FILM COMMISSION TORINO PIEMONTE

VIA CAGLIARI 42
10153 - TORINO (TO)
P.IVA 97601340017

Regolamento per la protezione dei dati personali, economici, sensibili e giudiziari 2015

ai sensi del Codice in Materia di Protezione dei Dati Personali
Decreto Legislativo 30 giugno 2003 n.196

Privacy

Indice

Capitolo 1

Regolamento per la protezione dei dati personali, economici, sensibili e giudiziari

1.1 Scopo

Il presente **Regolamento per la protezione dei dati personali, economici, sensibili e giudiziari** ha valore di ordine di servizio a cui si deve attenere tutto il personale dipendente e non; esso è redatto per soddisfare tutte le misure minime di sicurezza che debbono essere adottate in via preventiva da tutti coloro che trattano dati personali, conformemente a quanto previsto dal CODICE IN MATERIA DI PROTEZIONE DI DATI PERSONALI (Gazzetta Ufficiale 29 luglio 2003, Serie generale n. 174, Supplemento ordinario n. 123/L).

In esso sono trattati i requisiti per impostare e gestire un Sistema di Gestione della Sicurezza delle Informazioni (SGSI o ISMS dall'inglese Information Security Management System), ed include aspetti relativi alla sicurezza logica, fisica ed organizzativa, secondo lo Standard ISO/IEC 27001:2005.

Inoltre costituisce un valido strumento per la adozione delle misure idonee previste dall'articolo 31 dello stesso Codice e dal DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA.

Grazie al presente Regolamento è possibile ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, intendendosi per misure di sicurezza il complesso degli accorgimenti tecnici, informatici, organizzativi, logistici e procedurali di sicurezza. Si intende così proteggere l'organizzazione dalla commissione dei reati presupposto per la responsabilità amministrativa dell'ente quali delitti informatici e trattamento illecito di dati ai sensi dell'art. 24-bis del D.Lgs. 231/2001 (articolo aggiunto dalla L. 18 marzo 2008 n. 48, art. 7).

1.2 Campo di applicazione

Il Regolamento definisce le politiche e gli standard di sicurezza in merito al trattamento dei dati personali, economici, sensibili e giudiziari.

Il Regolamento riguarda il trattamento dei dati economici e di tutti i dati personali:

1. Sensibili
2. Giudiziari
3. Comuni

Il Regolamento si applica al trattamento di tutti i dati personali per mezzo di:

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

Il Regolamento deve essere conosciuto ed applicato da tutte le funzioni che fanno parte dell'organizzazione.

1.3 Riferimenti normativi

1. CODICE IN MATERIA DI DATI PERSONALI (Gazzetta Ufficiale 29 luglio 2003, Serie generale n. 174, Supplemento ordinario n. 123/L)
2. DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA (Arti. da 33 a 36 del codice)
3. STANDARD ISO/IEC serie 27000

Segue l'elenco dei provvedimenti legislativi di modifica ed integrazione del Codice:

- decreto legge 27 gennaio 2012, n. 3;
- decreto legge 6 dicembre 2011, n. 201 convertito, con modificazioni, dalla legge 22 dicembre 2011, n. 214;
- decreto legge 13 maggio 2011, n. 70 convertito, con modificazioni, dalla legge 12 luglio 2011, n. 106;
- legge 4 novembre 2010, n. 183;
- legge 29 luglio 2010, n. 120;
- decreto-legge del 25 settembre 2009, n. 135 convertito, con modificazioni, dalla legge 20 novembre 2009, n. 166;
- legge 4 marzo 2009, n. 15
- decreto-legge del 30 dicembre 2008, n. 207 convertito, con modificazioni, dalla legge 27 febbraio 2009, n. 14;
- decreto-legge 25 giugno 2008, n. 112 convertito, con modificazioni, dalla legge 6 agosto 2008 n. 133;
- decreto legislativo 30 maggio 2008, n. 109;
- legge 18 marzo 2008, n. 48, ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno
- decreto-legge 28 dicembre 2006, n. 300 convertito, con modificazioni, dalla legge 26 febbraio 2007, n. 17;
- decreto-legge 12 maggio 2006, n. 173 convertito, con modificazioni, dalla legge 12 luglio 2006, n. 228;
- decreto-legge 30 dicembre 2005, n. 273 convertito, con modificazioni, dalla legge 23 febbraio 2006, n. 51;
- decreto legge 30 novembre 2005, n. 245 convertito, con modificazioni, dalla legge 27 gennaio 2006, n. 21;
- decreto legislativo 7 settembre 2005, n. 209;

- decreto-legge 27 luglio 2005, n. 144 convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155;
- decreto-legge 30 dicembre 2004, n. 314 convertito, con modificazioni, dalla legge 1 marzo 2005, n. 26;
- decreto-legge 9 novembre 2004, n. 66 convertito, con modificazioni, dalla legge 27 dicembre 2004, n. 306;
- decreto-legge 24 giugno 2004, n. 158 convertito, con modificazioni, dalla legge 27 luglio 2004, n. 188;
- decreto-legge 29 marzo 2004, n. 81 convertito, con modificazioni, dalla legge 26 maggio 2004, n. 138;
- decreto legislativo 22 gennaio 2004, n. 42;
- decreto-legge 24 dicembre 2003, n. 354 convertito, con modificazioni, dalla legge 26 febbraio 2004, n. 45

Segue l'elenco dei provvedimenti di normazione internazionale:

- ISO/IEC 27000: Principles and vocabulary
- ISO/IEC 27001: Information security management system - Requirements
- ISO/IEC 27002: Information security management system - Best practice
- ISO/IEC 27003: Information security management system - Implementation guidance
- ISO/IEC 27004: Information security management system - metrics and measurement
- ISO/IEC 27005: Information security management system - Risk management

1.4 Definizioni

Cfr. Nota [1]

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

Dato personale Qualunque informazione relativa a persona fisica identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

Dati sensibili I dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

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

[1] le definizione risultano così modificate in base al DECRETO-LEGGE 6 dicembre 2011, n. 201 Disposizioni urgenti per la crescita, l'equità e il consolidamento dei conti pubblici. (GU n.284 del 6-12-2011 - Suppl. Ordinario n. 251) convertito con modificazioni dalla L. 22 dicembre 2011, n. 214 (in SO n. 276, relativo alla G.U. 27-12-2011, n. 300). In sostanza, dal concetto di dati personali sono stati esclusi quelli riferiti a persona giuridica, ente od associazione, limitandone l'ambito ai soli dati riferiti a persone fisiche.

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

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

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

Interessato La persona fisica cui si riferiscono i dati personali.

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

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

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

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

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

Comunicazione elettronica Ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico.

Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un abbonato o utente ricevente, identificato o identificabile.

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

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

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

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

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

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

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

1.5 Definizioni ulteriori

A seguito delle modificazioni normative introdotte nel corso del 2011, risulta utile all'interno di codesto documento, estendere le precedenti definizioni, introducendo

Dati aziendali o ontologici Qualunque informazione relativa a persona giuridica, ente od associazione identificati o identificabili, anche indirettamente.

Azienda o Ente interessato Persona giuridica, ente od associazione cui si riferiscono i dati.

Dati Economici Dati personali o aziendali che riguardano informazioni di carattere economico.

Dati genetici Dati sensibili riguardanti le informazioni sul genoma di una persona fisica.

Trattamenti effettuati per finalità amministrativo-contabili I trattamenti effettuati per finalità amministrativo-contabili sono quelli connessi allo svolgimento delle attività di natura organizzativa, amministrativa, finanziaria e contabile, a prescindere dalla natura dei dati trattati. In particolare, perseguono tali finalità le attività organizzative interne, quelle funzionali all'adempimento di obblighi contrattuali e precontrattuali, alla gestione del rapporto di lavoro in tutte le sue fasi, alla tenuta della contabilità e all'applicazione delle norme in materia fiscale, sindacale, previdenziale-assistenziale, di salute, igiene e sicurezza sul lavoro.

Capitolo 2

Ruoli, compiti e nomine

2.1 Titolare del trattamento dei dati personali

2.1.1 Compiti del titolare del trattamento dei dati personali

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

Il Titolare del trattamento deve assicurare e garantire direttamente che vengano adottate le misure di sicurezza ai sensi del CODICE IN MATERIA DI DATI PERSONALI e del DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA tese a ridurre al minimo il rischio di distruzione dei dati, accesso non autorizzato o trattamento non consentito, previe idonee istruzioni fornite per iscritto.

Il Titolare del trattamento, in relazione all'attività svolta, può individuare, nominare e incaricare per iscritto, se lo ritiene opportuno uno o più Responsabili della sicurezza dei dati che assicurino e garantiscano che vengano adottate le misure di sicurezza ai sensi del CODICE IN MATERIA DI DATI PERSONALI e del DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA. Qualora il Titolare del trattamento ritenga di non nominare alcun Responsabile della sicurezza dei dati, ne assumerà tutte le responsabilità e funzioni.

2.1.2 Nomina del titolare del titolare del trattamento dei dati personali

La nomina del titolare del Titolare del trattamento dei dati personali deve essere effettuata dal legale rappresentante della ditta, società, ente, associazione od organizzazione, mediante una lettera di incarico (MOD_TT) in cui sono specificate le responsabilità che gli sono affidate e deve essere controfirmata dall'interessato per accettazione.

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

2.2 Responsabile della sicurezza dei dati personali

2.2.1 Compiti del responsabile della sicurezza dei dati personali

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

1. Garantire che tutte le misure di sicurezza riguardanti i dati personali siano applicate.

2. Redigere ed aggiornare ad ogni variazione l'elenco delle sedi in cui vengono trattati i dati.
3. Redigere ed aggiornare ad ogni variazione l'elenco degli uffici in cui vengono trattati i dati.
4. Redigere ed aggiornare ad ogni variazione l'elenco delle banche dati oggetto di trattamento.
5. Se il trattamento è effettuato con mezzi informatici, redigere ed aggiornare ad ogni variazione l'elenco dei sistemi di elaborazione.
6. Definire e successivamente verificare con cadenza semestrale le modalità di acceso ai locali e le misure da adottare per la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità come specificato in seguito.
7. Decidere se affidare il trattamento dei dati in tutto o in parte all'esterno della struttura del titolare.
8. Qualora il trattamento dei dati sia stato affidato in tutto o in parte all'esterno della struttura del titolare controllare e garantire che tutte le misure di sicurezza riguardanti i dati personali siano applicate.
9. Se il trattamento è effettuato con mezzi informatici, individuare, nominare e incaricare per iscritto, uno o più Responsabili della gestione e della manutenzione degli strumenti elettronici.
10. Se il trattamento è effettuato con mezzi informatici, individuare, nominare e incaricare per iscritto, uno o più Incaricati della custodia delle copie delle credenziali qualora vi sia più di un incaricato del trattamento.
11. Se il trattamento è effettuato con mezzi informatici, individuare, nominare e incaricare per iscritto, uno o più Incaricati delle copie di sicurezza delle banche dati.
12. Custodire e conservare i supporti utilizzati per le copie dei dati .
13. Il Responsabile della sicurezza dei dati personali, in relazione all'attività svolta, può individuare, nominare e incaricare per iscritto, se lo ritiene opportuno uno o più Responsabili del trattamento con il compito di individuare, nominare e incaricare per iscritto, gli Incaricati del trattamento dei dati personali.
14. Qualora il Responsabile della sicurezza dei dati personali ritenga di non nominare alcun Responsabile del trattamento, ne assumerà tutte le responsabilità e funzioni.

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

2.2.2 Nomina del responsabile della sicurezza dei dati personali

La nomina di ciascun Responsabile della sicurezza dei dati personali deve essere effettuata dal Titolare del trattamento con una lettera di incarico (MOD_RST) in cui sono specificate le responsabilità che gli sono affidate e deve essere controfirmata dall'interessato per accettazione.

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

Il Titolare del trattamento deve informare ciascun Responsabile della sicurezza dei dati personali delle responsabilità che gli sono affidate in relazione a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dal CODICE IN MATERIA DI DATI PERSONALI (Gazzetta Ufficiale 29 luglio 2003, Serie generale n. 174, Supplemento ordinario n. 123/L) e dal DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA.

Il Titolare del trattamento deve consegnare a ciascun Responsabile della sicurezza dei dati personali una copia di tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina.

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

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

2.3 Responsabile del trattamento dei dati personali

2.3.1 Compiti del responsabile del trattamento dei dati personali

Il Responsabile del trattamento è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo che ha il compito di individuare, nominare e incaricare per iscritto, gli Incaricati del trattamento dei dati personali.

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

1. Nominare gli incaricati del trattamento per le Banche di dati che gli sono state affidate.
2. Di sorvegliare che il trattamento sia effettuato nei termini e nei modi stabiliti dal Codice in materia di dati personali.
3. Di dare le istruzioni adeguate agli incaricati del trattamento effettuato con strumenti elettronici e non.
4. Periodicamente, e comunque almeno annualmente, verifica la sussistenza delle condizioni per la conservazione dei profili di autorizzazione degli incaricati del trattamento dei dati personali.

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

2.3.2 Nomina dei responsabili del trattamento dei dati personali

La nomina di ciascun Responsabile del trattamento deve essere effettuata dal Responsabile della sicurezza dei dati personali con una lettera di incarico in cui sono specificate le responsabilità che gli sono affidate e deve essere controfirmata dall'interessato per accettazione.

Copia della lettera di nomina (MOD_RT) accettata deve essere conservata a cura del Responsabile della sicurezza dei dati personali in luogo sicuro.

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

Il Responsabile della sicurezza dei dati personali deve informare ciascun Responsabile del trattamento delle responsabilità che gli sono affidate in relazione a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dal CODICE IN MATERIA DI DATI PERSONALI (Gazzetta Ufficiale 29 luglio 2003, Serie generale n. 174, Supplemento ordinario n. 123/L) e dal DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA.

Il Responsabile della sicurezza dei dati personali deve consegnare a ciascun Responsabile del trattamento una copia di tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina.

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

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

2.4 Incaricato del trattamento dei dati personali

2.4.1 Compiti degli incaricati del trattamento dei dati personali

Gli Incaricati del trattamento sono le persone fisiche autorizzate a compiere operazioni di trattamento sui dati personali da un Responsabile del trattamento.

In particolare gli incaricati del trattamento dei dati personali debbono osservare le seguenti disposizioni:

1. Gli incaricati che hanno ricevuto credenziali di autenticazione per il trattamento dei dati personali, debbono conservare con la massima segretezza le parole chiave e i dispositivi di autenticazione in loro possesso e uso esclusivo.
2. La parola chiave, quando è prevista dal sistema di autenticazione, deve essere composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito.
3. La parola chiave non deve contenere riferimenti agevolmente riconducibili all'incaricato.
4. L'incaricato del trattamento deve modificarla al primo utilizzo e, successivamente, almeno ogni sei mesi.
5. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave deve essere modificata almeno ogni tre mesi.
6. Gli incaricati del trattamento non debbono in nessun caso lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento dei dati personali.
7. Gli incaricati del trattamento debbono controllare e custodire, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, gli atti e i documenti contenenti dati personali.
8. Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

2.4.2 Nomina degli incaricati del trattamento dei dati personali

La nomina di ciascun Incaricato del trattamento dei dati personali deve essere effettuata dal Responsabile del trattamento con una lettera di incarico in cui sono specificati i compiti che gli sono stati affidati che deve essere controfirmata dall'interessato per presa visione.

Copia della lettera di nomina (MOD_IT) firmata deve essere conservata a cura del Responsabile del trattamento in luogo sicuro.

Il Responsabile del trattamento deve informare ciascun Incaricato del trattamento dei dati personali delle responsabilità che gli sono affidate in relazione a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dal CODICE IN MATERIA DI DATI PERSONALI (Gazzetta

Ufficiale 29 luglio 2003, Serie generale n. 174, Supplemento ordinario n. 123/L) e dal DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA.

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

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

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

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

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

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

2.5 Sistema di autorizzazione

I Responsabili del trattamento hanno il compito di individuare gli Incaricati del trattamento per ogni tipologia di banca di dati personali trattata.
Il tipo di trattamento effettuato da ogni singolo Incaricato del trattamento può essere differenziato.

In particolare ad ogni Incaricato del trattamento può essere data dal Responsabile del trattamento la possibilità di:

1. Inserire nuove informazioni nella banca di dati personali
2. Consultare le informazioni, accedendovi in visualizzazione e stampa
3. Modificare le informazioni esistenti nella banca di dati personali
4. Annullare e cancellare le informazioni esistenti nella banca di dati personali
5. Trasportare e trasferire i supporti su cui sono memorizzati i dati (dossier, faldoni, documenti cartacei, hard disk, nastri magnetici, cd, dvd, ecc.
6. Esclusivamente conservare i supporti, senza accedere ai contenuti
7. Procedere con operazioni di diffusione dei dati
8. Manutenere e amministrare la banca di dati personali

Capitolo 3

Disposizioni fondamentali per il trattamento dei dati

3.1 Nomina e istruzioni agli incaricati

Per ogni archivio i Responsabili della sicurezza dei dati personali debbono definire l'elenco degli incaricati autorizzati ad accedervi e impartire istruzioni tese a garantire un controllo costante nell'accesso negli archivi.

Gli incaricati che trattano atti e documenti contenenti dati personali sono tenuti a conservarli e restituirli al termine delle operazioni.

Qualora i documenti contengano dati sensibili o giudiziari ai sensi dell'art. 4 del CODICE IN MATERIA DI DATI PERSONALI, gli incaricati del trattamento sono tenuti a conservarli fino alla restituzione in contenitori muniti di serratura.

L'accesso agli archivi contenenti documenti ove sono presenti dati sensibili o giudiziari è consentito, dopo l'orario di chiusura, previa identificazione e registrazione dei soggetti

3.2 Copie degli atti e dei documenti

In base a quanto stabilito dal CODICE IN MATERIA DI DATI PERSONALI (Gazzetta Ufficiale 29 luglio 2003, Serie generale n. 174, Supplemento ordinario n. 123/L) e dal DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA, è fatto divieto a chiunque di:

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

3.3 Elenco dei trattamenti di dati personali

3.3.1 Elenco delle sedi e degli uffici in cui vengono trattati i dati

Al Responsabile della sicurezza dei dati personali è affidato il compito di redigere e di aggiornare ad ogni variazione l'elenco delle sedi in cui viene effettuato il trattamento dei dati.

Per redigere l'Elenco delle sedi in cui vengono trattati i dati deve essere utilizzato il modulo MOD_LOC che deve essere aggiornato e conservato in luogo sicuro a cura del Responsabile della sicurezza dei dati personali.

3.3.2 Elenco degli archivi dei dati oggetto del trattamento

Al Responsabile della sicurezza dei dati personali 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 contenute indicando se si tratta di:

1. Dati personali
2. Dati sensibili
3. Dati giudiziari

ed eventualmente di

1. Dati aziendali o ontologici
2. Dati economici
3. Dati genetici

Per l'individuazione degli archivi dei dati oggetto del trattamento deve essere utilizzato il modulo MOD_TRT_XX (dove XX rappresenta un codice identificativo dell'archivio), che deve essere compilato e conservato dal Responsabile della sicurezza dei dati personali in luogo sicuro.

3.4 Distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati

3.4.1 Elenco dei soggetti autorizzati al trattamento dei dati

Il Responsabile della sicurezza dei dati personali ha il compito di assegnare le credenziali di autenticazione e di aggiornare l'elenco del personale autorizzato al trattamento dei dati utilizzando il già citato modulo MOD_IT, che deve essere conservato a cura del Responsabile della sicurezza dei dati personali, in luogo sicuro e deve essere trasmesso in copia controllata all'Incaricato della custodia delle copie delle credenziali di competenza.

3.4.2 Verifiche periodiche delle condizioni per il mantenimento delle autorizzazioni

Il Responsabile della sicurezza dei dati personali ha il compito di verificare ogni anno, entro il 31 dicembre, le credenziali di autenticazione e di aggiornare l'elenco dei soggetti autorizzati al trattamento dei dati utilizzando il modulo MOD_IT che deve essere conservato a cura del Responsabile della sicurezza dei dati personali, in luogo sicuro e deve essere trasmesso in copia controllata agli Incaricati della custodia delle copie delle credenziali di competenza.

3.5 Misure da adottare per la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità

3.5.1 Misure generali

In considerazione di quanto disposto dal CODICE IN MATERIA DI DATI PERSONALI (Gazzetta Ufficiale 29 luglio 2003, Serie generale n. 174, Supplemento ordinario n. 123/L) e dal DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA, è fatto divieto a chiunque di:

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

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

Al Responsabile della sicurezza dei dati personali è affidato il compito di redigere e di aggiornare ad ogni variazione l'elenco degli uffici in cui viene effettuato il trattamento dei dati, e di nominare per ciascun ufficio un 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 Responsabile della sicurezza dei dati personali deve definire le modalità di accesso agli uffici in cui sono presenti sistemi o apparecchiature di accesso ai dati trattati.

Il Responsabile della sicurezza dei dati personali deve informare con una comunicazione scritta l'incaricato dell'ufficio dei compiti che gli sono stati affidati utilizzando il modello MOD_ACL.

3.6 Formazione degli incaricati del trattamento

Il Responsabile del trattamento dei dati personali valuta, per ogni incaricato a cui ha affidato il trattamento, sulla base dell'esperienza, delle sue conoscenze, ed in funzione anche di eventuali opportunità offerte dall'evoluzione tecnologica, se è necessario pianificare interventi di formazione, che devono essere riportati nel modello MOD_FORMAZ.

La previsione di interventi formativi degli incaricati del trattamento, ha lo scopo principale di renderli edotti sui rischi che incombono sui dati, sulle misure disponibili per prevenire eventi dannosi, sui profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, sulle responsabilità che ne derivano e sulle modalità per aggiornarsi sulle misure minime adottate dal titolare.

La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali.

Al Responsabile della sicurezza dei dati personali è affidato il compito di verificare ogni anno, entro il 31 dicembre, le necessità di ulteriore formazione del personale incaricato di effettuare periodicamente le operazioni di copia di sicurezza delle banche di dati trattate.

3.7 Criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati all'esterno della struttura del titolare

3.7.1 Trattamenti di dati personali affidati all'esterno della struttura del titolare

Il Responsabile della sicurezza dei dati personali può decidere di affidare il trattamento dei dati in tutto o in parte all'esterno della struttura del titolare.

Il Responsabile della sicurezza dei dati personali, deve redigere e aggiornare ad ogni variazione l'elenco dei soggetti che effettuano il trattamento dei dati in tutto o in parte all'esterno della struttura del titolare, ed indicare per ognuno di essi il tipo di trattamento effettuato specificando:

1. i soggetti interessati
2. i luoghi dove fisicamente avviene il trattamento dei dati stessi
3. i responsabili del trattamento di dati personali

Per l'inventario dei soggetti a cui affidare il trattamento dei dati in tutto o in parte all'esterno della struttura del titolare, deve essere utilizzato il modulo MOD_EXT, che deve essere conservato a cura del Responsabile della sicurezza dei dati personali, in luogo sicuro.

Nel caso in cui, per il trattamento dei dati in tutto o in parte all'esterno della struttura del titolare, i responsabili del trattamento di dati personali non vengano espressamente nominati Responsabili del trattamento di dati personali affidati all'esterno della struttura del titolare (out-sourcing), ai sensi dell'art. 29 del CODICE IN MATERIA DI DATI PERSONALI, 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.

3.7.2 Criteri per la scelta degli enti terzi per il trattamento di dati personali affidati all'esterno della struttura del titolare

Il Responsabile della sicurezza dei dati personali, può affidare il trattamento dei dati in tutto o in parte all'esterno della struttura del titolare a quei soggetti terzi che abbiano i requisiti individuati all'art. 29 del CODICE IN MATERIA DI DATI PERSONALI (esperienza, capacità ed affidabilità).

Il Titolare a cui è stato affidato il trattamento dei dati all'esterno deve rilasciare una dichiarazione scritta da cui risulti che sono state adottate le misure idonee di sicurezza per il trattamento ai sensi del CODICE IN MATERIA DI DATI PERSONALI e del DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA.

3.7.3 Nomina dell'incaricato del trattamento in caso di trattamenti di dati personali affidati all'esterno della struttura del titolare

Per ogni trattamento affidato ad un soggetto esterno alla struttura del titolare, il Responsabile della sicurezza dei dati personali deve assicurarsi che siano rispettate le norme di sicurezza di un livello non inferiore a quanto stabilito per il trattamento interno.

Il Responsabile della sicurezza dei dati personali deve informare l'incaricato del trattamento dei dati affidato all'esterno alla struttura del titolare, dei compiti che gli sono assegnati in relazione a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dal CODICE IN MATERIA DI DATI PERSONALI e dal DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA.

L'incaricato del trattamento dei dati affidato all'esterno alla struttura del titolare deve accettare la nomina, secondo il modello MOD_EXT.

La nomina dell'Incaricato del trattamento dei dati affidato all'esterno alla struttura del titolare deve essere controfirmata per accettazione e copia della lettera di nomina accettata deve essere conservata a cura del Responsabile della sicurezza dei dati personali in luogo sicuro.

Capitolo 4

Trattamento con l'ausilio di strumenti elettronici

4.1 Elenco dei sistemi di elaborazione per il trattamento

Al Responsabile della sicurezza dei dati personali è affidato il compito di redigere e di aggiornare ad ogni variazione l'elenco dei sistemi di elaborazione con cui viene effettuato il trattamento dei dati.

Per ogni sistema deve essere specificato:

1. Il Responsabile della gestione e della manutenzione
2. Il nome dell'incaricato o degli incaricati che lo utilizzano
3. Il nome di uno o più Incaricati della custodia delle copie delle credenziali

Per ciascun sistema devono anche essere inventariati:

1. i software esistenti e le relative licenze
2. le memorie e gli elaboratori dei dati (es. computer, apparati di comunicazione e di rete, stampanti e periferiche non banali, hardware in generale, ecc.)
3. gli impianti e le infrastrutture di supporto e servizio (es. impianto elettrico, gruppi di continuità elettrogeni, rilevatori antincendio, ecc.)

Per l'Elenco dei sistemi di elaborazione deve essere utilizzato il modulo MOD_ELAB che deve essere conservato a cura del Responsabile della sicurezza dei dati personali in luogo sicuro.

Quando i sistemi di elaborazione coincidono con l'interso sistema informativo aziendale e ad esso sono deputati uno o più amministratori di sistema, il Responsabile della sicurezza dei dati personali può delegare ad essi la predisposizione e tenuta ddel modulo MOD_ELAB.

4.1.1 Gestione dei cambiamenti e aggiornamenti

I sistemi devono essere mantenuti aggiornati attraverso l'adozione delle patch rilasciate dai produttori e con idonee misure per garantire la continuità operativa nel tempo (business continuity).

Chiunque può proporre modifiche, integrazioni o migliorie ad un sistema. Queste richieste, se fondate, sono raccolte dall'Amministratore di Sistema affinchè il Responsabile della sicurezza dei dati personali analizzi quali sono adottabili secondo criteri di utilità e sicurezza. Tutte le modifiche

deliberate devono essere definite formalmente dal Responsabile della sicurezza dei dati personali, che sovrintende alla pianificazione, test, valutazione delle modifiche con particolare riguardo alle loro conseguenze, anche delegando una o più attività all'Amministratore di Sistema. Contestualmente e prima della definitiva implementazione devono essere predisposte soluzioni di ripiego in caso di anomalia. Per il passaggio alla produzione ci si rifà ai requisiti della delibera di adozione della modifica che ne deve specificare i criteri.

In particolare devono essere distinti ambienti di sviluppo e test da ambiente di produzione. La separazione può essere sia logica che fisica, ma per gli ambienti non di produzione si deve

- evitare l'utilizzo di dati sensibili o confidenziali o riservati, eventualmente previa anonimizzazione;
- ricorrere a profili utenti distinti da quelli di produzione.

Negli ambienti di produzione non dovrebbero essere presenti strumenti di sviluppo.

4.1.2 Gestione degli acquisti

Qualora si decidesse per sostituire o acquisire un sistema, prima di procedere all'acquisto, occorre a cura del Responsabile della sicurezza dei dati personali definire i requisiti per la sicurezza delle informazioni, così da poter effettuare i riscontri nelle specifiche/schede tecniche e concedere l'approvazione all'uso.

4.2 Sistema di autenticazione informatica

4.2.1 Procedura di identificazione

Nel caso in cui il trattamento di dati personali sia effettuato con strumenti elettronici, il Responsabile della sicurezza dei dati personali deve assicurarsi che il trattamento sia consentito solamente agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.

4.2.2 Identificazione dell'incaricato

Il Responsabile della sicurezza dei dati personali deve assicurare che il trattamento di dati personali, effettuato con strumenti elettronici, sia consentito solamente agli incaricati dotati di una o più credenziali di autenticazione tra le seguenti:

Un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo
Un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave
Una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.

Il Responsabile della sicurezza dei dati personali deve assicurarsi che il codice per l'identificazione, laddove utilizzato, non potrà essere assegnato ad altri incaricati, neppure in tempi diversi.

Il Responsabile della sicurezza dei dati personali deve assicurarsi che le credenziali di autenticazione non utilizzate da almeno sei mesi debbono essere disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.

Il Responsabile della sicurezza dei dati personali deve assicurarsi che le credenziali siano disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.

Ad ogni Incaricato del trattamento possono essere assegnate o associate individualmente una o più credenziali per l'autenticazione.

4.2.3 Caratteristiche della parola chiave

La parola chiave , quando è prevista dal sistema di autenticazione, deve essere composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito.

1. La parola chiave non deve contenere riferimenti agevolmente riconducibili all'incaricato.
2. La parola chiave deve essere modificata dall'incaricato del trattamento al primo utilizzo e, successivamente, almeno ogni sei mesi.
3. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave deve essere modificata almeno ogni tre mesi.

4.2.4 Cautele per assicurare la segretezza della componente riservata della credenziale

Gli incaricati debbono adottare le necessarie cautele per assicurare la segretezza della parola chiave e custodire diligentemente ogni altro dispositivo che gli è stato affidato per i sistemi di autenticazione informatica (badge magnetici, tessere magnetiche, ecc..).

In particolare è fatto divieto comunicare a chiunque altro incaricato le proprie credenziali di accesso al sistema informatico.

4.2.5 Istruzioni per non lasciare incustodito e accessibile lo strumento elettronico

Gli incaricati hanno l'obbligo di:

1. Non lasciare incustodito il proprio posto di lavoro.
2. Di chiudere tutte le applicazioni aperte o meglio ancora di spegnere il sistema informatico in caso di assenza prolungata.
3. Di attivare la configurazione del sistema informatico di lavoro in modo che automaticamente si attivi il blocco della stessa dopo un certo tempo di inattività dell'operatore, con richiesta di autenticazione per la riattivazione

4.3 Incaricato della custodia delle copie delle credenziali

4.3.1 Compiti degli incaricati della custodia delle copie delle credenziali

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

È compito degli Incaricati della custodia delle copie delle credenziali:

1. Gestire e custodire le credenziali per l'accesso ai dati degli Incaricati del trattamento.
2. Predisporre, per ogni incaricato del trattamento, una busta sulla quale è indicato il nome dell'incaricato e all'interno della busta deve essere indicata la credenziale usata. Le buste con le credenziali debbono essere conservate in luogo chiuso e protetto. Nel caso si utilizzi un sistema centralizzato di autenticazione, non è necessario predisporre le buste per gli incaricati, in quanto si utilizzano le funzioni del sistema stesso.

3. Istruire gli incaricati del trattamento sull'uso delle parole chiave, e sulle caratteristiche che debbono avere, e sulle modalità per la loro modifica in autonomia.
4. Revocare tutte le credenziali non utilizzate in caso di perdita della qualità che consentiva all'incaricato l'accesso ai dati personali.
5. Revocare le credenziali per l'accesso ai dati degli Incaricati del trattamento nel caso di mancato utilizzo per oltre 6 (sei) mesi.

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

4.3.2 Nomina degli incaricati della custodia delle copie delle credenziali

Il Responsabile della sicurezza dei dati personali nomina uno o più soggetti Incaricati della custodia delle copie delle credenziali a cui è conferito il compito di custodire le Parole chiave per l'accesso ai dati archiviati nei sistemi di elaborazione dei dati.

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

Il responsabile della sicurezza dei dati personali deve informare gli Incaricati della custodia delle copie delle credenziali della responsabilità che è stata loro affidata in relazione a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dal CODICE IN MATERIA DI DATI PERSONALI (Gazzetta Ufficiale 29 luglio 2003, Serie generale n. 174, Supplemento ordinario n. 123/L) e dal DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA.

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

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

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

4.3.3 Accesso straordinario

Gli Incaricati della custodia delle copie delle credenziali, hanno il compito di assicurare la disponibilità dei dati e degli strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema.

La custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza.

Gli Incaricati della custodia delle copie delle credenziali devono informare tempestivamente l'Incaricato del trattamento ogni qualvolta sia stato effettuato un tale tipo di intervento.

Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione.

4.4 Riferimenti normativi

Con i provvedimenti del 25 giugno 2009 (G.U. n. 149 del 30 giugno 2009)e del 27 novembre 2008 (G.U. n. 300 del 24 dicembre 2008) recante prescrizioni ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema e alla proroga dei termini per il loro adempimento, il Garante per la protezione dei dati personali ha deciso di richiamare l'attenzione di enti, amministrazioni, società private sulla figura professionale dell' amministratore di sistema e ha prescritto l'adozione di specifiche misure tecniche ed organizzative che agevolino la verifica sulla sua attività da parte di chi ha la titolarità delle banche dati e dei sistemi informatici.

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

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

Le misure e le cautele dovranno essere messe in atto da parte di tutte le aziende private e da tutti i soggetti pubblici, compresi gli uffici giudiziari, le forze di polizia, i servizi di sicurezza. Sono esclusi invece i trattamenti di dati, sia in ambito pubblico che privato, effettuati a fini amministrativo contabile, che pongono minori rischi per gli interessati.

4.5 Amministratori di sistema

Con la definizione di Amministratore di Sistema si individuano generalmente, in ambito informatico, figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti. Ai fini del provvedimento del Garante sono 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 e 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.

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).

Le funzioni tipiche dell'amministrazione di un sistema sono richiamate nel menzionato Allegato B, nella parte in cui prevede l'obbligo per i titolari di assicurare la custodia delle componenti riservate delle credenziali di autenticazione. Gran parte dei compiti previsti nel medesimo Allegato B spettano tipicamente all'amministratore di sistema: dalla realizzazione di copie di sicurezza (operazioni di backup e recovery dei dati) alla custodia delle credenziali alla gestione dei sistemi di autenticazione e di autorizzazione. Nel loro complesso, le norme predette mettono in rilievo la particolare capacità di azione propria degli amministratori di sistema e la natura fiduciaria delle relative mansioni, analoga a quella che, in un contesto del tutto differente, caratterizza determinati incarichi di custodia e altre attività per il cui svolgimento è previsto il possesso di particolari requisiti tecnico-organizzativi, di onorabilità, professionali, morali o di condotta, a oggi non contemplati per lo svolgimento di uno dei ruoli più delicati della società dell'informazione.

Il Responsabile della sicurezza dei dati personali soggetti all'ambito applicativo del Codice ed effettuati con strumenti elettronici, vista la particolare criticità del ruolo degli amministratori di sistema, deve 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; deve inoltre valutare con particolare cura l'attribuzione di funzioni tecniche propriamente corrispondenti o assimilabili a quelle di amministratore di sistema, 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.

4.5.1 Valutazione delle caratteristiche soggettive

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.

4.5.2 Designazioni individuali

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

4.5.3 Elenco degli amministratori di sistema

Gli estremi identificativi delle persone fisiche o giuridiche designate quali amministratori di sistema, con l'elenco delle funzioni ad essi attribuite, devono essere riportati nel Regolamento per la protezione dei dati personali, economici, sensibili e giudiziari, valevole come Documento programmatico sulla sicurezza, oppure, annotati comunque in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti anche da parte del Garante.

Qualora l'attività degli amministratori di sistema riguardi anche indirettamente servizi o sistemi che trattano o che permettono il trattamento di informazioni di carattere personale di lavoratori,

i titolari pubblici e privati nella qualità di datori di lavoro sono tenuti a rendere nota o conoscibile l'identità degli amministratori di sistema nell'ambito delle proprie organizzazioni, secondo le caratteristiche dell'azienda o del servizio, in relazione ai diversi servizi informatici cui questi sono preposti. Ciò, avvalendosi dell'informativa resa agli interessati ai sensi dell'art. 13 del Codice nell'ambito del rapporto di lavoro che li lega al titolare, oppure tramite il disciplinare tecnico la cui adozione è prevista dal provvedimento del Garante n. 13 del 1° marzo 2007 (in G.U. 10 marzo 2007, n. 58); in alternativa si possono anche utilizzare strumenti di comunicazione interna (a es., intranet aziendale, ordini di servizio a circolazione interna o bollettini). Ciò, salvi i casi in cui tale forma di pubblicità o di conoscibilità non sia esclusa in forza di un'eventuale disposizione di legge che disciplini in modo difforme uno specifico settore.

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

4.5.4 Verifica delle attività

L'operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica da parte dei titolari del trattamento, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.

4.5.5 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.

4.5.6 Compiti degli Amministratori di sistema

L'Amministratore di sistema è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo che sovrintende al buon funzionamento di banche di dati e di sistemi software complessi

È compito degli Amministratori di sistema:

1. sovrintendere al buon funzionamento di banche di dati e di sistemi software complessi
2. proteggere le banche dati e i sistemi software complessi dal rischio di intrusione o di accesso non autorizzato
3. registrare gli accessi alle banche di dati ed ai sistemi software complessi
4. Informare il Responsabile della sicurezza dei dati personali nella eventualità che si siano rilevati dei rischi relativamente alle misure di sicurezza riguardanti i dati personali.

Qualora il Responsabile della sicurezza dei dati personali ritenga di non nominare alcun Amministratore di sistema, ne assumerà tutte le responsabilità e funzioni.

4.5.7 Nomina degli amministratori di sistema

È onere del Responsabile della sicurezza dei dati personali, in relazione all'attività svolta, individuare, nominare e incaricare per iscritto, se lo ritiene opportuno, uno o più Amministratori di sistema.

Anche se non espressamente previsto dalla norma, è opportuno che il Responsabile della sicurezza dei dati personali nomini uno o più Amministratori di sistema, specificando le banche di dati e i sistemi software complessi che è chiamato a sovrintendere.

Il Responsabile della sicurezza dei dati personali deve informare ciascun Amministratore di sistema delle responsabilità che gli sono affidate in relazione a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dal CODICE IN MATERIA DI DATI PERSONALI (Gazzetta Ufficiale 29 luglio 2003, Serie generale n. 174, Supplemento ordinario n. 123/L) e dal DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA.

La nomina di uno o più Amministratori di sistema deve essere effettuata con una lettera di incarico (MOD_ADS) e deve essere controfirmata per accettazione e copia della lettera di nomina accettata deve essere conservata a cura del Responsabile della sicurezza dei dati personali in luogo sicuro.

La nomina dell'Amministratore di sistema è a tempo indeterminato, e decade per revoca o dimissioni dello stesso.

La nomina dell'Amministratore di sistema può essere revocata in qualsiasi momento dal Responsabile della sicurezza dei dati personali senza preavviso, ed eventualmente affidata ad altro soggetto.

4.6 Responsabili della gestione e della manutenzione degli strumenti elettronici

La figura di Responsabile della gestione e della manutenzione degli strumenti elettronici corrisponde ad un sotto tipo di Amministratore di sistema, che si occupa specificatamente dei sistemi di elaborazione e dei relativi sistemi operativi.

4.6.1 Compiti dei responsabili della gestione e della manutenzione degli strumenti elettronici

Il Responsabile della gestione e della manutenzione degli strumenti elettronici è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo che sovrintende agli strumenti di un sistema informativo, con finalità atte alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti.

È compito dei Responsabili della gestione e della manutenzione degli strumenti elettronici:

1. sovrintendere agli strumenti di un sistema informativo, con finalità atte alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti
2. Attivare le credenziali di autenticazione e attivare ove possibile e previsto le politiche di autorizzazione agli Incaricati del trattamento, su indicazione del Responsabile del trattamento, per tutti i trattamenti effettuati con strumenti informatici.
3. Definire quali politiche adottare per la protezione dei sistemi contro i virus informatici e verificarne l'efficacia con cadenza almeno semestrale.

4. Proteggere gli elaboratori dal rischio di intrusione (violazione del sistema da parte di hackers).
5. Informare il Responsabile della sicurezza dei dati personali nella eventualità che si siano rilevati dei rischi relativamente alle misure di sicurezza riguardanti i dati personali.

Qualora il Responsabile della sicurezza dei dati personali ritenga di non nominare alcun Responsabile della gestione e della manutenzione degli strumenti elettronici, ne assumerà tutte le responsabilità e funzioni.

4.6.2 Nomina dei responsabili della gestione e della manutenzione degli strumenti elettronici

È onere del Responsabile della sicurezza dei dati personali, in relazione all'attività svolta, individuare, nominare e incaricare per iscritto, se lo ritiene opportuno, uno o più Responsabili della gestione e della manutenzione degli strumenti elettronici a cui è conferito il compito di sovrintendere al buon funzionamento delle risorse del sistema informativo.

Anche se non espressamente previsto dalla norma, è opportuno che il Responsabile della sicurezza dei dati personali nomini uno o più Responsabili della gestione e della manutenzione degli strumenti elettronici, specificando gli elaboratori che è chiamato a sovrintendere.

Il Responsabile della sicurezza dei dati personali deve informare ciascun Responsabile della gestione e della manutenzione degli strumenti elettronici delle responsabilità che gli sono affidate in relazione a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dal CODICE IN MATERIA DI DATI PERSONALI (Gazzetta Ufficiale 29 luglio 2003, Serie generale n. 174, Supplemento ordinario n. 123/L) e dal DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA.

La nomina di uno o più Responsabili della gestione e della manutenzione degli strumenti elettronici deve essere effettuata con una lettera di incarico (MOD_RGSE) e deve essere controfirmata per accettazione e copia della lettera di nomina accettata deve essere conservata a cura del Responsabile della sicurezza dei dati personali in luogo sicuro.

Il Responsabile della sicurezza dei dati personali deve consegnare a ciascun Responsabile della gestione e della manutenzione degli strumenti elettronici una copia di tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina.

La nomina del Responsabile della gestione e della manutenzione degli strumenti elettronici è a tempo indeterminato, e decade per revoca o dimissioni dello stesso.

La nomina del Responsabile della gestione e della manutenzione degli strumenti elettronici può essere revocata in qualsiasi momento dal Responsabile della sicurezza dei dati personali dei dati senza preavviso, ed eventualmente affidata ad altro soggetto.

4.7 Sistema di autorizzazione

La politica di autorizzazioni, definita dal Responsabile del trattamento per ciascun Incaricato deve essere applicata anche per le banche di dati personali gestite elettronicamente, utilizzando gli strumenti elettronici presenti sui sistemi di elaborazione per verificarne l'applicazione, negando eventualmente l'accesso ai dati o impedendo le operazioni non consentite. È compito del Responsabile della gestione e della manutenzione degli strumenti elettronici, ove tali strumenti lo consentano, di definire, aggiornare e mantenere tali politiche.

4.8 Analisi dei rischi che incombono sui dati

4.8.1 Manutenzione dei sistemi di elaborazione dei dati

Il Responsabile della gestione e della manutenzione degli strumenti elettronici, anche avvalendosi di consulenti interni o esterni, deve verificare ogni anno:

1. la situazione delle apparecchiature hardware installate con cui vengono trattati i dati
2. la situazione delle apparecchiature periferiche
3. la situazione dei dispositivi di collegamento con le reti pubbliche

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

1. la sicurezza dei dati trattati.
2. il rischio di distruzione o di perdita.
3. il rischio di accesso non autorizzato o non consentito

Il Responsabile della gestione e della manutenzione degli strumenti elettronici deve, se necessario, aggiornare la relazione annuale dei rischi hardware conformemente al modulo MOD_RSK_HW

Il Responsabile della gestione e della manutenzione degli strumenti elettronici nel caso in cui esistano rischi evidenti debbono informare il Responsabile della sicurezza dei dati personali perché siano presi gli opportuni provvedimenti allo scopo di assicurare il corretto trattamento dei dati in conformità alle norme in vigore.

4.8.2 Manutenzione dei sistemi operativi e dei software installati

Al Responsabile della gestione e della manutenzione degli strumenti elettronici è affidato il compito di verificare ogni anno, la situazione dei Sistemi Operativi e delle applicazioni software installate sulle apparecchiature con cui vengono trattati i dati.

La verifica ha lo scopo di controllare l'affidabilità dei Sistemi Operativi e delle applicazioni software, per quanto riguarda:

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

Tenendo conto in particolare di:

1. Disponibilità di nuove versioni migliorative dei software utilizzati.
2. Segnalazioni di Patch, Fix o System-Pack per la rimozione di errori o malfunzionamenti.
3. Segnalazioni di Patch, Fix o System-Pack per l'introduzione di maggiori sicurezze contro i rischi di intrusione o di danneggiamento dei dati.

Il Responsabile della gestione e della manutenzione degli strumenti elettronici deve, se necessario, aggiornare la relazione annuale dei rischi sui software installati conformemente al modulo MOD_RSK_SW.

I Responsabili della gestione e della manutenzione degli strumenti elettronici, nel caso in cui esistano rischi evidenti, debbono informare il Responsabile della sicurezza dei dati personali affinché siano presi gli opportuni provvedimenti per assicurare il corretto trattamento dei dati in conformità alle norme in vigore.

4.9 Misure da adottare per garantire l'integrità e la disponibilità dei dati

Il Responsabile della gestione e della manutenzione degli strumenti elettronici al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita, stabilisce la periodicità con cui debbono essere effettuate le copie di sicurezza delle banca di dati trattati.

I criteri debbono essere definiti in relazione al tipo di rischio potenziale e in base al livello di tecnologia utilizzata.

Il Responsabile della gestione e della manutenzione degli strumenti elettronici, eventualmente per ogni banca di dati, deve predisporre le istruzioni di copia, verifica e ripristino dei dati, utilizzando il modulo MOD_BCKP.

Il Documento con le istruzioni di copia deve essere conservato a cura del Responsabile della sicurezza dei dati personali in luogo sicuro e deve essere trasmesso in copia controllata a ciascun incaricato delle copie di sicurezza delle banche dati.

In particolare per ogni banca di dati debbono essere definite le seguenti specifiche:

1. Il Tipo di supporto da utilizzare per le Copie di sicurezza dei dati.
2. Il numero di Copie di sicurezza dei dati effettuate ogni volta
3. Se i supporti utilizzati per le Copie di sicurezza dei dati sono riutilizzati e in questo caso con quale periodicità.
4. Se per effettuare le Copie di sicurezza dei dati si utilizzano procedure automatizzate e programmate.
5. Le modalità di controllo delle Copie di sicurezza dei dati.
6. La durata massima stimata di conservazione delle informazioni senza che ci siano perdite o cancellazione di dati.
7. Il nome dell'incaricato a cui è stato assegnato il compito di effettuare le Copie di sicurezza dei dati.
8. Le istruzioni e i comandi necessari per effettuare le Copie di sicurezza dei dati.
9. Le istruzioni e i comandi necessari per effettuare il ripristino delle Copie di sicurezza dei dati.

Al Responsabile della sicurezza dei dati personali è affidato il compito di verificare ogni anno, entro il 31 dicembre, le necessità di formazione del personale incaricato di effettuare periodicamente le Copie di sicurezza delle banca di dati trattate, in funzione anche di eventuali opportunità offerte dall'evoluzione tecnologica.

4.10 Incaricato delle copie di sicurezza delle banche dati

4.10.1 Compiti degli incaricati delle copie di sicurezza delle banche dati

L'Incaricato delle copie di sicurezza delle banche dati è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo che ha il compito di effettuare periodicamente le copie di sicurezza delle Banche di dati gestite.

È onere del Responsabile della sicurezza dei dati personali, in relazione all'attività svolta, individuare, nominare e incaricare per iscritto, se lo ritiene opportuno, uno o più Incaricati delle copie di sicurezza delle banche dati.

Al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita, stabilisce, con il supporto tecnico del Responsabile della gestione e della manutenzione degli strumenti elettronici la periodicità con cui debbono essere effettuate le copie di sicurezza delle Banche di Dati trattate.

I criteri debbono essere concordati con il Responsabile della gestione e della manutenzione degli strumenti elettronici 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 le seguenti specifiche:

1. Il Tipo di supporto da utilizzare per le Copie di Back-Up .
2. Il numero di Copie di Back-Up effettuate ogni volta.
3. Se i supporti utilizzati per le Copie di Back-Up sono riutilizzati e in questo caso con quale periodicità.
4. Se per effettuare le Copie di Back-Up si utilizzano procedure automatizzate e programmate.
5. Le modalità di controllo delle Copie di Back-Up .
6. La durata massima stimata di conservazione delle informazioni senza che ci siano perdite o cancellazione di dati.
7. L'Incaricato del trattamento a cui è stato assegnato il compito di effettuare le Copie di Back-Up .
8. Le istruzioni e i comandi necessari per effettuare le Copie di Back-Up .

È compito degli Incaricati delle copie di sicurezza delle banche dati:

1. Prendere tutti i provvedimenti necessari ad evitare la perdita o la distruzione dei dati e provvedere al ricovero periodico degli stessi con copie di sicurezza secondo i criteri stabiliti dal Responsabile della sicurezza dei dati personali.
2. Assicurarsi della qualità delle copie di sicurezza dei dati e della loro conservazione in luogo adatto e sicuro.
3. Assicurarsi della conservazione delle copie di sicurezza in luogo adatto e sicuro e ad accesso controllato.
4. Di provvedere a conservare con la massima cura e custodia i dispositivi utilizzati per le copie di sicurezza, impedendo l'accesso agli stessi dispositivi da parte di personale non autorizzato.
5. Di segnalare tempestivamente al Responsabile della gestione e della manutenzione degli strumenti elettronici, ogni eventuale problema dovesse verificarsi nella normale attività di copia delle banche dati.

Qualora il Responsabile della sicurezza dei dati personali ritenga di non nominare alcun Incaricato delle copie di sicurezza delle banche dati, ne assumerà tutte le responsabilità e funzioni.

4.10.2 Nomina degli incaricati delle copie di sicurezza delle banche dati

Il Responsabile della sicurezza dei dati personali nomina uno o più soggetti Incaricati delle copie di sicurezza delle banche dati a cui è conferito il compito di effettuare periodicamente le copie di sicurezza delle Banche di dati gestite.

Anche se non espressamente previsto dalla norma, è opportuno che il Responsabile della sicurezza dei dati personali nomini uno o più Incaricati delle copie di sicurezza delle banche dati, specificando gli elaboratori o le banche dati che è chiamato a sovrintendere.

Il Responsabile della sicurezza dei dati personali deve informare ciascun Incaricato delle copie di sicurezza delle banche dati delle responsabilità che gli sono affidate in relazione a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dal CODICE IN MATERIA DI DATI PERSONALI (Gazzetta Ufficiale 29 luglio 2003, Serie generale n. 174, Supplemento ordinario n. 123/L) e dal DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA.

La nomina di uno o più Incaricati delle copie di sicurezza delle banche dati deve essere effettuata con una lettera di incarico (MOD_ICSBD) e deve essere controfirmata per accettazione.

Copia della lettera di nomina accettata deve essere conservata a cura del Responsabile della sicurezza dei dati personali in luogo sicuro.

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

4.11 Istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili

Il Responsabile della sicurezza dei dati personali è responsabile della custodia e della conservazione dei supporti utilizzati per le copie dei dati.

Per ogni banca di dati deve essere individuato il luogo di conservazione copie dei dati in modo che sia convenientemente protetto dai potenziali rischi di:

1. Agenti chimici
2. Fonti di calore
3. Campi magnetici
4. Intrusioni e atti vandalici
5. Incendio
6. Allagamento
7. Furto

Nel modulo MOD_BCKP deve essere specificato il luogo di conservazione supporti utilizzati per le copie dei dati.

L'accesso ai supporti utilizzati per le copie dei dati è limitato per ogni banca di dati a:

1. Incaricati delle copie di sicurezza delle banche dati
2. Responsabile della sicurezza dei dati personali

4.12 Misure in caso di trattamento di dati sensibili o giudiziari

4.12.1 Protezione contro l'accesso abusivo

Al fine di garantire la sicurezza dei dati sensibili o giudiziari contro l'accesso abusivo, il Responsabile della sicurezza dei dati personali, stabilisce, con il supporto tecnico dei Responsabili della gestione e della manutenzione degli strumenti elettronici, 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 dal Responsabile della sicurezza dei dati personali in 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:

1. Le misure applicate per evitare intrusioni.
2. Le misure applicate per evitare contagi da Virus Informatici.

Deve essere utilizzato il modulo MOD_FW_AV che va conservato a cura del Responsabile della gestione e della manutenzione degli strumenti elettronici in luogo sicuro e deve essere trasmesso in copia al Responsabile della sicurezza dei dati personali.

4.12.2 Riutilizzo dei supporti rimovibili

Se il Responsabile della gestione e della manutenzione degli strumenti elettronici decide che i supporti magnetici contenenti dati sensibili o giudiziari non sono più utilizzabili per gli scopi per i quali erano stati destinati, deve provvedere a farne cancellare il contenuto annullando e rendendo intelligibili e tecnicamente in alcun modo ricostruibili le informazioni in esso contenute.

È compito del Responsabile della gestione e della manutenzione degli strumenti elettronici assicurarsi che in nessun caso vengano lasciate copie di Banche di dati contenenti dati sensibili o giudiziari, non più utilizzate, senza che ne venga cancellato il contenuto ed annullate e rese intelligibili e tecnicamente in alcun modo ricostruibili le informazioni in esso registrate.

4.12.3 Ripristino dell'accesso ai dati in caso di danneggiamento

La decisione di ripristinare la disponibilità dei dati in seguito a distruzione o danneggiamento è compito esclusivo del Responsabile della sicurezza dei dati personali.

La decisione di ripristinare la disponibilità dei dati deve essere presa rapidamente e in ogni caso la disponibilità dei dati deve essere ripristinata al massimo entro sette giorni.

Una volta valutata la assoluta necessità di ripristinare la disponibilità dei dati in seguito a distruzione o danneggiamento il Responsabile della sicurezza dei dati personali deve provvedere tramite l'Incaricato delle copie di sicurezza delle banche dati e tramite il Responsabile della gestione e della manutenzione degli strumenti elettronici all'operazione di ripristino dei dati.

La decisione di ripristinare la funzionalità degli elaboratori elettronici guasti, è compito esclusivo del Responsabile della sicurezza dei dati personali che si può avvalere del parere del Responsabile della gestione e della manutenzione degli strumenti elettronici.

La decisione di ripristinare la funzionalità degli elaboratori elettronici guasti deve essere presa rapidamente e in ogni caso la funzionalità deve essere ripristinata al massimo entro sette giorni.

4.13 Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali

Se nello svolgimento delle proprie attività, in particolare quelle industriali, commerciali, professionali o istituzionali, si è fatto uso di supporti che contengono dati personali, quando tali supporti giungono al termine del loro ciclo di impiego, il Responsabile della sicurezza dei dati personali, in collaborazione con il Responsabile della gestione e manutenzione degli strumenti elettronici deve provvedere alla distruzione o dismissione adottando 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 reimpiegate, riciclate o smaltite, compilando il registro MOD_RAEE.

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.

4.13.1 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

1. 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.

2. Formattazione a basso livello dei dispositivi di tipo hard disk (low-level formatting), 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;

3. 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).

4.13.2 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. In questo caso, i rifiuti di apparecchiature o supporti devono essere evidenziati (etichettatura), raccolti e conservati in aree speciali dedicate, prima di essere bonificati o distrutti.

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.

Capitolo 5

Ulteriori disposizioni per il trattamento

5.1 Periodicità di revisione del Regolamento

Entro il 31 marzo di ogni anno, il Titolare del trattamento di dati sensibili o di dati giudiziari deve verificare ed eventualmente predisporre una nuova versione del Regolamento in quanto valevole come Documento programmatico sulla sicurezza contenente idonee informazioni riguardo ai punti 19.1, 19.2, 19.3, 19.4, 19.5, 19.6, 19.7, 19.8 del DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA del CODICE IN MATERIA DI DATI PERSONALI (Gazzetta Ufficiale 29 luglio 2003, Serie generale n. 174, Supplemento ordinario n. 123/L).

5.2 Descrizione degli interventi effettuati da soggetti esterni

Nel caso in cui ci si avvale di soggetti esterni alla propria struttura, per provvedere alla riparazione il Responsabile della sicurezza dei dati personali, deve richiedere al tecnico che ha effettuato la riparazione, una descrizione scritta dell'intervento effettuato che ne attesti la conformità a quanto stabilito dal CODICE IN MATERIA DI DATI PERSONALI (Gazzetta Ufficiale 29 luglio 2003, Serie generale n. 174, Supplemento ordinario n. 123/L) e dal DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA.

5.3 Regolamento per l'attività di recupero crediti

La struttura nelle vesti del suo titolare del trattamento richiede agli incaricati che si occuperanno per suo conto di recupero crediti, finanziarie e concessionarie di pubblici servizi di attenersi alle seguenti normative nel rispetto delle prescrizioni del Garante per non incorrere in illeciti e per rispettare i principi posti a tutela dei diritti dei cittadini.

Non sono ammesse prassi invasive o lesive della dignità personale. Per sollecitare ed ottenere il pagamento di somme dovute non è lecito comunicare ingiustificatamente informazioni relative ai mancati pagamenti ad altri soggetti che non siano l'interessato (es. familiari, colleghi di lavoro o vicini di casa) ed esercitare indebite pressioni su quest'ultimo.

Non si deve far riscorso a telefonate preregistrate perché con questa modalità persone diverse dal debitore possono venire a conoscenza di una sua eventuale condizione di inadempienza.

Illecita è pure l'affissione da parte degli incaricati del recupero crediti di avvisi di mora sulla porta di casa, modalità questa che rende possibile la diffusione dei dati personali dell'interessato ad una serie indeterminata di soggetti.

Non si deve inoltre rendere visibile a persone estranee il contenuto di una comunicazione, come può accadere con l'utilizzo di cartoline postali o con l'invio di plichi recanti all'esterno la scritta "recupero crediti" o formule simili. É necessario, invece, che le sollecitazioni di pagamento vengano portate a conoscenza del solo debitore, usando plichi chiusi e senza scritte specifiche.

Gli incaricati delle società non possono usare altri dati se non quelli assolutamente necessari all'esecuzione del mandato (dati anagrafici, codice fiscale, ammontare del credito, recapiti telefonici).

Una volta assolto l'incarico e acquisite le somme, i dati devono essere cancellati.

5.4 Trattamenti in contitolarità

Qualunque trattamento di dati personali può essere svolto in contitolarità con altri soggetti. In alcuni casi la contitolarità deriva da una volontà esplicita, comune ed organizzata dei singoli soggetti titolari, che distribuiscono tra loro compiti, incarichi e misure di protezione, ma che detengono collegialmente la responsabilità delle decisioni in ordine alle finalità ed alle modalità del trattamento.

In altri casi, non esiste una reale volontà, quanto piuttosto l'adozione di una norma giuridica che impone ed attribuisce lo status di contitolare a soggetti che normalmente non operano nell'ambito del trattamento, ma che potrebbero esservi interessati e a cui va garantito il diritto di parteciparvi, trovandosi di norma in una posizione svantaggiata. Tale partecipazione si concretizza di solito con l'accesso alle informazioni, piuttosto che con l'attribuzione di un incarico di trattamento.

Nel seguito è presentata la casistica di trattamenti che sottostanno ad obblighi di legge e che determinano l' implicita contitolarità del trattamento tra diversi soggetti.

5.4.1 Libro soci

I provvedimenti del Garante del 19 dicembre 2000 e del 26 marzo 2009 resi in merito al diritto di ispezione al libro soci nelle società e cooperative, ribadiscono che la comunicazione dei dati personali può avvenire senza il consenso delle persone cui si riferiscono i dati, quando si tratta di adempiere ad un obbligo normativo. Nella fattispecie, l'art. 2422 cod. civ. riconosce ai soci il diritto di accedere alle informazioni obbligatoriamente annotate nel libro dei soci ai sensi dell'art. 2421 del Codice Civile (il numero delle azioni, il cognome e il nome dei titolari delle azioni nominative, i trasferimenti e i vincoli ad esse relativi e i versamenti eseguiti). Altre norme (art. 4 R.D. 29 marzo 1942, n. 239; art. 5, Legge 29 dicembre 1962, n. 1745) integrano i dati da annotarsi nel libro soci: in particolare, domicilio per le persone fisiche e sede principale per le persone giuridiche. Alla luce di tali dispositivi di Legge, il Garante ha confermato la liceità della richiesta dei dati anagrafici completi presenti nel libro soci da parte del socio che ne faccia richiesta ai sensi dell'art. 2422 cod. civ., eventualmente ottenendone estratti a proprie spese, senza che sia previamente necessario chiedere il consenso ai consoci interessati.

Per quanto riguarda ulteriori dati (e-mail, telefono, codice fiscale, ecc.) eventualmente raccolti e trattati, non essendovi al riguardo disposizioni di legge, risultano di completa ed esclusiva responsabilità del titolare del trattamento, il quale non è tenuto a condividere tali informazioni né potrebbe farlo senza aver prima acquisito il consenso di tutti gli interessati.

5.5 Trasporto di supporti contenenti dati sensibili

Qualora il trasporto di documenti o supporti informatici contenenti dati sensibili non avvenga ad opera degli incaricati del trattamento autorizzati a trattarne il contenuto, occorre avvalersi di soggetti (interni o esterni), preventivamente selezionati secondo le usuali procedure, che garantiscano la consegna senza accedere ai dati. In tal caso occorre anche:

- incaricare per iscritto i soggetti selezionati
- utilizzare contenitori (es. buste, scatole, ecc.) specifici che, qualora violati, evidenzino tale situazione (es. rottura di sigillo)

- accertarsi che in tutte le fasi, il supporto contenente dati sensibili rimanga integro

Capitolo 6

Diritti dell'interessato

6.1 Diritto di accesso ai dati personali

L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile.

L'interessato ha diritto di ottenere l'indicazione:

1. dell'origine dei dati personali;
2. delle finalità e modalità del trattamento;
3. della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici; d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2;
4. dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.

L'interessato ha diritto di ottenere:

1. l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati; b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
2. l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.

L'interessato ha diritto di opporsi, in tutto o in parte:

1. per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;
2. al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

6.2 Esercizio dei diritti

I diritti di cui all'articolo 7 sono esercitati con richiesta rivolta senza formalità al titolare o al responsabile, anche per il tramite di un incaricato, alla quale è fornito idoneo riscontro senza ritardo.

I diritti di cui all'articolo 7 non possono essere esercitati con richiesta al titolare o al responsabile o con ricorso ai sensi dell'articolo 145, se i trattamenti di dati personali sono effettuati:

1. in base alle disposizioni del decreto-legge 3 maggio 1991, n. 143, convertito, con modificazioni, dalla legge 5 luglio 1991, n. 197, e successive modificazioni, in materia di riciclaggio;
2. in base alle disposizioni del decreto-legge 31 dicembre 1991, n. 419, convertito, con modificazioni, dalla legge 18 febbraio 1992, n. 172, e successive modificazioni, in materia di sostegno alle vittime di richieste estorsive;
3. da Commissioni parlamentari d'inchiesta istituite ai sensi dell'articolo 82 della Costituzione; d) da un soggetto pubblico, diverso dagli enti pubblici economici, in base ad espressa disposizione di legge, per esclusive finalità inerenti alla politica monetaria e valutaria, al sistema dei pagamenti, al controllo degli intermediari e dei mercati creditizi e finanziari, nonché alla tutela della loro stabilità;
4. ai sensi dell'articolo 24, comma 1, lettera f), limitatamente al periodo durante il quale potrebbe derivarne un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive o per l'esercizio del diritto in sede giudiziaria;
5. da fornitori di servizi di comunicazione elettronica accessibili al pubblico relativamente a comunicazioni telefoniche in entrata, salvo che possa derivarne un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n.397;
6. per ragioni di giustizia, presso uffici giudiziari di ogni ordine e grado o il Consiglio superiore della magistratura o altri organi di autogoverno o il Ministero della giustizia;
7. ai sensi dell'articolo 53, fermo restando quanto previsto dalla legge 1° aprile 1981, n. 121.

Il Garante, anche su segnalazione dell'interessato, nei casi di cui al comma 2, lettere a), b), d), e) ed f), provvede nei modi di cui agli articoli 157, 158 e 159 e, nei casi di cui alle lettere c), g) ed h) del medesimo comma, provvede nei modi di cui all'articolo 160.

L'esercizio dei diritti di cui all'articolo 7, quando non riguarda dati di carattere oggettivo, può avere luogo salvo che concerna la rettificazione o l'integrazione di dati personali di tipo valutativo, relativi a giudizi, opinioni o ad altri apprezzamenti di tipo soggettivo, nonché "indicazione di condotte da tenersi o di decisioni in via di assunzione da parte del titolare del trattamento.

6.3 Modalità di esercizio

La richiesta rivolta al titolare o al responsabile può essere trasmessa anche mediante lettera raccomandata, telefax o posta elettronica. Il Garante può individuare altro idoneo sistema in riferimento a nuove soluzioni tecnologiche. Quando riguarda l'esercizio dei diritti di cui all'articolo 7, commi 1 e 2, la richiesta può essere formulata anche oralmente e in tal caso è annotata sinteticamente a cura dell'incaricato o del responsabile.

Nell'esercizio dei diritti di cui all'articolo 7 l'interessato può conferire, per iscritto, delega o procura a persone fisiche, enti, associazioni od organismi. L'interessato può, altresì, farsi assistere da una persona di fiducia.

I diritti di cui all'articolo 7 riferiti a dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione.

L'identità dell'interessato è verificata sulla base di idonei elementi di valutazione, anche mediante atti o documenti disponibili o esibizione o allegazione di copia di un documento di riconoscimento. La persona che agisce per conto dell'interessato esibisce o allega copia della procura, ovvero della delega sottoscritta in presenza di un incaricato o sottoscritta e presentata unitamente a copia fotostatica non autenticata di un documento di riconoscimento dell'interessato. Se l'interessato è una persona giuridica, un ente o un'associazione, la richiesta è avanzata dalla persona fisica legittimata in base ai rispettivi statuti od ordinamenti.

La richiesta di cui all'articolo 7, commi 1 e 2, è formulata liberamente e senza costrizioni e può essere rinnovata, salva l'esistenza di giustificati motivi, con intervallo non minore di novanta giorni.

6.4 Riscontro all'interessato

Per garantire l'effettivo esercizio dei diritti di cui all'articolo 7 il titolare del trattamento è tenuto ad adottare idonee misure volte, in particolare:

1. ad agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili;
2. a semplificare le modalità e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico.

I dati sono estratti a cura del responsabile o degli incaricati e possono essere comunicati al richiedente anche oralmente, ovvero offerti in visione mediante strumenti elettronici, sempre che in tali casi la comprensione dei dati sia agevole, considerata anche la qualità e la quantità delle informazioni. Se vi è richiesta, si provvede alla trasposizione dei dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica.

Salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprende tutti i dati personali che riguardano l'interessato comunque trattati dal titolare. Se la richiesta è rivolta ad un esercente una professione sanitaria o ad un organismo sanitario si osserva la disposizione di cui all'articolo 84, comma 1.

Quando l'estrazione dei dati risulta particolarmente difficoltosa il riscontro alla richiesta dell'interessato può avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti.

Il diritto di ottenere la comunicazione in forma intelligibile dei dati non riguarda dati personali relativi a terzi, salvo che la scomposizione dei dati trattati o la privazione di alcuni elementi renda incomprensibili i dati personali relativi all'interessato.

La comunicazione dei dati è effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile. In caso di comunicazione di codici o sigle sono forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato.

Quando, a seguito della richiesta di cui all'articolo 7, commi 1 e 2, lettere a), b) e c) non risulta confermata l'esistenza di dati che riguardano l'interessato, può essere chiesto un contributo spese non eccedente i costi effettivamente sopportati per la ricerca effettuata nel caso specifico.

Il contributo di cui al comma 7 non può comunque superare l'importo determinato dal Garante con provvedimento di carattere generale, che può individuarlo forfettariamente in relazione al caso in cui i dati sono trattati con strumenti elettronici e la risposta è fornita oralmente. Con il medesimo provvedimento il Garante può prevedere che il contributo possa essere chiesto quando i dati personali figurano su uno speciale supporto del quale è richiesta specificamente la riproduzione, oppure quando, presso uno o più titolari, si determina un notevole impiego di mezzi in relazione alla complessità o all'entità delle richieste ed è confermata l'esistenza di dati che riguardano l'interessato.

Il contributo di cui ai commi 7 e 8 è corrisposto anche mediante versamento postale o bancario, ovvero mediante carta di pagamento o di credito, ove possibile all'atto della ricezione del riscontro e comunque non oltre quindici giorni da tale riscontro.

Capitolo 7

Trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro

7.1 Premessa

Con riguardo alle operazioni di trattamento effettuate con dati personali (anche sensibili) di lavoratori operanti alle dipendenze di datori di lavoro privati, il Garante ha introdotto un insieme di linee guida, comprendenti precedenti decisioni dell'Autorità stessa.

Le indicazioni fornite non pregiudicano l'applicazione delle disposizioni di legge o di regolamento che stabiliscono divieti o limiti più restrittivi in relazione a taluni settori o a specifici casi di trattamento di dati (artt. 113, 114 e 184, comma 3, del Codice).

Le tematiche prese in considerazione si riferiscono prevalentemente alla comunicazione e alla diffusione dei dati, all'informativa che il datore di lavoro deve rendere ai lavoratori (art. 13 del Codice), ai dati idonei a rivelare lo stato di salute e il diritto d'accesso.

Le operazioni di trattamento riguardano per lo più:

- dati anagrafici di lavoratori (assunti o cessati dal servizio), dati biometrici, fotografie e dati sensibili riferiti anche a terzi, idonei in particolare a rivelare il credo religioso o l'adesione a sindacati; dati idonei a rivelare lo stato di salute, di regola contenuti in certificati medici o in altra documentazione prodotta per giustificare le assenze dal lavoro o per fruire di particolari permessi e benefici previsti anche nei contratti collettivi;
- informazioni più strettamente connesse allo svolgimento dell'attività lavorativa, quali la tipologia del contratto (a tempo determinato o indeterminato, a tempo pieno o parziale, etc.); la qualifica e il livello professionale, la retribuzione individuale corrisposta anche in virtù di provvedimenti ad personam; l'ammontare di premi; il tempo di lavoro anche straordinario; ferie e permessi individuali (fruiti o residui); l'assenza dal servizio nei casi previsti dalla legge o dai contratti anche collettivi di lavoro; trasferimenti ad altra sede di lavoro; procedimenti e provvedimenti disciplinari.

I medesimi dati sono:

- contenuti in atti e documenti prodotti dai lavoratori in sede di assunzione (rispetto ai quali, con riferimento alle informazioni raccolte mediante annunci contenenti offerte di lavoro, questa Autorità si è già pronunciata o nel corso del rapporto di lavoro;
- contenuti in documenti e/o file elaborati dal (o per conto del) datore di lavoro in pendenza del rapporto di lavoro per finalità di esecuzione del contratto e successivamente raccolti e conservati in fascicoli personali, archivi cartacei o elettronici aziendali;

- resi disponibili in albi e bacheche o, ancora, nelle intranet aziendali.

7.2 Il rispetto dei principi di protezione dei dati personali

Le predette informazioni di carattere personale possono essere trattate dal datore di lavoro nella misura in cui siano necessarie per dare corretta esecuzione al rapporto di lavoro; talvolta, sono anche indispensabili per attuare previsioni contenute in leggi, regolamenti, contratti e accordi collettivi.

In ogni caso, deve trattarsi di informazioni pertinenti e non eccedenti e devono essere osservate tutte le disposizioni della vigente disciplina in materia di protezione dei dati personali che trae origine anche da direttive comunitarie.

In particolare, il Codice in materia di protezione dei dati personali (Codice), in attuazione delle direttive 95/46/CE e 2002/58/CE, prescrive che il trattamento di dati personali avvenga:

- nel rispetto di principi di necessità e liceità e che riguardano la qualità dei dati (artt. 3 e 11);
- informando preventivamente e adeguatamente gli interessati (art. 13);
- chiedendo preventivamente il consenso solo quando, anche a seconda della natura dei dati, non sia corretto avvalersi di uno degli altri presupposti equipollenti al consenso (artt. 23, 24, 26 e 43 del Codice);
- rispettando, se si trattano dati sensibili o giudiziari, le prescrizioni impartite dal Garante nelle autorizzazioni anche di carattere generale rilasciate (artt. 26 e 27 del Codice; cfr., in particolare, l'autorizzazione generale n. 1/2005);
- adottando le misure di sicurezza idonee a preservare i dati da alcuni eventi tra i quali accessi ed utilizzazioni indebite, rispetto ai quali può essere chiamato a rispondere anche civilmente e penalmente (artt. 15, 31 e ss., 167 e 169 del Codice).

Il trattamento di dati personali riferibili a singoli lavoratori, anche sensibili, è lecito, se finalizzato ad assolvere obblighi derivanti dal contratto individuale (ad esempio, per verificare l'esatto adempimento della prestazione o commisurare l'importo della retribuzione, anche per lavoro straordinario, o dei premi da corrispondere, per quantificare le ferie e i permessi, per appurare la sussistenza di una causa legittima di assenza).

Alcuni scopi sono altresì previsti dalla contrattazione collettiva per la determinazione di circostanze relative al rapporto di lavoro individuale (ad esempio, per la fruizione di permessi o aspettative sindacali e periodi di comporto o rispetto alle percentuali di lavoratori da assumere con particolari tipologie di contratto) o, ancora, dalla legge (quali, ad esempio, le comunicazioni ad enti previdenziali e assistenziali).

Se queste finalità sono in termini generali lecite, occorre però rispettare il principio della compatibilità tra gli scopi perseguiti (art. 11, comma 1, lett. b), del Codice): lo scopo perseguito in concreto dal datore di lavoro sulla base del trattamento di dati personali non deve essere infatti incompatibile con le finalità per le quali i medesimi sono stati raccolti.

7.3 Titolare e responsabile del trattamento

7.3.1 Titolare e responsabile

Ai fini della protezione dei dati personali assume un ruolo rilevante identificare le figure soggettive che a diverso titolo possono trattare i dati, definendo chiaramente le rispettive attribuzioni, in particolare, quelle del titolare e del responsabile del trattamento (artt. 4, comma 1, lett. f) e g), 28 e

29 del Codice). In linea di principio, per individuare il titolare del trattamento rileva l'effettivo centro di imputazione del rapporto di lavoro, al di là dello schema societario formalmente adottato. Peraltro, specie nelle realtà imprenditoriali più articolate, questa identificazione può risultare non sempre agevole e tale circostanza costituisce in qualche caso un ostacolo anche per l'esercizio dei diritti di cui all'art. 7

7.3.2 Gruppi di imprese

Le società che appartengono a gruppi di imprese individuati in conformità alla legge (art. 2359 cod. civ.; d.lg. 2 aprile 2002, n. 74) hanno di regola una distinta ed autonoma titolarità del trattamento in relazione ai dati personali dei propri dipendenti e collaboratori (artt. 4, comma 1, lett. f) e 28 del Codice).

Tuttavia, nell'ambito dei gruppi, le società controllate e collegate possono delegare la società capogruppo a svolgere adempimenti in materia di lavoro, previdenza ed assistenza sociale per i lavoratori indicati dalla legge (Cfr. art. 1 della legge 11 gennaio 1979, n. 12; cfr. art. 31, comma 1, d.lg. 10 settembre 2003, n. 276; l. 14 febbraio 2003, n. 30): tale attività implica la designazione della società capogruppo quale responsabile del trattamento ai sensi dell'art. 29 del Codice.

Analoga soluzione (art. 31, comma 2, d.lg. n. 276/2003) deve essere adottata per i trattamenti di dati personali, aventi identica natura, effettuati nell'ambito dei consorzi di società cooperative (nei quali a tal fine può essere altresì designata una delle società consorziate).

7.3.3 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 (Nuovo T.U. 81/2008 Sicurezza sul 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 (art. 2087 cod. civ.), pone direttamente in capo al medico competente in materia di igiene e sicurezza dei luoghi di lavoro la sorveglianza sanitaria obbligatoria (e per quanto previsto dal Nuovo T.U. 81/2008 la modalità di gestione, trattamento e conservazione dei dati contenuti in cartelle cliniche).

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'azienda o l'unità produttiva, o presso lo studio del medico competente 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 fa richiesta; in caso di cessazione del rapporto di lavoro le cartelle sono trasmesse all'Istituto superiore prevenzione e sicurezza sul lavoro-Ispesl, in originale e in busta chiusa.

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 (il medico opera quale libero professionista, o quale dipendente del datore di lavoro o di aziende sanitarie locali).

Alle predette cartelle il datore di lavoro non può accedere, dovendo soltanto concorrere ad assicurarne un'efficace custodia nei locali aziendali (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.

In tal senso, peraltro, depongono anche le previsioni legislative che dispongono la comunicazione all'Ispesl della cartella sanitaria e di rischio in caso di cessione o cessazione del rapporto di lavoro, precludendosi anche in tali occasioni ogni loro conoscibilità da parte del datore di lavoro.

7.4 Dati biometrici e accesso ad aree riservate

In più circostanze, anche ricorrendo al procedimento previsto dall'art. 17 del Codice, è stato prospettato al Garante l'utilizzo di dati biometrici sul luogo di lavoro, con particolare riferimento all'impiego di tali informazioni per accedere ad aree specifiche dell'impresa.

Si tratta di dati ricavati dalle caratteristiche fisiche o comportamentali della persona a seguito di un apposito procedimento (in parte automatizzato) e poi risultanti in un modello di riferimento. Quest'ultimo consiste in un insieme di valori numerici ricavati, attraverso funzioni matematiche, dalle caratteristiche individuali sopra indicate, preordinati all'identificazione personale attraverso opportune operazioni di confronto tra il codice numerico ricavato ad ogni accesso e quello originariamente raccolto.

L'uso generalizzato e incontrollato di dati biometrici, specie se ricavati dalle impronte digitali, non è lecito. Tali dati, per la loro peculiare natura, richiedono l'adozione di elevate cautele per prevenire possibili pregiudizi a danno degli interessati, con particolare riguardo a condotte illecite che determinino l'abusiva ricostruzione dell'impronta, partendo dal modello di riferimento, e la sua ulteriore utilizzazione a loro insaputa.

L'utilizzo di dati biometrici può essere giustificato solo in casi particolari, tenuto conto delle finalità e del contesto in cui essi sono trattati e, in relazione ai luoghi di lavoro, per presidiare accessi ad aree sensibili, considerata la natura delle attività ivi svolte: si pensi, ad esempio, a processi produttivi pericolosi o sottoposti a segreti di varia natura o al fatto che particolari locali siano destinati alla custodia di beni, documenti segreti o riservati o oggetti di valore

Inoltre, nei casi in cui l'uso dei dati biometrici è consentito, la centralizzazione in una banca dati delle informazioni personali (nella forma del predetto modello) trattate nell'ambito del descritto procedimento di riconoscimento biometrico risulta di regola sproporzionata e non necessaria. I sistemi informativi devono essere infatti configurati in modo da ridurre al minimo l'utilizzazione di dati personali e da escluderne il trattamento, quando le finalità perseguite possono essere realizzate con modalità tali da permettere di identificare l'interessato solo in caso di necessità (artt. 3 e 11 del Codice).

In luogo, quindi, di modalità centralizzate di trattamento dei dati biometrici, deve ritenersi adeguato e sufficiente avvalersi di sistemi efficaci di verifica e di identificazione biometrica basati sulla lettura delle impronte digitali memorizzate, tramite il predetto modello cifrato, su un supporto posto nell'esclusiva disponibilità dell'interessato (una smart card o un dispositivo analogo) e privo di indicazioni nominative riferibili a quest'ultimo (essendo sufficiente attribuire a ciascun dipendente un codice individuale).

Tale modalità di riconoscimento, infatti, è idonea ad assicurare che possano accedere all'area riservata solo coloro che, autorizzati preventivamente, decidano su base volontaria di avvalersi della predetta carta o del dispositivo analogo. Il confronto delle impronte digitali con il modello

memorizzato sulla carta o sul dispositivo può essere realizzato ricorrendo a comuni procedure di confronto sulla carta o dispositivo stesso, evitando così la costituzione di un archivio di delicati dati biometrici. Del resto, in caso di smarrimento della carta o dispositivo, sono allo stato circoscritte le possibilità di abuso rispetto ai dati biometrici ivi memorizzati.

I dati personali necessari per realizzare il modello possono essere trattati esclusivamente durante la fase di registrazione; per il loro utilizzo, il titolare del trattamento deve raccogliere il preventivo consenso informato degli interessati.

In aggiunta alle misure di sicurezza minime prescritte dal Codice, devono essere adottati ulteriori accorgimenti a protezione dei dati, impartendo agli incaricati apposite istruzioni scritte alle quali attenersi, con particolare riguardo al caso di perdita o sottrazione delle carte o dispositivi loro affidati.

I dati memorizzati devono essere accessibili al personale preposto al rispetto delle misure di sicurezza all'interno dell'impresa, per l'esclusiva finalità della verifica della loro osservanza (rispettando peraltro la disciplina sul controllo a distanza dei lavoratori: art. 4, comma 2, l. 20 maggio 1970, n. 300, richiamato dall'art. 114 del Codice).

I dati raccolti non possono essere di regola conservati per un arco di tempo superiore a sette giorni e vanno assicurati, anche quando tale arco temporale possa essere lecitamente protratto, idonei meccanismi di cancellazione automatica dei dati.

Resta salva, per fattispecie particolari o in ragione di situazioni eccezionali non considerate in questa sede, la presentazione da parte di titolari del trattamento che intendano discostarsi dalle presenti prescrizioni, di apposito interpello al Garante, ai sensi dell'art. 17 del Codice.

7.5 Comunicazione e diffusione di dati personali

7.5.1 Comunicazione

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 (art. 24 del Codice), 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 (artt. 4, comma 1, lett. g) e h), 29 e 30). 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 a livello aziendale o all'interno di singole unità produttive, agli importi di premi aziendali di risultato individuati per fasce, o qualifiche/livelli professionali, anche nell'ambito di singole funzioni o unità organizzative).

7.5.2 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 aziendale (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 (art. 24, comma 1, lett. b), del Codice). 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.

7.5.3 Diffusione

In assenza di specifiche disposizioni normative che impongano al datore di lavoro la diffusione di dati personali riferiti ai lavoratori (art. 24, comma 1, lett. a) 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 (art. 24, comma 1, lett. b) del Codice). È il caso, ad esempio, dell'affissione nella bacheca aziendale di ordini di servizio, di turni lavorativi o feriali, oltre che di disposizioni riguardanti l'organizzazione 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 (art. 11 del Codice), 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.

7.5.4 Cartellini identificativi

Analogamente, si possono determinare altre forme di diffusione di dati personali quando dette informazioni debbano essere riportate ed esibite su cartellini identificativi appuntati ad esempio sull'abito o sulla divisa del lavoratore (di solito, con lo scopo di migliorare il rapporto fra operatori ed utenti o clienti).

In relazione allo svolgimento del rapporto di lavoro alle dipendenze di soggetti privati, l'obbligo di portare in modo visibile un cartellino identificativo può trovare fondamento in alcune prescrizioni contenute in accordi sindacali aziendali, il cui rispetto può essere ricondotto alle prescrizioni del contratto di lavoro. Tuttavia, in relazione al rapporto con il pubblico, si è ravvisata la sproporzione dell'indicazione sul cartellino di dati personali identificativi (generalità o dati anagrafici), ben potendo spesso risultare sufficienti altre informazioni (quali codici identificativi, il solo nome o il ruolo professionale svolto), per sé sole in grado di essere d'ausilio all'utenza.

7.5.5 Modalità di comunicazione

Salvi i casi in cui forme e modalità di divulgazione di dati personali discendano da specifiche previsioni (cfr. art. 174, comma 12, del Codice) 19, 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.

7.6 Dati idonei a rivelare lo stato di salute di lavoratori

7.6.1 Dati sanitari

Devono essere osservate cautele particolari anche nel trattamento dei dati sensibili del lavoratore (art. 4, comma 1, lett. d), del Codice) 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 21. 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 (cfr. già l'art. 8 della legge n. 300/1970).

In questo contesto, la disciplina generale contenuta nel Codice deve essere coordinata ed integrata, come si è visto (cfr. punto 3.3.), con altre regole settoriali o speciali. Resta comunque vietata la diffusione di dati sanitari (art. 26, comma 5, del Codice).

7.6.2 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 sopra descritta, 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.

7.6.3 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 (artt. 13 e 53 d.P.R. n. 1124/1965).

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, trattandosi di dati non rilevanti nel caso oggetto di denuncia (art. 11, commi 1 e 2 del Codice)

7.6.4 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 (ai sensi dell'art. 124, commi 1 e 2, d.P.R. n. 309/1990).

7.6.5 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 (art. 5, commi 1 e 2, l. 20 maggio 1970, n. 300) 29; 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, o su richiesta dell'Inps o della struttura sanitaria pubblica da esso indicata, sono effettuate dai medici dei servizi sanitari indicati dalle regioni (art. 2, l. n. 33/1980 cit.).

7.7 Informativa

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: i lavoratori devono conoscere quali dati il datore di lavoro stia raccogliendo sul loro conto (direttamente o da altre fonti), quali siano gli scopi delle operazioni di trattamento previste o effettuate per tali dati sia per il presente che per il futuro.

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 alla società, che effettuino, ad esempio, l'attività di gestione degli archivi amministrativi dei dipendenti), indicandolo chiaramente nell'informativa fornita.

7.8 Misure di sicurezza

7.8.1 Dati sanitari

Il datore di lavoro titolare del trattamento è tenuto ad adottare ogni misura di sicurezza, anche minima, prescritta dal Codice a protezione dei dati personali dei dipendenti comunque trattati nell'ambito del rapporto di lavoro, ponendo particolare attenzione all'eventuale natura sensibile dei medesimi (art. 31 ss. e Allegato B) al Codice).

Dette informazioni devono essere conservate separatamente da ogni altro dato personale dell'interessato; ciò, deve trovare attuazione anche con riferimento ai fascicoli personali cartacei dei dipendenti (ad esempio, utilizzando sezioni appositamente dedicate alla custodia dei dati sensibili, inclusi quelli idonei a rivelare lo stato di salute del lavoratore, da conservare separatamente o in modo da non consentirne una indistinta consultazione nel corso delle ordinarie attività amministrative).

Del pari, nei casi in cui i lavoratori producano spontaneamente certificati medici su modulistica diversa da quella prevista, il datore di lavoro non può, comunque, utilizzare ulteriormente tali informazioni (art. 11, comma 2, del Codice) e deve adottare gli opportuni accorgimenti per non rendere visibili le diagnosi contenute nei certificati (ad esempio, prescrivendone la circolazione in busta chiusa previo oscuramento di tali informazioni); ciò, al fine di impedire ogni accesso abusivo a tali dati da parte di soggetti non previamente designati come incaricati o responsabili (art. 31 e ss. del Codice).

7.8.2 Incaricati

Resta fermo l'obbligo del datore di lavoro di preporre alla custodia dei dati personali dei lavoratori apposito personale, specificamente incaricato del trattamento, che deve avere cognizioni in materia di protezione dei dati personali e ricevere una formazione adeguata. In assenza di un'adeguata formazione degli addetti al trattamento dei dati personali il rispetto della riservatezza dei lavoratori sul luogo di lavoro non potrà mai essere garantito

7.8.3 Misure fisiche ed organizzative

Il datore di lavoro deve adottare, tra l'altro (cfr. artt. 31 ss. del Codice), misure organizzative e fisiche idonee a garantire che:

- i luoghi ove si svolge il trattamento di dati personali dei lavoratori siano opportunamente protetti da indebite intrusioni;
- le comunicazioni personali riferibili esclusivamente a singoli lavoratori avvengano con modalità tali da escluderne l'indebita presa di conoscenza da parte di terzi o di soggetti non designati quali incaricati;
- siano impartite chiare istruzioni agli incaricati in ordine alla scrupolosa osservanza del segreto d'ufficio, anche con riguardo a dipendenti del medesimo datore di lavoro che non abbiano titolo per venire a conoscenza di particolari informazioni personali;
- sia prevenuta l'acquisizione e riproduzione di dati personali trattati elettronicamente, in assenza di adeguati sistemi di autenticazione o autorizzazione e/o di documenti contenenti informazioni personali da parte di soggetti non autorizzati 33;
- sia prevenuta l'involontaria acquisizione di informazioni personali da parte di terzi o di altri dipendenti: opportuni accorgimenti, ad esempio, devono essere presi in presenza di una particolare conformazione o dislocazione degli uffici, in assenza di misure idonee volte a prevenire la diffusione delle informazioni (si pensi al mancato rispetto di distanze di sicurezza o alla trattazione di informazioni riservate in spazi aperti, anziché all'interno di locali chiusi).

7.9 Esercizio dei diritti dell'interessato e riscontro

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 (art. 10) 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.

Il 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.

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 (art. 146 del Codice).

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.

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 (art. 10).

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.

7.9.1 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 (salvo quanto previsto per la trasposizione dei dati su supporto cartaceo: cfr. art. 10, comma 2, del Codice).

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 (art. 10, comma 4, del Codice). 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 (cfr. art. 4, comma 1, lett. f), del Codice).

Infine, 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).

Capitolo 8

Regolamentazione del sito web

8.1 Partita iva obbligatoria su sito web

Il numero di partita Iva deve essere indicato nella pagina dell'eventuale sito web utilizzato, anche qualora attraverso di esso non venga esercitata attività di commercio elettronico e, dunque, anche se il sito venga utilizzato per finalità meramente pubblicitarie o propagandistiche.

L'Agenzia delle entrate, con risoluzione n. 60/E del 16 maggio 2006, ha in tal modo chiarito l'ambito di applicazione dell'articolo 35, comma 1, del Dpr n. 633 del 1972 in materia di dichiarazioni di inizio, variazione e cessazione attività ai fini Iva, disposizione integralmente modificata dall'articolo 2, comma 1, Dpr 5 ottobre 2001, n. 404, in vigore dal 1° dicembre 2001.

8.2 Informativa presente nella home-page del sito

L'informativa si ispira alla Raccomandazione n. 2/2001 che le autorità europee per la protezione dei dati personali, riunite nel Gruppo istituito dall'art. 29 della direttiva n. 95/46/CE adottata il 17 maggio 2001 per individuare alcuni requisiti minimi per la raccolta di dati personali on-line, e, in particolare, le modalità, i tempi e la natura delle informazioni che i titolari del trattamento devono fornire agli utenti quando questi si collegano a pagine web, indipendentemente dagli scopi del collegamento.

Di seguito sono descritte le nozioni da riportare all'interno dell'informativa.

8.2.1 Titolare del trattamento

All'interno dell'informativa deve essere chiaramente indicato il titolare del trattamento dei dati del sito web. Infatti,a seguito della consultazione del sito esiste la possibilità di trattare dati relativi a persone identificate o identificabili.

8.2.2 Luogo di trattamento dei dati

Indicare le sedi dove avvengono i trattamenti connessi ai servizi web del sito e dichiarare se il personale addetto autorizzato al trattamento è interno e/o esterno. Indicare se i dati vengono diffusi, modalità e finalità della diffusione.

8.2.3 Tipi di dati trattati

Dati di navigazione

I sistemi informatici e le procedure software preposte al funzionamento dei siti web acquisiscono, nel corso del loro normale esercizio, alcuni dati personali la cui trasmissione è implicita nell'uso dei

protocolli di comunicazione di Internet.

Si tratta di informazioni che non sono raccolte per essere associate a interessati identificati, ma che per loro stessa natura potrebbero, attraverso elaborazioni ed associazioni con dati detenuti da terzi, permettere di identificare gli utenti.

In questa categoria di dati rientrano gli indirizzi IP o i nomi a dominio dei computer utilizzati dagli utenti che si connettono al sito, gli indirizzi in notazione URI (Uniform Resource Identifier) delle risorse richieste, l'orario della richiesta, il metodo utilizzato nel sottoporre la richiesta al server, la dimensione del file ottenuto in risposta, il codice numerico indicante lo stato della risposta data dal server (buon fine, errore, ecc.) ed altri parametri relativi al sistema operativo e all'ambiente informatico dell'utente. Indicare la metodologia di gestione, conservazione e cancellazione di tali dati.

Contatti al sito web attraverso la posta elettronica

L'invio facoltativo, esplicito e volontario di posta elettronica agli indirizzi indicati sul sito comporta la successiva acquisizione dell'indirizzo del mittente, necessario per rispondere alle richieste, nonché degli eventuali altri dati personali inseriti nella missiva. Specificare nell'informativa finalità e modalità della gestione ed eventuale conservazione delle informazioni acquisite

Cookies

Dare garanzie sul fatto che nessun dato personale degli utenti viene in proposito acquisito dal sito. Dichiarare inoltre che non viene fatto uso di cookies per la trasmissione di informazioni di carattere personale, né vengono utilizzati c.d. cookies persistenti di alcun tipo, ovvero sistemi per il tracciamento degli utenti.

8.2.4 Facoltatività del conferimento dei dati

A parte quanto specificato per i dati di navigazione, l'utente è libero di fornire i dati personali attraverso e-mail o form in quanto il loro mancato conferimento può comportare l'impossibilità di ottenere i servizi richiesti. Qualora venissero costruite attraverso le informazioni acquisite banche dati deve essere redatto un regolamento interno per la gestione delle banche dati e l'utente deve essere informato su un loro eventuale utilizzo per finalità commerciali e/o promozionali.

8.2.5 Modalità del trattamento

Indicare la tipologia di strumenti automatizzati adottati per il trattamento, la conservazione e il salvataggio dei dati Si dovranno inoltre dare adeguate garanzie sui metodi di raccolta, conservazione e protezione da eventuali intercettazioni delle informazioni acquisite.

8.2.6 Diritti degli interessati

I soggetti cui si riferiscono i dati personali hanno il diritto in qualunque momento di ottenere la conferma dell'esistenza o meno dei medesimi dati e di conoscerne il contenuto e l'origine, verificarne l'esattezza o chiederne l'integrazione o l'aggiornamento, oppure la rettificazione (art. 7 del d.lgs. n. 196/2003).

Ai sensi del medesimo articolo si ha il diritto di chiedere la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, nonché di opporsi in ogni caso, per motivi legittimi, al loro trattamento. Indicare chiaramente sul sito web l'indirizzo a cui rivolgersi per richiedere la cancellazione dei dati acquisiti attraverso il sito web.

8.3 Consenso on-line

Per le modalità di raccolta on-line del consenso della clientela si ha la necessità che i sistemi informativi dei siti web vengano configurati in modo da consentire agli interessati di esplicare pienamente il proprio diritto all'autodeterminazione informativa, prevedendo opzioni di tipo "positivo" (mediante l'inserimento di caselle di scelta, anziché di campi pre-selezionati su una tra le possibili scelte), così da permettere ad essi di esprimere liberamente le proprie scelte in ordine alle finalità legittimamente perseguibili da parte del titolare del trattamento.

Ad esempio è constatata la non conformità alle norme in materia di protezione dei dati della scelta di raccogliere in un unico contesto (condizioni generali di contratto), sia il consenso del cliente per accedere on-line ad alcuni servizi, sia il consenso per trattare i dati conferiti per la fruizione di quest'ultimi allo scopo di perseguire una finalità diversa, quale quella dell'invio di comunicazioni commerciali in forma elettronica intese a promuovere iniziative proprie o a veicolare iniziative promozionali nell'interesse di terzi. Un consenso manifestato nei termini appena descritti non può ritenersi valido, atteso che i clienti devono essere messi in condizione di esprimere consapevolmente e liberamente le proprie scelte in ordine al trattamento dei dati che li riguardano, manifestando il proprio consenso, quando questo è necessario, per ciascuna distinta finalità perseguita dal titolare.

Qualora ricorrano le condizioni di cui all'art. 130, comma 4, del Codice, norma in base alla quale il titolare del trattamento che utilizzi le coordinate di posta elettronica fornite dall'interessato nel contesto della vendita di un prodotto o di un servizio ai fini di vendita diretta di propri prodotti o servizi (e sempre che si tratti di servizi analoghi a quelli oggetto della vendita e l'interessato), può non richiedere il consenso qualora l'interessato, adeguatamente informato, non rifiuti tale uso, inizialmente o in occasione di successive comunicazioni. Affinché in tale ipotesi il trattamento si configuri come legittimo, occorre quindi accordare al cliente la possibilità di opporsi in maniera agevole e gratuitamente all'utilizzo delle coordinate di posta elettronica per finalità di vendita diretta, sin dalla fase di raccolta dei dati, come pure in occasione dell'invio di ogni comunicazione successiva.

Capitolo 9

Norme per posta elettronica e internet

9.1 Sintesi

I datori di lavoro pubblici e privati non possono controllare la posta elettronica e la navigazione in Internet dei dipendenti, se non in casi eccezionali. Spetta al datore di lavoro definire le modalità d'uso di tali strumenti ma tenendo conto dei diritti dei lavoratori e della disciplina in tema di relazioni sindacali.

Il Garante prescrive innanzitutto ai datori di lavoro di informare con chiarezza e in modo dettagliato i lavoratori sulle modalità di utilizzo di Internet e della posta elettronica e sulla possibilità che vengano effettuati controlli. Il Garante vieta poi la lettura e la registrazione sistematica delle e-mail così come il monitoraggio sistematico delle pagine web visualizzate dal lavoratore, perché ciò realizzerebbe un controllo a distanza dell'attività lavorativa vietato dallo Statuto dei lavoratori. Viene inoltre indicata tutta una serie di misure tecnologiche e organizzative per prevenire la possibilità, prevista solo in casi limitatissimi, dell'analisi del contenuto della navigazione in Internet e dell'apertura di alcuni messaggi di posta elettronica contenenti dati necessari all'azienda.

Il provvedimento raccomanda l'adozione da parte delle aziende di un disciplinare interno, definito coinvolgendo anche le rappresentanze sindacali, nel quale siano chiaramente indicate le regole per l'uso di Internet e della posta elettronica.

Il datore di lavoro è inoltre chiamato ad adottare ogni misura in grado di prevenire il rischio di utilizzi impropri, così da ridurre controlli successivi sui lavoratori. Per quanto riguarda Internet è opportuno ad esempio:

- individuare preventivamente i siti considerati correlati o meno con la prestazione lavorativa;
- utilizzare filtri che prevengano determinate operazioni, quali l'accesso a siti inseriti in una sorta di black list o il download di file musicali o multimediali.

Per quanto riguarda la posta elettronica, è opportuno che l'azienda:

- renda disponibili anche indirizzi condivisi tra più lavoratori (info@ente.it; urp@ente.it; ufficioreclami@ente.it), rendendo così chiara la natura non privata della corrispondenza;
- valuti la possibilità di attribuire al lavoratore un altro indirizzo (oltre quello di lavoro), destinato ad un uso personale;
- preveda, in caso di assenza del lavoratore, messaggi di risposta automatica con le coordinate di altri lavoratori cui rivolgersi;
- metta in grado il dipendente di delegare un altro lavoratore (fiduciario) a verificare il contenuto dei messaggi a lui indirizzati e a inoltrare al titolare quelli ritenuti rilevanti per l'ufficio, ciò in caso di assenza prolungata o non prevista del lavoratore interessato e di improrogabili necessità legate all'attività lavorativa.

Qualora queste misure preventive non fossero sufficienti a evitare comportamenti anomali, gli eventuali controlli da parte del datore di lavoro devono essere effettuati con gradualità. In prima battuta si dovranno effettuare verifiche di reparto, di ufficio, di gruppo di lavoro, in modo da individuare l'area da richiamare all'osservanza delle regole. Solo successivamente, ripetendosi l'anomalia, si potrebbe passare a controlli su base individuale.

9.2 Premessa

Per conformare alle disposizioni vigenti il trattamento di dati personali effettuato per verificare il corretto utilizzo nel rapporto di lavoro della posta elettronica e della rete Internet, occorre muovere da alcune premesse:

1. compete ai datori di lavoro assicurare la funzionalità e il corretto impiego di tali mezzi da parte dei lavoratori, definendone le modalità d'uso nell'organizzazione dell'attività lavorativa, tenendo conto della disciplina in tema di diritti e relazioni sindacali;

2. spetta ad essi adottare idonee misure di sicurezza per assicurare la disponibilità e l'integrità di sistemi informativi e di dati, anche per prevenire utilizzi indebiti che possono essere fonte di responsabilità (artt. 15, 31 ss., 167 e 169 del Codice);

3. emerge l'esigenza di tutelare i lavoratori interessati anche perché l'utilizzazione dei predetti mezzi, già ampiamente diffusi nel contesto lavorativo, è destinata ad un rapido incremento in numerose attività svolte anche fuori della sede lavorativa;

4. l'utilizzo di Internet da parte dei lavoratori può infatti formare oggetto di analisi, profilazione e integrale ricostruzione mediante elaborazione di log file della navigazione web ottenuti, ad esempio, da un proxy server o da un altro strumento di registrazione delle informazioni. I servizi di posta elettronica sono parimenti suscettibili (anche attraverso la tenuta di log file di traffico e-mail e l'archiviazione di messaggi) di controlli che possono giungere fino alla conoscenza da parte del datore di lavoro (titolare del trattamento) del contenuto della corrispondenza;

5. le informazioni così trattate contengono dati personali anche sensibili riguardanti lavoratori o terzi, identificati o identificabili.

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 (artt. 2 e 41, secondo comma, Cost.; art. 2087 cod. civ.; cfr. altresì l'art. 2, comma 5, Codice dell'amministrazione digitale (d.lg. 7 marzo 2005, n. 82), riguardo al diritto ad ottenere che il trattamento dei dati effettuato mediante l'uso di tecnologie telematiche sia conformato al rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato).
Non a caso, nell'organizzare l'attività lavorativa e gli strumenti utilizzati, diversi datori di lavoro hanno prefigurato modalità d'uso che, tenendo conto del crescente lavoro in rete e di nuove tariffe di traffico forfettarie, assegnano aree di lavoro riservate per appunti strettamente personali, ovvero consentono usi moderati di strumenti per finalità private.

9.3 Principi generali

Si tiene conto del diritto alla protezione dei dati personali, della necessità che il trattamento sia disciplinato assicurando un elevato livello di tutela delle persone, nonché dei principi di semplificazione, armonizzazione ed efficacia (artt. 1 e 2 del Codice). Alcune disposizioni di settore, fatte

salve dal Codice, prevedono specifici divieti o limiti, come quelli posti dallo Statuto dei lavoratori sul controllo a distanza (artt. 113, 114 e 184, comma 3, del Codice; artt. 4 e 8 l. 20 maggio 1970, n. 300). La disciplina di protezione dei dati va coordinata con regole di settore riguardanti il rapporto di lavoro e il connesso utilizzo di tecnologie.

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

- il principio di necessità, secondo cui i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite (art. 3 del Codice; par. 5.2);
- il principio di correttezza, secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori (art. 11, comma 1, lett. a), del Codice). Le tecnologie dell'informazione (in modo più marcato rispetto ad apparecchiature tradizionali) permettono di svolgere trattamenti ulteriori rispetto a quelli connessi ordinariamente all'attività lavorativa. Ciò, all'insaputa o senza la piena consapevolezza dei lavoratori, considerate anche le potenziali applicazioni di regola non adeguatamente conosciute dagli interessati (v. par. 3);
- i trattamenti devono essere effettuati per finalità determinate, esplicite e legittime (art. 11, comma 1, lett. b), del Codice: par. 4 e 5), osservando il principio di pertinenza e non eccedenza (par. 6). Il datore di lavoro deve trattare i dati nella misura meno invasiva possibile; le attività di monitoraggio devono essere svolte solo da soggetti preposti (par. 8) ed essere mirate sull'area di rischio, tenendo conto della normativa sulla protezione dei dati e, se pertinente, del principio di segretezza della corrispondenza

9.4 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 (art. 4, secondo comma, Statuto dei lavoratori;allegato VII, par. 3 d.lg. n. 626/1994 e successive integrazioni e modificazioni in materia di uso di attrezzature munite di videoterminali, il quale esclude la possibilità del controllo informatico all'insaputa dei lavoratori).

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

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

9.4.1 Disciplinare

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

A seconda dei casi andrebbe ad esempio specificato:

- se determinati comportamenti non sono tollerati rispetto alla navigazione in Internet (ad es., il download di software o di file musicali), oppure alla tenuta di file nella rete interna;

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

9.4.2 Informativa (art. 13 del Codice)

All'onere del datore di lavoro di prefigurare e pubblicizzare una policy interna rispetto al corretto uso dei mezzi e agli eventuali controlli, si affianca il dovere di informare comunque gli interessati ai sensi dell'art. 13 del Codice, anche unitamente agli elementi indicati ai punti 3.1. e 3.2.. Rispetto a eventuali controlli gli interessati hanno infatti il diritto di essere informati preventivamente, e in modo chiaro, sui trattamenti di dati che possono riguardarli.
Le finalità da indicare possono essere connesse a specifiche esigenze organizzative, produttive e di sicurezza del lavoro, quando comportano un trattamento lecito di dati (art. 4, secondo comma, l. n. 300/1970); possono anche riguardare l'esercizio di un diritto in sede giudiziaria. Devono essere tra l'altro indicate le principali caratteristiche dei trattamenti, nonché il soggetto o l'unità organizzativa ai quali i lavoratori possono rivolgersi per esercitare i propri diritti.

9.5 Apparecchiature preordinate al controllo a distanza

Con riguardo al principio secondo cui occorre perseguire finalità determinate, esplicite e legittime (art. 11, comma 1, lett. b), del Codice), il datore di lavoro può riservarsi di controllare (direttamente o attraverso la propria struttura) l'effettivo adempimento della prestazione lavorativa e, se necessario, il corretto utilizzo degli strumenti di lavoro (cfr. artt. 2086, 2087 e 2104 cod. civ.). Nell'esercizio di tale prerogativa occorre rispettare la libertà e la dignità dei lavoratori, in particolare per ciò che attiene al divieto di installare apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori (art. 4, primo comma, l. n. 300/1970), tra cui sono certamente comprese

strumentazioni hardware e software mirate al controllo dell'utente di un sistema di comunicazione elettronica. Il trattamento dei dati che ne consegue è illecito, a prescindere dall'illiceità dell'installazione stessa. Ciò, anche quando i singoli lavoratori ne siano consapevoli.

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 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 (art. 11, comma 2, del Codice).

9.6 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 (art. 4, comma 2), di sistemi che consentono indirettamente un controllo a distanza (c.d. controllo preterintenzionale) e determinano un trattamento di dati personali riferiti o riferibili ai lavoratori. 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 di lavoratori e sindacati 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 (artt. 3, 11, comma 1, lett. d) e 22, commi 3 e 5, del Codice; aut. gen. al trattamento dei dati sensibili n. 1/2005, punto 4). Dal punto di vista organizzativo è quindi opportuno che:

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

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

9.7 Internet: la navigazione web

Il datore di lavoro, per ridurre il rischio di usi impropri della navigazione in Internet (consistenti in attività non correlate alla prestazione lavorativa quali la visione di siti non pertinenti, l'upload o il download di file, l'uso di servizi di rete con finalità ludiche o estranee all'attività), deve adottare opportune misure che possono, così, prevenire controlli successivi sul lavoratore. Tali controlli, leciti o meno a seconda dei casi, possono determinare il trattamento di informazioni personali, anche non pertinenti o idonei a rivelare convinzioni religiose, filosofiche o di altro genere, opinioni politiche, lo stato di salute o la vita sessuale (art. 8 l. n. 300/1970; artt. 26 e 113 del Codice; Provv. 2 febbraio 2006, cit.).

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

- individuazione di categorie di siti considerati correlati o meno con la prestazione lavorativa;
- configurazione di sistemi o utilizzo di filtri che prevengano determinate operazioni 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.

9.8 Posta elettronica

Il contenuto dei messaggi di posta elettronica, come pure i dati esteriori delle comunicazioni e i file allegati, riguardano forme di corrispondenza assistite da garanzie di segretezza tutelate anche costituzionalmente, la cui ratio risiede nel proteggere il nucleo essenziale della dignità umana e il pieno sviluppo della personalità nelle formazioni sociali; un'ulteriore protezione deriva dalle norme penali a tutela dell'inviolabilità dei segreti (artt. 2 e 15 Cost.; Corte cost. 17 luglio 1998, n. 281 e 11 marzo 1993, n. 81; art. 616, quarto comma, c.p.; art. 49 Codice dell'amministrazione digitale). Tuttavia, con specifico riferimento all'impiego della posta elettronica nel contesto lavorativo e in ragione della veste esteriore attribuita all'indirizzo di posta elettronica nei singoli casi, può risultare dubbio se il lavoratore, in qualità di destinatario o mittente, utilizzi la posta elettronica operando quale espressione dell'organizzazione datoriale o ne faccia un uso personale pur operando in una struttura lavorativa.

La mancata esplicitazione di una policy al riguardo può determinare anche una legittima aspettativa del lavoratore, o di terzi, di confidenzialità rispetto ad alcune forme di comunicazione. Tali incertezze si riverberano sulla qualificazione, in termini di liceità, del comportamento del datore di lavoro che intenda apprendere il contenuto di messaggi inviati all'indirizzo di posta elettronica usato dal lavoratore (posta in entrata) o di quelli inviati da quest'ultimo (posta in uscita).

É quindi particolarmente opportuno che si adottino accorgimenti anche per prevenire eventuali trattamenti in violazione dei principi di pertinenza e non eccedenza. Si tratta di soluzioni che possono risultare utili per contemperare le esigenze di ordinato svolgimento dell'attività lavorativa con la prevenzione di inutili intrusioni nella sfera personale dei lavoratori, nonché violazioni della disciplina sull'eventuale segretezza della corrispondenza.

In questo quadro è opportuno che:

- il datore di lavoro renda disponibili indirizzi di posta elettronica condivisi tra più lavoratori (ad esempio, info@ente.it, ufficiovendite@ente.it, ufficioreclami@società.com, urp@ente.it, etc.), eventualmente affiancandoli a quelli individuali (ad esempio, m.rossi@ente.it, rossi@società.com, mario.rossi@società.it);
- il datore di lavoro valuti la possibilità di attribuire al lavoratore un diverso indirizzo destinato ad uso privato del lavoratore;
- 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 aziendale per la protezione dei dati), l'attivazione di un analogo accorgimento, avvertendo gli interessati;
- in previsione della possibilità che, in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, si debba conoscere il contenuto dei messaggi di posta elettronica, l'interessato sia messo in grado di delegare un altro lavoratore (fiduciario) a verificare il contenuto di messaggi e a inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. A cura del titolare del trattamento, di tale attività dovrebbe essere redatto apposito verbale e informato il lavoratore interessato alla prima occasione utile;
- i messaggi di posta elettronica contengano un avvertimento ai destinatari nel quale sia dichiarata l'eventuale natura non personale dei messaggi stessi, precisando se le risposte potranno essere conosciute nell'organizzazione di appartenenza del mittente e con eventuale rinvio alla predetta policy datoriale.

9.9 Controlli

Nell'effettuare controlli sull'uso degli strumenti elettronici deve essere evitata un'interferenza ingiustificata sui diritti e sulle libertà fondamentali di lavoratori, come pure di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata. L'eventuale controllo è lecito solo se sono rispettati i principi di pertinenza e non eccedenza.

Nel caso in cui un evento dannoso o una situazione di pericolo non sia stato impedito con preventivi accorgimenti tecnici, il datore di lavoro può adottare eventuali misure che consentano la verifica di comportamenti anomali. Deve essere per quanto possibile preferito un controllo preliminare su dati aggregati, riferiti all'intera struttura lavorativa o a sue aree. Il controllo anonimo può concludersi con un avviso generalizzato relativo ad un rilevato utilizzo anomalo degli strumenti aziendali e con l'invito ad attenersi scrupolosamente a compiti assegnati e istruzioni impartite. L'avviso può essere circoscritto a dipendenti afferenti all'area o settore in cui è stata rilevata l'anomalia. In assenza di successive anomalie non è di regola giustificato effettuare controlli su base individuale.

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

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

la conservazione temporanea dei dati relativi all'uso degli strumenti elettronici deve essere giustificata da una finalità specifica e comprovata e limitata al tempo necessario a raggiungerla (v. art. 11, comma 1, lett. e), del Codice). Un eventuale prolungamento dei tempi di conservazione va valutato come eccezionale e può aver luogo solo in relazione:

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

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

9.10 Liceità del trattamento

I datori di lavoro privati e gli enti pubblici economici possono effettuare lecitamente il trattamento dei dati personali diversi da quelli sensibili:

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

Per tale bilanciamento si è tenuto conto delle garanzie che lo Statuto prevede per il controllo indiretto a distanza presupponendo non il consenso degli interessati, ma un accordo con le rappresentanze sindacali (o, in difetto, l'autorizzazione di un organo periferico dell'amministrazione del lavoro).

L'eventuale trattamento di dati sensibili è consentito con il consenso degli interessati o, senza il consenso, nei casi previsti dal Codice (in particolare, esercizio di un diritto in sede giudiziaria, salvaguardia della vita o incolumità fisica; specifici obblighi di legge anche in caso di indagine giudiziaria: art. 26).

Per quanto riguarda i soggetti pubblici restano fermi i differenti presupposti previsti dal Codice a seconda della natura dei dati, sensibili o meno (artt. 18-22 e 112).

In tutti i casi predetti resta impregiudicata la facoltà del lavoratore di opporsi al trattamento per motivi legittimi (art. 7, comma 4, lett. a), del Codice).

9.11 Soggetti preposti

Nel caso di eventuali interventi per esigenze di manutenzione del sistema, va posta opportuna cura nel prevenire l'accesso a dati personali presenti in cartelle o spazi di memoria assegnati a dipendenti. Resta fermo l'obbligo dei soggetti preposti al connesso trattamento dei dati (in particolare, gli incaricati della manutenzione) di svolgere solo operazioni strettamente necessarie al perseguimento delle relative finalità, senza realizzare attività di controllo a distanza, anche di propria iniziativa. Resta parimenti ferma la necessità che, nell'individuare regole di condotta dei soggetti che operano quali amministratori di sistema o figure analoghe cui siano rimesse operazioni connesse al regolare funzionamento dei sistemi, sia svolta un'attività formativa sui profili tecnico-gestionali e di sicurezza delle reti, sui principi di protezione dei dati personali e sul segreto nelle comunicazioni.

9.12 Misure da adottare e divieti

Le misure prescritte e da adottare da parte del titolare del trattamento sono:

1. la predisposizione di un'informativa per specificare le modalità di utilizzo della posta elettronica e della rete Internet da parte dei lavoratori, indicando chiaramente le modalità di uso degli strumenti messi a disposizione e se, in che misura e con quali modalità vengano effettuati controlli;
2. l'adozione e la pubblicizzazione di un disciplinare interno;
3. l'adozione di misure di tipo organizzativo affinché; si proceda ad un'attenta valutazione dell'impatto sui diritti dei lavoratori; si individui preventivamente (anche per tipologie) a quali lavoratori è accordato l'utilizzo della posta elettronica e dell'accesso a Internet; si individui quale ubicazione è riservata alle postazioni di lavoro per ridurre il rischio di impieghi abusivi;
4. l'adozione di misure di tipo tecnologico, rispetto alla navigazione in Internet;
5. l'adozione di misure di tipo tecnologico, rispetto all'utilizzo della posta elettronica.

Vige inoltre il divieto per i datori di lavoro privati e pubblici, ai sensi dell'art. 154, comma 1, lett. d), del Codice, di effettuare trattamenti di dati personali mediante sistemi hardware e software che mirano al controllo a distanza di lavoratori, svolti in particolare mediante:

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

Tuttavia si individuano, ai sensi dell'art. 24, comma 1, lett. g), del Codice, i casi nei quali il trattamento dei dati personali di natura non sensibile possono essere effettuati per perseguire un legittimo interesse del datore di lavoro anche senza il consenso degli interessati: esercizio di un diritto in sede giudiziaria, salvaguardia della vita o incolumità fisica; specifici obblighi di legge anche in caso di indagine giudiziaria.