistema a doppio binario" a seconda del tipo di dati oggetto di trattamento, fissando una gradazione nella tutela della riservatezza, che parte da un livello minimo per i dati cosiddetti comuni fino ad arrivare ad una soglia di intangibilità pressoché assoluta, se non a determinate rigide

condizioni, che è posta a tutela dei dati cosiddetti sensibili, vale a dire le informazioni idonee a rivelare lo stato di salute o la vita sessuale dell'interessato.

Tale caratteristica fondamentale si riflette anche nella disposizione sul diritto di accesso: il Codice stabilisce che le disposizioni di cui alla legge n. 241/1990 e s.m.i. si applicano "anche per ciò che concerne i tipi di dati sensibili e giudiziari e le operazioni di trattamento eseguibili in esecuzione di una richiesta di accesso", statuendo che le attività finalizzate all'applicazione di tale disciplina si considerano di rilevante interesse pubblico.

Il legislatore ha quindi confermato le posizioni emerse in giurisprudenza: sostanzialmente l'accesso ai documenti amministrativi contenenti dati sensibili non si discosta, enne sue concrete modalità operative, da quanto previsto, con riferimento agli atti contenenti dati comuni, dovendo concedersi l'accesso nei limiti previsti dalle leggi e dalle disposizioni regolamentari in materia.

Anche in tal caso, quindi, potrà essere ammessa solo la visione, ma non l'estrazione di copia ovvero la trascrizione della documentazione richiesta.

La natura sensibile del dato personale costituisce dunque un limite invalicabile anche per la pubblica amministrazione, che può concedere il diritto di accesso unicamente alle condizioni di stretta interpretazione fissate dal Codice.

Esso prevede esplicitamente un'eccezione alla sua piena applicabilità, stabilendo che il trattamento dei dati in questione è consentito unicamente nell'ipotesi in cui "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 o libertà fondamentale e inviolabile.

3.9.2 Riscontro del Titolare/Datore di lavoro

Il Titolare/Datore di lavoro destinatario della richiesta è tenuto a fornire un riscontro completo alla richiesta del lavoratore interessato, senza limitarsi alla sola elencazione delle tipologie di dati detenuti, ma comunicando in modo chiaro e intelligibile tutte le informazioni in suo possesso.

3.9.3 Tempestività del riscontro

Il riscontro deve essere fornito nel termine di 15 giorni dal ricevimento dell'istanza dell'interessato (ritualmente presentata); il termine più lungo, pari a 30 giorni, può essere osservato, dandone comunicazione all'interessato, solo se le operazioni necessarie per un integrale riscontro sono di particolare complessità o se ricorre altro giustificato motivo.

Pertanto il datore di lavoro, specie nelle realtà produttive di grande dimensione, deve pertanto predisporre procedure organizzative adeguate per dare piena attuazione alle disposizioni del Codice in materia di accesso ai dati e all'esercizio degli altri diritti, anche attraverso l'impiego di appositi programmi finalizzati ad una accurata selezione dei dati relativi a singoli lavoratori, nonché alla semplificazione delle modalità e alla compressione dei tempi per il riscontro.

3.9.4 Modalità del riscontro

Il riscontro può essere fornito anche oralmente; tuttavia, in presenza di una specifica istanza, il datore di lavoro è tenuto a trasporre i dati su supporto cartaceo o informatico o a trasmetterli all'interessato per via telematica.

Muovendo dalla previsione dell'art. 10, comma 1, del Codice, secondo cui il titolare deve predisporre accorgimenti idonei "a semplificare le modalità e a ridurre i tempi per il riscontro al richiedente", può risultare legittima la richiesta dell'interessato di ricevere la comunicazione dei dati in questione presso la propria sede lavorativa o la propria abitazione.

3.9.5 Dati personali e documentazione

Come più volte dichiarato dal Garante, l'esercizio del diritto di accesso consente di ottenere, ai sensi dell'art. 10 del Codice, solo la comunicazione dei dati personali relativi al richiedente detenuti dal titolare del trattamento e da estrarre da atti e documenti; non permette invece di richiedere a quest'ultimo il diretto e illimitato accesso a documenti e ad intere tipologie di atti, o la creazione di documenti allo stato inesistenti negli archivi, o la loro innovativa aggregazione secondo specifiche modalità prospettate dall'interessato o, ancora, di ottenere, sempre e necessariamente, copia dei documenti detenuti, ovvero di pretendere particolari modalità di riscontro.

Specie nei casi in cui è elevata la mole di informazioni personali detenute dal titolare del trattamento, il diritto di accesso ai dati può essere soddisfatto mettendo a disposizione dell'interessato il fascicolo personale, dal quale successivamente possono essere estratte le informazioni personali.

La scelta circa l'eventuale esibizione o consegna in copia di atti e documenti contenenti i dati personali richiesti può essere effettuata dal titolare del trattamento nel solo caso in cui l'estrapolazione dei dati personali da tali documenti risulti particolarmente difficoltosa per il titolare medesimo; devono essere poi omessi eventuali dati personali riferiti a terzi. L'adozione di tale modalità di riscontro non comporta l'obbligo in capo al titolare di fornire copia di tutti i documenti che contengano i medesimi dati personali dell'interessato, quando gli stessi dati siano conservati in più atti, lettere o note.

Nel fornire riscontro ad una richiesta di accesso formulata ai sensi degli artt. 7 e 8 del Codice, il titolare del trattamento deve, poi, comunicare i dati richiesti ed effettivamente detenuti, e non è tenuto a ricercare o raccogliere altri dati che non siano nella propria disponibilità e non siano oggetto, in alcuna forma, di attuale trattamento da parte dello stesso (o perché originariamente trattati e non più disponibili, ovvero perché, come nel caso di dati contenuti nella corrispondenza intercorsa, in qualunque forma, tra dipendenti di un determinato datore di lavoro, non siano mai stati nell'effettiva e libera disponibilità di quest'ultimo (si pensi al caso di dati contenuti nella corrispondenza intercorsa tra dipendenti) – al di là dei profili di tutela della segretezza della corrispondenza che pur vengono in rilievo–, non competerebbero le decisioni in ordine alle loro finalità e modalità di trattamento.

3.9.6 Aggiornamento

Infine, l'utente e/o il lavoratore può ottenere l'aggiornamento dei dati personali a sé riferiti.

In ordine, poi, all'eventuale richiesta di rettifica dei dati personali indicati nel profilo professionale del lavoratore, la medesima può avvenire solo in presenza della prova dell'effettiva e legittima attribuibilità delle qualifiche rivendicate dall'interessato, ad esempio in base a "decisioni o documenti del datore di lavoro o di terzi, obblighi derivanti dal contratto di lavoro, provvedimenti di organi giurisdizionali relativi all'interessato o altri titoli o atti che

permettano di ritenere provata, agli effetti e sul piano dell'applicazione della [disciplina di protezione dei dati personali], la richiesta dell'interessato" (che può comunque far valere in altra sede, sulla base di idoneo materiale probatorio, la propria pretesa al riconoscimento della qualifica o mansione rivendicata).

4. DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITÀ

4.1. Titolare del trattamento

Il Decreto Legislativo n. 196 del 30.06.2003 indica come "titolare", *la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza*.

Nel caso in cui il trattamento è effettuato da una pubblica amministrazione, titolare del trattamento è l'entità nel suo complesso ovvero l'unità o l'organismo periferico che esercita un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento.

È onere del Titolare del trattamento individuare, nominare e incaricare per iscritto uno o più Responsabili del trattamento dei dati, che assicurino e garantiscano che vengano adottate le misure di sicurezza ai sensi degli artt. 31-36 del D.Lgs. n. 196/2003.

Il Titolare del trattamento affida al Responsabile del trattamento dei dati il compito di adottare le misure tese a ridurre al minimo il rischio di distribuzione dei dati, l'accesso non autorizzato o il trattamento non consentito, previe idonee istruzioni fornite per iscritto.

Tra i compiti che la Legge assegna al Titolare e che non sono delegabili, è prevista la vigilanza sul rispetto da parte dei Responsabili (qualora designati) delle proprie istruzioni, nonché sulla puntuale osservanza delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

L'Ente ha quindi le seguenti responsabilità:

- proporre le procedure per la sicurezza del dati e ne verifica le necessita di aggiornamento;
- amministrare la sicurezza informatica dell'intero sistema;
- effettuare periodici controlli e verifiche in merito al rispetto delle prescrizioni contenute nel presente Documento Programmatico sulla Sicurezza;
- valutare periodicamente il livello di rischio di sicurezza dei dati.

4.2 Il Responsabile del trattamento

Il Decreto Legislativo n. 196 del 30.06.2003 indica come "responsabile", *la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali*.

In relazione all'attività del Titolare del trattamento, è prevista la possibilità di nomina di uno o più Responsabili del trattamento, con compiti diversi a seconda delle funzioni svolte.

Il Titolare del trattamento affida ai singoli Responsabili del trattamento (qualora designati) l'onere di individuare, nominare ed incaricare per iscritto uno o più incaricati del trattamento.

Il Responsabile del trattamento dei dati ha il compito di:

- redigere ed aggiornare, ad ogni variazione, l'elenco dei sistemi di elaborazione connessi in rete pubblica, nonché l'elenco delle tipologie dei trattamenti effettuati;

- attribuire, con l'ausilio degli Amministratori di sistema, ad ogni Utente (USER) o incaricato un codice identificativo personale (USER-ID) per l'utilizzazione dell'elaboratore, che deve essere individuale e non riutilizzabile;
- autorizzare i singoli incaricati del trattamento e della manutenzione, nel caso di trattamento di dati sensibili ed eventualmente giudiziari, qualora si utilizzino elaboratori accessibili in rete; per gli stessi dati, qualora il trattamento sia effettuato tramite elaboratori accessibili in rete disponibili al pubblico, saranno oggetto di autorizzazione anche gli strumenti da utilizzare;
- verificare, con l'ausilio degli amministratori di sistema, con cadenza almeno semestrale, l'efficacia dei programmi di protezione ed antivirus, nonché definire eventuali modalità di accesso ai locali e/o misure indicate nei successivi capitoli;
- garantire che tutte le misure di sicurezza riguardanti i dati in possesso dell'Ente siano applicate solo all'interno della stessa ed eventualmente al di fuori della stessa, qualora siano cedute a soggetti terzi quali Responsabili del trattamento tutte o parte delle attività di trattamento;
- informare il titolare nella eventualità che siano rilevati dei rischi e/o delle non rispondenze alle norme di sicurezza e di eventuali incidenti;
- promuovere lo svolgimento di un continuo programma di addestramento degli Incaricati del Trattamento e mantenere attivo un programma di controllo e monitoraggio della corrispondenza con le regole di sicurezza;
- promuovere e garantire l'esecuzione di un eventuale programma di audit.

4.2.1 Nomina del Responsabile del trattamento dei dati

Il Titolare del trattamento dei dati deve informare ciascun Responsabile del trattamento dei dati, così come individuato nel Regolamento, delle responsabilità che gli sono affidate in relazione a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dal D. Lgs. n. 196/2003.

A ciascun Responsabile del trattamento il Titolare del trattamento deve impartire adeguata formazione sulle norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina.

La nomina del Responsabile del trattamento deve essere riportata per iscritto con eventuale delibera e/o con atto scritto da parte dell'Ente, è a tempo indeterminato, decade per revoca o dimissioni dello stesso e può essere revocata in qualsiasi momento dal Titolare del trattamento dei dati senza preavviso, ed eventualmente affidata ad altro soggetto.

Si tenga presente, altresì, che il legislatore ha provveduto a definire con maggiore compiutezza anche la figura del "responsabile": nessun trattamento di dati personali può essere svolto all'interno di una struttura complessa da chi non abbia ricevuto una specifica designazione in tal senso, in mancanza della quale la conoscenza dei dati da parte degli addetti ai lavori si configura come una comunicazione esterna ed in quanto tale assoggettata alle norme più stringenti previste per tale operazione.

4.3 Amministratore di sistema

Con la definizione di "amministratore di sistema" si individua generalmente, in ambito informatico, la figura professionale finalizzata alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti.

Ai fini del provvedimento del Garante “Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema del 27 novembre 2008”, vengono però considerate tali anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi.

Gli amministratori di sistema così ampiamente individuati, pur non essendo preposti ordinariamente a operazioni che implicano una comprensione del dominio applicativo (significato dei dati, formato delle rappresentazioni e semantica delle funzioni), nelle loro consuete attività sono, in molti casi, concretamente "responsabili" di specifiche fasi lavorative che possono comportare elevate criticità rispetto alla protezione dei dati.

Attività tecniche quali il salvataggio dei dati (backup/recovery), l'organizzazione dei flussi di rete, la gestione dei supporti di memorizzazione e la manutenzione hardware comportano infatti, in molti casi, un'effettiva capacità di azione su informazioni che va considerata a tutti gli effetti alla stregua di un trattamento di dati personali; ciò, anche quando l'amministratore non consulti "in chiaro" le informazioni medesime.

Lo svolgimento delle mansioni di un amministratore di sistema, anche a seguito di una sua formale designazione quale responsabile o incaricato del trattamento, comporta di regola la concreta capacità, per atto intenzionale, ma anche per caso fortuito, di accedere in modo privilegiato a risorse del sistema informativo e a dati personali cui non si è legittimati ad accedere rispetto ai profili di autorizzazione attribuiti.

L'individuazione dei soggetti idonei a svolgere le mansioni di amministratore di sistema riveste una notevole importanza, costituendo una delle scelte fondamentali che, unitamente a quelle relative alle tecnologie, contribuiscono a incrementare la complessiva sicurezza dei trattamenti svolti, e va perciò curata in modo particolare evitando incauti affidamenti.

La rilevanza, la specificità e la particolare criticità del ruolo dell'amministratore di sistema sono state considerate anche dal legislatore il quale ha individuato, con diversa denominazione, particolari funzioni tecniche che, se svolte da chi commette un determinato reato, integrano ad esempio una circostanza aggravante. Ci si riferisce, in particolare, all'abuso della qualità di operatore di sistema prevista dal codice penale per le fattispecie di accesso abusivo a sistema informatico o telematico (art. 615 ter) e di frode informatica (art. 640 ter), nonché per le fattispecie di danneggiamento di informazioni, dati e programmi informatici (artt. 635 bis e ter) e di danneggiamento di sistemi informatici e telematici (artt. 635 quater e quinques) di recente modifica (ad es., l'art. 5 l. 18 marzo 2008, n. 48 che prevede, oltre a una maggiore pena, la procedibilità d'ufficio nel caso in cui il reato sia commesso con "abuso della qualità di operatore del sistema").

Ai sensi dell’art. 154, comma 1, lett. h) del Codice il Garante, nel segnalare al Titolare del Trattamento soggetto all'ambito applicativo del Codice ed effettuato con strumenti elettronici la particolare criticità del ruolo degli amministratori di sistema, richiama l'attenzione del medesimo titolare sulla necessità di adottare idonee cautele volte a prevenire e ad accertare eventuali accessi non consentiti ai dati personali, in specie quelli realizzati con abuso della qualità di amministratore di sistema; richiama inoltre l'attenzione sull'esigenza di valutare con particolare cura

l'attribuzione di funzioni tecniche propriamente corrispondenti o assimilabili a quelle di amministratore di sistema (system administrator), amministratore di base di dati (database administrator) o amministratore di rete (network administrator), laddove queste siano esercitate in un contesto che renda ad essi tecnicamente possibile l'accesso, anche fortuito, a dati personali. Ciò, tenendo in considerazione l'opportunità o meno di tale attribuzione e le concrete modalità sulla base delle quali si svolge l'incarico, unitamente alle qualità tecniche, professionali e di condotta del soggetto individuato, da vagliare anche in considerazione delle responsabilità, specie di ordine penale e civile (artt. 15 e 169 del Codice), che possono derivare in caso di incauta o inidonea designazione.

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

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

È compito dell'Amministratore di sistema:

- Coadiuvare il Titolare nell'individuare, nominare e incaricare per iscritto un Custode delle passwords, qualora vi siano più incaricati del trattamento effettuato con mezzi informatici;
- Prendere tutti i provvedimenti necessari ad evitare la perdita o la distribuzione dei dati e provvedere al ricovero periodico degli stessi con copie di back-up;
- Assicurarsi della qualità delle copie di back-up dei dati e della loro conservazione in luogo adatto;
- Fare in modo che sia prevista la disattivazione dei codici identificativi personali (USER-ID), in caso di perdita della qualità che consentiva all'utente o incaricato l'accesso all'elaboratore, oppure nel caso di mancato utilizzo dei codici identificativi personali (USER-ID) per oltre 3/6 mesi a seconda della tipologia di dati;
- Proteggere gli elaboratori dal rischio di intrusione (violazione del sistema da parte di "hackers") e dal rischio di virus mediante idonei programmi.
- Svolgere materialmente le operazioni necessarie a garantire il funzionamento del sistema informatico, sotto la direzione del Responsabile del trattamento.
- Svolgere i compiti attribuiti dal Documento Programmatico sulla Sicurezza di propria competenza.
- informare il titolare nella eventualità che siano rilevati dei rischi e/o delle non rispondenze alle norme di sicurezza e di eventuali incidenti.

4.3.1 Nomina degli Amministratori di sistema

L'Amministratore di sistema, così come individuato nel Regolamento, sovrintende alle risorse del sistema operativo di un elaboratore o di un sistema di banche dati.

Il Titolare del trattamento dei dati e/o il Responsabile del trattamento può nominare ulteriori Amministratori di sistema, specificando gli elaboratori o le banche dati che è chiamato a sovrintendere, informandolo delle

responsabilità che gli sono state affidate in relazione a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dal D. Lgs. n. 196/2003.

La lettera d'incarico deve essere controfirmata dall'interessato per presa visione e copia della stessa deve essere conservata a cura del Titolare del trattamento dei dati in luogo apposito.

La designazione quale amministratore di sistema deve essere in ogni caso individuale e recare l'elencazione degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato e i dati trattati devono essere menzionati su carta intestata e/o su modulo apposito.

Gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni ad essi attribuite, devono essere riportati in apposito modulo e/o su carta intestata, e/o annotati comunque in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti anche da parte del Garante.

Agli Amministratori di sistema il Titolare del trattamento e/o il Responsabile del trattamento deve impartire adeguata formazione su quanto di competenza presente nel Documento Programmatico sulla Sicurezza e sulle norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina.

4.3.2 Registrazione degli accessi

Devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste.

Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi.

4.4 Custode delle passwords

Il Custode delle passwords è colui il quale ha il compito di gestire e custodire le passwords per l'accesso ai dati da parte degli incaricati.

Il Custode delle passwords deve disporre, per ogni incaricato del trattamento, una busta sulla quale è indicato lo USER-ID utilizzato: all'interno della busta deve essere indicata la password usata per accedere alla banca di dati.

Le buste con le passwords debbono essere conservate in luogo chiuso e protetto.

È altresì possibile che l'Ente identifichi eventuali metodiche alternative ritenute ugualmente valide affinchè le password siano reperibili in caso di bisogno ad opera ad esempio dell'Amministratore di Sistema, ma non vulnerabili all'utilizzo improprio delle stesse.

Il Custode delle passwords deve revocare tutte le passwords non utilizzate per un periodo superiore a 3/6 (tre/sei) mesi, a seconda della tipologia dei dati trattati.

Inoltre il Custode delle passwords deve:

- Attivare le nuove utenze e, contestualmente alla comunicazione di nome utente e password, deve coadiuvare il Responsabile del trattamento nella formazione dei nuovi utenti sui contenuti del Documento Programmatico sulla Sicurezza di propria pertinenza e sulle modalità comportamentali conseguenti.
- Verificare almeno una volta all'anno l'elenco delle persone autorizzate ad accedere agli archivi.

- Mettere in atto tutte le indicazioni del Documento Programmatico sulla Sicurezza relative alla gestione delle parole chiave.
- Informare il Titolare e/o il Responsabile del trattamento nella eventualità che siano rilevati dei rischi e/o delle non rispondenze alle norme di sicurezza e di eventuali incidenti.

4.4.1 Nomina del Custode delle passwords

L'Amministratore di Sistema e/o il Responsabile del trattamento e/o il Titolare nomina uno o più Custodi delle passwords cui è conferito il compito di custodire le parole chiave o passwords per l'accesso ai dati archiviati nei sistemi di elaborazione dei dati.

La nomina di ciascun Custode delle passwords deve essere effettuata con una lettera di incarico, deve essere controfirmata dall'interessato per accettazione e copia della lettera di nomina accettata deve essere conservata a cura dell'Amministratore di Sistema e/o il Responsabile del trattamento e/o loro incaricato in luogo apposito.

L'Amministratore di Sistema e/o il Responsabile del trattamento e/o loro incaricato deve informare ciascun Custode delle passwords della responsabilità che gli è stata affidata in relazione a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dal D. Lgs. n. 196/2003.

A ciascun Custode delle passwords l'Amministratore di Sistema e/o il Responsabile del trattamento e/o loro incaricato deve impartire adeguata formazione su quanto di competenza presente nel Documento Programmatico sulla Sicurezza e sulle norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina.

La nomina del Custode delle passwords è a tempo indeterminato, decade per revoca o dimissioni dello stesso e può essere revocata in qualsiasi momento dall'Amministratore di sistema senza preavviso, ed essere affidata ad altro soggetto.

4.5 Gli incaricati

Gli Incaricati del trattamento dei dati personali, con specifico riferimento alla sicurezza, hanno le seguenti responsabilità:

svolgere le attività previste dai trattamenti secondo le prescrizioni contenute nel presente Documento Programmatico sulla Sicurezza e le direttive del Titolare e/o del Responsabile;

non modificare i trattamenti esistenti o introdurne nuovi senza l'esplicita autorizzazione del responsabile;

rispettare e far rispettare le norme di sicurezza per la protezione dei dati personali;

informare il Titolare e/o il Responsabile del trattamento nella eventualità che siano rilevati dei rischi e/o delle non rispondenze alle norme di sicurezza e di eventuali incidenti di sicurezza che coinvolgano dati personali

4.5.1 Nomina degli Incaricati del trattamento

Al Titolare e/o ai Responsabili del trattamento (qualora designati) è affidato il compito di nominare, con comunicazione scritta, uno o più Incaricati del trattamento dei dati.

La nomina di ciascun Incaricato del trattamento dei dati deve essere effettuata con una lettera di incarico e/o per semplificare tale adempimento, in considerazione della frequenza con cui il personale viene soggetto a rotazione

e avvicendamento all'interno delle strutture amministrative, il Codice considera equivalente alla designazione nominativa degli incaricati, la preposizione del personale ad un'unità organizzativa (ad esempio, tramite un ordine di servizio) per la quale venga altresì individuato per iscritto l'ambito del trattamento consentito agli addetti che operano all'interno della medesima unità.

Gli incaricati del trattamento sono i soli che possono materialmente effettuare le operazioni di trattamento di dati personali. Gli incaricati operano sotto la diretta autorità del titolare o del responsabile, previa designazione espressa per iscritto, contenente la puntuale individuazione dell'ambito del trattamento loro consentito e l'indicazione delle istruzioni cui devono attenersi nello svolgimento del trattamento.

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

Agli incaricati deve essere assegnata una parola chiave, e, laddove previsto, un codice identificativo personale.

La nomina degli incaricati deve essere conservata a cura del responsabile del trattamento per la sicurezza e/o dei rispettivi responsabili di settore dei dati in luogo apposito. Agli incaricati del trattamento il Titolare e/o il Responsabile del trattamento per la sicurezza dei dati deve consegnare una copia di tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina.

La nomina degli incaricati è a tempo indeterminato e decade per revoca, per sue dimissioni, per modifica o con il venir meno dei compiti che giustificavano il trattamento dei dati personali.

Si tenga presente, altresì, che il legislatore ha provveduto a definire con maggiore compiutezza anche la figura dell' "incaricato": nessun trattamento di dati personali può essere svolto all'interno di una struttura complessa da chi non abbia ricevuto una specifica designazione in tal senso, in mancanza della quale la conoscenza dei dati da parte degli addetti ai lavori si configura come una comunicazione esterna ed in quanto tale assoggettata alle norme più stringenti previste per tale operazione.

5. ANALISI DEI RISCHI

E' stata rieffettuata l'analisi dei rischi dei dati trattati che si può così sintetizzare:

A) le tipologie di dati in funzione degli strumenti utilizzati;

B) la pericolosità della conoscenza di tali dati per la privacy dell'interessato in funzione del grado di interesse per terzi;

C) la tipologia di dati in funzione delle unità organizzative Enteli che li trattano;

D) i fattori di rischio connessi alle singole unità organizzative;

E) le tipologie di rischio in funzione della loro entità.

Quanto riportato sotto forma di singole matrici, per permetterne una più semplice comprensione e visualizzazione, viene in un secondo momento riunito in una considerazione generale sul sistema ad oggi in atto.

Vediamo quindi in dettaglio quanto detto in merito alla considerazione di tutti quei fattori ad oggi ritenuti importanti per un'adeguata analisi del sistema attuale.

A) Tipologia di Dati / Strumenti Utilizzati

Nella seguente matrice si procede a riportare la **tipologia dei dati trattati dal Titolare**, correlata alla tipologia di strumento utilizzato per la stessa, riportando nella casella di intersezione il simbolo ❍:

Tipologia di dati	Strumenti Utilizzati	
	A	B
dati comuni dei cittadini	❍	❍
dati sensibili dei cittadini idonei a rivelare lo stato di salute;	❍	❍
dati sensibili dei cittadini idonei a rivelare l'origine razziale o etnica;	❍	❍
dati sensibili dei cittadini idonei a rivelare l'adesione a partiti, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale;	❍	❍
dati per contratti d'appalto e gare, contabilità, atti amministrativi, determine, derivanti da atti notarili, etc.	❍	❍
dati giudiziari dei cittadini e/o fornitori	❍	❍
dati per istruzione pratiche di patrocinio, atti di liquidazione, etc.	❍	❍
dati inerenti pubblicità e affissioni	❍	❍
dati inerenti tasse per occupazioni spazi e aree pubbliche e quanto ad essi correlato	❍	❍
dati relativi alla viabilità, alle contravvenzioni e quanto ad essi connesso	❍	❍
dati relativi alle concessioni edilizie, all'ecologia ambiente e quanto ad essi connesso	❍	❍
dati relativi ai settori cimiteriale, sportivo, manutenzione strade, spettacoli mercati, caccia e quanto ad essi connesso	❍	❍
dati inerenti la TARSU sia per le attività commerciali che per le civili abitazioni, notifiche, sgravi e accertamenti, contenziosi tributati TARSU, e quanto ad essi correlato	❍	❍
dati inerenti tributi, cartelle esattoriali, cartelle ICI, contenziosi tributati ICI e quanto ad essi correlato	❍	❍
dati inerenti il patrimonio di beni mobili e immobili, dell'economato e quanto ad essi correlato	❍	❍

Tipologia di dati	Strumenti Utilizzati	
	A	B
dati relativi a pratiche legali, giudiziari, atti difensivi, atti amministrativi e quanto ad essi correlato	❍	❍
dati relativi allo stato civile, documentazione anagrafica e liste elettorali	❍	❍
dati comuni del personale dipendente (quali quelli necessari al rapporto di lavoro, alla reperibilità ed alla corrispondenza con gli stessi, ai rapporti fiscali)	❍	❍
dati del personale dipendente, relativi alle presenze in Ente (dallo stesso forniti per l'espletamento dei rapporti lavorativi)	❍	❍
dati del personale che presta servizio presso l'Ente (quali quelli necessari al rapporto di lavoro, alla reperibilità ed alla corrispondenza con gli stessi, ai rapporti fiscali)	❍	❍
dati sensibili del personale dipendente, (dallo stesso forniti per l'espletamento dei rapporti lavorativi)	❍	❍
dati sensibili dei dipendenti e/o del personale che presta servizio per conto dell'Ente idonei a rivelare l'adesione a partiti, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale	❍	❍
dati comuni di terzi (forniti dagli utenti per l'espletamento degli incarichi affidati all'Ente, compresi quelli necessari per disposizioni fiscali o afferenti alla reperibilità ed alla corrispondenza con gli stessi)	❍	❍
dati comuni dei fornitori (concernenti la reperibilità e la corrispondenza con gli stessi, nonché inerenti ai rapporti fiscali o dati di natura bancaria strettamente necessari ai rapporti contrattuali)	❍	❍
dati comuni di altri professionisti cui l'Ente affida incarichi (quali quelli concernenti la reperibilità e la corrispondenza con gli stessi, nonché inerenti ai rapporti fiscali)	❍	❍

Legenda

A = Schedari ed altri supporti cartacei custoditi nelle aree di accesso controllato;

B = Elaboratori;

B) Pericolosità per l'Interessato / Grado di interesse da parte di Terzi

Nella seguente matrice si procede a una stima del grado di rischio, che dipende dalla **tipologia dei dati trattati dal Titolare**, combinando il fattore della loro appetibilità per i terzi, con quello che esprime la loro pericolosità per la privacy del soggetto cui i dati si riferiscono e riportando nella casella ritenuta ad oggi idonea il numero identificativo associato alle tipologie di dati trattati secondo quanto riportato in legenda.

Legenda

1	**dati comuni dei cittadini**
2	**dati sensibili dei cittadini** idonei a rivelare lo stato di salute;
3	**dati sensibili dei cittadini** idonei a rivelare l'origine razziale o etnica;
4	**dati sensibili dei cittadini** idonei a rivelare l'adesione a partiti, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale;
5	**dati per contratti d'appalto e gare, contabilità, atti amministrativi, determine**, derivanti da atti notarili, etc.
6	**dati giudiziari dei cittadini e/o fornitori**
7	**dati per istruzione pratiche di patrocinio, atti di liquidazione**, etc.
8	**dati inerenti pubblicità e affissioni**
9	**dati inerenti tasse per occupazioni spazi e aree pubbliche** e quanto ad essi correlato
10	**dati relativi alla viabilità, alle contravvenzioni** e quanto ad essi connesso
11	**dati relativi alle concessioni edilizie, all'ecologia ambiente** e quanto ad essi connesso
12	**dati relativi ai settori cimiteriale, sportivo, manutenzione strade, spettacoli mercati, caccia** e quanto ad essi connesso
13	**dati inerenti la TARSU** sia per le attività commerciali che per le civili abitazioni, notifiche, sgravi e accertamenti, contenziosi tributati TARSU, e quanto ad essi correlato
14	**dati inerenti tributi**, cartelle esattoriali, cartelle ICI, contenziosi tributati ICI e quanto ad essi correlato
15	**dati inerenti il patrimonio** di beni mobili e immobili, dell'economato e quanto ad essi correlato
16	**dati relativi a pratiche legali**, giudiziari, atti difensivi, atti amministrativi e quanto ad essi correlato
17	**dati relativi allo stato civile, documentazione anagrafica e liste elettorali**
18	**dati comuni del personale dipendente** (quali quelli necessari al rapporto di lavoro, alla reperibilità ed alla corrispondenza con gli stessi, ai rapporti fiscali)
19	**dati del personale dipendente**, relativi alle presenze in Ente (dallo stesso forniti per l'espletamento dei rapporti lavorativi)
20	**dati del personale che presta servizio presso l'Ente** (quali quelli necessari al rapporto di lavoro, alla reperibilità ed alla corrispondenza con gli stessi, ai rapporti fiscali)
21	**dati sensibili del personale dipendente**, (dallo stesso forniti per l'espletamento dei rapporti lavorativi)
22	**dati sensibili dei dipendenti e/o del personale che presta servizio** per conto dell'Ente idonei a rivelare l'adesione a partiti, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale
23	**dati comuni di terzi** (forniti dagli utenti per l'espletamento degli incarichi affidati all'Ente, compresi quelli necessari per disposizioni fiscali o afferenti alla reperibilità ed alla corrispondenza con gli stessi)
24	**dati comuni dei fornitori** (concernenti la reperibilità e la corrispondenza con gli stessi, nonché inerenti ai rapporti fiscali o dati di natura bancaria strettamente necessari ai rapporti contrattuali)
25	**dati comuni di altri professionisti** cui l'Ente affida incarichi (quali quelli concernenti la reperibilità e la corrispondenza con gli stessi, nonché inerenti ai rapporti fiscali)

GRADO DI INTERESSE PER I TERZI					
	ELEVATO	**===**	**===**	**===**	**===**
	ALTO	**===**	**===**	**===**	**===**
	MEDIO	**===**	**(3), (4), (6) (16), (17)**	**===**	**===**
	BASSO	**(1), (5), (8), (9), (10), (11), (12), (15), (18), (19), (20), (23), (24), (25)**	**(2), (7), (13), (14), (21), (22)**	**===**	**===**
		BASSO	**MEDIO**	**ALTO**	**ELEVATO**

PERICOLOSITA' PER LA PRIVACY DELL'INTERESSATO

C) Tipologia di Dati / Settori di Riferimento

Nella seguente matrice si procede a riportare la **tipologia dei dati trattati dal Titolare**, correlata ai Settori di Riferimento che si occupa della stessa, riportando nella casella di intersezione il simbolo ❍:

Tipologia di dati	Settori									
	1	2	3	4	5	6	7	8	9	10
dati comuni dei cittadini		❍	❍		❍	❍	❍	❍	❍	❍
dati sensibili dei cittadini idonei a rivelare lo stato di salute;		❍	❍					❍	❍	❍
dati sensibili dei cittadini idonei a rivelare l'origine razziale o etnica;		❍	❍		❍					
dati sensibili dei cittadini idonei a rivelare l'adesione a partiti, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale;		❍	❍							
dati per contratti d'appalto e gare, contabilità, atti amministrativi, determine, derivanti da atti notarili, etc.			❍	❍						
dati per istruzione pratiche di patrocinio, atti di liquidazione, etc.			❍			❍				
dati inerenti pubblicità e affissioni			❍	❍		❍			❍	
dati inerenti tasse per occupazioni spazi e aree pubbliche e quanto ad essi correlato			❍	❍		❍			❍	
dati relativi alla viabilità, alle contravvenzioni e quanto ad essi connesso									❍	
dati relativi alle concessioni edilizie, all'ecologia ambiente e quanto ad essi connesso			❍				❍			
dati relativi ai settori cimiteriale, sportivo, manutenzione strade, spettacoli mercati, caccia e quanto ad essi connesso			❍	❍		❍		❍		
dati inerenti la TARSU sia per le attività commerciali che per le civili abitazioni, notifiche, sgravi e accertamenti, contenziosi tributati TARSU, e quanto ad essi correlato			❍	❍						
dati inerenti tributi, cartelle esattoriali, cartelle ICI, contenziosi tributati ICI e quanto ad essi correlato			❍	❍					❍	
dati inerenti il patrimonio di beni mobili e immobili, dell'economato e quanto ad essi correlato			❍	❍				❍		

Tipologia di dati	Settori									
	1	2	3	4	5	6	7	8	9	10
dati relativi a pratiche legali, giudiziari, atti difensivi, atti amministrativi e quanto ad essi correlato		❍	❍				❍			
dati relativi allo stato civile, documentazione anagrafica e liste elettorali			❍		❍				❍	
dati comuni del personale dipendente (quali quelli necessari al rapporto di lavoro, alla reperibilità ed alla corrispondenza con gli stessi, ai rapporti fiscali)			❍							
dati del personale dipendente, relativi alle presenze in Ente (dallo stesso forniti per l'espletamento dei rapporti lavorativi)			❍							
dati del personale che presta servizio presso l'Ente (quali quelli necessari al rapporto di lavoro, alla reperibilità ed alla corrispondenza con gli stessi, ai rapporti fiscali)			❍							
dati sensibili del personale dipendente, (dallo stesso forniti per l'espletamento dei rapporti lavorativi)			❍							
dati sensibili dei dipendenti e/o del personale che presta servizio per conto dell'Ente idonei a rivelare l'adesione a partiti, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale			❍							
dati comuni di terzi (forniti dai clienti per l'espletamento degli incarichi affidati all'Ente, compresi quelli necessari per disposizioni fiscali o afferenti alla reperibilità ed alla corrispondenza con gli stessi)	❍		❍							
dati comuni dei fornitori (concernenti la reperibilità e la corrispondenza con gli stessi, nonché inerenti ai rapporti fiscali o dati di natura bancaria strettamente necessari ai rapporti contrattuali)			❍							
dati comuni di altri professionisti cui l'Ente affida incarichi (quali quelli concernenti la reperibilità e la corrispondenza con gli stessi, nonché inerenti ai rapporti fiscali)		❍	❍							

Legenda

1. Settore Staff - Ufficio di Gabinetto
2. Settore Staff – Ufficio Legale
3. Settore Affari Generali e Risorse Umane
4. Settore Risorse Finanziarie
5. Settore Servizi al Cittadino
6. Settore Attività Produttive, SUAP, Sport, Turismo e Attività Culturali
7. Settore Territorio e Ambiente
8. Settore Lavori Pubblici
9. Settore Polizia Municipale
10. Settore Servizi Pubblici Locali

D) Fattori di Rischio / Settori

Nella seguente tabella si evidenziano i ***fattori di rischio*** cui sono soggetti gli strumenti (in senso generico) con cui l'Ente procede al trattamento dei dati personali.

Il simbolo ❍, posto nella casella di intersezione, significa che l'esposizione al rischio è media; il simbolo ● significa che l'esposizione al rischio è elevata; il simbolo == che ad oggi non si ravvisa alcun rischio.

Fattori di Rischio	Settori									
	1	2	3	4	5	6	7	8	9	10
Rischio d'area, legato al verificarsi di eventi distruttivi	❍	❍	❍	❍	❍	❍	❍	❍	❍	❍
Rischio d'area, legato all'accesso non autorizzato nei locali	❍	❍	❍	❍	❍	❍	❍	❍	❍	❍
Rischio di guasti tecnici di hardware, software e supporti	❍	❍	❍	❍	❍	❍	❍	❍	❍	❍
Rischio di penetrazione logica nelle reti di comunicazione	==	==	==	==	==	==	==	==	==	==
Rischio di utilizzo di beni e strumenti da parte di personale non autorizzato	❍	❍	❍	❍	❍	❍	❍	❍	❍	❍
Rischio di utilizzo di beni e strumenti, in maniera difforme da quanto previsto, da parte del personale interno	==	==	==	==	==	==	==	==	==	==
Rischio perdita delle caratteristiche di correttezza, completezza e congruità logica	==	==	==	==	==	==	==	==	==	==
Rischio di modifica non controllata del contenuto delle banche dati	==	==	==	==	==	==	==	==	==	==
Rischio di copia non autorizzata dei dati contenuti nelle banche dati	==	==	==	==	==	==	==	==	==	==
Rischio di distruzione delle banche dati	==	==	==	==	==	==	==	==	==	==
Rischio legato ad atti di sabotaggio	==	==	==	==	==	==	==	==	==	==
Rischio legato ad errori umani	❍	❍	❍	❍	❍	❍	❍	❍	❍	❍

Legenda

1. Settore Staff - Ufficio di Gabinetto
2. Settore Staff – Ufficio Legale
3. Settore Affari Generali e Risorse Umane
4. Settore Risorse Finanziarie
5. Settore Servizi al Cittadino
6. Settore Attività Produttive, SUAP, Sport, Turismo e Attività Culturali
7. Settore Territorio e Ambiente
8. Settore Lavori Pubblici
9. Settore Polizia Municipale
10. Settore Servizi Pubblici Locali

E) Tipologia di Rischio / Entità del Rischio

Nella seguente matrice si procede a riportare la tipologia di rischi cui l'Ente può andare incontro, correlata all'entità di rischio della stessa, riportando nella casella di intersezione il simbolo ❍:

Tipologia di Rischio	Entità del Rischio			
	BASSO	MEDIO	ALTO	ELEVATO
Comportamento degli operatori				
sottrazione di credenziali di autenticazione	❍			
carenza di consapevolezza, disattenzione o incuria	❍			
comportamenti sleali o fraudolenti	❍			
negligenza	❍			
manomissioni		❍		
incidente		❍		
errore materiale		❍		
Eventi relativi agli strumenti				
azione di virus informatici	❍			
azione di programmi suscettibili di recare danno	❍			
spamming		❍		
tecniche di sabotaggio	❍			
Incapacità di ripristino delle copie di back-up		❍		
esportazione illegittima di informazioni / dati		❍		
malfunzionamento, indisponibilità o degrado degli strumenti	❍			
accessi esterni non autorizzati		❍		
intercettazione di informazioni in rete	❍			
Eventi relativi al contesto fisico - ambientale				
ingressi non autorizzati a locali / aree ad accesso ristretto		❍		
sottrazione di strumenti contenenti dati		❍		
eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche)		❍		
incendi, allagamenti, condizioni ambientali…, eventi dolosi, accidentali o dovuti a incuria		❍		
guasto a sistemi complementari (impianto elettrico, climatizzazione…)	❍			
errori umani nella gestione della sicurezza fisica		❍		

Per quanto concerne l'Ente nel suo complesso, l'analisi dei rischi si può sintetizzare come segue:

- Il **rischio di accesso ai locali dell'Ente**, può essere definito ***medio*** perché si tiene conto sia delle possibilità di accesso non consentito che delle misure ad oggi in atto in alcuni settori maggiormente a rischio.

- Il **rischio di accesso alle aree** può essere definito ***medio*** perché si tiene conto sia delle possibilità di accesso non consentito che delle misure ad oggi in atto in alcuni settori maggiormente a rischio.
- Il **rischio di accesso ai singoli strumenti** da parte di persone non autorizzate può essere definito ***basso***, essendovi sempre personale nelle aree dove si trovano gli strumenti.
- Le aree ed i locali potrebbero essere interessati da **eventi naturali**, quali incendi, allagamenti e corto circuiti, pur avendo l'Ente provveduto ad adottare le disposizioni di sicurezza stabilite dalla legislazione vigente in materia. Essendo l'Ente dotata di dispositivi tecnici dichiarati adeguati, il rischio può comunque definirsi ***basso***.
- Per quanto riguarda gli **strumenti elettronici**, il rischio può essere definito ***medio***, essendo state ad oggi adottate dall'Ente le misure di sicurezza, tendenti a ridurre il rischio gravante sui dati e derivante dalla gestione di detti strumenti.
- Per quanto riguarda la **documentazione cartacea**, il rischio può essere definito ***medio***, essendo i contenitori dotati di chiusura a chiave, non accessibili se non in presenza delle risorse designate, ed essendo state adottate le altre misure indicate, fatta eccezione ovviamente per gli eventi naturali.
- Per quanto riguarda i **supporti di memorizzazione**, il rischio di deterioramento (a breve termine) dei dati da essi portati può essere ritenuto ***medio***, considerando sia la frequenza con cui vengono effettuati i backup, che la mole di dati trattati dall'Ente.

Ad oggi in funzione di quanto analizzato è contemplato dall'Ente l'effettuazione di eventi formativi mirati alla formazione dei Responsabili del trattamento designati dall'Ente, che a loro volta potranno formare e informare gli incaricati al trattamento, al fine di aumentare la conoscenza dei meccanismi relativi alla privacy ed assicurare così una maggiore sicurezza dei dati trattati, secondo le loro caratteristiche peculiari.

L'Ente si proporrà di analizzare l'eventuale interferenza sulla sicurezza data dalle modalità comportamentali e/o strutturali intrinseche alla natura della stessa organizzazione.

6. MISURE GIÀ ATTIVE E MISURE DA ADOTTARE

6.1. Misure di sicurezza contro il rischio di distruzione o perdita di dati

6.1.1 Criteri e procedure per garantire l'integrità dei dati

Al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita, il Titolare e/o il Responsabile del trattamento dei dati stabilisce, con il supporto tecnico dell'Amministratore di sistema, la periodicità con cui debbono essere effettuate le copie di sicurezza delle banche di dati trattati (periodicità che non deve però superare, per quanto pratico e ragionevole, la settimana).

I criteri debbono essere definiti dal Titolare e/o il Responsabile del trattamento dei dati in relazione al tipo di rischio potenziale e in base al livello di tecnologia utilizzata. In particolare per ogni banca di dati debbono essere definite almeno alcune delle seguenti specifiche, quelle ritenute più essenziali dal Titolare e/o dal Responsabile:

- il tipo di supporto da utilizzare per le copie di back-up;
- il numero di copie di back-up effettuate ogni volta;
- se i supporti utilizzati per le copie di back-up sono riutizzati e in questo caso con quale periodicità;
- se per effettuare le copie di back-up si utilizzano le procedure automatizzate e programmate;
- le modalità di controllo delle copie di back-up;
- la durata massima stimata di conservazione delle informazioni senza che ci siano perdite o cancellazione di dati;
- l'incaricato del trattamento a cui è stato assegnato il compito di effettuare le copie di back-up;
- le istruzioni e i comandi necessari per effettuare le copie di back-up.
- per redigere il documento con le istruzioni di copia deve essere utilizzato apposito modulo descrittivo per le banche di dati che deve essere conservato a cura del Titolare e/o Responsabile del trattamento dei dati in luogo apposito.

6.1.2 Protezione da virus informatici

Al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita di dati a causa di virus informatici, il Titolare e/o il Responsabile del trattamento dei dati e/o loro incaricato stabilisce, eventualmente con il supporto tecnico dell'Amministratore di sistema, quali protezioni software adottare in relazione all'evoluzione tecnologica dei sistemi disponibili sul mercato.

Il Titolare e/o il Responsabile del trattamento dei dati o loro incaricato stabilisce inoltre la periodicità, almeno ogni sei mesi, con cui debbono essere effettuati gli aggiornamenti dei sistemi antivirus utilizzati per ottenere un accettabile standard di sicurezza delle banche dati trattati.

I criteri debbono essere definiti dall'Amministratore di sistema in relazione al tipo di rischio potenziale e in base al livello di tecnologia utilizzata. In particolare per ogni sistema debbono essere definite le seguenti specifiche:

- il tipo di programma utilizzato
- la periodicità di aggiornamenti

Per ogni sistema, qualora si riscontrasse una problematica, deve essere predisposto apposito modulo di rilevazione e/o comunicazione interna, sul quale debbono essere annotati eventuali virus rilevati e, se possibile, la fonte di isolare o comunque trattare con precauzione i possibili portatori di infezioni informatiche.

I moduli compilati ed aggiornati dagli Incaricati del trattamento debbono essere conservati a cura del Titolare e/o il Responsabile del trattamento dei dati o loro incaricato dei dati in luogo apposito e debbono essere eventualmente forniti all'Amministratore di sistema.

6.1.2.1 Metodi per la prevenzione dei virus

Un virus informatico è un programma eseguibile da un computer con le seguenti caratteristiche:

Ha la capacità di "inglobarsi" cioè confondersi alle istruzioni di altri programmi presenti modificandoli;

E' in grado di replicarsi, ossia di copiare se stesso in altri programmi, talvolta in computer differenti mediante la rete cui il computer infettato è connesso;

Passato un certo tempo prestabilito, necessario per effettuare la replicazione, il virus comincia agisce eseguendo ciò per il quale è stato scritto che, per esempio, può essere distruggere o prelevare dati e/o programmi presenti sul computer.

Un virus può trasmettersi:

1. Attraverso programmi provenienti da fonti non ufficiali;
2. Attraverso le macro dei programmi di automazione d'ufficio;
3. Attraverso la rete locale;
4. Attraverso falle di sicurezza presenti nei programmi di uso comune (es, Internet Explorer, Outlook).

Una volta conosciuta la loro struttura, i virus sono facilmente identificabili ed eliminabili da programmi, detti appunto **Antivirus**, scritti appositamente; questi ricercano negli altri programmi presenti sul computer la sequenza di istruzioni che caratterizza il virus; ciò è però possibile solo se i virus sono noti, e cioè se è nota, almeno in parte, la sequenza di istruzioni con cui sono stati scritti,diversa per ogni virus.

Alcune significative avvisaglie della presenza del virus sono:

1. Presenza di effetti inconsueti nel video (messaggi di avvertimento dal significato non chiaro, effetti sonori)
2. Il computer ha un rallentamento complessivo di una certa entità
3. Vengono frequentemente cancellati dati o programmi
4. Esiste un'intensa attività di rete anche quando non si utilizzano programmi per la navigazione o la posta elettronica

Buone norme per evitare di essere infettati, sono:

a) Usare 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 bisogna mai utilizzare programmi non autorizzati, con particolare riferimento ai videogiochi, che sono spesso utilizzati per veicolare virus.

b) Non utilizzare mai programmi insicuri prima di una scansione

I programmi che provengono da fonti insicure vanno preventivamente sottoposti ad una scansione da parte del software antivirus, e quindi eseguiti.

E' buona norma, inoltre, effettuare una scansione anche successivamente alla prima esecuzione del programma, in modo da verificare che non sia stato iniettato il virus nella memoria RAM.

c) ***Proteggere i dischetti in scrittura quando possibile***

In tal modo si eviteranno scritture accidentali, magari innescate da un virus che tenta di propagarsi. I virus non possono in ogni caso aggirare la protezione meccanica.

d) ***Non diffondere messaggi di provenienza dubbia***

Se vengono ricevuti messaggi che avvisano di un nuovo virus pericolosissimo, è opportuno fare le opportune verifiche: le email di questo tipo sono detti con terminologia anglosassone *hoax* (termine spesso tradotto in italiano con "bufala"), l'equivalente delle "leggende metropolitane" della rete. Spesso, tali messaggi vengono artatamente spediti da un mittente di fiducia (amici, parenti, colleghi). Analogamente, tutti i messaggi che invitano a "diffondere la notizia quanto più possibile" sono *hoax*. Anche se parlano di temi di impatto (fame nel mondo, situazione delle donne negli stati arabi, bambini in fin di vita, guadagni miracolosi); si tratta di *hoax* aventi spesso scopi molto simili a quelli dei virus, cioè utilizzare indebitamente le risorse informatiche. Queste attività sono vietate dagli standard di Internet e contribuire alla loro diffusione può portare alla terminazione del proprio accesso.

e) ***Assicurarsi che il 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 sulle "impronte digitali" dei nuovi virus. Questi file di identificativi sono rilasciati, di solito, con maggiore frequenza rispetto alle nuove versioni dei motori di ricerca dei virus. E' utile Informarsi con il responsabile del trattamento dati per maggiori dettagli.

6.1.3 Infezioni e contagio da virus informatici

Nel caso in cui su uno o più sistemi si dovesse verificare perdita di informazioni o danni a causa di infezione o contagio da virus informatici l'amministratore di sistema deve provvedere a:

- isolare il sistema;
- verificare se ci sono altri sistemi infettati con lo stesso virus informatico;
- identificare l'antivirus adatto e bonificare il sistema infetto;
- installare l'antivirus adatto su tutti gli altri sistemi che ne sono sprovvisti;

L'Amministratore di sistema deve inoltre compilare apposito documento di rilevazione delle Non Conformità; tali moduli compilati devono essere conservati a cura del Titolare e/o del Responsabile del trattamento dei dati in luogo apposito.

6.1.4 Firewall

Il firewall è uno strumento di notevole utilità per la sicurezza della rete Entele. Esso consente una protezione che salvaguarda il computer nel momento in cui esso accede ad altre reti (rete locale, LAN, Internet) o trasmette dati e informazioni attraverso le stesse. Esso è studiato per proteggere i punti d'accesso, ossia di ingresso e d'uscita, alla rete con cui il computer è connesso.

Il Firewall può essere un applicativo software (solitamente detto 'firewall personale'), cioè un programma installabile localmente sul computer, o può essere costituito da componenti hardware indipendenti, cioè elementi fisici, che autorizzano o negano l'accesso o il traffico di dati tra un computer e l'esterno.

Attraverso un firewall è possibile specificare i programmi e i servizi che possono essere collegati alla rete, autorizzare o negare le connessioni verso altri computer o indirizzi IP (cioè il numero che identifica in maniera esclusiva un computer), autorizzare o negare le connessioni tramite porte (connessioni nelle quali vengono trasferite informazioni in entrata/uscita verso l'esterno, e viceversa), autorizzare o negare l'accesso alle cartelle condivise presenti sul computer, disciplinare gli accessi mediante regole miste e dipendenti da fattori di natura diversa (giorni della settimana, orari di esercizio, utenti)

Selezione del Firewall

La scelta del Firewall non è unica, ma dipende da fattori come il tipo di rete che si ha in Ente, la sua complessità, il numero di postazioni utilizzate

Un Firewall di tipo hardware è sconsigliato per una rete semplice con poche postazioni poiché richiede un'istallazione, una manutenzione ed un aggiornamento che in alcuni casi comportano approfondite conoscenze di gestione delle reti; in tal caso, dunque, è meglio adottare una soluzione software. In caso contrario invece può essere consigliabile una soluzione hardware che permetta di proteggere l'intera rete con un unico dispositivo senza dover installare un Firewall per ogni postazione.

Nel caso in cui si scelga di utilizzare una soluzione software, potrebbe risultare comodo optare per una soluzione che integri cioè al suo interno sia un Antivirus sia un Firewall, in modo da dover acquistare, e soprattutto imparare ad utilizzare un unico programma. L'importanza di quest'ultimo aspetto non è affatto da trascurare poiché la presenza nella stessa rete di diversi software di protezione può generare fenomeni di incompatibilità o di debolezza qualora vi sia una difformità nelle impostazioni di configurazione; in tutti questi casi, la protezione potrebbe non risultare adeguata.

Inoltre, dal punto di vista della gestione complessiva è più agevole l'aggiornamento di un solo software che di diversi programmi.

Alcuni sistemi operativi (es. Windows XP, Linux) possiedono un sistema integrato di Firewall, che è possibile utilizzare in alternativa ai software specifici.

L'aggiornamento del Firewall deve essere fatto almeno annualmente (almeno semestralmente in caso di trattamento di dati sensibili e/o giudiziari).

Configurazione del Firewall

La configurazione del Firewall non è cosa intuitiva per chi non ha una buona dimestichezza con l'uso del computer, perché si incontrano concetti tipo porte di comunicazione, indirizzi IP, protocolli, e altri concetti tecnici che spesso non sono conosciuti. Inoltre, occorre tenere conto della duplice protezione offerta dal firewall, cioè dall'esterno verso l'interno, e dall'interno verso l'esterno.

Nel primo caso, la protezione riguarda l'accesso al computer in cui viene installato il Firewall, cioè la politica di accesso ai servizi del sistema. Ad esempio, può essere utile restringere l'accesso al servizio di condivisione di file della rete microsoft (SMB) soltanto ad un ristretto numero di computer.

Nel secondo caso, la protezione riguarda i servizi accessibili dal sistema, ed i software installati che possono utilizzare tali servizi. Ad esempio, può essere utile garantire l'accesso al servizio http soltanto al browser predefinito, impedendolo ad altri software malevoli.

In tal senso, l'utilizzo del software consente di monitorare il sistema, in quanto consente di rilevare i tentativi di accesso alla rete esterna richiesti dai software installati.

La configurazione appropriata di un Firewall è, pertanto, particolarmente complessa, specie quando la realtà da trattare è articolata ed eterogenea. Qualora l'Ente non riesca da sola ad installare il Firewall, è opportuno interpellare un consulente che effettui un'analisi approfondita dei canali di comunicazione e delle possibili vulnerabilità.

Misure di sicurezza contro il rischio di accesso non autorizzato

6.2.1 Norme generali di prevenzione

In considerazione di quanto disposto dal D. Lgs. n. 196/2003, è fatto divieto a chiunque di:

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

6.2.2 Procedure per controllare l'accesso ai locali in cui vengono trattati i dati

Al Titolare e/o Responsabile del trattamento dei dati è affidato il compito di redigere e di aggiornare ad ogni variazione l'elenco degli uffici in cui viene effettuato il trattamento dei dati, nominando eventualmente un apposito Incaricato con il compito di controllare direttamente i sistemi, le apparecchiature o i registri di accesso ai locali allo scopo di impedire intrusioni o danneggiamenti.

Il Titolare e/o Responsabile del trattamento dei dati, qualora necessario, deve definire le modalità di accesso agli uffici in cui sono presenti sistemi o apparecchiature di accesso ai dati trattati.

Il Titolare e/o Responsabile del trattamento dei dati deve quindi informare con una comunicazione scritta l'Incaricato dell'ufficio (qualora nominato) dei compiti che gli sono stati affidati utilizzando apposito modulo.

6.2.3 Identificazione degli elaboratori connessi in rete pubblica

All'Amministratore di sistema è affidato il compito di redigere e di aggiornare ad ogni variazione l'elenco dei sistemi di elaborazione connessi in rete pubblica.

Per ogni sistema deve essere specificato, per quanto pratico e ragionevole, l'Incaricato del trattamento e/o l'Amministratore del sistema e/o il Custode della password.

Per l'inventario dei sistemi di elaborazione deve essere utilizzato apposito modulo e/o carta intestata dell'Ente, che deve essere conservato a cura del Titolare e/o Responsabile del trattamento dei dati in luogo apposito.

6.2.4 Criteri e procedure per garantire la sicurezza delle trasmissioni dei dati

Al fine di garantire la sicurezza delle trasmissioni dei dati tra le sedi dislocate nel territorio, attraverso l'utilizzo di apparecchi di trasmissione dati, quali "Modem" e "Router", il Titolare e/o il Responsabile del trattamento dei dati stabilisce, con il supporto tecnico dell'Amministratore di sistema, le misure tecniche da adottare in rapporto al rischio di intercettazione o di intrusione o di hacker su ogni sistema collegato in rete pubblica.

I criteri debbono essere definiti dall'Amministratore di sistema relazione al tipo di rischio potenziale e in base al livello di tecnologia utilizzata. In particolare per ogni sistema interessato debbono essere definite le seguenti specifiche:
Le misure applicate per evitare intrusione
Le misure applicate per evitare contagi da virus informatici

6.2.5 Procedure di assegnazione degli user-id

Il Titolare e/o Responsabile del trattamento dei dati, in accordo con l'Amministratore di sistema, deve definire le modalità di assegnazione dei nomi identificativi per consentire a ciascun incaricato del trattamento di accedere ai sistemi di trattamento delle banche di dati.

Non sono ammessi nomi identificativi di gruppo (per quanto pratico e ragionevole), con la sola eccezione dei codici identificativi assegnati per l'amministrazione di sistema, relativamente ai sistemi operativi che prevedono un unico livello di accesso.

In ogni caso, un codice identificativo assegnato ad un Incaricato del trattamento deve essere annullato dell'Incaricato del trattamento ha dato le dimissioni.

6.2.6 Procedure di assegnazione delle passwords

Il Titolare e/o Responsabile del trattamento dei dati deve definire in accordo con l'Amministratore di sistema le modalità di assegnazione delle passwords.

La definizione dei criteri di assegnazione di delle password è descritta in apposito modulo. In relazione al tipo di banca dati trattata, l'Amministratore del sistema può decidere che ogni utente Incaricato del trattamento possa modificare autonomamente la propria password di accesso. In questo caso la modifica equivale alla comunicazione al Custode del cambio della password.

6.2.7 Linea guida per la scelta delle password

Il più semplice metodo per l'accesso illecito a un sistema consiste nell'indovinare la password dell'utente legittimo. In molti casi sono stati procurati seri danni al sistema informativo a causa di un accesso protetto da password "deboli". La scelta di password "forti" è, quindi, parte essenziale della sicurezza informatica.

Azioni da NON fare

a) NON scrivere la password da nessuna parte che possa essere letta facilmente, soprattutto vicino al computer.
b) NON dire a nessuno la propria password. Ricordarsi che lo scopo principale per cui usate una password è assicurare che nessun altro possa utilizzare le proprie risorse o possa farlo col nome dell'incaricato cui è assegnata la password.
c) Quando si immette la password NON fare guardare a nessuno quello che state battendo sulla tastiera.
d) NON scegliere password che si possano trovare in un dizionario. Su alcuni sistemi è possibile "provare" tutte le passwords contenute in un dizionario per vedere quale sia quella giusta.
e) NON credere che usare parole straniere renderà più difficile il lavoro di scoperta, infatti chi vuole scoprire una password è dotato di molti dizionari delle più svariate lingue.
f) NON usare il proprio nome utente. È la password più semplice da indovinare.
g) NON usare passwords che possano in qualche modo essere legate al soggetto che deve utilizzarla come, ad esempio, il proprio nome, quello dei propri moglie/marito, figli, cane, date di nascita, numeri di telefono etc.

Azioni da Fare

a) Cambiare la password a intervalli regolari. Chiedere al proprio Amministratore di sistema quali sono le sue raccomandazioni sulla frequenza del cambio; a seconda del tipo di sistema l'intervallo raccomandato per il cambio può andare da tre (per i dati sensibili) fino a sei mesi (per i dati personali).
b) Usare password lunghe almeno otto caratteri possibilmente con un misto di lettere, numeri e segni di interpunzione.
c) Utilizzate passwords distinte (per quanto pratico e ragionevole) per sistemi con diverso grado di sensibilità. In alcuni casi la password viaggiano in chiaro sulla rete e possono essere quindi intercettate, per cui, oltre a cambiarla spesso, è importante che sia diversa per quella usata da sistemi "sicuri". Il tipo di password in assoluto più sicura è quella associata a un supporto di identificazione come un dischetto o una carta a microprocessore; la password utilizzata su un sistema di questo tipo non deve essere usata in nessun altro sistema. In caso di dubbio, consultate il vostro amministratore di sistema.

Come scegliere una password

Le migliori password sono quelle facili da ricordare ma, allo stesso tempo, difficili da indovinare, come quelle che si possono ottenere comprimendo frasi lunghe. La frase *"C'era una volta una gatta che aveva una macchia nera sul muso"* può ad esempio fornire, tra le tante possibilità, "Cr1Vlt1Gtt".

Ecco alcuni altri esempi:

Frase	Possibile password
57% di Finlandesi hanno detto si alla EU	57%DFNHDSAEU
Roma è la capitale d'Italia	RMCPIEST
"Esc" si trova in alto a sinistra	"E"stULK
Tutto è bene quel che finisce bene	TEBQCFNBN

Misure di sicurezza relative a elaboratori non accessibili da altri elaboratori o terminali

Ogni incaricato provvederà alla periodica sostituzione della propria parola chiave, provvedendo ad informare di ciò il soggetto preposto alla custodia delle parole chiave.

Ulteriori misure di sicurezza relative a elaboratori accessibili in rete:

a) I codici identificativi personali per l'utilizzazione dell'elaboratore devono essere assegnati e gestiti in modo che ne sia prevista la disattivazione in caso di perdita della qualità che consentiva l'accesso all'elaboratore o di mancato utilizzo dei medesimi per un periodo superiore ai sei mesi.
b) I programmi in dotazione, di protezione contro il rischio di intrusione o danneggiamento ad opera di terzi, devono essere verificati, quanto a efficacia ed aggiornamento, con cadenza almeno semestrale.
c) L'accesso all'elaboratore sarà consentito sulla base di autorizzazioni assegnate, singolarmente o per gruppi di lavoro, agli incaricati del trattamento o della manutenzione; se si tratta di elaboratori accessibili mediante una rete di telecomunicazioni disponibili al pubblico sono oggetto di autorizzazione anche gli strumenti che possono essere utilizzati per l'interconnessione mediante reti disponibili al pubblico;
d) L'autorizzazione, se riferita agli strumenti, dovrà individuare i singoli elaboratori attraverso i quali è possibile accedere per effettuare operazioni di trattamento;
e) Le autorizzazioni all'accesso sono rilasciate e revocate solo dal titolare e/o dal responsabile;
f) Periodicamente, e comunque almeno una volta l'anno, dovrà essere verificata la sussistenza delle condizioni per le autorizzazioni all'accesso;
g) L'autorizzazione all'accesso deve in ogni caso intendersi limitata ai soli dati la cui conoscenza è necessaria e sufficiente per lo svolgimento delle operazioni di trattamento o di manutenzione.
h) La validità delle richieste di accesso ai dati personali deve essere verificata prima di consentire l'accesso stesso;
i) Deve essere vietata l'utilizzazione di un medesimo codice identificativo personale per accedere in contemporanea alla stessa applicazione da diverse stazioni di lavoro.

Localizzazione e limitazioni all'accesso dei servers

Per quanto concerne il server del CED, esso è locato presso il Data Center, presso la sede centrale dell'Ente: esso è dotato di porta blindata, oltre la registrazione degli accessi, come riportato in precedenza.

Per quanto riguarda invece il server della Polizia Municipale è locato in apposito locale presso il Comando Centrale.

6.3 Misure di sicurezza contro il rischio di trattamento non consentito

Per quanto riguarda le aree ed i locali, essi possono essere colpiti da eventi naturali o accessi di terzi non autorizzati; ma, come si evince dall'Analisi dei Rischi al Capitolo 5 del presente Documento Programmatico, la probabilità che queste situazioni possano verificarsi è bassa.

Per quanto riguarda i software contenuti negli strumenti elettronici, possono verificarsi errori, virus, intercettazioni dei dati.

Per quanto riguarda gli strumenti elettronici, possono verificarsi malfunzionamenti, guasti, eventi naturali, alterazioni delle trasmissioni.

Inoltre si è disposto che tutti gli utilizzatori di strumenti elettronici non lascino incustodito, o accessibile, lo strumento elettronico stesso.

Si è inoltre disposto che essi verifichino la provenienza delle email e non operino operazioni di sharing.

Ogni computer che può effettuare il collegamento è dotato di dispositivo antivirus che viene aggiornato con funzione automatica e con scansione per ogni aggiornamento antivirus, e comunque almeno semestrale. È dotato di antivirus anche il server, per maggiore cautela. Stesso dicasi per il Firewall: Ogni computer che può effettuare il collegamento è dotato di dispositivo firewall che viene aggiornato con funzione automatica e con scansione per ogni aggiornamento, e comunque almeno semestrale.

Per i computer è prevista la funzione di aggiornamento automatico del sistema fornito dalla casa madre mediante lo strumento di update.

Analogo sistema di aggiornamento automatico è previsto per l'antivirus. E' stata data istruzione che, qualora nessun aggiornamento del sistema fosse segnalato automaticamente per un periodo di mesi 6, si provveda comunque ad attivare la funzione di controllo per verificare l'esistenza o meno di detti aggiornamenti automatici.

E' stato disposto l'obbligo di provvedere ad un back- dei dati e dei sistemi installati sul server su cd rom, i quali vengono conservati e chiusi in un cassetto e/o altro contenitore munito di serratura, e si è data disposizione di verificare, effettuato il back-up, la leggibilità del supporto e che una volta a settimana si proceda a verifica a campione della leggibilità dei dati.

La tempistica di effettuazione del back-up può essere al massimo settimanale per i dati dinamici (cioè in continuo aggiornamento) e mensile o con frequenza inferiore per i dati statici (cioè dati che non vengono aggiornati con continuità, a seconda delle loro caratteristiche).

Una copia di back-up può essere depositata presso altra sede designata dal Titolare e/o Responsabile del trattamento dei dati.

Le comunicazioni a mezzo posta e/o a mezzo fax, dovranno essere tempestivamente smistate e consegnate ai destinatari. Quando è dato un ordine di stampa, il documento stampato dovrà essere prontamente prelevato e consegnato all'interessato.

6.3.1 Personale autorizzato al trattamento dei dati

Al Titolare e/o Responsabile del trattamento dei dati o loro incaricato è affidato il compito di redigere di aggiornare ad ogni variazione l'elenco degli Incaricati del trattamento autorizzati al trattamento dei dati personali. In particolare, in caso di trattamento automatizzato di dati, per ogni Incaricato del trattamento deve essere indicato lo user-id assegnato.

In caso di dimissioni di un Incaricato del trattamento o di revoca delle autorizzazioni al trattamento dei dati, il Titolare e/o Responsabile del trattamento dei dati deve trarne immediata comunicazione al Custode delle password e all'Amministratore di sistema di competenza che provvederanno a disattivare la possibilità di accesso sistema per i soggetti in questione.

Per redigere l'elenco degli Incaricati del trattamento deve essere utilizzato apposito modulo e/o carta intestata dell'Ente, che deve essere conservata cura del Titolare e/o Responsabile del trattamento dei dati o loro incaricato in luogo apposito e deve essere comunicato all'Amministratore di sistema e/o al Custode delle passwords di competenza.

6.3.2 Verifiche periodiche delle condizioni per il mantenimento delle autorizzazioni

Al Titolare e/o all'Amministratore di sistema (o suo incaricato) è affidato il compito di verificare ogni anno, possibilmente entro il 31 marzo, le autorizzazioni di accesso ai dati oggetto del trattamento e di aggiornare l'elenco degli utenti autorizzati utilizzando apposito modulo e/o carta intestata dell'Ente che deve essere conservato a cura del Titolare e/o Responsabile del trattamento dei dati o loro incaricato in luogo apposito.

6.3.3 Definizione dei criteri di assegnazione dei permessi di accesso ai dati

Al Titolare e/o all'Amministratore di sistema è affidato il compito di redigere e di aggiornare ad ogni variazione la tabella dei Permessi di accesso che indica per ogni banca di dati tipi di permesso di accesso per ogni incaricato il trattamento autorizzato. In particolare per ogni Incaricato del trattamento e per ogni banca di dati devono essere indicati, qualora ritenuto opportuno dall'Ente, i privilegi assegnati tra i seguenti: Inserimento di dati, Lettura e stampa di dati, Variazione di dati, Cancellazione di dati.

La tabella dei permessi di accesso dev'essere redatta utilizzando apposito modulo e/o carta intestata dell'Ente che deve essere conservato a cura del Titolare e/o Responsabile del trattamento dei dati (o loro incaricato) in luogo apposito.

6.3.4 Verifiche periodiche delle condizioni per il mantenimento dei permessi di accesso ai dati

Al Titolare e/o all'Amministratore di sistema (o suo incaricato) è affidato il compito di verificare ogni anno, possibilmente entro il 31 marzo, le necessità di accesso ai dati oggetto del trattamento e di aggiornare l'elenco degli utenti autorizzati utilizzando apposito modulo e/o carta intestata dell'Ente che deve essere conservato luogo apposito.

6.3.5 Controlli e audit

Nel corso dell'operatività lavorativa, il Titolare può prevedere la possibilità di verificare e controllare dell'operato di tutte le figure designate (responsabili, incaricati, amministratori di sistema).

Tale operato può essere oggetto, con cadenza preferibilmente annuale, di un'attività di verifica da parte del titolare del trattamento, in modo da controllare la rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.

Nel corso delle attività ispettive disposte da Titolare bisogna tener presente quale importanza rivestano i ruoli di system administrator e/o di network administrator e/o database administrator.

6.3.5.1 Audits interni

Le attività di verifica consistono nel riscontro dell'evidenza oggettiva mediante risultanze documentate in dettaglio, della conformità degli aspetti esaminati alle prescrizioni applicabili contenute nei documenti di riferimento.

L'Ente effettua periodicamente verifiche ispettive interne al fine di accertare e garantire che le modalità operative siano conformi a quanto pianificato e ai requisiti della legislazione vigente in materia.

I risultati delle Verifiche Ispettive Interne vengono documentati e portati all'attenzione delle risorse interessate i quali devono attivare tempestive azioni per eliminare le eventuali Non Conformità emerse e le loro cause.

L'Ente ha definito un sistema di Verifiche Ispettive Interne (V.I.I.) allo scopo di:

- Verificare che le modalità operative siano conformi ai requisiti della legislazione vigente in materia;
- Stabilire che i singoli trattamenti siano correttamente svolti in accordo a quanto riportato nel presente Documento Programmatico sulla Sicurezza che li regolamentano e quindi determinare il grado di applicazione dello stesso;
- Evidenziare tutto quanto possa inficiare la corretta applicazione di quanto riportato nel presente Documento Programmatico sulla Sicurezza al fine di consentire l'identificazione e definizione di idonee azioni di miglioramento;
- Valutare successivamente l'efficacia delle azioni di miglioramento attuate per poterle standardizzare e interiorizzarle, consolidando in tal modo l'azione di miglioramento continuo.
- Verificare l'accesso fisico ai locali dove si svolge il trattamento;
- Verificare periodicamente (almeno ogni sei mesi) il corretto utilizzo delle parole chiave e dei profili di accesso degli incaricati. Verificare l'integrità dei dati e delle loro copia di backup;
- Verificare la sicurezza del eventuale trasmissioni in rete;
- Verificare la bontà di conservazione dei documenti cartacei;
- Verificare la distruzione dei supporti magnetici che non possono che essere utilizzati;
- Verificare il livello di formazione degli incaricati.

Programmazione delle Verifiche Ispettive Interne: Le VII devono essere programmate affinché tutti i trattamenti siano verificati con frequenza relazionata allo loro importanza, complessità e/o la criticità e, comunque, in modo tale che tutte siano verificati almeno una volta l'anno.

Allo scopo il Titolare e/o il Responsabile del trattamento, o loro incaricato, predispone ogni anno un **Piano annuale delle verifiche ispettive** (o documento similare del Sistema di Gestione della Qualità) nel quale individuare:

- i trattamenti da sottoporre a VII e le relative funzioni responsabili;
- le date indicative in cui verranno eseguite le verifiche ispettive.

Detto **Piano annuale delle verifiche ispettive** (o documento similare), deve essere sottoposto ad approvazione del Titolare e/o Responsabile del trattamento dei dati e, successivamente, divulgato e/o reso noto a tutte le funzioni interessate.

Definizione delle Voci da Valutare: Le VII devono essere preparate adeguatamente e con anticipo rispetto alla loro esecuzione dal responsabile e dal personale aziendale di cui intende, eventualmente, avvalersi in relazione alle specifiche capacità e all'indipendenza da responsabilità dirette nell'attività da ispezionare. Gli elementi da tenere a riferimento per la definizione delle voci da valutare sono essenzialmente i requisiti della legislazione vigente in materia e i requisiti specifici individuati nel presente Documento Programmatico sulla Sicurezza riguardanti i singoli trattamenti.

Esecuzione delle Verifiche Ispettive: il Responsabile alle frequenze stabilite effettua le Verifiche Ispettive in ogni singolo Settore seguendo e/o impostando la rispettiva **Audit Check List** (o documento similare) delle voci da valutare. Nell'esecuzione della verifica vengono valutati il grado di conoscenza delle modalità operative, la relativa applicazione e la formalizzazione delle attività secondo quanto richiesto.

La V.I.I. deve iniziare con una riunione di apertura tra il gruppo di verifica ed il responsabile della Funzione verificata per illustrare obiettivi e modalità di esecuzione della verifica stessa.

La V.I.I. deve essere eseguita sulla base dei documenti di riferimento delle attività da verificare e del programma concordato nella riunione di apertura, avendo cura di riscontrare l'evidenza oggettiva della conformità delle attività esaminate, documentando la risultanze attraverso precisi e dettagliati richiami ai riscontri effettuati.

Se l'andamento della verifica ispettiva lo rende necessario, è possibile estendere l'indagine ad attività e/o ad aspetti non previsti nel programma della verifica stessa. Allo scopo, il gruppo di verifica può anche dividersi per verificare più aspetti contemporaneamente. In tal caso, al responsabile del Gruppo di Verifica spetta il compito di coordinare le attività del gruppo di verifica.

La verifica ispettiva interna deve terminare con una riunione di chiusura nella quale il responsabile del gruppo di verifica presenta al responsabile della Funzione verificata e/o all'Alta Direzione i rilievi emersi fornendo i dovuti riscontri oggettivi

Valutazione delle Verifiche Ispettive: A conclusione della verifica ispettiva, il gruppo di verifica deve redigere il rapporto della verifica ispettiva, documentando quanto emerso nel corso della verifica stessa. In tale rapporto devono essere registrate le eventuali non conformità e/o osservazioni emerse, i documenti esaminati, i luoghi e/o le aree e l'eventuale personale coinvolto nella verifica stessa. Tale rapporto deve essere consegnato dal Responsabile del Gruppo di Verifica al Responsabile, o suo incaricato, (se il Resp. del Gruppo di Verifica è esterno) affinché lo porti all'attenzione del Responsabile del trattamento dei generico settore, e ne conserva copia (se il Resp. del Gruppo di Verifica è il Responsabile, o suo incaricato). Le NC rilevate devono essere riportate dal Titolare e/o Responsabile del trattamento dei dati e/o loro incaricato sul modulo per la rilevazione delle Non Conformità o documento similare secondo quanto previsto nel paragrafo seguente.

Comunicazione Esiti: Al termine delle V.I.I., i risultati vengono presentati in una riunione cui partecipano, tutte le risorse interne o esterne interessate alla verifica. In tale riunione vengono eventualmente stabiliti gli interventi correttivi da attuare e le successive responsabilità/ tempistiche/ modalità di verifica degli stessi.

Richiesta Azioni di Miglioramento e Interventi Correttivi: Conseguentemente al rapporto, se sono emerse non conformità rilevanti o potenziali, il Responsabile, o suo incaricato, deve richiedere alla Funzione interessata di attuare tempestivamente delle idonee **Azioni di Miglioramento**.

I responsabili individuati devono attivarsi con sollecitudine per avviare gli interventi correttivi (cosa, come, quando, chi), stabiliti.

Verifiche Ispettive Interne Non Programmate: Qualora si determinino condizioni tali da eseguire verifiche ispettive, queste devono essere gestite dal Titolare e/o Responsabile del trattamento dei dati, o suo incaricato, secondo le stesse modalità previste per quelle programmate. In tal caso, tempestivamente, il Titolare e/o Responsabile del trattamento dei dati, o suo incaricato, deve nominare il responsabile della verifica ispettiva e, in relazione alle effettive disponibilità, concordare con tutti gli interessati la data nella quale eseguire la verifica stessa.

Stabilita tale data, il responsabile della verifica ispettiva deve predisporre e notificare alla persona interessata il relativo programma della verifica. Sono da considerarsi verifiche ispettive non programmate anche quelle che si rendono necessarie per la verifica delle azioni correttive e preventive intraprese.

Se per motivi di urgenza non è possibile anticipare alla persona interessata il relativo programma, questo deve essere consegnato, discusso e concordato in occasione dell'apertura della verifica stessa.

RIFERIMENTI

- Mod. PAVI;
- Mod. PVI;
- Mod. ACL;
- Mod RVI.

6.3.6 Gestione delle Non Conformità

La gestione delle Non Conformità si integra con le procedure specifiche di analisi del sistema. Obiettivi di tale sistema sono:

- Individuare eventuali tipologie di trattamenti che non soddisfino i requisiti qui specificati;
- Innescare le azioni correttive atte ad eliminare o ridurre le non conformità stesse ed i costi conseguenti;
- Definire le responsabilità aziendali in caso di presenza di Non Conformità
- Garantire il perseguimento della politica di continuo miglioramento del sistema.

Rilevazione e registrazione

Le Non Conformità che sono individuate in una qualsiasi fase lavorativa da ogni risorsa Entele sui trattamenti effettuati; applicazione e metodologia delle modalità operative tecniche e/o gestionali previste dall'Ente durante tutte le attività lavorative della stessa in merito al trattamento dei dati personali in Ente.

La Non Conformità rilevata va registrata sul documento apposito del Sistema di Gestione della Qualità per la rilevazione delle Non Conformità nella sezione apposita.

Inoltro al Responsabile

Questo documento, compilato nella parte apposita, datato e siglato, va consegnato al Responsabile, o suo incaricato, a cui spetta l'eventuale valutazione della Non Conformità e/o Reclamo tramite l'accertamento di questi 2 parametri: (A) che la Non Conformità non influisca gravemente sulla qualità del trattamento; (B) che, anche se non grave, questa Non Conformità sia casuale e/o non ripetibile.

Trattamento della NC

Quando si riscontrano problematiche e/o Non Conformità si richiede una loro risoluzione. Nella valutazione secondo quanto riportato precedentemente occorre che il Responsabile, o suo incaricato, provveda alla risoluzione della stessa mediante un'adeguata Azione Correttiva alla fine della quale occorre dare una valutazione di andamento ed effettuare una verifica di risoluzione della problematica e/o Non Conformità.

In caso di soluzione positiva del Problema potrebbe eventualmente occorrere impostare, inoltre, un Azione Preventiva allo scopo di prevenire un eventuale ulteriore e/o sviluppo del Problema.

Le Azioni Correttive da intraprendere sono registrate sul documento apposito del Sistema di Gestione della Qualità nella sezione apposita.

Verifica efficacia

La tipologia di trattamento non conforme, successivamente al trattamento della Non Conformità, verrà sottoposto a ricontrollo.

L'efficacia del trattamento nell'eliminare la Non Conformità deve essere verificata da parte di personale interno abilitato con il controllo documentato, tramite registrazione, da parte del Titolare e/o Responsabile del trattamento dei dati e gli esiti di tale verifica devono essere riportati nell'apposito spazio del documento apposito.

Se negativo il Titolare e/o Responsabile del trattamento dei dati, o suo incaricato, formulerà un'ulteriore proposta di risoluzione, dietro verifica ed approvazione del Titolare e/o Responsabile del trattamento dei dati.

Se positivo il Titolare e/o Responsabile del trattamento dei dati, o suo incaricato, ufficializzerà, con l'apposizione della sua firma sull'apposito documento la chiusura della Azione risolutrice della NC.

RIFERIMENTI

- Mod. AC/AP/GdR.

6.3.7 Gestione delle Azioni Correttive e Preventive

Quando si verifica una problematica e/o Non Conformità si provvede alla valutazione ed alla risoluzione della stessa. Viene valutata la possibilità di individuare azioni per eliminare la causa della problematica e/o Non Conformità al fine di prevenirne il ripetersi (Azione Correttiva su Non Conformità reali).

***Richiesta di Azione Correttiva/Preventiva**:* La Funzione che richiede l'attivazione di una Azione Correttiva e/o Preventiva deve usufruire del documento per la rilevazione delle Non Conformità o documento similare compilando la parte del documento medesimo.

Deve aver cura in particolare di riportare una descrizione idonea del problema che ha generato la richiesta e, quando possibile, di allegare tutta l'eventuale documentazione di supporto che attesti l'importanza del problema. Qualora la Funzione richiedente non sia il Titolare e/o Responsabile del trattamento dei dati, il modulo così compilato deve essere inoltrato allo stesso, o suo incaricato, per la valutazione della natura e dell'entità della N.C.

***Valutazione Richiesta di Azione Correttiva/ Preventiva**:* Ricevuta la richiesta, il Titolare e/o Responsabile del trattamento dei dati, o suo incaricato (con l'eventuale collaborazione delle risorse interessate e/o pertinenti al problema), valuta attentamente la necessità di attivare o meno l'azione, con la sua tipologia e tempistica, di Azione Correttiva e/o Preventiva e procede a valutarne la necessità e/o l'urgenza della stessa.

Nel caso di richiesta non accettata, il Titolare e/o Responsabile del trattamento dei dati, o suo incaricato, deve indicare le motivazioni e comunicarle alla Funzione richiedente.

Attivazione di Azione Correttiva/Preventiva: A richiesta accettata, il Titolare e/o Responsabile del trattamento dei dati, o suo incaricato, valuta la possibilità di procedere autonomamente o di individuare altre funzioni insieme alle quali effettuare un'analisi delle possibili cause del problema presentato e valutare l'adeguata soluzione e formalizza le decisioni sull'apposito documento.

In ogni caso, è necessario riportare sul documento almeno le seguenti informazioni:

- individuazione della possibile causa della non conformità;
- pianificazione generale della soluzione adottata;
- responsabilità dell'attuazione della soluzione adottata;
- definizione dei tempi e delle modalità di verifica dell'efficacia della soluzione adottata.

***Verifica Efficacia di Azione Correttiva/Preventiva**:* Nei tempi e nei modi stabiliti deve essere verificata l'efficacia della soluzione adottata nell'eliminare la causa della non conformità che ha generato l'azione stessa. Gli esiti

di tale verifica e le relative motivazioni devono essere riportate nell'apposito documento del Sistema di Gestione della Qualità, unitamente ai riferimenti ad eventuale documentazione di supporto.

Questo documento viene conservato in ufficio, presso apposita carpetta e/o raccoglitore, dal Responsabile, o suo incaricato.

RIFERIMENTI

- Mod. AC/AP/GdR.

6.4. Manutenzione delle apparecchiature e dei sistemi trattamento dei dati

6.4.1 Manutenzione dei sistemi di elaborazione dei dati

All'Amministratore di sistema (o suo incaricato) è affidato il compito di verificare ogni anno la situazione delle apparecchiature hardware installate con cui vengono trattati dati, delle apparecchiature periferiche, ed in particolare dei dispositivi di collegamento con le reti pubbliche.

Le verifica lo scopo di controllare l'affidabilità del sistema, per quanto riguarda:

- La sicurezza dei dati trattati
- Il rischio di distruzione o di perdita
- Il rischio di accesso non autorizzato o non consentito tenendo conto anche dell'evoluzione tecnologica.

L'Amministratore di sistema deve compilare apposito modulo e/o riportare ciò su carta intestata dell'Ente.

Nel caso in cui esistessero rischi evidenti l'Amministratore di sistema deve informare il Titolare del trattamento e/o il Responsabile perchè siano presi opportuni provvedimenti allo scopo di assicurare il corretto trattamento dei dati in conformità alle norme in vigore.

6.4.2 Manutenzione dei sistemi operativi

All'Amministratore di sistema (o suo incaricato) è affidato il compito di verificare ogni anno la situazione dei sistemi operativi installati sulle apparecchiature con le quali vengono trattati dati.

Le verifica ha lo scopo di controllare l'affidabilità dei sistemi operativi per quanto riguarda la sicurezza dei dati trattati, il rischio di distruzione o di perdita, il rischio di accesso non autorizzato o non consentito tenendo conto in particolare di:

- Disponibilità di nuove versioni migliorative dei sistemi operativi utilizzati;
- Segnalazioni di Patch, Fix o Sistem-Pack per la rimozione di errori o malfunzionamenti;
- Segnalazioni Patch, Fix o Sistem-Pack per l'introduzione di maggiori sicurezze contro i rischi di intrusione o di danneggiamento dei dati.

L'Amministratore di sistema deve compilare apposito modulo interno e/o riportare ciò su carta intestata dell'Ente. Nel caso in cui esistessero rischi evidenti l'amministratore di sistema deve informare il Titolare del trattamento perchè siano presi gli opportuni provvedimenti allo scopo di assicurare il corretto trattamento dei dati in conformità alle norme in vigore.

6.4.3 Manutenzione delle applicazioni software

All'Amministratore di sistema è affidato il compito di verificare ogni anno la situazione delle applicazioni installate sulle apparecchiature con cui vengono trattati dati.

La verifica ha lo scopo di controllare l'affidabilità del software applicativo per quanto riguarda la sicurezza dei dati trattati, il rischio di distruzione o perdita, il rischio di accesso non autorizzato o non consentito tenendo conto in particolare della disponibilità di nuove versioni migliorative delle applicazioni installate che consentano maggiori sicurezza contro i rischi di intrusione o di danneggiamento dei dati.

L'Amministratore di sistema deve compilare apposito modulo interno e/o riportare ciò su carta intestata dell'Ente.

Nel caso in cui esistano rischi evidenti il l'Amministratore di sistema deve informare il Titolare del trattamento perchè siano presi opportuni provvedimenti allo scopo di assicurare il corretto trattamento dei dati in conformità alle norme in vigore.

6.4.4 Dismisssione di strumenti elettronici

Qui di seguito vengono riportati lo stralcio del provvedimento a carattere generale del 13 ottobre 2008 emanato dal Garante sui rifiuti di apparecchiature elettriche ed elettroniche e successivamente alcune metodiche utilizzabili dall'Ente al fine di rispettare quanto in oggetto.

6.4.4.1 Stralcio del provvedimento del 13 ottobre 2008 sui rifiuti di apparecchiature elettriche ed elettroniche

… OMISSIS …

VISTI gli atti d'ufficio relativi alla problematica del rinvenimento di dati personali all'interno di apparecchiature elettriche ed elettroniche cedute a un rivenditore per la dismissione o la vendita o a seguito di riparazioni e sostituzioni; viste, altresì, le recenti notizie di stampa in ordine al rinvenimento da parte dell'acquirente di un disco rigido usato, commercializzato attraverso un sito Internet, di dati bancari relativi a oltre un milione di individui contenuti nel disco medesimo;

VISTO il d.lg. 25 luglio 2005, n. 151 (Attuazione delle direttive 2002/95/Ce, 2002/96/Ce e 2003/108/Ce, relative alla riduzione dell'uso di sostanze pericolose nelle apparecchiature elettriche ed elettroniche, nonché allo smaltimento dei rifiuti), che prevede misure e procedure finalizzate a prevenire la produzione di rifiuti di apparecchiature elettriche e elettroniche, nonché a promuovere il reimpiego, il riciclaggio e altre forme di recupero di tali rifiuti in modo da ridurne la quantità da avviare allo smaltimento (cfr. art. 1, comma 1, lett. a) e b));

CONSIDERATO che l'applicazione della disciplina contenuta nel menzionato d.lg. n. 151/2005, mirando (tra l'altro) a privilegiare il recupero di componenti provenienti da rifiuti di apparecchiature elettriche ed elettroniche (Raee), anche nella forma del loro reimpiego o del riciclaggio in beni oggetto di (nuova) commercializzazione (cfr. in particolare artt. 1 e 3, comma 1, lett. e) ed f), d.lg. n. 151/2005), comporta un rischio elevato di "circolazione" di componenti elettroniche "usate" contenenti dati personali, anche sensibili, che non siano stati cancellati in modo idoneo, e di conseguente accesso ad essi da parte di terzi non autorizzati (quali, ad esempio, coloro che provvedono alle predette operazioni propedeutiche al riutilizzo o che acquistano le apparecchiature sopra indicate);

CONSIDERATO che il "reimpiego" consiste nelle operazioni che consentono l'utilizzo dei rifiuti elettrici ed elettronici o di loro componenti "allo stesso scopo per il quale le apparecchiature erano state originariamente concepite, compresa l'utilizzazione di dette apparecchiature o di loro componenti successivamente alla loro consegna presso i centri di raccolta, ai distributori, ai riciclatori o ai fabbricanti" (art. 3, comma 1, lett. e), d.lg. n. 151/2005) e il "riciclaggio" consiste nel "ritrattamento in un processo produttivo dei materiali di rifiuto per la loro funzione originaria o per altri fini" (art. 3, comma 1, lett. e), d.lg. n. 151/2005);

CONSIDERATO che rischi di accessi non autorizzati ai dati memorizzati sussistono anche in relazione a rifiuti di apparecchiature elettriche ed elettroniche avviati allo smaltimento (art. 3, comma 1, lett. i), d.lg. n. 151/2005);

RILEVATA la necessità di richiamare l'attenzione su tali rischi di persone giuridiche, pubbliche amministrazioni, altri enti e persone fisiche che, avendone fatto uso nello svolgimento delle proprie attività, in particolare quelle industriali, commerciali, professionali o istituzionali (di seguito sinteticamente individuati con la locuzione "titolari del trattamento": art. 4, comma 1, lett. f) del Codice), dismettono sistemi informatici o, più in generale, apparecchiature elettriche ed elettroniche contenenti dati personali (come pure dei soggetti che, su base individuale o collettiva, provvedono al reimpiego, al riciclaggio o allo smaltimento dei rifiuti di dette apparecchiature);

RILEVATO che la disciplina di cui al citato d.lg. n. 151/2005 e alla normativa secondaria che ne è derivata (allo stato contenuta nel d.m. 25 settembre 2007, n. 185, recante "Istituzione e modalità di funzionamento del registro nazionale dei soggetti obbligati al finanziamento dei sistemi di gestione dei rifiuti di apparecchiature elettriche ed elettroniche (Raee)", nell'ulteriore d.m. del 25 settembre 2007, recante "Istituzione del Comitato di vigilanza e di controllo sulla gestione dei Raee", nonché nel d.m. 8 aprile 2008, recante "Disciplina dei centri di raccolta dei rifiuti urbani raccolti in modo differenziato come previsto dall'art. 183, comma 1, lettera cc) del decreto legislativo 3 aprile 2006, n. 152 e successive modifiche") lascia impregiudicati gli obblighi che gravano sui titolari del trattamento relativamente alle misure di sicurezza nel trattamento dei dati personali (e la conseguente responsabilità);

RILEVATO che ogni titolare del trattamento deve quindi adottare appropriate misure organizzative e tecniche volte a garantire la sicurezza dei dati personali trattati e la loro protezione anche nei confronti di accessi non autorizzati che possono verificarsi in occasione della dismissione dei menzionati apparati elettrici ed elettronici (artt. 31 ss. del Codice); ciò, considerato anche che, impregiudicati eventuali accordi che prevedano diversamente, produttori, distributori e centri di assistenza di apparecchiature elettriche ed elettroniche non risultano essere soggetti, in base alla particolare disciplina di settore, a specifici obblighi di distruzione dei dati personali eventualmente memorizzati nelle apparecchiature elettriche ed elettroniche a essi consegnate;

RILEVATO che le misure da adottare in occasione della dismissione di componenti elettrici ed elettronici suscettibili di memorizzare dati personali devono consistere nell'effettiva cancellazione o trasformazione in forma non intelligibile dei dati personali negli stessi contenute, sì da impedire a soggetti non autorizzati che abbiano a vario titolo la disponibilità materiale dei supporti di venirne a conoscenza non avendone diritto (si pensi, ad esempio, ai dati personali memorizzati sul disco rigido dei personal computer o nelle cartelle di posta elettronica, oppure custoditi nelle rubriche dei terminali di comunicazione elettronica);

CONSIDERATO che tali misure risultano allo stato già previste quali misure minime di sicurezza per i trattamenti di dati sensibili o giudiziari, sulla base delle regole 21 e 22 del disciplinare tecnico in materia di misure minime di sicurezza che disciplinano la custodia e l'uso dei supporti rimovibili sui quali sono memorizzati i dati, che

vincolano il riutilizzo dei supporti alla cancellazione effettiva dei dati o alla loro trasformazione in forma non intelligibile;

RITENUTO che i titolari del trattamento, in occasione della dismissione delle menzionate apparecchiature elettriche ed elettroniche, qualora siano sprovvisti delle necessarie competenze e strumentazioni tecniche per la cancellazione dei dati personali, possono ricorrere all'ausilio o conferendo incarico a soggetti tecnicamente qualificati in grado di porre in essere le misure idonee a cancellare effettivamente o rendere non intelligibili i dati, quali centri di assistenza, produttori e distributori di apparecchiature che attestino l'esecuzione di tali operazioni o si impegnino ad effettuarle;

RITENUTO che chi procede al reimpiego o al riciclaggio di rifiuti di apparecchiature elettriche ed elettroniche o di loro componenti debba comunque assicurarsi dell'inesistenza o della non intelligibilità di dati personali sui supporti, acquisendo, ove possibile, l'autorizzazione a cancellarli o a renderli non intelligibili;

CONSIDERATO che, ferma restando l'adozione di ulteriori opportune cautele volte a prevenire l'indebita acquisizione di informazioni personali, anche fortuita, da parte di terzi, le predette misure, suscettibili di aggiornamento alla luce dell'evoluzione tecnologica, possono in particolare consistere, a seconda dei casi, anche nelle procedure di cui agli allegati documenti, che costituiscono parte integrante del presente provvedimento;

RITENUTA la necessità di curare la conoscenza tra il pubblico della disciplina rilevante in materia di trattamento dei dati personali e delle relative finalità, nonché delle misure di sicurezza dei dati (art. 154, comma 1, lett. h), del Codice), con riferimento alla dismissione di apparecchiature elettriche ed elettroniche, anche attraverso la pubblicazione del presente provvedimento sulla Gazzetta Ufficiale della Repubblica Italiana;

… OMISSIS …

TUTTO CIÒ PREMESSO IL GARANTE

1. ai sensi dell'art. 154, comma 1, lett. h) del Codice, richiama l'attenzione di persone giuridiche, pubbliche amministrazioni, altri enti e persone fisiche che, avendone fatto uso nello svolgimento delle proprie attività, in particolare quelle industriali, commerciali, professionali o istituzionali, non distruggono, ma dismettono supporti che contengono dati personali, sulla necessità di adottare idonei accorgimenti e misure, anche con l'ausilio di terzi tecnicamente qualificati, volti a prevenire accessi non consentiti ai dati personali memorizzati nelle apparecchiature elettriche ed elettroniche destinate a essere:
   a. reimpiegate o riciclate;
   b. smaltite.

   Tali misure e accorgimenti possono essere attuate anche con l'ausilio o conferendo incarico a terzi tecnicamente qualificati, quali centri di assistenza, produttori e distributori di apparecchiature che attestino l'esecuzione delle operazioni effettuate o che si impegnino ad effettuarle.

   Chi procede al reimpiego o al riciclaggio di rifiuti di apparecchiature elettriche ed elettroniche o di loro componenti è comunque tenuto ad assicurarsi dell'inesistenza o della non intelligibilità di dati personali sui supporti, acquisendo, ove possibile, l'autorizzazione a cancellarli o a renderli non intelligibili.

… OMISSIS …

6.4.4.2 Reimpiego e riciclaggio di rifiuti di apparecchiature elettriche ed elettroniche

In caso di reimpiego e riciclaggio di rifiuti di apparecchiature elettriche ed elettroniche le misure e gli accorgimenti volti a prevenire accessi non consentiti ai dati personali in esse contenuti, adottati nel rispetto delle normative di settore, devono consentire l'effettiva cancellazione dei dati o garantire la loro non intelligibilità.

Tali misure, anche in combinazione tra loro, devono tenere conto degli standard tecnici esistenti e possono consistere, tra l'altro, in:

Misure tecniche preventive per la memorizzazione sicura dei dati, applicabili a dispositivi elettronici o informatici:

1. Cifratura di singoli file o gruppi di file, di volta in volta protetti con parole-chiave riservate, note al solo utente proprietario dei dati, che può con queste procedere alla successiva decifratura. Questa modalità richiede l'applicazione della procedura di cifratura ogni volta che sia necessario proteggere un dato o una porzione di dati (file o collezioni di file), e comporta la necessità per l'utente di tenere traccia separatamente delle parole-chiave utilizzate.
2. Memorizzazione dei dati sui dischi rigidi (hard-disk) dei personal computer o su altro genere di supporto magnetico od ottico (cd-rom, dvd-r) in forma automaticamente cifrata al momento della loro scrittura, tramite l'uso di parole-chiave riservate note al solo utente. Può effettuarsi su interi volumi di dati registrati su uno o più dispositivi di tipo disco rigido o su porzioni di essi (partizioni, drive logici, file-system) realizzando le funzionalità di un c.d. file-system crittografico (disponibili sui principali sistemi operativi per elaboratori elettronici, anche di tipo personal computer, e dispositivi elettronici) in grado di proteggere, con un'unica parola-chiave riservata, contro i rischi di acquisizione indebita delle informazioni registrate. L'unica parola-chiave di volume verrà automaticamente utilizzata per le operazioni di cifratura e decifratura, senza modificare in alcun modo il comportamento e l'uso dei programmi software con cui i dati vengono trattati.

Misure tecniche per la cancellazione sicura dei dati, applicabili a dispositivi elettronici o informatici:

3. Cancellazione sicura delle informazioni, ottenibile con programmi informatici (quali wiping program o file shredder) che provvedono, una volta che l'utente abbia eliminato dei file da un'unità disco o da analoghi supporti di memorizzazione con i normali strumenti previsti dai diversi sistemi operativi, a scrivere ripetutamente nelle aree vuote del disco (precedentemente occupate dalle informazioni eliminate) sequenze casuali di cifre "binarie" (zero e uno) in modo da ridurre al minimo le probabilità di recupero di informazioni anche tramite strumenti elettronici di analisi e recupero di dati.

   Il numero di ripetizioni del procedimento considerato sufficiente a raggiungere una ragionevole sicurezza (da rapportarsi alla delicatezza o all'importanza delle informazioni di cui si vuole impedire l'indebita acquisizione) varia da sette a trentacinque e incide proporzionalmente sui tempi di applicazione delle procedure, che su dischi rigidi ad alta capacità (oltre i 100 gigabyte) possono impiegare diverse ore o alcuni giorni), a secondo della velocità del computer utilizzato.
4. Formattazione "a basso livello" dei dispositivi di tipo hard disk (low-level formatting–LLF), laddove effettuabile, attenendosi alle istruzioni fornite dal produttore del dispositivo e tenendo conto delle possibili conseguenze tecniche su di esso, fino alla possibile sua successiva inutilizzabilità;
5. Demagnetizzazione (degaussing) dei dispositivi di memoria basati su supporti magnetici o magneto-ottici (dischi rigidi, floppy-disk, nastri magnetici su bobine aperte o in cassette), in grado di garantire la cancellazione rapida delle

informazioni anche su dispositivi non più funzionanti ai quali potrebbero non essere applicabili le procedure di cancellazione software (che richiedono l'accessibilità del dispositivo da parte del sistema a cui è interconnesso).

6.4.4.3 Smaltimento di rifiuti elettrici ed elettronici

In caso di smaltimento di rifiuti elettrici ed elettronici, l'effettiva cancellazione dei dati personali dai supporti contenuti nelle apparecchiature elettriche ed elettroniche può anche risultare da procedure che, nel rispetto delle normative di settore, comportino la distruzione dei supporti di memorizzazione di tipo ottico o magneto-ottico in modo da impedire l'acquisizione indebita di dati personali.

La distruzione dei supporti prevede il ricorso a procedure o strumenti diversi a secondo del loro tipo, quali:

- sistemi di punzonatura o deformazione meccanica;
- distruzione fisica o di disintegrazione (usata per i supporti ottici come i cd-rom e i dvd);
- demagnetizzazione ad alta intensità.

6.5. Misure di sicurezza per il trattamento dei dati effettuato con strumenti non automatizzati

6.5.1 Nomina ed istruzione degli incaricati

Per ogni archivio il Titolare e/o il Responsabile del trattamento dei dati deve definire l'elenco degli incaricati autorizzati ad accedervi ed impartire istruzioni tese a garantire un controllo costante nell'accesso degli archivi. Gli Incaricati che trattano atti e documenti contenenti dati personali sono tenuti a conservarli e restituirli al termine delle operazioni.

Qualora i documenti dovessero contenere dati sensibili e/o giudiziari (ai sensi degli articoli 22 e 59 del Decreto Legislativo n. 196 del 2003) gli incaricati sono tenuti a conservarli fino alla restituzione in contenitori muniti di serratura.

L'accesso agli archivi contenenti documenti dove sono presenti dati sensibili è consentito, se previsto, dopo l'orario di chiusura, previa identificazione e registrazione dei soggetti.

6.5.2 Copia degli atti e documenti

Quanto indicato al punto precedente si applica anche a qualunque tipo di copia effettuata sui documenti contenenti dati personali.

7. MODALITÀ DI RIPRISTINO DEI DATI

7.1. Custodia e conservazione dei supporti utilizzati per il back-up dei dati

L'Amministratore di sistema (o suo incaricato) è responsabile della custodia e della conservazione di supporti utilizzati per il back-up dei dati. L'adozione di un efficiente ed efficace sistema di backup, ossia produrre copie di riserva dei dati, è un'attività fondamentale della realtà lavorativa.

I computer, come qualunque altra apparecchiatura hardware, sono soggetti ad usura nel tempo e quindi è probabile che prima o poi si danneggino e causino la perdita dei dati contenuti in essi.

Inoltre, occorre tener presente che l'errore umano è uno dei fenomeni più frequenti, e spesso sono proprio gli operatore a cancellare o modificare inavvertitamente i dati.

E' perciò buona norma eseguire backup frequenti, almeno mensilmente, come previsto dalla legge,o meglio settimanalmente/quotidianamente; benché possa risultare noioso, avere un backup aggiornato a disposizione può salvare l'Ente da spiacevoli conseguenze, soprattutto di carattere legale.

Soluzioni alternative prevedono un sistema di backup automatico, che effettui le operazioni di copia in modo autonomo, una volta identificate le risorse da proteggere. La tecnologia, comunque, mette a disposizione diversi prodotti dalle caratteristiche e dai prezzi adatti alle più svariate esigenze.

E' importante effettuare una valutazione tenendo conto, oltre che delle proprie esigenze, anche di tutti gli altri aspetti relativi alla sicurezza.

La scelta del tipo di supporto hardware da utilizzare per il backup dei dati dipende dai seguenti aspetti:

- dimensione dei dati;
- frequenza di aggiornamento delle copie;
- tempo di ripristino;
- tempo di conservazione delle copie.

E' consigliabile prediligere supporti di tipo removibile come CD, DVD, Hard Disk (interni e/o esterni), Nastri o Pen Drive, da custodire in luoghi appositi ed archiviati in maniera ordinata, in modo da permettere un rapido recupero dei dati in caso di necessità.

Per ogni banca dati, le aree in cui alloggiare le unità di backup devono essere individuate in modo che siano protette, per quanto pratico e ragionevole, da: agenti chimici, fonti di calore, campi magnetici, intrusioni od atti vandalici, incendio, allagamento, furto.

L'accesso ai supporti utilizzati per il back-up dei dati è limitato per ogni banca di dati a:

- Responsabile del trattamento della sicurezza dei dati
- eventuale Responsabile del trattamento di competenza
- Incaricato del trattamento di competenza
- Amministratore di sistema di competenza

7.2 Utilizzo e riutilizzo dei supporti magnetici

Sono considerati supporti di memorizzazione i nastri magnetici, le cassette (cartridge), i dischi magnetici o ottici rimovibili, i CD-ROM che contengono informazioni personali.

I supporti contenenti dati sensibili devono, se possibile, essere marcati con un'opportuna etichetta recante la dicitura: "Contiene dati personali sensibili".

I supporti contenenti dati (eventualmente sensibili) devono essere custoditi in contenitori muniti di serratura.

Se l'Amministratore di sistema (o suo incaricato) decide che i supporti magnetici utilizzati per le copie di back-up delle banche di dati trattate non sono più utilizzabili per gli scopi per i quali erano stati destinati, dove provvedere a farne cancellare il contenuto annullando e rendendo illeggibili le informazioni in esso contenute.

È compito dell'Amministratore di sistema (o suo incaricato) assicurarsi che in nessun caso vengano lasciate copie di back-up delle banche di dati trattate, non più utilizzate, senza che ne venga cancellato il contenuto ed annullate e rese illeggibili le informazioni in esso registrate.

7.1.3 Disaster Recovery

Nell'ipotesi di distruzione o danneggiamento dei dati o degli strumenti elettronici, si predispone apposito piano di ripristino degli stessi, impartendosi le seguenti istruzioni:

a) Avvertire il Titolare e/o il Responsabile del trattamento e l'incaricato che ha in custodia il c.d. di back up nonché i CD contenenti i vari software dell'Ente installati sugli strumenti elettronici;
b) Rivolgersi immediatamente e chiedere l'intervento del tecnico manutentore della ditta eventualmente incaricata sollecitandone al più presto l'assistenza;
c) Reinstallati i programmi danneggiati o distrutti, sempre che non sia necessario sostituire l'intero hardware, provvedere a reinstallare tutti i dati contenuti nel c.d. di back up;
d) Provvedere all'aggiornamento dei sistemi operativi una volta reinstallati;
e) Dare incarico al tecnico manutentore di suggerire ogni altra misura;
f) In ogni caso, viene data esplicita istruzione che il ripristino dei dati e dei sistemi sia effettuato entro e non oltre 7 giorni;
g) Al fine di evitare eventi di perdita e di danneggiamento degli strumenti elettronici e dei dati in essi contenuti, si prevede che per due volte all'anno sia effettuata manutenzione in modo adeguato dal tecnico incaricato (interno e/o esterno).

8. FORMAZIONE DEL PERSONALE

La formazione degli incaricati viene effettuata all'ingresso in servizio, in occasione di cambiamenti di mansioni (che implichino modifiche rilevanti rispetto al trattamento di dati personali), all'installazione di nuovi strumenti per il trattamento dei dati, e comunque con frequenza annuale (almeno per fare il punto sull'evoluzione degli aspetti legati alla sicurezza nel trattamento dei dati personali).

Essa tende a sensibilizzare gli incaricati sulle tematiche di sicurezza, facendo comprendere i rischi che incombono sui dati e le responsabilità (con specificazione delle sanzioni connesse penali e disciplinari) che riguardano il trattamento dei dati personali, sulle misure disponibili per prevenire eventi dannosi e sulle modalità per aggiornarsi sulle misure di sicurezza adottate dal Titolare.

Inoltre, essa tende alla compiuta spiegazione del concetto di quale sia la natura ed il contenuto dei dati sensibili, con l'invito a segnalare eventuali disfunzioni dei sistemi operativi e, in caso di dubbio, di richiedere al titolare se un dato possa avere o meno natura sensibile. La formazione è fatta dal Titolare e/o dal Responsabile del trattamento dei dati o mediante soggetti esterni specializzati.

8.1. Piano di formazione degli incaricati ad effettuare il back-up

Al Responsabile del trattamento dei dati è affidato il compito di verificare ogni anno, entro il 31 marzo, le necessità di formazione del personale incaricato di effettuare periodicamente le operazioni di back-up delle banche di dati trattate.

Per ogni incaricato del trattamento il Responsabile del trattamento dei dati definisce, sulla base dell'esperienza e delle sue conoscenze, ed in funzione anche di eventuali opportunità offerte dall'evoluzione tecnologica, se è necessaria una formazione tecnica adeguata, utilizzando apposito modulo che deve essere trasmesso in copia controllata al Titolare del trattamento.

8.2. Piano di formazione del personale autorizzato al trattamento dei dati

Al Titolare e/o al Responsabile del trattamento dei dati o loro incaricato è affidato il compito di verificare ogni anno, entro il 31 marzo, le necessità di formazione del personale Incaricato del trattamento dei dati con lo scopo di fornire ogni informazione necessaria a migliorare la sicurezza di trattamento dei dati.

Per ogni utente, il Titolare e/o il Responsabile del trattamento dei dati o loro incaricato, definisce, sulla base dell'esperienza e delle sue conoscenze, ed in funzione anche di eventuali variazioni nella normativa, le necessità di formazione, utilizzando apposito modulo che deve essere trasmesso in copia controllata al Titolare del trattamento.

8.3. Gestione della Formazione

E' responsabilità del Titolare e/o del Responsabile del trattamento dei dati mettere a disposizione risorse umane adeguate per attuare e migliorare il Sistema di Gestione del trattamento dei dati. L'adeguatezza di tali risorse deve essere verificata annualmente.

La competenza del personale che esegue attività che possono influenzare il corretto trattamento dei dati viene assicurata attraverso le seguenti modalità:

Definizione delle competenze

I requisiti minimi di competenza del personale si rilevano dalle lettere d'incarico con cui vengono individuati i campi d'azione degli incaricati.

Formazione/addestramento e valutazione

Al fine di assicurare le competenze necessarie, ove carenti, e la consapevolezza della rilevanza e dell'importanza delle attività svolte da ciascuna funzione nel raggiungimento degli obiettivi per la sicurezza dei dati, sono definite opportune attività di formazione/ addestramento.

Generalmente la necessità di addestramento si presenta in questi casi: N.C. ripetute dallo stesso operatore e/o nuove modalità operative utilizzate dall'incaricato.

Tale definizione avviene in diverse fasi:

- ***Annuale***, a seguito dell'analisi delle attività il Titolare e/o il Responsabile e/o il loro incaricato, prepara un **Piano Annuale di Addestramento e Formazione** (o documento similare del Sistema di Gestione della Qualità) dove indica il personale che necessita di addestramento o formazione, la descrizione dell'attività formativa ed i tempi di realizzazione, oltre l'indicazione dell'ente istruttore (interno o esterno alla Ente).
- ***In Process***, è facoltà del Titolare e/o del Responsabile e/o del loro incaricato, anche dietro sollecito di altre funzioni e/o di VII e/o Non Conformità rilevate, prevedere ulteriori esigenze formative, al di là di quelle pianificate, per particolari esigenze che insorgessero nel corso delle attività della Ente. A tal'uopo il Titolare e/o il Responsabile del trattamento dei dati o loro incaricato può seguire l'iter di compilazione del documento apposito in cui tale proposta dovrà essere approvata dal Titolare e/o provvedere (a seguito di mandato da parte della Direzione) alla diretta effettuazione dell'addestramento. In tal caso, per registrare l'effettuazione dell'addestramento sarà utilizzato l'apposito documento.

Le attività approvate dal Titolare possono essere eseguite sia all'interno dell'Ente, nel qual caso è il Titolare e/o il Responsabile del trattamento dei dati o loro incaricato che si preoccupa della organizzazione, sia all'esterno presso strutture dedicate.

In caso di **addestramento** svolto all'**esterno**, sarà cura dell'usufruente farsi rilasciare gli attestati opportuni e consegnarli al Titolare e/o al Responsabile del trattamento dei dati o loro incaricato, al suo rientro.

In caso di **addestramento interno,** le attività di addestramento e formazione andranno registrate dal Titolare e/o dal Responsabile del trattamento dei dati o loro incaricato, su apposito documento di registrazione, in cui verranno riportati i nominativi di tutti i partecipanti al corso, gli argomenti trattati, la durata dello stesso ed indicazioni sulla docenza.

L'eventuale **efficacia** delle attività di formazione e addestramento può essere verificata in modo indiretto mediante la verifica della pratica giornaliera e/o direttamente tramite test.

Sarà eventualmente a carico del Titolare e/o del Responsabile del trattamento dei dati o loro incaricato (nel caso di corsi interni) la valutazione dell'esito del corso ed il grado di apprendimento dei partecipanti, attraverso predisposizione, se ritenuto necessario, di un opportuno questionario di valutazione del corso e dell'apprendimento dei partecipanti.

Qui si riporta un elenco non esaustivo degli argomenti su cui effettuare la formazione programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali.

Essi si possono così riassumere:

- un'analisi dettagliata ed aggiornata delle vigenti disposizioni di legge, con riferimenti anche alle normative europee;
- disposizioni legislative in tema di tutela dei dati e criminalità informatica;
- analisi spiegazione dei ruoli: titolare, responsabile, incaricato, amministratore di sistema, custode delle password, interessato;
- analisi del decreto legislativo 196 del 30.06.2003 e s.m.i. e panoramica sugli adempimenti;
- misure minime ed appropriate di sicurezza con particolare riferimento a: criteri logici, fisici ed organizzativi per la protezione dei sistemi informativi, prevenzione e contenimento del danno, strumenti di protezione hardware e software (in particolare antivirus e misure antihacker), contenitori di sicurezza, sistemi antintrusione, importanza e modalità di realizzazione delle operazioni di backup, ecc. ;
- rischi che incombono sui dati e misure disponibili per prevenire eventi dannosi;
- profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività e delle responsabilità che ne derivano;
- modalità per aggiornarsi sulle misure minime adottate dal titolare;
- istruzioni sull'utilizzo di software per la ricezione di posta elettronica e sulla potenziale pericolosità di apertura di file allegati di messaggi di e-mail, soprattutto da mittenti sconosciuti;
- disposizioni di utilizzo dei soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati;
- disposizioni di prelievo dei soli documenti che vengono loro affidati per lo svolgimento delle operazioni di trattamento;
- disposizioni di buona convivenza in seno all'Ente evitando di pubblicizzare dentro e/o fuori l'Ente situazioni o questioni personali inerenti colleghi;
- istruzioni di riservatezza in merito all'ambito lavorativo: tutto quello che avviene all'interno dell'Ente non deve essere divulgato all'esterno e/o a personale non autorizzato.

Inoltre, per quanto concerne l'utilizzo della mail e/o di internet, i temi (non esaustivi) che possono essere affrontati sono i seguenti:

- se determinati comportamenti non sono tollerati rispetto alla "navigazione" in Internet (ad es., il *download* di *software* o di *file* musicali), oppure alla tenuta di file nella rete interna;
- in quale misura è consentito utilizzare anche per ragioni personali servizi di posta elettronica o di rete, anche solo da determinate postazioni di lavoro o caselle oppure ricorrendo a sistemi di *webmail*, indicandone le modalità e l'arco temporale di utilizzo (ad es., fuori dall'orario di lavoro o durante le pause, o consentendone un uso moderato anche nel tempo di lavoro);
- quali informazioni sono memorizzate temporaneamente (ad es., le componenti di *file* di *log* eventualmente registrati) e chi (anche all'esterno) vi può accedere legittimamente;

- se e quali informazioni sono eventualmente conservate per un periodo più lungo, in forma centralizzata o meno (anche per effetto di copie di *back up*, della gestione tecnica della rete o di *file* di *log*);
- se, e in quale misura, il datore di lavoro si riserva di effettuare controlli in conformità alla legge, anche saltuari o occasionali, indicando le ragioni legittime – specifiche e non generiche – per cui verrebbero effettuati (anche per verifiche sulla funzionalità e sicurezza del sistema) e le relative modalità (precisando se, in caso di abusi singoli o reiterati, vengono inoltrati preventivi avvisi collettivi o individuali ed effettuati controlli nominativi o su singoli dispositivi e postazioni);
- quali conseguenze, anche di tipo disciplinare, il datore di lavoro si riserva di trarre qualora constati che la posta elettronica e la rete Internet sono utilizzate indebitamente;
- le soluzioni prefigurate per garantire, con la cooperazione del lavoratore, la continuità della attività lavorativa in caso di assenza del lavoratore stesso (specie se programmata), con particolare riferimento all'attivazione di sistemi di risposta automatica ai messaggi di posta elettronica ricevuti;
- se sono utilizzabili modalità di uso personale di mezzi con pagamento o fatturazione a carico dell'interessato;
- quali misure sono adottate per particolari realtà lavorative nelle quali debba essere rispettato l'eventuale segreto professionale cui siano tenute specifiche figure professionali.

RIFERIMENTI

- Mod. PAAF
- Mod. AAF
- Mod. SPAF

9. TUTELA DEL LAVORATORE

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

Il luogo di lavoro è una formazione sociale nella quale va assicurata la tutela dei diritti, delle libertà fondamentali e della dignità degli interessati garantendo che, in una cornice di reciproci diritti e doveri, sia assicurata l'esplicazione della personalità del lavoratore e una ragionevole protezione della sua sfera di riservatezza nelle relazioni personali e professionali.

9.1 Codice in materia di protezione dei dati e discipline di settore

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

Discipline di settore - Alcune disposizioni di settore, fatte salve dal Codice, prevedono specifici divieti o limiti, come quelli posti dallo Statuto dei lavoratori sul controllo a distanza. La disciplina di protezione dei dati va coordinata con regole di settore riguardanti il rapporto di lavoro e il connesso utilizzo di tecnologie, nelle quali è fatta salva o richiamata espressamente.

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

a) il principio di *necessità*, secondo cui i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite;
b) il principio di *correttezza*, secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori. Le tecnologie dell'informazione (in modo più marcato rispetto ad apparecchiature tradizionali) permettono di svolgere trattamenti ulteriori rispetto a quelli connessi ordinariamente all'attività lavorativa. Ciò, all'insaputa o senza la piena consapevolezza dei lavoratori, considerate anche le potenziali applicazioni di regola non adeguatamente conosciute dagli interessati;
c) i trattamenti devono essere effettuati per finalità *determinate*, *esplicite* e *legittime*, osservando il principio di *pertinenza* e *non eccedenza*. Il datore di lavoro deve trattare i dati *"nella misura meno invasiva possibile"*; le attività di monitoraggio devono essere svolte solo da soggetti preposti ed essere *"mirate sull'area di rischio, tenendo conto della normativa sulla protezione dei dati e, se pertinente, del principio di segretezza della corrispondenza"*.

9.2 Controlli e correttezza nel trattamento

In base al richiamato principio di correttezza, l'eventuale trattamento deve essere ispirato ad un canone di trasparenza, come prevede anche la disciplina di settore.

Grava quindi sul datore di lavoro l'onere di indicare in ogni caso, chiaramente e in modo particolareggiato, quali siano le modalità di utilizzo degli strumenti messi a disposizione ritenute corrette e se, in che misura e con quali

modalità vengano effettuati controlli. Ciò, tenendo conto della pertinente disciplina applicabile in tema di informazione, concertazione e consultazione delle organizzazioni sindacali.

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

10. TRATTAMENTO DEI DATI AFFIDATI ALL'ESTERNO

10.1 Trattamento dei dati in out-sourcing

Il Titolare del trattamento può decidere di affidare il trattamento dei dati in tutto o in parte a soggetti terzi, in out-sourcing, nominandoli Responsabili del trattamento.

In questo caso debbono essere specificati i soggetti interessati ed i luoghi dove fisicamente avviene il trattamento dei dati stessi.

Nel caso in cui questi non vengano espressamente nominati, i responsabili del trattamento in out-sourcing devono intendersi autonomi titolari del trattamento e quindi soggetti ai corrispettivi obblighi, e pertanto rispondono direttamente ed in via esclusiva per le eventuali violazioni alla legge.

Il Titolare e/o il Responsabile del trattamento dei dati o loro incaricato, cui è affidato tale specifico incarico, deve redigere e aggiornare ad ogni variazione l'elenco dei soggetti che effettuano il trattamento dei dati in qualità di responsabile del trattamento, con particolare attenzione a quei soggetti che effettuano il trattamento dei dati in qualità di Responsabile del trattamento, con particolare attenzione a quei soggetti terzi in out-sourcing, ed indicare per ognuno di essi il tipo di trattamento effettuato. Per l'inventario dei soggetti terzi, in out-soucing, deve essere utilizzato apposito modulo, che deve essere conservato a cura del Responsabile del trattamento in luogo apposito.

Nel caso di servizi di amministrazione di sistema affidati in outsourcing il titolare deve conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema.

10.2 Criteri per la scelta degli Enti Terzi a cui affidare il trattamento dei dati in out-sourcing

Il Titolare del trattamento può nominare Responsabile del trattamento in out-sourcing quei soggetti terzi che abbiano i requisiti di esperienza, capacità, affidabilità.

Il Responsabile del trattamento dei dati in out-sourcing deve rilasciare una dichiarazione scritta al Titolare del trattamento da cui risulti che sono state adottate le misure di sicurezza per il trattamento dei dati secondo quanto disposto dal D. Lgs. n. 196/2003.

In special modo se venga affidato a soggetti esterni il trattamento di dati sensibili, per avere la garanzia che essi adottano le misure minime di sicurezza.

Alle ditte che provvedano ad effettuare eventuali prestazioni che comportano accesso di estranei all'Ente, viene dato incarico scritto con richiesta di specificazione dei nominativi delle persone che accedono ad espresso invito a limitarsi alle sole attività pertinenti alla prestazione per cui accedono.

10.3 Nomina del responsabile del trattamento dei dati in out-sourcing

Per ogni trattamento affidato ad un soggetto esterno nominato Responsabile del trattamento in out-sourcing, il Titolare del trattamento deve assicurarsi che siano rispettate le norme di sicurezza di un livello non inferiore a quello stabilito per il trattamento interno.

Il Titolare del trattamento deve informare il Responsabile del trattamento dei dati in out-sourcing dei compiti che gli sono affidati in relazione a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dal D. Lgs. n. 196/2003.

Il Responsabile del trattamento dei dati in out-sourcing deve accettare la nomina, utilizzando apposito modulo.

La nomina del Responsabile del trattamento dei dati in out-sourcing deve essere controfirmata per accettazione e copia della lettera di nomina accettata deve essere conservata cura del Titolare del trattamento in luogo sicuro.

11. CIFRATURA DEI DATI

In seno all'attività lavorativa si trattano con strumenti informatici dati idonei a rilevare lo stato di salute e/o la vita sessuale e/o di natura sindacale del personale, nonché dati sensibili dell'utenza, per cui il Titolare e/o Responsabile del trattamento dei dati e/o l'Amministratore di Sistema provvede a individuare, laddove non già previsto dal sistema informatico in uso, i criteri da adottare per la cifratura o per la separazione dei dati personali mediante apposita registrazione su carta intestata dell'Ente.

12. REVISIONE DEL DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Il presente documento programmatico sulla sicurezza aggiornato nel presente mese verrà revisionato annualmente entro il 31 marzo ed eventualmente sottoposto modifiche, qualora trascorso il periodo intercorrente tra la data di stesura e la data su indicata si siano verificate eventuali variazioni del livello di rischio e/o di trattamenti effettuati dall'Ente a cui sono soggetti i dati personali e/o eventuali modifiche della tecnologia informatica.

L'intero documento è da considerarsi un documento dinamico che dovrà essere adottato contestualmente all'evoluzione organizzativa ed agli eventuali cambiamenti riscontrabili nell'Ente. Pertanto sarà opportuno porre in revisione tutto il sistema di gestione interna della sicurezza dei dati almeno una volta l'anno. Nell'attesa dell'adeguamento conservano validità le regole in vigore.

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

Una sua copia potrà eventualmente essere consegnata, previa autorizzazione del Titolare del trattamento e/o del Responsabile del trattamento dei dati:

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

13. GLOSSARIO

A	
Autenticazione Informatica	Insieme di strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità.
B	
Banca dati	Qualsiasi complesso organizzato di dati personali, ripartiti in uno o più unità dislocate in uno o più siti.
Blocco	La conservazione dei dati personali con sospensione temporanea di ogni altra operazione del trattamento.
C	
Comunicazione	Il dare conoscenza dei dati personali o uno soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa disposizione o consultazione.
Comunicazione elettronica	Ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un abbonato o utente ricevente, identificato o identificabile.
Correttezza del trattamento dei dati personali (criterio)	Ha la funzione di regolare l'interazione tra sfere di interessi generata dal trattamento dei dati personali, per garantire un controllo su eventuali condotte abusive
Credenziali di autenticazione	I dati e di dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica.
D	
Dati giudiziari	I dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.
Dati identificativi	I dati personali che permettono l'identificazione diretta dell'interessato.
Dati relativi al traffico	Qualsiasi dato sottoposto al trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione
Dati relativi all'ubicazione	Ogni dato trattato in una rete di comunicazione elettronica che indica la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico
Dati sensibili	I dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico sindacale, nonché i dati per personali idonei a rivelare lo stato di salute e la vita sessuale.
Dato anonimo	Il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile.
Dato personale	Qualunque informazione relativa a persona fisica, persona giuridica, ente o associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.
Diffusione	Il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa disposizione o consultazione.
G	
Garante	Il Garante opera in piena autonomia e con indipendenza di giudizio e di valutazione. Il Garante è organo collegiale costituito da quattro componenti, eletti due dalla Camera dei Deputati e due dal Senato della Repubblica con voto limitato. I componenti sono scelti tra

	persone che assicurano indipendenza e che sono esperti di riconosciuta competenza delle materie del diritto o dell'informatica, garantendo la presenza di entrambe le qualificazioni.
I	
Identità personale	Consiste nel complesso delle attività pubbliche del soggetto, rilevanti per la connotazione della sua personalità.. L' essenza dell'identità personale è nel diritto dell'individuo a non veder modificato, offuscato o comunque alterato (attraverso i trattamenti dei dati personali) il proprio patrimonio intellettuale, ideologico, etico, professionale, quale estrinsecatosi nell'ambiente sociale in cui vive.
Incaricati	Le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile
Interessato	La persona fisica, la persona giuridica, l'ente o associazione cui si riferiscono i dati personali
Interpello preventivo	Salvi i casi in cui il decorso del termine esporrebbe taluno a pregiudizi imminenti ed irreparabili, il ricorso al Garante può essere proposto sono dopo che è stata avanzata richiesta sul medesimo oggetto titolare o al responsabile, e sono decorsi i termini previsti dal presente articolo, ovvero è stato opposto alla ed alla richiesta un diniego anche parziale.
L	
Liceità del trattamento dei dati personali (criterio)	Ha la funzione di selezionare gli interessi meritevoli di tutela costituiti dal rispetto dei diritti delle libertà fondamentali, dalla dignità dell'interessato, dalla riservatezza, dal identità personale e dal diritto alla protezione dati personali. Gli interessi meritevoli di tutela, che fondano il giudizio di liceità, non sono solo quelli di cui all'art. 2 del TUP, ma anche quelli contenuti in altre norme che, al di fuori del TUP, salvaguardano gli interessi connessi al trattamento dei dati personali. La liceità quindi costituisce un limite all'autonomia sia del titolare del trattamento dati, sia dell'interessato, allo scopo di rendere tale autonomia compatibile con rispetto degli interessi - del soggetto cui i dati si riferiscono, dei terzi ed anche della collettività - individuati nel TUP e nelle altre norme di legge.
M	
Misure minime	Il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi
N	
Necessità (principio di)	I sistemi informativi e di programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettono di identificare l'interessato solo in caso di necessità
P	
Parola chiave	Componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o da altri dati in forma elettronica
Posta elettronica	Messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente, fino a che ricevente non ha preso conoscenza
Profilo di autorizzazione	Insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti
Protezione dei dati personali (diritto alla)	Ha come finalità la regolamentazione di un'attività pericolosa che altri soggetti compiono su informazioni che ci riguardano (ed ha carattere di garanzia da altrui abusi)
R	
Reclamo	Il reclamo contiene un'indicazione per quanto possibile dettagliata dei fatti e delle circostanze su cui si fonda, delle disposizioni che si considerano violate e delle misure richieste, nonché gli estremi identificativi del titolare, del responsabile, ove conosciuto, e dell'istante. Il reclamo è sottoscritto dagli interessati, o da associazioni che li rappresentano ed è presento al Garante senza particolari formalità.

	Il reclamo reca in allegato la documentazione utile ai fini della sua valutazione e l'eventuale procura, e indica un recapito per l'invio di comunicazioni anche tramite posta elettronica, telefax o telefono
Reclamo (procedimento)	Esauriti all'istruttoria preliminare, sei reclamo non è manifesta mentre infondate sussistano i presupposti prodotta il provvedimento, il garante, anche prima della definizione procedimento: a. prima di descrivere le misure di cui alla lettera b), ove il divieto il blocco ai sensi del lettera c), può invitare il titolare, anche in contraddittorio con l'interessato, ad effettuare il blocco spontaneamente; b. prescrive al titolare le misure opportune o necessarie per rendere il trattamento conforme alle disposizioni vigenti; c. dispone il blocco o vieta, in tutto o in parte, il trattamento che risulta illecito o non corretto anche per effetto della mancata adozione delle misure necessarie di cui alla lettera b), oppure quando, in considerazione della natura dei dati o, comunque, delle modalità del trattamento o degli effetti che esso può determinare, vi è il concreto rischio di verificarsi di un pregiudizio rilevante per uno o più interessati; d. può vietare in tutto o in parte il trattamento di dati relativi a singoli soggetti che si pone in contrasto con rilevanti interessi della collettività.
Responsabile	La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento dei dati personali.
Rete pubblica di Comunicazioni	Una rete di comunicazioni elettroniche utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico.
Reti di comunicazione elettronica	I sistemi di trasmissione, le apparecchiature di commutazione o di instradamento e altre risorse che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, incluse le reti satellitari, le reti terrestri mobili e fisse a commutazione di circuito ed a commutazione di pacchetto, compresa Internet, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui sono utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazioni trasportato.
Ricorso	Il ricorso è proposto nei confronti del titolare e indica: a. gli estremi identificativi del ricorrente, dell'eventuale procuratore speciale, del titolare e, ove conosciuto, del responsabile eventualmente designato per il ricorso dell'interessato in caso di esercizio dei diritti di cui all'art. 7 del Codice; b. la data della richiesta presentata al titolare o al responsabile ai sensi dell'art. 8, comma 1, del Codice oppure del pregiudizio imminente ed irreparabile che permette di prescindere dalla richiesta medesima; c. gli elementi posti a fondamento della domanda; d. il provvedimento richiesto al Garante; e. il domicilio eletto ai fini del procedimento.
Riservatezza	Attiene al complesso delle vicende private del soggetto, sottratte all'altrui scrutinio. È quindi una specificazione del diritto all'intimità privata, inteso come esigenza dell'uomo al godimento pieno ed esclusivo, della intimità della propria persona e delle proprie azioni.
	S
Scopi scientifici	Le finalità di studio e di indagine sistematica finalizzata allo sviluppo delle conoscenze scientifiche in uno specifico settore.
Scopi statistici	Le finalità di indagine statistica o di produzione di risultati statistici, anche a mezzo di sistemi informativi statistici.
Scopi storici	Le finalità di studio, indagine, ricerca e documentazione di figure, fatti e circostanze del passato.
Segnalazione	Atto che ha lo scopo, se non è possibile presentare un reclamo circostanziato, di sollecitare un controllo da parte del Garante sulla disciplina rilevante in materia di trattamento dati personali.
Servizio a valore aggiunto	Il servizio che richiede il trattamento dei dati relativi al traffico o dei dati relativi all'ubicazione diversi dai dati relativi al traffico, oltre a quanto è necessario per la trasmissione di una comunicazione o della relativa fatturazione.

Servizio di comunicazione elettronica	I servizi consistenti esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazione elettroniche, compresi i servizi di trasmissione nelle reti utilizzate per la diffusione circolare radiotelevisiva, nei limiti previsti dall'art. 2, lettera c), della direttiva 2002/21/CE del Parlamento Europeo e del Consiglio, del 7 marzo 2002.
Sicurezza	È tutto ciò che riguarda la protezione dei beni dello studio professionale e dell'impresa. L'obiettivo della sicurezza in particolare è proteggere il valore che i beni costituiscono per l'attività professionale ed imprenditoriale.
Sistema di autorizzazione	L'insieme di strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.
Sistema informativo	È un sottosistema del sistema organizzativo che gestisce le informazioni necessarie per il perseguimento degli scopi dell'Ente. Il concetto di "sistema informativo" è indipendente dalla sua automatizzazione: il sistema informatico costituisce la porzione automatizzata del sistema informativo che gestisce informazioni con tecnologia informatica.
Sistema organizzativo	È un insieme di risorse e regole per lo svolgimento coordinato di attività/processi al fine del perseguimento degli scopi propri dell'attività imprenditoriale e professionale.
Strumenti elettronici	Gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento.
	T
Titolare	La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo di sicurezza.
Trattamento	Qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'Ente, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca dati.
	U
Utente	Qualsiasi persona fisica che utilizza un servizio di comunicazione elettronica accessibile al pubblico, per motivi privati o commerciali, senza esservi necessariamente abbonata.

Parere - 21 gennaio 2010
Bollettino del n. 112/gennaio 2010
[doc. web n. 1694419]
Pubblicità degli incarichi conferiti dalle amministrazioni pubbliche - 21 gennaio 2010

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vice presidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti e del dott. Daniele De Paoli, segretario generale reggente;

VISTA la richiesta di parere del Ministro per la pubblica amministrazione e l'innovazione;

VISTO l'art. 154, commi 4 e 5, del Codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003, n. 196);

VISTA la documentazione in atti;

VISTE le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

RELATORE il prof. Francesco Pizzetti;

PREMESSO

Con nota del Capo di Gabinetto del Ministro per la pubblica amministrazione e l'innovazione è stato richiesto il parere del Garante – di cui si dovrà dare menzione nel preambolo - in ordine a uno schema di regolamento recante "determinazione dei limiti massimi del trattamento economico onnicomprensivo a carico della finanza pubblica per i rapporti di lavoro dipendente o autonomo", in attuazione delle disposizioni di cui ai commi da 44 a 52-bis dell'articolo 3 della legge 24 dicembre 2007, n. 244 (infra: legge finanziaria per il 2008).

Il provvedimento in esame - adottato ai sensi dell'articolo 17, comma 2, della legge 23 agosto 1988, n. 400 - disciplina il limite massimo delle retribuzioni e degli emolumenti direttamente o indirettamente erogati a carico delle pubbliche finanze per i rapporti di lavoro dipendente o autonomo. In particolare, lo schema di regolamento – ferma restando la disciplina speciale prevista per la Banca d'Italia e le "altre Autorità indipendenti" - individua, in conformità alla norma primaria, i "soggetti conferenti" gli emolumenti e le retribuzioni nei seguenti: amministrazioni statali di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165; agenzie; enti pubblici economici e non economici; enti di ricerca; università; società non quotate a totale o prevalente partecipazione pubblica e le loro controllate.

Lo schema di regolamento definisce, inoltre, in modo puntuale l'ambito dei soggetti destinatari delle retribuzioni e degli emolumenti, comprendendo in tale categoria coloro che percepiscono somme in virtù di contratti d'opera di natura continuativa, di contratti di collaborazione coordinata e continuativa ovvero di collaborazione a progetto, individuando altresì – salve le eccezioni specificamente delineate - il tetto massimo annuale delle retribuzioni e degli emolumenti nella somma corrispondente al trattamento economico annuale complessivo spettante per la carica di Primo Presidente della Corte di Cassazione.

RILEVATO

1. Di particolare interesse sotto il profilo della protezione dei dati personali risulta il solo articolo 5 del provvedimento in esame, che obbliga il soggetto conferente a pubblicare sul proprio sito istituzionale ogni conferimento riconducibile alla disciplina prevista dal regolamento, specificando il tipo di incarico, la durata, il compenso previsto e il nominativo del soggetto destinatario, nonché tutti gli altri eventuali "incarichi, rapporti o simili" comunicati dal destinatario. Ai sensi del comma 2 dello stesso articolo 5, infatti, il destinatario è tenuto a comunicare al soggetto conferente tutti gli incarichi in corso, al fine di accertare il limite massimo annuale. Sul punto è opportuno rilevare come, ai sensi del comma 44 dell'articolo 3 della legge finanziaria per il 2008, la pubblicazione dell'atto di spesa sul sito dell'Amministrazione o del soggetto interessato costituisce condizione indispensabile per l'attuazione del medesimo atto.

La disciplina sancita dal Codice in materia di protezione dei dati personali consente la diffusione di dati personali, da parte di soggetti pubblici, in presenza di una norma di legge o di regolamento che preveda espressamente tale

trattamento (art. 19, comma 3) e, da parte di soggetti privati ed enti pubblici economici, anche in assenza del consenso dell'interessato, qualora ciò sia necessario per adempiere a un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria (art. 24, comma 1, lettera a).

Pertanto, in relazione alle fattispecie riconducibili alla disciplina di cui all'articolo 3, commi da 44 a 52-bis, della legge finanziaria per il 2008 e allo schema di regolamento in esame, la normativa in materia di protezione dei dati personali non osta alla pubblicazione dei dati personali previsti dal medesimo regolamento, mediante inserzione sul sito del soggetto conferente e comunque con modalità idonee a rispettare i principi di cui all'articolo 11 del Codice, con particolare riferimento alla conservazione dei dati per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti.

2. Al fine di evitare interpretazioni del dettato normativo di volta in volta difformi, si richiama altresì l'attenzione dell'Amministrazione sull'opportunità di chiarire se l'obbligo di pubblicità degli eventuali "incarichi, rapporti o simili" comunicati dal destinatario, ai sensi dell'articolo 5, comma 2, dello schema di regolamento, riguardi anche il compenso ricevuto ovvero esclusivamente la natura e il contenuto del rapporto.

3. In relazione all'informativa di cui all'ultimo capoverso del modulo di comunicazione trasmesso unitamente allo schema di regolamento, si ravvisa la necessità di integrarne il contenuto con riferimento alla possibilità che i dati conferiti siano pubblicati sul sito del soggetto conferente secondo le modalità normativamente previste, al fine di rendere l'informativa pienamente conforme al disposto di cui all'articolo 13 del Codice.

IL GARANTE

esprime parere favorevole sullo schema di regolamento recante "determinazione dei limiti massimi del trattamento economico onnicomprensivo a carico della finanza pubblica per i rapporti di lavoro dipendente o autonomo", con le seguenti osservazioni:

a) valuti l'Amministrazione l'opportunità di chiarire se l'obbligo di pubblicità degli eventuali "incarichi, rapporti o simili" di cui all'articolo 5, comma 1, dello schema di regolamento, riguardi anche il compenso ricevuto ovvero esclusivamente la natura e il contenuto del rapporto;

b) si integri il contenuto dell'informativa di cui all'ultimo capoverso del modulo di comunicazione trasmesso unitamente allo schema di regolamento, con riferimento alla possibilità che i dati conferiti siano pubblicati sul sito del soggetto conferente secondo le modalità normativamente previste.

Roma, 21 gennaio 2010
IL PRESIDENTE Pizzetti
IL RELATORE Pizzetti
IL SEGRETARIO GENERALE REGGENTE De Paoli

Ordinanza ingiunzione / Revoca - 23 settembre 2010
Bollettino del n. 119/settembre 2010
[doc. web n. 1771632]
Ordinanza di ingiunzione nei confronti di Regione Puglia - 23 settembre 2010
Registro delle deliberazioni Del. n. 45 del 23 settembre 2010

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, alla presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vicepresidente, del dott. Giuseppe Fortunato, componente e del dott. Daniele De Paoli, segretario generale;

ESAMINATO il rapporto dell'Ufficio del Garante per la protezione dei dati personali predisposto ai sensi dell'art. 17 della legge 24 novembre 1981, n. 689, relativo al verbale di contestazione per violazione amministrativa redatto in data 1° ottobre 2009 nei confronti della Regione Puglia, con sede in Bari Lungomare Nazario Sauro n. 33, per la violazione

dell'art. 22 in relazione all'art. 164 bis, comma 3 del Codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2006, n. 196, di seguito denominato "Codice");

CONSIDERATO il provvedimento di divieto del Garante datato 17 settembre 2009 e adottato ai sensi dell'art. 154, comma 1, lettera *d*), del Codice, dal quale è emerso che, anche a fronte di quanto già rilevato con analogo provvedimento dell'Autorità datato 18 gennaio 2007, la Regione, pubblicando dati idonei a rilevare lo stato di salute di soggetti disabili nel bollettino Ufficiale datato 11 aprile 2006 n. 45, li rende liberamente consultabili anche tramite i propri siti istituzionali con particolare riferimento all'indirizzo http://www.regione.puglia.it/....., in violazione di quanto disposto dall'art. 22, comma 8, del Codice;

VISTO il verbale n. 21326/64444 del 1° ottobre 2009 con cui è stata contestata alla predetta Regione la violazione prevista dall'art. 162, comma 2-*bis* in combinato disposto con l'art. 164-*bis*, comma 3, del Codice, informandola della facoltà di effettuare il pagamento in misura ridotta ai sensi dell'art. 16 della legge n. 689/1981;

RILEVATO dal predetto rapporto che non risulta essere stato effettuato il pagamento in misura ridotta;

VISTO lo scritto difensivo inviato ai sensi dell'art. 18 della legge n. 689/1981 nel quale la Regione ha rilevato che:

- dall'esame dei provvedimenti dell'Autorità datati 18 gennaio 2007 e 17 settembre 2009 si osserva come il fatto che ha determinato la violazione amministrativa contestata possa consistere *"(…) nella pubblicazione degli elenchi e delle graduatorie del bollettino Ufficiale della Regione Puglia dell'11 aprile 2006 n. 45"* ovvero *"(…) nella pubblicazione degli elenchi e delle graduatorie contenuti nel BURP nel sito istituzionale della Regione Puglia"*. In entrambe i casi la contestazione appare illegittima atteso che *"(…) l'Autorità avrebbe dovuto e potuto chiedere alla Regione la rimozione della pagina http://www.regione.puglia.it/... di cui al provvedimento di settembre 2009, già con provvedimento di gennaio 2007. Allo stesso modo già con provvedimento (gennaio 2007), avrebbe potuto prescrivere alla Regione quanto ha poi stabilito nel secondo provvedimento (settembre 2009), ossia il divieto di diffusione dei dati illecitamente trattati mediante la consultazione in qualsiasi forma del citato BURP e non soltanto mediante consultazione di una specifica pagina web"*;
- si rileva poi che *"(…) il procedimento amministrativo che ci occupa si è concluso oltre il termine di 90 gg previsto dalle disposizioni applicabili"*, atteso che il *dies a quo* dal quale far decorrere i 90 giorni del termine previsto, deve essere individuato nel 14 luglio 2009, data di notifica all'Autorità del ricorso presentato dal sig. XY;
- inoltre, il provvedimento del 17 settembre 2009 riporta impropriamente che alla pagina web http://www.regione.puglia.it/... sarebbero stati pubblicati i *"documenti relativi agli elenchi e alle graduatorie di disabili già oggetto del provvedimento del 18 gennaio 2007"*, atteso che, come si evince dalla documentazione prodotta, risultano invece pubblicate solo una parte delle predette graduatorie ovvero quelle relative alle disabilità motorie;
- sulla quantificazione del pagamento in misura ridotta, poi, si osserva come l'importo indicato per l'oblazione della sanzione contestata (80.000,00 euro) è errato, considerato che l'ammontare della sanzione edittale, ai sensi del combinato disposto degli artt. 162, comma 2-*bis* modificato dalla legge 20 novembre 2009 n 166 e 164-bis, comma 3, del Codice, determina una sanzione (da euro 20.000,00 a euro 240.000,00) definibile in via breve con il pagamento di quarantamila euro (40.000,00);
- nel caso di specie, inoltre, *"(…) le sanzioni applicabili (…) dovrebbero essere quelle che erano vigenti al tempo del verificarsi della condotta illecita in virtù del principio di irretroattività e legalità previsto dall'art. 1 della legge 689/1981 (…)"*, facendo quindi risalire l'azione commissiva che ha generato l'illecito contestato *"(…) all'11 aprile 2006, ossia alla data di pubblicazione del Bollettino Ufficiale della Regione Puglia n. 45 (…)"*. Peraltro, qualora quello contestato fosse qualificato come illecito amministrativo di carattere "permanente", troverebbero applicazione i principi già statuiti dalla Corte di Cassazione Sez. lavoro n. 4119 del 17 aprile 1991 (secondo cui nel campo delle violazioni amministrative, in ipotesi di successione di leggi, opera il principio penalistico della norma più favorevole al reo) e dal Tar. Toscana n. 702 del 7 dicembre 1996 (per il quale deve ritenersi contenuto nella legge n. 689/1981 il principio dell'applicazione della sanzione più favorevole al reo di cui all'art. 2, 3° comma c.p., quand'anche la violazione amministrativa si configuri quale illecito permanente);

- sulla quantificazione dell'eventuale sanzione pecuniaria, rileva come una più attenta valutazione dei criteri di cui all'art. 11 della legge n. 689/1981, considerati anche alla luce della condotta tenuta dalla Regione nonché della pregevole attività sociale nel corso della quale sarebbe stata commessa la violazione, dovrebbe condurre *"(…) ove non si dovesse disporre l'archiviazione degli atti, all'applicazione di una sanzione pecuniaria quanto più prossima ai minimi edittali"*. Sul punto, poi, preme sottolineare come, se si è ritenuta l'applicazione delle ipotesi aggravate di cui all'art. 164-bis, comma 3, nessuna valutazione è stata fatta circa lo svolgimento, da parte della Regione *"(…) di una attività sociale meritevole di tutela quale quella relativa ad un bando pubblicato dall'assessorato alla solidarietà (…) rivolto a soggetti disabili (…)"*, ai fini dell'applicazione dei casi di minore gravità di cui all'art. 164-*bis*, comma 1;

RITENUTO che le argomentazioni addotte non risultano idonee ad escludere la responsabilità in ordine a quanto contestato poiché:

- il fatto che ha determinato l'adozione dei provvedimenti di divieto del 2007 e del 2009 è rappresentato dalla diffusione dei dati personali idonei a rivelare lo stato di salute degli interessati disabili; ai fini della qualificazione giuridica del fatto non rilevano le modalità con le quali tale diffusione avviene. D'altro canto, quelli in argomento, sono provvedimenti inibitori dell'Autorità che, sulla base dell'art. 154, comma 1, lett. *d*), del Codice, il Garante può adottare in via d'urgenza, anche d'ufficio, in tutti i casi in cui, come quello di specie, sussiste il rischio di un pregiudizio rilevante per gli interessati;
- l'accertamento della violazione amministrativa (*dies a quo*), disciplinato dall'art. 13 della legge n. 689/1981, consiste nel rilievo di fatti integranti un illecito amministrativo che implica anche una necessaria valutazione e qualificazione dei fatti. A tal fine è stato, pertanto, avviato un procedimento amministrativo *ex* art. 143 del Codice i cui esiti hanno condotto all'adozione del provvedimento inibitorio del 17 settembre 2009. E' proprio nel momento dell'adozione del provvedimento da parte del Garante che si determina la qualificazione giuridica del fatto da cui origina l'autonomo procedimento sanzionatorio. Come infatti chiaramente indicato nell'atto di avvio di detto procedimento (contestazione), l'accertamento della violazione è ricondotto alle motivazioni riportate nel provvedimento del 17 settembre 2009, che è stato coerentemente notificato al contravventore in data 15 ottobre 2009, ovvero entro i termini previsti dall'art. 13 della legge n. 689/1981. Del resto, come già ribadito dalla Corte di cassazione (ex multis Cass. Sez. II n. 12830/2006), *"(…) l'attività di accertamento dell'illecito non coincide con il momento in cui viene acquisito il fatto nella sua materialità, ma deve essere intesa come comprensiva del tempo necessario alla valutazione dei dati acquisiti e afferenti agli elementi (soggettivi e oggettivi) dell'infrazione (…)"*;
- con riferimento all'indicazione delle graduatorie che risultano ancora pubblicate nel 2009 e di cui al provvedimento del 17 settembre 2009, anche accogliendo la precisazione formulata dalla Regione negli scritti difensivi circa la presenza solo delle graduatorie delle persone con disabilità motorie ossia, come precisato, soltanto le ultime 4 delle 12 graduatorie richiamate nel provvedimento, resta impregiudicato il fatto che, per sua stessa ammissione, l'Ente ha diffuso dati idonei a rivelare lo stato di salute di un cospicuo numero di soggetti (circa 2.800) affetti da disabilità motorie. Quanto dedotto, quindi, non influisce sul procedimento logico del provvedimento che ha accertato l'illiceità del trattamento e la violazione da cui origina la contestazione; né appare idonea a modificare sostanzialmente le valutazioni alla base della contestazione della sanzione nella forma aggravata di cui all'art. 164-*bis*, comma 3, atteso che la violazione coinvolge un numero di interessati che, anche se ridotto rispetto a quello originariamente ritenuto (4.500), resta comunque particolarmente elevato;
- il carattere di "permanenza" dell'illecito contestato deriva dal fatto che la Regione, così come accertato dal provvedimento del 2009, (che peraltro non risulta essere stato impugnato) ha protratto nel tempo la propria condotta e che, conseguentemente, l'offesa derivante da tale condotta, da un lato ha assunto carattere continuativo e dall'altro poteva essere fatta cessare con effetti utili, indipendentemente dalla contestazione. Tale qualificazione dell'illecito implica la necessaria applicazione del principio *tempus regit actum*, che disciplina l'applicazione di norme che si succedono nel tempo, unitamente a quanto disposto dall'art. 1, comma 2, della legge n. 689/1981. Quanto sopra comporta che, all'illecito permanente contestato, debba applicarsi la norma

sanzionatoria vigente al momento del suo accertamento ovvero alla data di adozione del provvedimento dell'Autorità del 17 settembre 2009 e non quelle in vigore alla data di pubblicazione del Bollettino Ufficiale della Regione Puglia n. 45 dell'11 aprile 2006. E' pertanto applicabile, al caso di specie, l'art. 162, comma 2-b*is*, nella formulazione anteriore alle modifiche introdotte dalla legge 20 novembre 2009, n 166, che prevedeva una sanzione da 20.000,00 a 120.000,00 euro. La riduzione a 10.000,00 euro del minimo edittale della sanzione è entrata in vigore, invece, in data 25 novembre 2009 quindi successivamente alla data di accertamento, contestazione e notifica della violazione. Da quanto sopra discende, pertanto, la correttezza della quantificazione del pagamento in misura ridotta pari a 80.000,00 euro, a fronte della sanzione contestata;

- risultano, poi, pacifiche le valutazioni che hanno determinato l'applicazione dell'art. 164-*bis*, comma 3 -mentre la Regione ritiene erroneamente ravvisabili i casi di minore gravità di cui al comma 1 del medesimo articolo- atteso che, proprio in considerazione dell'evidente valenza sociale dell'attività relativa al *"(…) bando pubblicato dall'Assessorato alla solidarietà dell'ente regionale rivolto a soggetti disabili e finalizzato alla distribuzione di un contributo monetario per l'acquisto di un personal computer"* si dovevano adottare tutte le cautele per evitare di arrecare pregiudizio ai numerosi interessati, diffondendone illecitamente i dati via Internet in violazione della legge (art. 22, comma 8 del Codice);

RILEVATO, pertanto, che la Regione ha effettuato un trattamento di dati personali idonei a rilevare lo stato di salute diffondendoli anche tramite il portale *web* istituzionale, contravvenendo, così, al divieto di diffusione degli stessi ai sensi dell'art. 22, comma 8 del Codice;

VISTO l'art. 162, comma 2-*bis*, del Codice, nella formulazione antecedente alla modifica apportata con la legge 20 novembre 2009 n. 166, che punisce la violazione delle disposizioni indicate nell'art. 167 del Codice, tra le quali quella di cui all'art. 22, comma 8, del medesimo Codice, con la sanzione amministrativa del pagamento di una somma da ventimila euro a centoventimila euro

VISTO l'art. 164-bis, comma 3, del Codice che, per i casi di maggiore gravità quali la maggiore rilevanza del pregiudizio per uno o più interessati ovvero quando la violazione coinvolge numerosi interessati, prevede il raddoppio dei limiti minimo e massimo delle sanzioni previste dal Codice e che pertanto la sanzione amministrativa applicabile deve essere quantificata da un minimo di quarantamila (40.000,00) a un massimo di duecentoquarantamila (240.000,00) euro;

VISTA la legge 24 novembre 1981 n. 689, e successive modificazioni e integrazioni;

RITENUTO di dover determinare l'ammontare della sanzione pecuniaria, avuto riguardo ai parametri indicati nell'art. 11 della legge 24 novembre 1981 n. 689, valutati anche in relazione all'opera svolta dall'agente, alla gravità della violazione e alle condizioni economiche del contravventore, nella misura del minimo pari alla somma di quarantamila/00 euro;

VISTA la documentazione in atti;

VISTE le osservazioni dell'Ufficio, formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

RELATORE il dott. Giuseppe Fortunato;

ORDINA

alla Regione Puglia, con sede in Bari Lungomare Nazario Sauro n. 33, in persona del legale rappresentante pro-tempore, di pagare la somma di euro 40.000,00 (quarantamila) a titolo di sanzione amministrativa pecuniaria per la violazione dell'art. 162, comma 2 bis in combinato disposto con l'art. 164 bis, comma 3 del Codice, indicata in motivazione;

INGIUNGE

alla medesima Regione di pagare la somma di euro 40.000,00 (quarantamila) secondo le modalità indicate in allegato, entro 30 giorni dalla notificazione del presente provvedimento, pena l'adozione dei conseguenti atti esecutivi a norma dall'art. 27 della legge 24 novembre 1981, n. 689, prescrivendo che, entro il termine di giorni 10 (dieci) dal versamento, sia inviata a questa Autorità, in originale o in copia autentica, quietanza dell'avvenuto versamento;

DA' ATTO CHE

avverso il presente provvedimento, ai sensi dell'art. 152 del Codice, può essere proposta opposizione davanti al tribunale ordinario del luogo ove ha sede il titolare del trattamento entro il termine di trenta giorni dalla notificazione del presente provvedimento.

Roma, 23 settembre 2010
IL PRESIDENTE Pizzetti
IL RELATORE Fortunato
IL SEGRETARIO GENERALE De Paoli

Parere - 02 dicembre 2010
Bollettino del n. 122/dicembre 2010
[doc. web n. 1779678]
Modalità tecniche relative alla trasmissione da parte dei Comuni delle informazioni relative alla richiesta di iscrizione nell'anagrafe degli italiani residenti all'estero - 2 dicembre 2010

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vicepresidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti e del dott. Daniele De Paoli, segretario generale;

VISTO il Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196);

VISTA la richiesta di parere dell'Agenzia delle entrate in merito allo schema di provvedimento del Direttore dell'Agenzia concernente le *"modalità tecniche relative alla trasmissione da parte dei Comuni delle informazioni relative alla richiesta di iscrizione nell'anagrafe degli italiani residenti all'estero in attuazione dell'art. 83, comma 16, del d.l. 25 giugno 2008, n. 112, convertito, con modificazioni, dalla legge n. 133 del 6 agosto 2008"* (nota del 4 giugno 2010, prot. n. 2010/88170);

VISTA la nota dell'Agenzia delle entrate - Direzione Centrale Audit e Sicurezza - Settore sicurezza, Ufficio normative speciali con la quale è stato trasmesso un documento ad integrazione della precedente richiesta (nota del 27 agosto 2010);

VISTA la nota dell'Agenzia delle entrate - Direzione Centrale Audit e Sicurezza - Settore sicurezza, Ufficio normative speciali che modifica la precedente nota del 4 giugno 2010 relativamente alla "tipologia di dati trattati" (nota del 3 settembre 2010, prot. n. 2010/125990);

VISTA la nota dell'Agenzia delle entrate - Direzione Centrale Audit e Sicurezza - Settore sicurezza, Ufficio normative centrali con la quale sono stati forniti alcuni chiarimenti tecnici concernenti il collegamento INA SAIA (nota dell'11 ottobre 2010, prot. n. 2010/142989);

VISTO il provvedimento del Direttore dell'Agenzia delle entrate del 3 dicembre 2007 sul quale il Garante ha espresso il proprio parere in data 25 luglio 2007;

VISTA la documentazioni in atti;

VISTE le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

RELATORE il dott. Giuseppe Fortunato;

PREMESSO

L'Agenzia delle entrate ha sottoposto al Garante, per l'acquisizione del relativo parere, uno schema di provvedimento del Direttore dell'Agenzia concernente le "modalità tecniche relative alla trasmissione da parte dei Comuni delle

informazioni relative alla richiesta di iscrizione nell'anagrafe degli italiani residenti all'estero in attuazione dell'art. 83, comma 16, del d.l. 25 giugno 2008, n. 112, convertito con modificazioni dalla legge n. 133 del 6 agosto 2008".

L'art. 83, comma 16, del d.l. 25 giugno 2008 n. 112, convertito, con modificazioni, dalla legge 6 agosto 2008, n. 133, prevede che *"ai fini di assicurare maggiore effettività alla previsione di cui all'art. 1 del decreto legge 30 settembre 2005, n. 203, convertito, con modificazioni, dalla legge 2 dicembre 2005, n. 248, i comuni, entro i sei mesi successivi alla richiesta di iscrizione nell'anagrafe degli italiani residenti all'estero, confermano all'Ufficio dell'Agenzia delle entrate competente per l'ultimo domicilio fiscale che il richiedente ha effettivamente cessato la residenza nel territorio nazionale. Per il triennio successivo alla predetta richiesta di iscrizione l'effettività della cessazione della residenza nel territorio nazionale è sottoposta a vigilanza da parte dei comuni e dell'Agenzia delle entrate* (…)."

L'Agenzia ha, inoltre, precisato che le informazioni relative alla richiesta di iscrizione nell'Anagrafe degli italiani residenti all'estero (di seguito AIRE) sono suscettibili di utilizzo ai fini dell'accertamento dei tributi statali e del criterio di ripartizione della quota spettante ai singoli comuni, in attuazione dei punti 6.1 e 11.4 del provvedimento del Direttore dell'Agenzia delle entrate del 3 dicembre 2007, concernente le modalità di partecipazione dei comuni all'attività di accertamento fiscale ai sensi dell'art. 1 del decreto legge 30 settembre 2005, n. 203, convertito, con modificazioni, dalla legge 2 dicembre 2005, n. 248.

Lo schema di provvedimento in esame prevede, in particolare, quanto segue:

a) Trasmissione dei dati dei residenti all'estero da parte dei comuni all'Agenzia delle entrate. I comuni, entro sei mesi dalla richiesta, devono comunicare all'ufficio dell'Agenzia delle entrate competente per l'ultimo domicilio fiscale la cessazione della residenza nel territorio nazionale dei cittadini italiani che hanno fatto richiesta di iscrizione all'AIRE.

A tal fine i comuni devono inviare i seguenti elementi:

1) nome, cognome, codice fiscale, sesso, data di nascita, comune o stato estero di nascita, provincia di nascita dei soggetti che richiedono l'iscrizione all'AIRE;
2) denominazione e codice catastale del comune;
3) data di iscrizione all'AIRE;
4) conferma della cessazione della residenza nel territorio nazionale, quando ci sia l'effettività dell'espatrio e non sia stato attivato il procedimento amministrativo di controllo;
5) conferma dell'avvio di un procedimento di verifica anagrafica (informazione inseribile solo se non si ha la conferma della cessazione della residenza di cui al punto 4);
6) conferma della chiusura del procedimento di conferma di espatrio (informazione inseribile solo se non si ha la conferma della cessazione della residenza di cui al punto 4) nel caso in cui il procedimento amministrativo di controllo abbia accertato l'effettività dell'espatrio del soggetto;
7) conferma della chiusura del procedimento con mancata conferma di espatrio e cancellazione dall'AIRE (informazione inseribile solo se non si ha la conferma della cessazione della residenza di cui al punto 4), nel caso in cui il procedimento amministrativo di controllo abbia accertato la non effettività dell'espatrio del soggetto;
8) eventuali annotazioni del funzionario responsabile della comunicazione e, a seguito di specifica richiesta da parte dell'Ufficio dell'Agenzia che riceve la comunicazione, ulteriore documentazione disponibile;
9) nome, cognome, codice fiscale, telefono e indirizzo e-mail del funzionario responsabile della comunicazione, necessari al solo fine di facilitare la richiesta di eventuali ulteriori chiarimenti da parte dell'Ufficio dell'Agenzia che riceve la comunicazione.

b) Finalità del trattamento. L'Agenzia ha evidenziato che il suddetto trattamento di dati personali risulta necessario al fine di favorire l'azione di contrasto all'evasione fiscale e contributiva nell'ambito dello svolgimento delle funzioni istituzionali dell'Agenzia medesima e dei comuni, consentendo l'individuazione dei soggetti che, pur risultando formalmente residenti all'estero, hanno di fatto nel comune il domicilio ovvero la residenza ai sensi dell'art. 43, commi 1 e 2, del codice civile (cfr. art 1, d.l. 30 luglio 2005, n. 203; provvedimento del Direttore dell'Agenzia del 3 dicembre 2007).

c) Modalità di trasmissione dei dati. La trasmissione dei suddetti dati avviene in modalità via web tramite il sistema INA-SAIA, già utilizzato per lo scambio di informazioni tra comuni e Anagrafe tributaria. Nello specifico, l'Agenzia ha rappresentato che il servizio telematico si basa su una infrastruttura di sicurezza che prevede una porta di accesso dell'Agenzia ai domini applicativi del Centro nazionale per i servizi demografici (Cnsd) inserita in apposita zona di sicurezza della rete telematica dell'Anagrafe tributaria e che utilizza il protocollo Backbone INA (Indice Nazionale delle Anagrafi) che certifica lo scambio e l'integrità del contenuto informativo tra i soggetti fornitori e/o fruitori.

OSSERVA

Il Direttore dell'Agenzia delle entrate ha sottoposto al Garante, per l'acquisizione del relativo parere, uno schema di provvedimento concernente le "modalità tecniche relative alla trasmissione da parte dei Comuni delle informazioni relative alla richiesta di iscrizione nell'anagrafe degli italiani residenti all'estero in attuazione dell'art. 83, comma 16, del d.l. 25 giugno 2008, n. 112, convertito con modificazioni dalla legge n. 133 del 6 agosto 2008".

Per lo svolgimento delle finalità sopra descritte, l'Agenzia delle entrate ha individuato taluni dati personali riguardanti i cittadini residenti all'estero che i comuni devono trasmettergli via web tramite un meccanismo denominato INA-SAIA.

L'INA è il sistema incardinato nell'infrastruttura tecnologica e di sicurezza del Centro nazionale per i servizi demografici (Cnsd), istituito presso il Ministero dell'Interno-Dipartimento per gli affari Interni e Territoriali – Direzione Centrale per i servizi Demografici. Tale sistema, alimentato e costantemente aggiornato, tramite collegamento informatico, da tutti i comuni, "promuove la circolarità delle informazioni anagrafiche essenziali al fine di consentire alle amministrazioni pubbliche centrali e locali collegate la disponibilità, in tempo reale, dei dati relativi alle generalità, alla cittadinanza, alla famiglia anagrafica nonché all'indirizzo anagrafico delle persone residenti in
Italia, certificati dai comuni e, limitatamente al codice fiscale, dall'Agenzia delle Entrate" (art. 1, comma 6, della legge 24 dicembre 1954, n. 1228, così come modificato dall'art. 1-nonies del d.l. 31 marzo 2005, n. 44, approvato dalla legge di conversione 31 maggio 2005, n. 88 e successivamente dall'art. 50 del d.l. 31 maggio 2010, n. 78, convertito con legge 30 luglio 2010, n. 122). Il regolamento di gestione dell'INA, adottato con decreto del Ministero dell'Interno n. 240 del 13 ottobre 2005, che recepisce sostanzialmente le osservazioni formulate dall'Autorità (nota del 13 febbraio 2004), prevede, in particolare l'utilizzo di un sistema di gestione della sicurezza delle informazioni improntato agli standard internazionali ISO 1779 E BS 7799, ritenuto idoneo a garantire la sicurezza dei dati trattati in conformità alle disposizioni contenute negli artt. 31 e seguenti del Codice nonché nel Disciplinare tecnico in materia di misure minime di sicurezza (All. B) al Codice).

In tale quadro, il Garante non ha rilievi da formulare sullo schema di provvedimento del Direttore dell'Agenzia delle entrate in esame.

TUTTO CIO' PREMESSO IL GARANTE

ai sensi dell'articolo 154, commi 4 e 5, del Codice, esprime parere favorevole sullo schema di provvedimento del Direttore dell'Agenzia delle entrate concernente le *"modalità tecniche relative alla trasmissione da parte dei Comuni delle informazioni relative alla richiesta di iscrizione nell'anagrafe degli italiani residenti all'estero, in attuazione dell'art. 83, comma 16, del d.l. 25 giugno 2008, n. 112, convertito con modificazioni dalla legge n. 133 del 6 agosto 2008"*.

Roma, 2 dicembre 2010
IL PRESIDENTE Pizzetti
IL RELATORE Fortunato
IL SEGRETARIO GENERALE De Paoli

Comunicato stampa - 27 aprile 2010
Videosorveglianza: sistemi integrati e telecamere intelligenti a prova di privacy
Il Garante fissa le nuove regole per l'uso dei sistemi di videosorveglianza

Sistemi integrati di videosorveglianza solo nel rispetto di specifiche garanzie per la libertà delle persone. Appositi cartelli per segnalare la presenza di telecamere collegate con le sale operative delle forze di polizia. Obbligo di sottoporre alla verifica del Garante privacy, prima della loro attivazione, i sistemi che presentino rischi per i diritti e le libertà fondamentali delle persone, come i sistemi tecnologicamente avanzati o "intelligenti".

Conservazione a tempo delle immagini registrate. Rigorose misure di sicurezza a protezione delle immagini e contro accessi non autorizzati.

L'Autorità Garante per la protezione dei dati personali ha varato le nuove regole alle quali soggetti pubblici e privati dovranno conformarsi per installare telecamere e sistemi di videosorveglianza. Il periodo per adeguarsi è stato fissato, a seconda degli adempimenti, da un minimo di sei mesi ad un massimo di un anno.

Il provvedimento generale, che sostituisce quello del 2004 e introduce importanti novità, si è reso necessario non solo alla luce dell'aumento massiccio di sistemi di videosorveglianza per diverse finalità (prevenzione, accertamento e repressione dei reati, sicurezza pubblica, tutela della proprietà privata, controllo stradale, etc.), ma anche in considerazione dei numerosi interventi legislativi adottati in materia: tra questi, quelli più recenti che hanno attribuito ai sindaci e ai comuni specifiche competenze in materia di incolumità pubblica e di sicurezza urbana, così come le norme, anche regionali, che hanno incentivato l'uso di telecamere.

Il provvedimento, di cui è stato relatore Francesco Pizzetti, in via di pubblicazione sulla Gazzetta Ufficiale, tiene conto delle osservazioni formulate dal Ministero dell'interno e dall'Anci.

Ecco in sintesi le regole fissate dal Garante.

Principi generali

• **Informativa**: i cittadini che transitano nelle aree sorvegliate devono essere informati con cartelli della presenza delle telecamere, i cartelli devono essere resi visibili anche quando il sistema di videosorveglianza è attivo in orario notturno. Nel caso in cui i sistemi di videosorveglianza installati da soggetti pubblici e privati (esercizi commerciali, banche, aziende etc.) siano collegati alle forze di polizia è necessario apporre uno specifico cartello (*allegato n. 2*), sulla base del modello elaborato dal Garante. Le telecamere installate a fini di tutela dell'ordine e della sicurezza pubblica non devono essere segnalate, ma il Garante auspica comunque l'utilizzo di cartelli che informino i cittadini.

• **Conservazione**: le immagini registrate possono essere conservate per periodo limitato e fino ad un massimo di 24 ore, fatte salve speciali esigenze di ulteriore conservazione in relazione a indagini. Per attività particolarmente rischiose (es. banche) è ammesso un tempo più ampio, che non può superare comunque la settimana. Eventuali esigenze di allungamento dovranno essere sottoposte a verifica preliminare del Garante.

Settori di particolare interesse

• **Sicurezza urbana**: i Comuni che installano telecamere per fini di sicurezza urbana hanno l'obbligo di mettere cartelli che ne segnalino la presenza, salvo che le attività di videosorveglianza siano riconducibili a quelle di tutela specifica della sicurezza pubblica, prevenzione, accertamento o repressione dei reati. La conservazione dei dati non può superare i 7 giorni, fatte salve speciali esigenze.

• **Sistemi integrati**: per i sistemi che collegano telecamere tra soggetti diversi, sia pubblici che privati, o che consentono la fornitura di servizi di videosorveglianza "in remoto" da parte di società specializzate (es. società di vigilanza, Internet providers) mediante collegamento telematico ad un unico centro, sono obbligatorie specifiche misure di sicurezza (es. contro accessi abusivi alle immagini). Per alcuni sistemi è comunque necessaria la verifica preliminare del Garante.

• **Sistemi intelligenti**: per i sistemi di videosorveglianza "intelligenti" dotati di software che permettono l'associazione di immagini a dati biometrici (es. "riconoscimento facciale") o in grado, ad esempio, di riprendere e registrare automaticamente comportamenti o eventi anomali e segnalarli (es. "motion detection") è obbligatoria la verifica preliminare del Garante.

• **Violazioni al codice della strada**: obbligatori i cartelli che segnalino i sistemi elettronici di rilevamento delle infrazioni. Le telecamere devono riprendere solo la targa del veicolo (non quindi conducente, passeggeri, eventuali pedoni). Le fotografie o i video che attestano l'infrazione non devono essere inviati al domicilio dell'intestatario del veicolo.

• **Deposito rifiuti**: lecito l'utilizzo di telecamere per controllare discariche di sostanze pericolose ed "eco piazzole" per monitorare modalità del loro uso, tipologia dei rifiuti scaricati e orario di deposito.

Settori specifici

• **Luoghi di lavoro**: le telecamere possono essere installate solo nel rispetto dello norme in materia di lavoro. Vietato comunque il controllo a distanza dei lavoratori, sia all'interno degli edifici, sia in altri luoghi di prestazione del lavoro (es. cantieri, veicoli).

• **Ospedali e luoghi di cura**: no alla diffusione di immagini di persone malate mediante monitor quando questi sono collocati in locali accessibili al pubblico. E' ammesso, nei casi indispensabili, il monitoraggio da parte del personale sanitario dei pazienti ricoverati in particolari reparti (es.rianimazione), ma l'accesso alle immagini deve essere consentito solo al personale autorizzato e ai familiari dei ricoverati.

• **Istituti scolastici**: ammessa l'installazione di sistemi di videosorveglianza per la tutela contro gli atti vandalici, con riprese delimitate alle sole aree interessate e solo negli orari di chiusura.

• **Taxi**: le telecamere non devono riprendere in modo stabile la postazione di guida e la loro presenza deve essere segnalata con appositi contrassegni.

• **Trasporto pubblico**: lecita l'installazione su mezzi di trasporto pubblico e presso le fermate, ma rispettando limiti precisi (es.angolo visuale circoscritto, riprese senza l'uso di zoom).

• **Webcam** a scopo turistico: la ripresa delle immagini deve avvenire con modalità che non rendano identificabili le persone.

Soggetti privati.

• **Tutela delle persone e della proprietà**: contro possibili aggressioni, furti, rapine, danneggiamenti, atti di vandalismo, prevenzione incendi, sicurezza del lavoro ecc. si possono installare telecamere senza il consenso dei soggetti ripresi, ma sempre sulla base delle prescrizioni indicate dal Garante.

Roma, 27 aprile 2010

Prescrizioni del Garante [art. 154, 1 c) del Codice] - 08 aprile 2010
Bollettino del n. 115/aprile 2010
[doc. web n. 1712680]
Provvedimento in materia di videosorveglianza - 8 aprile 2010
(Gazzetta Ufficiale n. 99 del 29 aprile 2010)

Sommario

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vice presidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti e del dott. Daniele De Paoli, segretario generale reggente;

VISTO lo schema del provvedimento in materia di videosorveglianza approvato dal Garante il 22 dicembre 2009 e trasmesso al Ministero dell'Interno, all'Unione delle Province d'Italia (UPI) ed all'Associazione Nazionale Comuni Italiani (ANCI), al fine di acquisirne preventivamente le specifiche valutazioni per i profili di competenza;

CONSIDERATE le osservazioni formulate dall' ANCI con note del 25 febbraio 2010 (prot. n. 10/Area INSAP/AR/crc-10) e del 29 marzo 2010 (prot. n. 17/*Area* INSAP/AR/a*r*-10);

CONSIDERATE le osservazioni formulate dal Ministero dell'Interno con nota del 26 febbraio 2010;

VISTO il Codice in materia di protezione dei dati personali (*d.lg. 30 giugno 2003, n. 196*);

VISTE le osservazioni dell'Ufficio, formulate dal segretario generale ai sensi dell'art. 15 del regolamento n. 1/2000;

RELATORE il prof. Francesco Pizzetti;

1. PREMESSA

Il trattamento dei dati personali effettuato mediante l'uso di sistemi di videosorveglianza non forma oggetto di legislazione specifica; al riguardo si applicano, pertanto, le disposizioni generali in tema di protezione dei dati personali. Il Garante ritiene necessario intervenire nuovamente in tale settore con il presente provvedimento generale che sostituisce quello del 29 aprile 2004.

Ciò in considerazione sia dei numerosi interventi legislativi in materia, sia dell'ingente quantità di quesiti, segnalazioni, reclami e richieste di verifica preliminare in materia sottoposti a questa Autorità.

Nel quinquennio di relativa applicazione, infatti, talune disposizioni di legge hanno attribuito ai sindaci e ai comuni specifiche competenze volte a garantire l'incolumità pubblica e la sicurezza urbana, mentre altre norme, statali e regionali, hanno previsto altresì forme di incentivazione economica a favore delle amministrazioni pubbliche e di

soggetti privati al fine di incrementare l'utilizzo della videosorveglianza quale forma di difesa passiva, controllo e deterrenza di fenomeni criminosi e vandalici.

2. TRATTAMENTO DEI DATI PERSONALI E VIDEOSORVEGLIANZA: PRINCIPI GENERALI

La raccolta, la registrazione, la conservazione e, in generale, l'utilizzo di immagini configura un trattamento di dati personali (*art. 4, comma 1, lett. b), del Codice*). È considerato dato personale, infatti, qualunque informazione relativa a persona fisica identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione.

Un'analisi non esaustiva delle principali applicazioni dimostra che la videosorveglianza è utilizzata a fini molteplici, alcuni dei quali possono essere raggruppati nei seguenti ambiti generali:

1) protezione e incolumità degli individui, ivi ricompresi i profili attinenti alla sicurezza urbana, all'ordine e sicurezza pubblica, alla prevenzione, accertamento o repressione dei reati svolti dai soggetti pubblici, alla razionalizzazione e miglioramento dei servizi al pubblico volti anche ad accrescere la sicurezza degli utenti, nel quadro delle competenze ad essi attribuite dalla legge;

2) protezione della proprietà;

3) rilevazione, prevenzione e controllo delle infrazioni svolti dai soggetti pubblici, nel quadro delle competenze ad essi attribuite dalla legge;

4) acquisizione di prove.

La necessità di garantire, in particolare, un livello elevato di tutela dei diritti e delle libertà fondamentali rispetto al trattamento dei dati personali consente la possibilità di utilizzare sistemi di videosorveglianza, purché ciò non determini un'ingerenza ingiustificata nei diritti e nelle libertà fondamentali degli interessati.

Naturalmente l'installazione di sistemi di rilevazione delle immagini deve avvenire nel rispetto, oltre che della disciplina in materia di protezione dei dati personali, anche delle altre disposizioni dell'ordinamento applicabili, quali ad es. le vigenti norme dell'ordinamento civile e penale in materia di interferenze illecite nella vita privata, sul controllo a distanza dei lavoratori, in materia di sicurezza presso stadi e impianti sportivi, o con riferimento a musei, biblioteche statali e archivi di Stato, in relazione ad impianti di ripresa sulle navi da passeggeri adibite a viaggi nazionali e, ancora, nell'ambito dei porti, delle stazioni ferroviarie, delle stazioni delle ferrovie metropolitane e nell'ambito delle linee di trasporto urbano.

In tale quadro, pertanto, è necessario che:

a) il trattamento dei dati attraverso sistemi di videosorveglianza sia fondato su uno dei presupposti di liceità che il Codice prevede espressamente per i soggetti pubblici da un lato (svolgimento di funzioni istituzionali: *artt. 18-22 del Codice*) e, dall'altro, per soggetti privati ed enti pubblici economici (es. adempimento ad un obbligo di legge, provvedimento del Garante di c.d. "bilanciamento di interessi" - v., in proposito, punto 6.2 - o consenso libero ed espresso: *artt. 23-27 del Codice*). Si tratta di presupposti operanti in settori diversi e che sono pertanto richiamati separatamente nei successivi paragrafi del presente provvedimento relativi, rispettivamente, all'ambito pubblico e a quello privato;

b) ciascun sistema informativo ed il relativo programma informatico vengano conformati già in origine in modo da non utilizzare dati relativi a persone identificabili quando le finalità del trattamento possono essere realizzate impiegando solo dati anonimi (es., configurando il programma informatico in modo da consentire, per monitorare il traffico, solo riprese generali che escludano la possibilità di ingrandire le immagini e rendere identificabili le persone). Lo impone il *principio di necessità*, il quale comporta un obbligo di attenta configurazione di sistemi informativi e di programmi informatici per ridurre al minimo l'utilizzazione di dati personali (*art. 3 del Codice*);

c) l'attività di videosorveglianza venga effettuata nel rispetto del c.d. principio di proporzionalità nella scelta delle modalità di ripresa e dislocazione (es. tramite telecamere fisse o brandeggiabili, dotate o meno di zoom), nonché nelle varie fasi del trattamento che deve comportare, comunque, un trattamento di dati pertinenti e non eccedenti rispetto alle finalità perseguite (*art. 11, comma 1, lett. d) del Codice*).

3. ADEMPIMENTI APPLICABILI A SOGGETTI PUBBLICI E PRIVATI

3.1. Informativa

Gli interessati devono essere sempre informati che stanno per accedere in una zona videosorvegliata; ciò anche nei casi di eventi e in occasione di spettacoli pubblici (es. concerti, manifestazioni sportive).
A tal fine, il Garante ritiene che si possa utilizzare lo stesso modello semplificato di informativa "minima", indicante il titolare del trattamento e la finalità perseguita, già individuato ai sensi dell'art. 13, comma 3, del Codice nel provvedimento del 2004 e riportato in *fac-simile* nell'allegato n. 1 al presente provvedimento.
Il modello è ovviamente adattabile a varie circostanze. In presenza di più telecamere, in relazione alla vastità dell'area oggetto di rilevamento e alle modalità delle riprese, potranno essere installati più cartelli.
Il supporto con l'informativa:
• deve essere collocato prima del raggio di azione della telecamera, anche nelle sue immediate vicinanze e non necessariamente a contatto con gli impianti;
• deve avere un formato ed un posizionamento tale da essere chiaramente visibile in ogni condizione di illuminazione ambientale, anche quando il sistema di videosorveglianza sia eventualmente attivo in orario notturno;
• può inglobare un simbolo o una stilizzazione di esplicita e immediata comprensione, eventualmente diversificati al fine di informare se le immagini sono solo visionate o anche registrate.
Il Garante ritiene auspicabile che l'informativa, resa in forma semplificata avvalendosi del predetto modello, poi rinvii a un testo completo contenente tutti gli elementi di cui all'art. 13, comma 1, del Codice, disponibile agevolmente senza oneri per gli interessati, con modalità facilmente accessibili anche con strumenti informatici e telematici (in particolare, tramite reti Intranet o siti Internet, affissioni in bacheche o locali, avvisi e cartelli agli sportelli per gli utenti, messaggi preregistrati disponibili digitando un numero telefonico gratuito).
In ogni caso il titolare, anche per il tramite di un incaricato, ove richiesto è tenuto a fornire anche oralmente un'informativa adeguata, contenente gli elementi individuati dall'art. 13 del Codice.
3.1.1. Informativa e sicurezza
Talune disposizioni del Codice, tra le quali quella riguardante l'obbligo di fornire una preventiva informativa agli interessati, non sono applicabili al trattamento di dati personali effettuato, anche sotto forma di suoni e immagini, dal *"Centro elaborazione dati del Dipartimento di pubblica sicurezza o da forze di polizia sui dati destinati a confluirvi in base alla legge, ovvero da organi di pubblica sicurezza o altri soggetti pubblici per finalità di tutela dell'ordine e della sicurezza pubblica, prevenzione, accertamento o repressione dei reati,effettuati in base ad espressa disposizione di legge che preveda specificamente il trattamento" (art. 53 del Codice).*
Alla luce di tale previsione del Codice, i predetti titolari del trattamento di dati personali devono osservare i seguenti principi:
a) l'informativa può non essere resa quando i dati personali sono trattati per il perseguimento delle finalità di tutela dell'ordine e della sicurezza pubblica, prevenzione, accertamento o repressione dei reati;
b) il trattamento deve comunque essere effettuato in base ad espressa disposizione di legge che lo preveda specificamente.
3.1.2. Ulteriori specificazioni: l'informativa eventuale nella videosorveglianza effettuata per finalità di tutela dell'ordine e della sicurezza pubblica, prevenzione, accertamento o repressione dei reati
Il Garante, al fine di rafforzare la tutela dei diritti e delle libertà fondamentali degli interessati, ritiene fortemente auspicabile che l'informativa, benché non obbligatoria, laddove l'attività di videosorveglianza sia espletata ai sensi dell'art. 53 del Codice, sia comunque resa in tutti i casi nei quali non ostano in concreto specifiche ragioni di tutela e sicurezza pubblica o di prevenzione, accertamento o repressione dei reati.
Ciò naturalmente all'esito di un prudente apprezzamento volto a verificare che l'informativa non ostacoli, ma anzi rafforzi, in concreto l'espletamento delle specifiche funzioni perseguite, tenuto anche conto che rendere palese l'utilizzo dei sistemi di videosorveglianza può, in molti casi, svolgere una efficace funzione di deterrenza.
A tal fine i titolari del trattamento possono rendere nota la rilevazione di immagini tramite impianti di videosorveglianza attraverso forme anche semplificate di informativa, che evidenzino, mediante l'apposizione nella cartellonistica di riferimenti grafici, simboli, diciture, l'utilizzo di tali sistemi per finalità di tutela dell'ordine e della sicurezza pubblica, prevenzione, accertamento o repressione dei reati.

In ogni caso resta fermo che, anche se i titolari si avvalgono della facoltà di fornire l'informativa, resta salva la non applicazione delle restanti disposizioni del Codice tassativamente indicate dall'art. 53, comma 1, lett. *a*) e *b*).
Va infine sottolineato che deve essere obbligatoriamente fornita un'idonea informativa in tutti i casi in cui, invece, i trattamenti di dati personali effettuati tramite l'utilizzo di sistemi di videosorveglianza dalle forze di polizia, dagli organi di pubblica sicurezza e da altri soggetti pubblici non siano riconducibili a quelli espressamente previsti dall'art. 53 del Codice (es. utilizzo di sistemi di rilevazioni delle immagini per la contestazione delle violazioni del Codice della strada).

3.1.3. Informativa da parte dei soggetti privati che effettuano collegamenti con le forze di polizia

I trattamenti di dati personali effettuati da soggetti privati tramite sistemi di videosorveglianza, direttamente collegati con le forze di polizia, esulano dall'ambito di applicazione dell'art. 53 del Codice. Pertanto, l'attivazione del predetto collegamento deve essere reso noto agli interessati. A tal fine, il Garante ritiene che si possa utilizzare il modello semplificato di informativa "minima" - indicante il titolare del trattamento, la finalità perseguita ed il collegamento con le forze di polizia- individuato ai sensi dell'art. 13, comma 3, del Codice e riportato in *fac-simile* nell'allegato n. 2 al presente provvedimento. Nell'ambito del testo completo di informativa reso eventualmente disponibile agli interessati, tale collegamento deve essere reso noto.
Al predetto trattamento si applicano le prescrizioni contenute nel punto 4.6
La violazione delle disposizioni riguardanti l'informativa di cui all'art. 13, consistente nella sua omissione o inidoneità (es. laddove non indichi comunque il titolare del trattamento, la finalità perseguita ed il collegamento con le forze di polizia), è punita con la sanzione amministrativa prevista dall'art. 161 del Codice. Le diverse problematiche riguardanti le competenze attribuite ai comuni in materia di sicurezza urbana sono esaminate al punto 5.1.

3.2. Prescrizioni specifiche

3.2.1. Verifica preliminare

I trattamenti di dati personali nell'ambito di una attività di videosorveglianza devono essere effettuati rispettando le misure e gli accorgimenti prescritti da questa Autorità come esito di una verifica preliminare attivata d'ufficio o a seguito di un interpello del titolare (*art. 17 del Codice*), quando vi sono rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità degli interessati, in relazione alla natura dei dati o alle modalità di trattamento o agli effetti che può determinare. In tali ipotesi devono ritenersi ricompresi i sistemi di raccolta delle immagini associate a dati biometrici. L'uso generalizzato e incontrollato di tale tipologia di dati può comportare, in considerazione della loro particolare natura, il concreto rischio del verificarsi di un pregiudizio rilevante per l'interessato, per cui si rende necessario prevenire eventuali utilizzi impropri, nonché possibili abusi.
Ad esempio, devono essere sottoposti alla verifica preliminare di questa Autorità i sistemi di videosorveglianza dotati di *software* che permetta il riconoscimento della persona tramite collegamento o incrocio o confronto delle immagini rilevate (es. morfologia del volto) con altri specifici dati personali, in particolare con dati biometrici, o sulla base del confronto della relativa immagine con una campionatura di soggetti precostituita alla rilevazione medesima.
Un analogo obbligo sussiste con riferimento a sistemi c.d. intelligenti, che non si limitano a riprendere e registrare le immagini, ma sono in grado di rilevare automaticamente comportamenti o eventi anomali, segnalarli, ed eventualmente registrarli. In linea di massima tali sistemi devono considerarsi eccedenti rispetto alla normale attività di videosorveglianza, in quanto possono determinare effetti particolarmente invasivi sulla sfera di autodeterminazione dell'interessato e, conseguentemente, sul suo comportamento. Il relativo utilizzo risulta comunque giustificato solo in casi particolari, tenendo conto delle finalità e del contesto in cui essi sono trattati, da verificare caso per caso sul piano della conformità ai principi di necessità, proporzionalità, finalità e correttezza (*artt. 3 e 11 del Codice*).
Deve essere sottoposto a verifica preliminare l'utilizzo di sistemi integrati di videosorveglianza nei casi in cui le relative modalità di trattamento non corrispondano a quelle individuate nei punti 4.6 e 5.4 del presente provvedimento.
Ulteriori casi in cui si rende necessario richiedere una verifica preliminare riguardano l'allungamento dei tempi di conservazione dei dati delle immagini registrate oltre il previsto termine massimo di sette giorni derivante da speciali esigenze di ulteriore conservazione, a meno che non derivi da una specifica richiesta dell'autorità giudiziaria o di polizia giudiziaria in relazione a un'attività investigativa in corso (v. punto 3.4).

Comunque, anche fuori dalle predette ipotesi, in tutti i casi in cui i trattamenti effettuati tramite videosorveglianza hanno natura e caratteristiche tali per cui le misure e gli accorgimenti individuati nel presente provvedimento non sono integralmente applicabili, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che possono determinare, il titolare del trattamento è tenuto a richiedere una verifica preliminare a questa Autorità.

3.2.2. Esclusione della verifica preliminare

Il titolare del trattamento di dati personali effettuato tramite sistemi di videosorveglianza non deve richiedere una verifica preliminare purché siano rispettate tutte le seguenti condizioni:

a) il Garante si sia già espresso con un provvedimento di verifica preliminare in relazione a determinate categorie di titolari o di trattamenti;

b) la fattispecie concreta, le finalità del trattamento, la tipologia e le modalità d'impiego del sistema che si intende adottare, nonché le categorie dei titolari, corrispondano a quelle del trattamento approvato;

c) si rispettino integralmente le misure e gli accorgimenti conosciuti o concretamente conoscibili prescritti nel provvedimento di cui alla lett. *a*) adottato dal Garante. Resta inteso che il normale esercizio di un impianto di videosorveglianza, non rientrante nelle ipotesi previste al precedente punto 3.2.1, non deve essere sottoposto all'esame preventivo del Garante, sempreché il trattamento medesimo avvenga con modalità conformi al presente provvedimento.

Resta altresì inteso che nessuna approvazione implicita può desumersi dal semplice inoltro al Garante di documenti relativi a progetti di videosorveglianza (spesso generici e non valutabili a distanza) cui non segua un esplicito riscontro dell'Autorità, in quanto non si applica il principio del silenzio-assenso.

3.2.3. Notificazione

E' regola generale che i trattamenti di dati personali devono essere notificati al Garante solo se rientrano in casi specificamente previsti (*art. 37 del Codice*). In relazione a quanto stabilito dalla lett. *f*), del comma 1, dell'art. 37, questa Autorità ha già disposto che non vanno comunque notificati i trattamenti di dati effettuati per esclusive finalità di sicurezza o di tutela delle persone o del patrimonio ancorché relativi a comportamenti illeciti o fraudolenti, quando immagini o suoni raccolti siano conservati temporaneamente. Al di fuori di tali precisazioni, il trattamento, che venga effettuato tramite sistemi di videosorveglianza e che sia riconducibile a quanto disposto dall'art. 37 del Codice, deve essere preventivamente notificato a questa Autorità. La mancata o incompleta notificazione ai sensi degli artt. 37 e 38 del Codice è punita con la sanzione amministrativa prevista dall'art. 163.

3.3. Misure di sicurezza da applicare ai dati personali trattati mediante sistemi di videosorveglianza e soggetti preposti

3.3.1. Misure di sicurezza

I dati raccolti mediante sistemi di videosorveglianza devono essere protetti con idonee e preventive misure di sicurezza, riducendo al minimo i rischi di distruzione, di perdita, anche accidentale, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità della raccolta, anche in relazione alla trasmissione delle immagini (artt. 31 e ss. del Codice).

Devono quindi essere adottate specifiche misure tecniche ed organizzative che consentano al titolare di verificare l'attività espletata da parte di chi accede alle immagini o controlla i sistemi di ripresa (se soggetto distinto dal titolare medesimo, nel caso in cui questo sia persona fisica). E' inevitabile che - in considerazione dell'ampio spettro di utilizzazione di sistemi di videosorveglianza, anche in relazione ai soggetti e alle finalità perseguite nonché della varietà dei sistemi tecnologici utilizzati - le misure minime di sicurezza possano variare anche significativamente. E' tuttavia necessario che le stesse siano quanto meno rispettose dei principi che seguono:

a) in presenza di differenti competenze specificatamente attribuite ai singoli operatori devono essere configurati diversi livelli di visibilità e trattamento delle immagini (v. punto 3.3.2). Laddove tecnicamente possibile, in base alle caratteristiche dei sistemi utilizzati, i predetti soggetti, designati incaricati o, eventualmente, responsabili del trattamento, devono essere in possesso di credenziali di autenticazione che permettano di effettuare, a seconda dei compiti attribuiti ad ognuno, unicamente le operazioni di propria competenza;

b) laddove i sistemi siano configurati per la registrazione e successiva conservazione delle immagini rilevate, deve essere altresì attentamente limitata la possibilità, per i soggetti abilitati, di visionare non solo in sincronia con la ripresa,

ma anche in tempo differito, le immagini registrate e di effettuare sulle medesime operazioni di cancellazione o duplicazione;

c) per quanto riguarda il periodo di conservazione delle immagini devono essere predisposte misure tecniche od organizzative per la cancellazione, anche in forma automatica, delle registrazioni, allo scadere del termine previsto (v. punto 3.4);

d) nel caso di interventi derivanti da esigenze di manutenzione, occorre adottare specifiche cautele; in particolare, i soggetti preposti alle predette operazioni possono accedere alle immagini solo se ciò si renda indispensabile al fine di effettuare eventuali verifiche tecniche ed in presenza dei soggetti dotati di credenziali di autenticazione abilitanti alla visione delle immagini;

e) qualora si utilizzino apparati di ripresa digitali connessi a reti informatiche, gli apparati medesimi devono essere protetti contro i rischi di accesso abusivo di cui all'art. 615-*ter* del codice penale;

f) la trasmissione tramite una rete pubblica di comunicazioni di immagini riprese da apparati di videosorveglianza deve essere effettuata previa applicazione di tecniche crittografiche che ne garantiscano la riservatezza; le stesse cautele sono richieste per la trasmissione di immagini da punti di ripresa dotati di connessioni wireless (tecnologie *wi-fi, wi-max, Gprs*).

3.3.2. Responsabili e incaricati

Il titolare o il responsabile devono designare per iscritto tutte le persone fisiche, incaricate del trattamento, autorizzate sia ad accedere ai locali dove sono situate le postazioni di controllo, sia ad utilizzare gli impianti e, nei casi in cui sia indispensabile per gli scopi perseguiti, a visionare le immagini (*art. 30 del Codice*). Deve trattarsi di un numero delimitato di soggetti, specie quando il titolare si avvale di collaboratori esterni.

Occorre altresì individuare diversi livelli di accesso in corrispondenza delle specifiche mansioni attribuite ad ogni singolo operatore, distinguendo coloro che sono unicamente abilitati a visionare le immagini dai soggetti che possono effettuare, a determinate condizioni, ulteriori operazioni (es. registrare, copiare, cancellare, spostare l'angolo visuale, modificare lo zoom, ecc.) (v. punto 3.3.1). Vanno osservate le regole ordinarie anche per ciò che attiene all'eventuale designazione di responsabili del trattamento (*art. 29 del Codice*).

Il mancato rispetto di quanto previsto nelle lettere da a) ad f) del punto 3.3.1 comporta l'applicazione della sanzione amministrativa stabilita dall'art. 162, comma 2-*ter*, del Codice.

L'omessa adozione delle misure minime di sicurezza comporta l'applicazione della sanzione amministrativa stabilita dall'art. 162, comma 2-*bis*, ed integra la fattispecie di reato prevista dall'art. 169 del Codice.

3.4. Durata dell'eventuale conservazione

Nei casi in cui sia stato scelto un sistema che preveda la conservazione delle immagini, in applicazione del principio di proporzionalità (*v. art. 11, comma 1, lett. e),del Codice*), anche l'eventuale conservazione temporanea dei dati deve essere commisurata al tempo necessario - e predeterminato - a raggiungere la finalità perseguita.

La conservazione deve essere limitata a poche ore o, al massimo, alle ventiquattro ore successive alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura di uffici o esercizi, nonché nel caso in cui si deve aderire ad una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria.

Solo in alcuni casi, per peculiari esigenze tecniche (mezzi di trasporto) o per la particolare rischiosità dell'attività svolta dal titolare del trattamento (ad esempio, per alcuni luoghi come le banche può risultare giustificata l'esigenza di identificare gli autori di un sopralluogo nei giorni precedenti una rapina), può ritenersi ammesso un tempo più ampio di conservazione dei dati che, sulla scorta anche del tempo massimo legislativamente posto per altri trattamenti, si ritiene non debba comunque superare la settimana.

Per i comuni e nelle sole ipotesi in cui l'attività di videosorveglianza sia finalizzata alla tutela della sicurezza urbana, alla luce delle recenti disposizioni normative, il termine massimo di durata della conservazione dei dati è limitato *"ai sette giorni successivi alla rilevazione delle informazioni e delle immagini raccolte mediante l'uso di sistemi di videosorveglianza, fatte salve speciali esigenze di ulteriore conservazione"*.

In tutti i casi in cui si voglia procedere a un allungamento dei tempi di conservazione per un periodo superiore alla settimana, una richiesta in tal senso deve essere sottoposta ad una verifica preliminare del Garante (v. punto 3.2.1), e

comunque essere ipotizzato dal titolare come eccezionale nel rispetto del principio di proporzionalità. La congruità di un termine di tempo più ampio di conservazione va adeguatamente motivata con riferimento ad una specifica esigenza di sicurezza perseguita, in relazione a concrete situazioni di rischio riguardanti eventi realmente incombenti e per il periodo di tempo in cui venga confermata tale eccezionale necessità. La relativa congruità può altresì dipendere dalla necessità di aderire ad una specifica richiesta di custodire o consegnare una copia specificamente richiesta dall'autorità giudiziaria o dalla polizia giudiziaria in relazione ad un'attività investigativa in corso.

Il sistema impiegato deve essere programmato in modo da operare al momento prefissato l'integrale cancellazione automatica delle informazioni allo scadere del termine previsto da ogni supporto, anche mediante sovraregistrazione, con modalità tali da rendere non riutilizzabili i dati cancellati. In presenza di impianti basati su tecnologia non digitale o comunque non dotati di capacità di elaborazione tali da consentire la realizzazione di meccanismi automatici di expiring dei dati registrati, la cancellazione delle immagini dovrà comunque essere effettuata nel più breve tempo possibile per l'esecuzione materiale delle operazioni dalla fine del periodo di conservazione fissato dal titolare.

Il mancato rispetto dei tempi di conservazione delle immagini raccolte e del correlato obbligo di cancellazione di dette immagini oltre il termine previsto comporta l'applicazione della sanzione amministrativa stabilita dall'art. 162, comma 2-*ter*, del Codice.

3.5. Diritti degli interessati

Deve essere assicurato agli interessati identificabili l'effettivo esercizio dei propri diritti in conformità al Codice, in particolare quello di accedere ai dati che li riguardano, di verificare le finalità, le modalità e la logica del trattamento (*art. 7 del Codice*).

La risposta ad una richiesta di accesso a dati conservati deve riguardare tutti quelli attinenti al richiedente identificabile e può comprendere eventuali dati riferiti a terzi solo nei limiti previsti dal Codice, ovvero nei soli casi in cui la scomposizione dei dati trattati o la privazione di alcuni elementi renda incomprensibili i dati personali relativi all'interessato (*art. 10, comma 5, del Codice*).

In riferimento alle immagini registrate non è in concreto esercitabile il diritto di aggiornamento, rettificazione o integrazione in considerazione della natura intrinseca dei dati raccolti, in quanto si tratta di immagini raccolte in tempo reale riguardanti un fatto obiettivo (*art. 7, comma 3, lett. a), del Codice*). Viceversa, l'interessato ha diritto di ottenere il blocco dei dati qualora essi siano trattati in violazione di legge (*art. 7, comma 3, lett. b), del Codice*).

4. SETTORI SPECIFICI

4.1. Rapporti di lavoro

Nelle attività di sorveglianza occorre rispettare il divieto di controllo a distanza dell'attività lavorativa, pertanto è vietata l'installazione di apparecchiature specificatamente preordinate alla predetta finalità: non devono quindi essere effettuate riprese al fine di verificare l'osservanza dei doveri di diligenza stabiliti per il rispetto dell'orario di lavoro e la correttezza nell'esecuzione della prestazione lavorativa (ad es. orientando la telecamera sul *badge*).

Vanno poi osservate le garanzie previste in materia di lavoro quando la videosorveglianza è resa necessaria da esigenze organizzative o produttive, ovvero è richiesta per la sicurezza del lavoro: in tali casi, ai sensi dell'art. 4 della l. n. 300/1970, gli impianti e le apparecchiature, "*dai quali può derivare anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere installati soltanto previo accordo con le rappresentanze sindacali aziendali, oppure, in mancanza di queste, con la commissione interna. In difetto di accordo, su istanza del datore di lavoro, provvede l'Ispettorato del lavoro, dettando, ove occorra, le modalità per l'uso di tali impianti" (v., altresì, artt. 113 e 114 del Codice; art. 8 l. n. 300/1970 cit.; art. 2 d.lg. n. 165/2001).*

Tali garanzie vanno osservate sia all'interno degli edifici, sia in altri contesti in cui è resa la prestazione di lavoro, come, ad esempio, nei cantieri edili o con riferimento alle telecamere installate su veicoli adibiti al servizio di linea per il trasporto di persone (artt. 82, 85-87, d.lg. 30 aprile 1992, n. 285, "*Nuovo codice della strada*") o su veicoli addetti al servizio di noleggio con conducente e servizio di piazza (taxi) per trasporto di persone (le quali non devono riprendere in modo stabile la postazione di guida, e le cui immagini, raccolte per finalità di sicurezza e di eventuale accertamento di illeciti, non possono essere utilizzate per controlli, anche indiretti, sull'attività lavorativa degli addetti, v. punto 4.4).

Il mancato rispetto di quanto sopra prescritto comporta l'applicazione della sanzione amministrativa stabilita dall'art. 162, comma 2-*ter*, del Codice. L'utilizzo di sistemi di videosorveglianza preordinati al controllo a distanza dei lavoratori o ad effettuare indagini sulle loro opinioni integra la fattispecie di reato prevista dall'art. 171 del Codice.

Sotto un diverso profilo, eventuali riprese televisive sui luoghi di lavoro per documentare attività od operazioni solo per scopi divulgativi o di comunicazione istituzionale o aziendale, e che vedano coinvolto il personale dipendente, possono essere assimilati ai trattamenti temporanei finalizzati alla pubblicazione occasionale di articoli, saggi ed altre manifestazioni del pensiero. In tal caso, alle stesse si applicano le disposizioni sull'attività giornalistica contenute nel Codice (*artt. 136 e ss.*), fermi restando, comunque, i limiti al diritto di cronaca posti a tutela della riservatezza, nonché l'osservanza del codice deontologico per l'attività giornalistica ed il diritto del lavoratore a tutelare la propria immagine opponendosi, per motivi legittimi, alla sua diffusione (*art. 7, comma 4, lett. a), del Codice*).

4.2. Ospedali e luoghi di cura

L'eventuale controllo di ambienti sanitari e il monitoraggio di pazienti ricoverati in particolari reparti o ambienti (ad es. unità di rianimazione, reparti di isolamento), stante la natura sensibile di molti dati che possono essere in tal modo raccolti, devono essere limitati ai casi di comprovata indispensabilità, derivante da specifiche esigenze di cura e tutela della salute degli interessati.

Devono essere inoltre adottati tutti gli ulteriori accorgimenti necessari per garantire un elevato livello di tutela della riservatezza e della dignità delle persone malate, anche in attuazione di quanto prescritto dal provvedimento generale del 9 novembre 2005 adottato in attuazione dell'art. 83 del Codice.

Il titolare deve garantire che possano accedere alle immagini rilevate per le predette finalità solo i soggetti specificamente autorizzati (es. personale medico ed infermieristico). Particolare attenzione deve essere riservata alle modalità di accesso alle riprese video da parte di terzi legittimati (familiari, parenti, conoscenti) di ricoverati in reparti dove non sia consentito agli stessi di recarsi personalmente (es. rianimazione), ai quali può essere consentita, con gli adeguati accorgimenti tecnici, la visione dell'immagine solo del proprio congiunto o conoscente.

Le immagini idonee a rivelare lo stato di salute non devono essere comunque diffuse (*art. 22, comma 8, del Codice*).

In tale quadro, va assolutamente evitato il rischio di diffusione delle immagini di persone malate su *monitor* collocati in locali liberamente accessibili al pubblico. Il mancato rispetto di quanto sopra prescritto comporta l'applicazione della sanzione amministrativa stabilita dall'art. 162, comma 2-*ter*, del Codice. La diffusione di immagini in violazione dell'art. 22, comma 8, del Codice, oltre a comportare l'applicazione della sanzione amministrativa prevista dall'art. 162, comma 2-*bis*, integra la fattispecie di reato stabilita dall'art. 167, comma 2.

4.3. Istituti scolastici

L'eventuale installazione di sistemi di videosorveglianza presso istituti scolastici deve garantire *"il diritto dello studente alla riservatezza"* (*art. 2, comma 2, d.P.R. n. 249/1998*), prevedendo opportune cautele al fine di assicurare l'armonico sviluppo delle personalità dei minori in relazione alla loro vita, al loro processo di maturazione ed al loro diritto all'educazione.

4.3.1. In tale quadro, può risultare ammissibile l'utilizzo di tali sistemi in casi di stretta indispensabilità, al fine di tutelare l'edificio ed i beni scolastici da atti vandalici, circoscrivendo le riprese alle sole aree interessate ed attivando gli impianti negli orari di chiusura degli istituti; è vietato, altresì, attivare le telecamere in coincidenza con lo svolgimento di eventuali attività extrascolastiche che si svolgono all'interno della scuola.

4.3.2. Laddove la ripresa delle immagini riguardi anche le aree perimetrali esterne degli edifici scolastici, l'angolo visuale deve essere delimitato alle sole parti interessate, escludendo dalle riprese le aree non strettamente pertinenti l'edificio.

4.3.3. Il mancato rispetto di quanto prescritto ai punti 4.3.1 e 4.3.2 comporta l'applicazione della sanzione amministrativa stabilita dall'art. 162, comma 2-ter, del Codice.

4.4. Sicurezza nel trasporto pubblico

4.4.1. Alcune situazioni di particolare rischio possono fare ritenere lecita l'installazione di sistemi di videosorveglianza sia su mezzi di trasporto pubblici, sia presso le fermate dei predetti mezzi.

4.4.2. La localizzazione delle telecamere e le modalità di ripresa devono essere determinate nel rispetto dei richiamati principi di necessità, proporzionalità e finalità; pertanto, occorre evitare riprese particolareggiate nei casi in cui le stesse non sono indispensabili in relazione alle finalità perseguite.

4.4.3. I titolari del trattamento dovranno poi provvedere a fornire la prevista informativa agli utenti del servizio di trasporto urbano. Gli autobus, i tram, i taxi ed i veicoli da noleggio con o senza conducente dotati di telecamere dovranno pertanto portare apposite indicazioni o contrassegni che diano conto con immediatezza della presenza dell'impianto di videosorveglianza, anche utilizzando a tal fine il *fac-simile* riportato nell'allegato n. 1 al presente provvedimento, e indicanti, comunque, il titolare del trattamento, nonché la finalità perseguita.

4.4.4. Specifiche cautele devono essere osservate laddove vengano installati impianti di videosorveglianza presso le aree di fermata, in prossimità delle quali possono transitare anche soggetti diversi dagli utenti del servizio di trasporto pubblico. In particolare, l'angolo visuale delle apparecchiature di ripresa deve essere strettamente circoscritto all'area di permanenza, permettendo l'inquadratura solo della pensilina e di altri arredi urbani funzionali al servizio di trasporto pubblico (tabelle degli orari, paline recanti l'indicazione degli autobus in transito, ecc.), con esclusione della zona non immediatamente circostante e comunque dell'area non direttamente funzionale rispetto alle esigenze di sicurezza del sistema di traffico e trasporto. Anche in tale ipotesi occorre evitare le riprese inutilmente particolareggiate o tali da rilevare caratteristiche eccessivamente dettagliate degli individui che stazionano presso le fermate. L'esistenza delle telecamere deve essere opportunamente evidenziata nelle predette aree di fermata.

4.4.5. Fermo restando che la violazione delle disposizioni riguardanti l'informativa di cui all'art. 13 è punita con la sanzione amministrativa prevista dall'art. 161 del Codice e l'utilizzo di sistemi di videosoreglianza preordinati al controllo a distanza dei lavoratori integra la fattispecie di reato prevista dall'art. 171, il mancato rispetto di quanto prescritto al punto 4.4.4 comporta l'applicazione della sanzione amministrativa stabilita dall'art. 162, comma 2-*ter*, del Codice.

4.5. Utilizzo di web cam o camera-on-line a scopi promozionali-turistici o pubblicitari

Le attività di rilevazione di immagini a fini promozionali-turistici o pubblicitari, attraverso *web cam* devono avvenire con modalità che rendano non identificabili i soggetti ripresi. Ciò in considerazione delle peculiari modalità del trattamento, dalle quali deriva un concreto rischio del verificarsi di un pregiudizio rilevante per gli interessati: le immagini raccolte tramite tali sistemi, infatti, vengono inserite direttamente sulla rete Internet, consentendo a chiunque navighi sul web di visualizzare in tempo reale i soggetti ripresi e di utilizzare le medesime immagini anche per scopi diversi dalle predette finalità promozionali-turistiche o pubblicitarie perseguite dal titolare del trattamento.

4.6. Sistemi integrati di videosorveglianza

In ottemperanza del principio di economicità delle risorse e dei mezzi impiegati, si è incrementato il ricorso a sistemi integrati di videosorveglianza tra diversi soggetti, pubblici e privati, nonché l'offerta di servizi centralizzati di videosorveglianza remota da parte di fornitori (società di vigilanza, *Internet service providers*, fornitori di servizi video specialistici, ecc.). Inoltre, le immagini riprese vengono talvolta rese disponibili, con varie tecnologie o modalità, alle forze di polizia.

Nell'ambito dei predetti trattamenti, sono individuabili le seguenti tipologie di sistemi integrati di videosorveglianza:

a) *gestione coordinata di funzioni e servizi tramite condivisione, integrale o parziale, delle immagini riprese da parte di diversi e autonomi titolari del trattamento*, i quali utilizzano le medesime infrastrutture tecnologiche; in tale ipotesi, i singoli titolari possono trattare le immagini solo nei termini strettamente funzionali al perseguimento dei propri compiti istituzionali ed alle finalità chiaramente indicate nell'informativa, nel caso dei soggetti pubblici, ovvero alle sole finalità riportate nell'informativa, nel caso dei soggetti privati;

b) *collegamento telematico di diversi titolari del trattamento ad un "centro" unico gestito da un soggetto terzo*; tale soggetto terzo, designato responsabile del trattamento ai sensi dell'art. 29 del Codice da parte di ogni singolo titolare, deve assumere un ruolo di coordinamento e gestione dell'attività di videosorveglianza senza consentire, tuttavia, forme di correlazione delle immagini raccolte per conto di ciascun titolare;

c) sia nelle predette ipotesi, sia nei casi in cui l'attività di videosorveglianza venga effettuata da un solo titolare, si può anche attivare un *collegamento dei sistemi di videosorveglianza con le sale o le centrali operative degli organi di*

polizia. L'attivazione del predetto collegamento deve essere reso noto agli interessati. A tal fine, il Garante ritiene che si possa utilizzare il modello semplificato di informativa "minima" - indicante il titolare del trattamento, la finalità perseguita ed il collegamento con le forze di polizia individuato ai sensi dell'art. 13, comma 3, del Codice e riportato in *fac-simile* nell'allegato n. 2 al presente provvedimento. Tale collegamento deve essere altresì reso noto nell'ambito del testo completo di informativa reso eventualmente disponibile agli interessati (v. punto 3.1.3).

Le modalità di trattamento sopra elencate richiedono l'adozione di specifiche misure di sicurezza ulteriori rispetto a quelle individuate nel precedente punto 3.3.1, quali:

1) adozione di sistemi idonei alla registrazione degli accessi logici degli incaricati e delle operazioni compiute sulle immagini registrate, compresi i relativi riferimenti temporali, con conservazione per un periodo di tempo congruo all'esercizio dei doveri di verifica periodica dell'operato dei responsabili da parte del titolare, comunque non inferiore a sei mesi;

2) separazione logica delle immagini registrate dai diversi titolari. Il mancato rispetto delle misure previste ai punti 1) e 2) comporta l'applicazione della sanzione amministrativa stabilita dall'art. 162, comma 2-*ter*, del Codice.

Fuori dalle predette ipotesi, in tutti i casi in cui i trattamenti effettuati tramite sistemi integrati di videosorveglianza hanno natura e caratteristiche tali per cui le misure e gli accorgimenti sopra individuati non siano integralmente applicabili, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che possono determinare, il titolare del trattamento è tenuto a richiedere una verifica preliminare a questa Autorità (v. punto 3.2.1).

5. SOGGETTI PUBBLICI

I soggetti pubblici, in qualità di titolari del trattamento (*art. 4, comma 1, lett. f), del Codice*), possono trattare dati personali nel rispetto del principio di finalità, perseguendo scopi determinati, espliciti e legittimi (*art. 11, comma 1, lett. b), del Codice*), soltanto per lo svolgimento delle proprie funzioni istituzionali. Ciò vale ovviamente anche in relazione a rilevazioni di immagini mediante sistemi di videosorveglianza (*art. 18, comma 2, del Codice*).

I soggetti pubblici sono tenuti a rispettare, al pari di ogni titolare di trattamento effettuato tramite sistemi di videosorveglianza, i principi enunciati nel presente provvedimento.

Anche per i soggetti pubblici sussiste l'obbligo di fornire previamente l'informativa agli interessati (*art. 13 del Codice*), ferme restando le ipotesi prese in considerazione al punto 3.1.1. Pertanto, coloro che accedono o transitano in luoghi dove sono attivi sistemi di videosorveglianza devono essere previamente informati in ordine al trattamento dei dati personali. A tal fine, anche i soggetti pubblici possono utilizzare il modello semplificato di informativa "minima", riportato in *fac-simile* nell'allegato n. 1 al presente provvedimento (v. punto 3.1).

5.1. Sicurezza urbana

Recenti disposizioni legislative in materia di sicurezza hanno attribuito ai sindaci il compito di sovrintendere alla vigilanza ed all'adozione di atti che sono loro attribuiti dalla legge e dai regolamenti in materia di ordine e sicurezza pubblica, nonché allo svolgimento delle funzioni affidati ad essi dalla legge in materia di sicurezza e di polizia giudiziaria. Al fine di prevenire e contrastare determinati pericoli che minacciano l'incolumità pubblica e la sicurezza urbana, il sindaco può altresì adottare provvedimenti, anche contingibili e urgenti, nel rispetto dei principi generali dell'ordinamento. Infine, il sindaco, quale ufficiale del Governo, concorre ad assicurare la cooperazione della polizia locale con le forze di polizia statali, nell'ambito delle direttive di coordinamento impartite dal Ministero dell'interno.

Da tale quadro emerge che sussistono specifiche funzioni attribuite sia al sindaco, quale ufficiale del Governo, sia ai comuni, rispetto alle quali i medesimi soggetti possono utilizzare sistemi di videosorveglianza in luoghi pubblici o aperti al pubblico al fine di tutelare la sicurezza urbana.

Non spetta a questa Autorità definire il concetto di sicurezza urbana e delimitarne l'ambito operativo rispetto a quelli di ordine e sicurezza pubblica; purtuttavia, resta inteso che, nelle ipotesi in cui le attività di videosorveglianza siano assimilabili alla tutela della sicurezza pubblica, nonché alla prevenzione, accertamento o repressione dei reati, trova applicazione l'art. 53 del Codice (v. punto 3.1.1).

In ogni caso, si ribadisce l'auspicio che, nelle predette ipotesi, l'informativa, benché non obbligatoria, venga comunque resa, specie laddove i comuni ritengano opportuno rendere noto alla cittadinanza l'adozione di misure e accorgimenti, quali l'installazione di sistemi di videosorveglianza, volti al controllo del territorio e alla protezione degli individui.

5.2. Deposito dei rifiuti

In applicazione dei richiamati principi di liceità, finalità e proporzionalità, l'utilizzo di sistemi di videosorveglianza risulta lecito con riferimento alle attività di controllo volte ad accertare l'utilizzo abusivo di aree impiegate come discariche di materiali e di sostanze pericolose solo se non risulta possibile, o si riveli non efficace, il ricorso a strumenti e sistemi di controllo alternativi.

Analogamente, l'utilizzo di sistemi di videosorveglianza è lecito se risultano inefficaci o inattuabili altre misure nei casi in cui si intenda monitorare il rispetto delle disposizioni concernenti modalità, tipologia ed orario di deposito dei rifiuti, la cui violazione è sanzionata amministrativamente (art. 13, l. 24 novembre 1981, n. 689).

5.3. Utilizzo di dispositivi elettronici per la rilevazione di violazioni al Codice della strada

Gli impianti elettronici di rilevamento automatizzato delle infrazioni, utilizzati per documentare la violazione delle disposizioni in materia di circolazione stradale, analogamente all'utilizzo di sistemi di videosorveglianza, comportano un trattamento di dati personali.

5.3.1. L'utilizzo di tali sistemi è quindi lecito se sono raccolti solo dati pertinenti e non eccedenti per il perseguimento delle finalità istituzionali del titolare, delimitando a tal fine la dislocazione e l'angolo visuale delle riprese in modo da non raccogliere immagini non pertinenti o inutilmente dettagliate. In conformità alla prassi ed al quadro normativo di settore riguardante talune violazioni del Codice della strada, il Garante prescrive quanto segue:

a) gli impianti elettronici di rilevamento devono circoscrivere la conservazione dei dati alfanumerici contenuti nelle targhe automobilistiche ai soli casi in cui risultino non rispettate le disposizioni in materia di circolazione stradale;

b) le risultanze fotografiche o le riprese video possono individuare unicamente gli elementi previsti dalla normativa di settore per la predisposizione del verbale di accertamento delle violazioni (*es., ai sensi dell'art. 383 del d.P.R. n. 495/1992, il tipo di veicolo, il giorno, l'ora e il luogo nei quali la violazione è avvenuta*); deve essere effettuata una ripresa del veicolo che non comprenda o, in via subordinata, mascheri, per quanto possibile, la porzione delle risultanze video/fotografiche riguardanti soggetti non coinvolti nell'accertamento amministrativo (es., pedoni, altri utenti della strada);

c) le risultanze fotografiche o le riprese video rilevate devono essere utilizzate solo per accertare le violazioni delle disposizioni in materia di circolazione stradale anche in fase di contestazione, ferma restando la loro accessibilità da parte degli aventi diritto;

d) le immagini devono essere conservate per il periodo di tempo strettamente necessario in riferimento alla contestazione, all'eventuale applicazione di una sanzione e alla definizione del possibile contenzioso in conformità alla normativa di settore, fatte salve eventuali esigenze di ulteriore conservazione derivanti da una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria;

e) le fotografie o le immagini che costituiscono fonte di prova per le violazioni contestate non devono essere inviate d'ufficio al domicilio dell'intestatario del veicolo unitamente al verbale di contestazione, ferma restando la loro accessibilità agli aventi diritto;

f) in considerazione del legittimo interesse dell'intestatario del veicolo di verificare l'autore della violazione e, pertanto, di ottenere dalla competente autorità ogni elemento a tal fine utile, la visione della documentazione video-fotografica deve essere resa disponibile a richiesta del destinatario del verbale; al momento dell'accesso, dovranno essere opportunamente oscurati o resi comunque non riconoscibili i passeggeri presenti a bordo del veicolo.

Il mancato rispetto di quanto sopra prescritto nelle lettere da a) ad f) comporta l'applicazione della sanzione amministrativa stabilita dall'art. 162, comma 2-ter, del Codice.

5.3.2. Anche i conducenti dei veicoli e le persone che accedono o transitano in aree dove sono attivi sistemi elettronici di rilevazione automatizzata delle violazioni devono essere previamente informati in ordine al trattamento dei dati personali (*art. 13 del Codice*).

Particolari disposizioni normative vigenti individuano già talune ipotesi (come, ad es., in caso di rilevamento a distanza dei limiti di velocità) in cui l'amministrazione pubblica è tenuta a informare gli utenti in modo specifico in ordine all'utilizzo di dispositivi elettronici. L'obiettivo da assicurare è quello di un'efficace informativa agli interessati, che può essere fornita dagli enti preposti alla rilevazione delle immagini attraverso più soluzioni.

Un'idonea informativa in materia può essere anzitutto assicurata mediante l'utilizzo di strumenti appropriati che rendano agevolmente conoscibile l'esistenza e la presenza nelle aree interessate degli strumenti di rilevamento di immagini. A tal fine, svolgono un ruolo efficace gli strumenti di comunicazione al pubblico e le iniziative periodiche di diffusa informazione (*siti web*, comunicati scritti); tali forme di informazione possono essere eventualmente integrate con altre modalità (es., volantini consegnati all'utenza, pannelli a messaggio variabile, annunci televisivi e radiofonici, reti civiche e altra comunicazione istituzionale).

A integrazione di tali strumenti di comunicazione e informazione, va considerato il contributo che possono dare appositi cartelli. A tal fine, il modello semplificato di informativa "minima", riportato nel *fac-simile* in allegato, può essere utilizzato nei casi in cui la normativa in materia di circolazione stradale non prevede espressamente l'obbligo di informare gli utenti relativamente alla presenza di dispositivi elettronici volti a rilevare automaticamente le infrazioni.

Come si è detto, la normativa di settore prevede espressamente, in alcuni casi (es., rilevamento a distanza dei limiti di velocità, dei sorpassi vietati), l'obbligo di rendere nota agli utenti l'installazione degli impianti elettronici di rilevamento automatizzato delle infrazioni. In questi stessi casi è quindi possibile fare a meno di fornire un'ulteriore, distinta informativa rispetto al trattamento dei dati che riproduca gli elementi che sono già noti agli interessati per effetto degli avvisi di cui alla disciplina di settore in tema di circolazione stradale (*art. 13, comma 2, del Codice*). L'installazione di questi ultimi appositi avvisi previsti dal Codice della strada permette già agli interessati di percepire vari elementi essenziali in ordine al trattamento dei propri dati personali. Pertanto, gli avvisi che segnalano adeguatamente l'attivazione di dispositivi elettronici di rilevazione automatica delle infrazioni possono essere considerati idonei ad adempiere all'obbligo di fornire l'informativa di cui all'art. 13 del Codice.

Infine, l'obbligo di fornire tale informativa deve ritenersi soddisfatto anche quando il titolare del trattamento, pur mancando una previsione normativa che obblighi specificamente a segnalare la rilevazione automatizzata, la segnali comunque utilizzando avvisi analoghi a quelli previsti dal Codice della strada. La violazione delle disposizioni riguardanti l'informativa di cui all'art. 13 è punita con la sanzione amministrativa prevista dall'art. 161 del Codice.

5.3.3. Qualora si introducano sistemi di rilevazione degli accessi dei veicoli ai centri storici e alle zone a traffico limitato, i comuni dovranno rispettare quanto previsto dal d.P.R. 22 giugno 1999, n. 250. Tale normativa prevede che i dati trattati possono essere conservati solo per il periodo necessario per contestare le infrazioni e definire il relativo contenzioso, ferma restando l'accessibilità agli stessi per fini di polizia giudiziaria o di indagine penale (*art. 3 d.P.R. n. 250/1999*).

5.4. Ulteriori avvertenze per i sistemi di videosorveglianza posti in essere da enti pubblici e, in particolare, da enti territoriali

Anche gli enti territoriali e, in generale, i soggetti pubblici operanti sul territorio effettuano attività di videosorveglianza in forma integrata, tramite la compartecipazione ad un medesimo sistema di rilevazione, al fine di economizzare risorse e mezzi impiegati nell'espletamento delle più diverse attività istituzionali.

Questa Autorità ha già individuato al punto 4.6 un quadro di specifiche garanzie in ordine alle corrette modalità che vengono qui ulteriormente richiamate, in particolare con riferimento all'attività del controllo sul territorio da parte dei comuni, anche relativamente a quanto disposto in materia di videosorveglianza comunale.

In particolare:

a) l'utilizzo condiviso, in forma integrale o parziale, di sistemi di videosorveglianza tramite la medesima infrastruttura tecnologica deve essere configurato con modalità tali da permettere ad ogni singolo ente e, in taluni casi, anche alle diverse strutture organizzative dell'ente, l'accesso alle immagini solo nei termini strettamente funzionali allo svolgimento dei propri compiti istituzionali, evitando di tracciare gli spostamenti degli interessati e di ricostruirne il percorso effettuato in aree che esulano dalla competenza territoriale dell'ente;

b) nei casi in cui un "centro" unico gestisca l'attività di videosorveglianza per conto di diversi soggetti pubblici, i dati personali raccolti dovranno essere trattati in forma differenziata e rigorosamente distinta, in relazione alle competenze istituzionali della singola pubblica amministrazione.

Il titolare del trattamento è tenuto a richiedere una verifica preliminare a questa Autorità fuori dalle predette ipotesi, ed in tutti i casi in cui i trattamenti effettuati tramite sistemi integrati di videosorveglianza hanno natura e caratteristiche

tali per cui le misure e gli accorgimenti sopra individuati non siano integralmente applicabili, in relazione alla natura dei dati o alle modalità del trattamento, agli effetti che possono determinare o, a maggior ragione, con riferimento a quei sistemi per i quali già il punto 3.2.1 la richiede (es. sistemi di raccolta delle immagini associate a dati biometrici o c.d. intelligenti, cioè in grado di rilevare automaticamente comportamenti o eventi
anomali, segnalarli, ed eventualmente registrarli).

6. PRIVATI ED ENTI PUBBLICI ECONOMICI

6.1. Trattamento di dati personali per fini esclusivamente personali

L'installazione di sistemi di videosorveglianza -come si rileva dall'esame di numerose istanze pervenute all'Autorità viene sovente effettuata da persone fisiche per fini esclusivamente personali. In tal caso va chiarito che la disciplina del Codice non trova applicazione qualora i dati non siano comunicati sistematicamente a terzi ovvero diffusi, risultando comunque necessaria l'adozione di cautele a tutela dei terzi (*art. 5, comma 3*, del Codice, che fa salve le disposizioni in tema di responsabilità civile e di sicurezza dei dati). In tali ipotesi possono rientrare, a titolo esemplificativo, strumenti di videosorveglianza idonei ad identificare coloro che si accingono ad entrare in luoghi privati (videocitofoni ovvero altre apparecchiature che rilevano immagini o suoni, anche tramite registrazione), oltre a sistemi di ripresa installati nei pressi di immobili privati ed all'interno di condomini e loro pertinenze (quali posti auto e *box*).

Benché non trovi applicazione la disciplina del Codice, al fine di evitare di incorrere nel reato di interferenze illecite nella vita privata (*art. 615-bis c.p.*), l'angolo visuale delle riprese deve essere comunque limitato ai soli spazi di propria esclusiva pertinenza (ad esempio antistanti l'accesso alla propria abitazione) escludendo ogni forma di ripresa, anche senza registrazione di immagini, relativa ad aree comuni (cortili, pianerottoli, scale, garage comuni) ovvero ad ambiti antistanti l'abitazione di altri condomini.

6.2. Trattamento di dati personali per fini diversi da quelli esclusivamente personali

6.2.1. Consenso

Nel caso in cui trovi applicazione la disciplina del Codice, il trattamento di dati può essere lecitamente effettuato da privati ed enti pubblici economici solamente se vi sia il consenso preventivo dell'interessato, oppure se ricorra uno dei presupposti di liceità previsti in alternativa al consenso (*artt. 23 e 24 del Codice*).

Nel caso di impiego di strumenti di videosorveglianza la possibilità di acquisire il consenso risulta in concreto limitata dalle caratteristiche stesse dei sistemi di rilevazione che rendono pertanto necessario individuare un'idonea alternativa nell'ambito dei requisiti equipollenti del consenso di cui all'art. 24, comma 1, del Codice.

6.2.2. Bilanciamento degli interessi

Tale alternativa può essere ravvisata nell'istituto del bilanciamento di interessi (*art. 24, comma 1, lett. g), del Codice*). Il presente provvedimento dà attuazione a tale istituto, individuando i casi in cui la rilevazione delle immagini può avvenire senza consenso, qualora, con le modalità stabilite in questo stesso provvedimento, sia effettuata nell'intento di perseguire un legittimo interesse del titolare o di un terzo attraverso la raccolta di mezzi di prova o perseguendo fini di tutela di persone e beni rispetto a possibili aggressioni, furti, rapine, danneggiamenti, atti di vandalismo, o finalità di prevenzione di incendi o di sicurezza del lavoro.

A tal fine, possono essere individuati i seguenti casi, in relazione ai quali, con le precisazioni di seguito previste, il trattamento può lecitamente avvenire pure in assenza del consenso.

6.2.2.1. Videosorveglianza (con o senza registrazione delle immagini)

Tali trattamenti sono ammessi in presenza di concrete situazioni che giustificano l'installazione, a protezione delle persone, della proprietà o del patrimonio aziendale.

Nell'uso delle apparecchiature volte a riprendere, con o senza registrazione delle immagini, aree esterne ad edifici e immobili (perimetrali, adibite a parcheggi o a carico/scarico merci, accessi, uscite di emergenza), resta fermo che il trattamento debba essere effettuato con modalità tali da limitare l'angolo visuale all'area effettivamente da proteggere, evitando, per quanto possibile, la ripresa di luoghi circostanti e di particolari che non risultino rilevanti (vie, edifici, esercizi commerciali, istituzioni ecc.).

6.2.2.2. Riprese nelle aree condominiali comuni

Qualora i trattamenti siano effettuati dal condominio (anche per il tramite della relativa amministrazione), si evidenzia che tale specifica ipotesi è stata recentemente oggetto di una segnalazione da parte del Garante al Governo ed al Parlamento; ciò in relazione all'assenza di una puntuale disciplina che permetta di risolvere alcuni problemi applicativi evidenziati nell'esperienza di questi ultimi anni. Non è infatti chiaro se l'installazione di sistemi di videosorveglianza possa essere effettuata in base alla sola volontà dei comproprietari, o se rilevi anche la qualità di conduttori. Non è parimenti chiaro quale sia il numero di voti necessario per la deliberazione condominiale in materia (se occorra cioè l'unanimità ovvero una determinata maggioranza).

7. PRESCRIZIONI E SANZIONI

Il Garante invita tutti i titolari dei trattamenti di dati personali effettuati tramite sistemi di videosorveglianza ad attenersi alle prescrizioni indicate nel presente provvedimento.

Le misure necessarie prescritte con il presente provvedimento devono essere osservate da tutti i titolari di trattamento. In caso contrario il trattamento dei dati è, a seconda dei casi, illecito oppure non corretto, ed espone:

• all'inutilizzabilità dei dati personali trattati in violazione della relativa disciplina (*art. 11, comma 2, del Codice*);

• all'adozione di provvedimenti di blocco o di divieto del trattamento disposti dal Garante (*art. 143, comma 1, lett. c*), del Codice), e di analoghe decisioni adottate dall'autorità giudiziaria civile e penale;

• all'applicazione delle pertinenti sanzioni amministrative o penali (*artt. 161 e ss. del Codice*).

TUTTO CIÒ PREMESSO IL GARANTE:

1. prescrive ai sensi dell'art. 154, comma 1, lett. c), del Codice, ai titolari del trattamento di dati personali effettuato tramite sistemi di videosorveglianza, di adottare al più presto e, comunque, entro e non oltre i distinti termini di volta in volta indicati decorrenti dalla data di pubblicazione del presente provvedimento nella Gazzetta Ufficiale della Repubblica italiana, le misure e gli accorgimenti illustrati in premessa e di seguito individuati concernenti l'obbligo di:

a) entro dodici mesi, rendere l'informativa visibile anche quando il sistema di videosorveglianza sia eventualmente attivo in orario notturno (punto 3.1);

b) entro sei mesi, sottoporre i trattamenti che presentano rischi specifici per i diritti e le libertà fondamentali degli interessati, alla verifica preliminare ai sensi dell'art. 17 del Codice (punto 3.2.1);

c) entro dodici mesi, adottare, le misure di sicurezza a protezione dei dati registrati tramite impianti di videosorveglianza (punto 3.3);

d) entro sei mesi, adottare le misure necessarie per garantire il rispetto di quanto indicato nei punti 4.6 e 5.4, per quanto concerne i sistemi integrati di videosorveglianza;

2. individua, nei termini di cui in motivazione, ai sensi dell'art. 24, comma 1, lett. *g*), del Codice, i casi nei quali il trattamento dei dati personali mediante videosorveglianza può essere effettuato da soggetti privati ed enti pubblici economici, nei limiti e alle condizioni indicate, per perseguire legittimi interessi e senza richiedere il consenso degli interessati (punto 6.2.2);

3. individua nell'allegato 1, ai sensi dell'art. 13, comma 3, del Codice, un modello semplificato di informativa utilizzabile alle condizioni indicate in motivazione (punto 3.1);

4. individua nell'allegato 2, ai sensi dell'art. 13, comma 3, del Codice, un modello semplificato di informativa utilizzabile alle condizioni indicate in motivazione, al fine di rendere noto agli interessati l'attivazione di un collegamento del sistema di videosorveglianza con le forze di polizia (punti 3.1.3 e 4.6, lett. c));

5. segnala l'opportunità che, anche nell'espletamento delle attività di cui all'art. 53 del Codice, l'informativa, benché non obbligatoria, sia comunque resa in tutti i casi nei quali non ostano in concreto specifiche ragioni di tutela e sicurezza pubblica o di prevenzione, accertamento o repressione dei reati (punto 5.1);

6. dispone, ai sensi dell'art. 143, comma 2, del Codice, che copia del presente provvedimento sia trasmessa al Ministero della giustizia-Ufficio pubblicazione leggi e decreti per la sua pubblicazione sulla *Gazzetta Ufficiale* della Repubblica italiana.

Roma, 8 aprile 2010

IL PRESIDENTE F.to Pizzetti
IL RELATORE F.to Pizzetti
IL SEGRETARIO GENERALE REGGENTE F.to De Paoli

NOTE

ALLEGATI

ALLEGATO n. 1

• Per le modalità di utilizzazione del modello, cfr. punto 3.1.

• Se le immagini non sono registrate, sostituire il termine "registrazione" con quello di "rilevazione".

ALLEGATO n. 2

• Per le modalità di utilizzazione del modello, cfr. punti 3.1.3 e 4.6, lett. *c*).

• Se le immagini non sono registrate, sostituire il termine "registrazione" con quello di "rilevazione".

Verifica preliminare: conservazione di immagini per un periodo eccedente i tempi fissati dal provvedimento generale Garante in materia di videosorveglianza - 4 novembre 2010

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vicepresidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti, e del dott. Daniele De Paoli, segretario generale;

ESAMINATA la richiesta di verifica preliminare presentata da ST Incard s.r.l. ai sensi dell'art. 17 del d.lg. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali);
Visto il provvedimento generale in materia di videosorveglianza dell'8 aprile 2010 (doc. web n. 1712680), con particolare riferimento al punto 3.4;
ESAMINATA la documentazione acquisita agli atti;
VISTE le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;
RELATORE il prof. Francesco Pizzetti;

PREMESSO

1. L'istanza della società.

1.1. ST Incard s.r.l., società operante nel settore della "progettazione e produzione di "smart card" principalmente per i mercati GSM, Bancario e Identification", ha formulato istanza di verifica preliminare ai sensi dell'art. 17 del Codice al fine di poter conservare, per un arco temporale pari a 90 giorni, le immagini registrate attraverso il sistema di videosorveglianza installato presso la sede operativa della società, sita in Marcianise (CE); ciò, in deroga a quanto previsto dal Garante con il provvedimento generale in materia di videosorveglianza dell'8 aprile 2010, che prevede un termine massimo di conservazione delle immagini pari a sette giorni.
L'istanza avanzata dalla società muove dall'assunto che l'attività produttiva svolta sarebbe *"di fatto assimilabile a quella di una zecca di stato, che produce denaro contante"* e che, correlativamente, le carte bancarie e le carte GSM realizzate costituirebbero *"prodotti finali ad altissimo rischio di illecito"* (*cfr.* all. "B" all'istanza, pp. 3 e 6).
Tali prodotti sarebbero destinati a segmenti di mercato nel quale *"gli "operatori", ai fini della [loro] commercializzazione […], chiedono tassativamente al "produttore" […] di garantire elevati standard di sicurezza certificati"*; ciò si tradurrebbe nella necessità per le stesse aziende di adottare *"stringenti misure di sicurezza e di controllo"* idonee a superare il vaglio degli appositi enti certificatori (tra i più noti, VISA, MASTERCARD, GSM Association), il cui benestare costituirebbe presupposto *"per il rilascio e/o rinnovo delle [stesse] certificazioni"*.
Tra gli standard di sicurezza predisposti dalla società figura, appunto, la conservazione delle immagini registrate per un arco temporale di 90 giorni. Tale periodo di conservazione risponderebbe all'esigenza di rafforzare le misure di prevenzione e contrasto contro possibili comportamenti fraudolenti (allo stato mai verificatisi), consentendo l'accertamento a posteriori, attraverso *"una serie di analisi retroattive che coinvolgono le diverse fasi [della] produzione"*, di eventuali illeciti di natura penale (in particolare, furti, contraffazioni e truffe) posti in essere prevalentemente da personale operante presso la società (*cfr.* nota del 3 maggio 2010, p. 4; *cfr.* anche nota del 30 giugno 2010, p. 2); illeciti che, anche in ragione delle diverse fasi che contraddistinguono la produzione dei supporti (cui si aggiungono i tempi di spedizione al cliente e di successiva attivazione delle "card" ad opera dell'utente finale), potrebbero essere scoperti anche a notevole distanza di tempo dalla loro commissione.
Per tali ragioni, secondo la società, il termine massimo di conservazione delle immagini, individuato dall'Autorità nel menzionato provvedimento generale, risulterebbe inadeguato, in quanto non consentirebbe di *"poter recuperare, attraverso la registrazione, il momento in cui la carta è stata prodotta, così da verificare tutto il processo produttivo e rilevare eventuali atti criminosi verificatisi nel corso delle diverse fasi produttive"*; e ciò a tacere del fatto che la conservazione delle immagini per un arco temporale di 90 giorni sarebbe richiesta dagli stessi enti certificatori quale "periodo minimo", anche in vista del rilascio/rinnovo delle stesse certificazioni.
A tale riguardo, la società ha peraltro precisato di aver rappresentato agli enti certificatori l'esistenza di alcuni "vincoli legali" concernenti la conservazione delle immagini, manifestando a più riprese –ancorché, allo stato, invano– la necessità di una riconsiderazione dei tempi di conservazione alla luce delle attuali previsioni normative; nondimeno, la società ha evidenziato che la mancata conservazione delle immagini per i tempi prolungati richiesti dai suoi committenti potrebbe incidere sullo stesso rinnovo delle certificazioni e sulla conclusione di futuri contratti per la produzione e distribuzione delle suddette smart card.
1.2. A corredo della propria istanza, la società ha fatto pervenire:
a) la policy adottata in materia di videosorveglianza (nella quale vengono ribadite le motivazioni già enunciate nella propria richiesta di autorizzazione, avuto riguardo alle *"potenziali azioni illecite realizzabili con i materiali prodotti"* e

alle *"esplicite richieste di sicurezza imposte dai clienti e da questi ultimi verificate con costanti e periodici programmi di audit e di certificazione"*, oltre all'esistenza di altri "sistemi di sicurezza a protezione delle aree esterne e interne all'azienda");

b) la copia di alcuni estratti relativi alle "prescrizioni" impartite dagli enti certificatori in tema di videosorveglianza, dalle quali, pur risultando confermati i tempi di conservazione delle immagini frutto di videosorveglianza, risulta che, ove prescrizioni legali vigenti nell'ordinamento precludano la possibilità di utilizzare tali sistemi, debbano essere implementate misure di controllo compensative;

c) la copia dell'accordo sindacale sottoscritto con le organizzazioni di rappresentanza dei lavoratori in conformità all'art. 4 della legge n. 300/1970.

La società, che in un primo momento si era riservata di produrre anche documentazione proveniente dagli enti certificatori e attestante *"i tempi necessari per l'accertamento delle truffe"*, oltre che *"i tempi e le modalità necessarie per l'indagine su come e quando si sia verificato l'atto criminoso"*, ha successivamente precisato, stante alcune difficoltà riscontrate nell'acquisizione del materiale, di non essere in grado di poterla fornire in tempi brevi (cfr. nota pervenuta il 6 settembre 2010).

2. I principi di pertinenza e non eccedenza e di proporzionalità.

La richiesta formulata dalla società – che ha ad oggetto il trattamento di dati personali (consistente nella raccolta, registrazione e, per quanto qui di interesse, nella successiva conservazione dell'immagine degli interessati, in particolare dei lavoratori) mediante il sistema di videosorveglianza già installato presso di essa – deve essere valutata, tenuto conto degli elementi complessivamente acquisiti, soprattutto alla luce dei principi di pertinenza e non eccedenza e di proporzionalità stabiliti dall'art. 11, comma 1, lett. *d*) ed *e*) del Codice per la protezione dei dati personali.

Al riguardo, occorre anzitutto rilevare che l'esame della documentazione prodotta ha evidenziato, diversamente da quanto sostenuto dalla società, che le "prescrizioni" impartite dagli enti certificatori sono "derogabili" nel caso in cui sussistano "restrizioni legali" relative all'utilizzo di sistemi di videosorveglianza, come si evince da due degli estratti allegati alla richiesta di autorizzazione ("*If legal restrictions preclude the use of CCTV equipment, compensating controls must be implemented"* – vedi "Global Physical Security Requirements for Card Vendors, October 2008").

Inoltre, sotto distinto profilo, vale rilevare che non è risultata provata (nonostante l'offerta di produzione documentale originariamente formulata, rimasta senza esito) l'asserita necessità di conservare per un così esteso arco temporale le immagini riprese a mezzo dell'impianto di videosorveglianza utilizzato; ciò, peraltro, a fronte di una semplice prospettazione di ipotetiche condotte criminose che, allo stato, non risultano essersi mai concretamente verificate presso l'impianto di Marcianise, verosimilmente anche in ragione delle numerose misure di sicurezza già approntate dalla società e analiticamente evidenziate nella nota del 30 giugno 2010 (accessi controllati; sensori di allarme e di movimento; sistemi di criptazione dei dati; divieto di utilizzo di strumenti di archiviazione nelle aree destinate alla produzione dei supporti; ecc.), tali da far risultare gli indicati tempi di conservazione come eccedenti e sproporzionati.

Infine, a quanto appena rilevato deve aggiungersi che la stessa giurisprudenza giuslavoristica ha ripetutamente riconosciuto al datore di lavoro la possibilità, nel rispetto delle garanzie previste dall'ordinamento (in particolare, gli artt. 2, 3 e 6 della legge n. 300/1970), di adibire a mansioni di vigilanza e tutela del patrimonio aziendale anche propri dipendenti, a mezzo dei quali poter controllare l'attività di altri lavoratori per accertare eventuali comportamenti fraudolenti estranei alla prestazione lavorativa e incidenti sull'integrità del patrimonio aziendale (tra le tante, cfr. Cass. 9 giugno 1989, n. 2813; Cass. 18 febbraio 1997, n. 1455, non diversamente, Cass. 3 luglio 2001, n. 8998).

Di conseguenza, alla luce degli elementi acquisiti, deve ritenersi che la pretesa di ST Incard s.r.l. di conservare per 90 giorni le immagini registrate mediante l'impianto di videosorveglianza installato presso la sede di Marcianise non possa essere accolta, perché in contrasto con i principi di pertinenza e non eccedenza e di proporzionalità stabiliti dall'art. 11, comma 1, lett. d) ed e) del Codice.

L'odierna pronunzia, resa sulla scorta delle attuali acquisizioni istruttorie, non preclude all'Autorità di adottare una diversa determinazione nel caso in cui la ST Incard s.r.l. proponga una nuova domanda maggiormente documentata, da valutare alla luce della normativa esistente.

TUTTO CIÒ PREMESSO IL GARANTE

rigetta l'istanza formulata da ST Incard s.r.l. per conservare, per un periodo eccedente il termine massimo di sette giorni fissato dall'Autorità con il provvedimento generale dell'8 aprile 2010, le immagini registrate mediante l'impianto di videosorveglianza installato presso la sede di Marcianise, perché in contrasto con i principi di pertinenza e non eccedenza e di proporzionalità stabiliti dall'art. 11, comma 1, lett. *d*) ed *e*) del Codice per la protezione dei dati personali.

Roma, 4 novembre 2010
IL PRESIDENTE Pizzetti
IL RELATORE Pizzetti
IL SEGRETARIO GENERALE De Paoli

Comunicato stampa - 16 febbraio 2011

Immobili di proprietà pubblica e norme sulla privacy

La risposta del Garante a due enti pubblici milanesi

Le norme sulla protezione dei dati personali non pongono ostacoli alla conoscenza dei nominativi degli affittuari degli immobili di proprietà di enti pubblici da parte dei consiglieri comunali, provinciali e regionali, laddove la richiesta sia utile per l'espletamento del loro mandato.

Lo ha chiarito il Garante privacy in risposta ai quesiti posti nei giorni scorsi da parte di due strutture milanesi, Ospedale Maggiore Policlinico e Pio Albergo Trivulzio, riguardo alla messa a disposizione dei dati relativi agli immobili di loro proprietà.

La normativa sulla protezione dei dati personali - ha sottolineato l'Autorità - "non rappresenta un ostacolo alla trasparenza amministrativa, specie laddove quest'ultima riguardi il corretto utilizzo di beni e risorse da parte di soggetti pubblici".

In tale quadro, i consiglieri comunali provinciali e regionali hanno il diritto di ottenere dalle amministrazioni di riferimento, nonché dalle loro aziende ed enti dipendenti, tutte le notizie e le informazioni utili per l'espletamento del loro mandato. Spetta dunque alle due strutture ospedaliere verificare che le richieste dei consiglieri siano riferite al mandato istituzionale. I consiglieri, da parte loro, una volta ottenute tali informazioni, sono comunque tenuti a garantire la necessaria riservatezza nel caso in cui i dati ricevuti siano sensibili o tali da ledere la dignità delle persone.

Anche riguardo alla conoscenza di tali informazioni da parte dei media, le norme sulla privacy - ha ricordato il Garante – non hanno inciso in modo restrittivo su quelle relative alla trasparenza amministrativa e all'accesso ai documenti.

Spetta, anche in questo caso, all'amministrazione verificare se accogliere, sulla base dell'interesse e dei motivi rappresentati dagli organi di informazione, l'istanza di accesso. Una volta ritenuta legittima la richiesta di accesso, il giornalista sarà tenuto a valutare l'interesse pubblico nella diffusione delle informazioni lecitamente acquisite e verificare che esse siano pertinenti e non eccedenti, e comunque non lesive della dignità delle persone interessate.

Per quanto riguarda, infine, la pubblicazione sui siti web di dati personali relativi agli affittuari, il Garante ha precisato che essa è in generale ammessa se prevista da una norma di legge o di regolamento. In mancanza di tale presupposto, gli enti interessati possono comunque prevedere la diffusione di tali informazioni nell'ambito del Piano triennale per la trasparenza e l'integrità che ogni amministrazione è tenuta a predisporre. Anche in questo caso, nella diffusione dei dati deve essere sempre rispettato il principio di pertinenza e non eccedenza.

Roma, 16 febbraio 2011