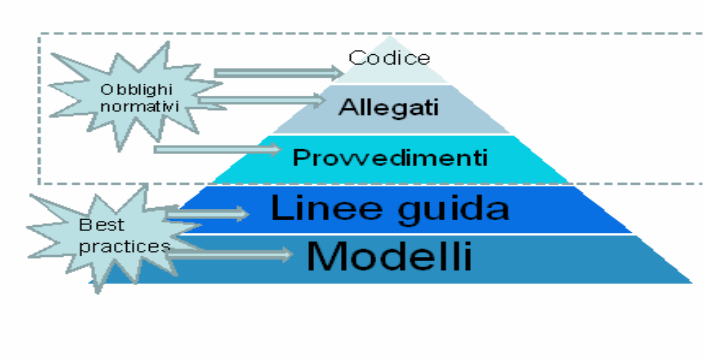
Privacy e Adempimenti per le Piccole e Medie Imprese

Aspetti normativi e pratici per una corretta attuazione del d.lgs. 196/2003

Programma

- **Breve introduzione al codice privacy**
- **Le misure minime di sicurezza (Allegato B)**
- **Videosorveglianza: il provvedimento generale del 2010**
- **Il nuovo art. 4 dello statuto dei lavoratori**
- **Le linee guida del Garante per posta elettronica e Internet**
- **Il regolamento interno: come predisporre le policy aziendali sull'utilizzo degli strumenti e sui relativi controlli**
- **Cookie: il provvedimento del 2014**
- **Il nuovo Regolamento Europeo: cosa ci attende**
- **Esempi concreti di ispezione del Garante**

Le Fonti della pricvacy



N/b prestare attenzione ai sensi di quale norma sono deliberati i provvedimenti del Garante: art. 154 comma 1 let. h) (fine divulgativo) o art. 154 comma 1 let. c) (prescrizioni obbligatorie)

Prossimamente…

Nuovo Regolamento Privacy U.E.

Probabile approvazione entro giugno 2016

TITOLO I Principi generali della norma

Non tutti i dati sono uguali di fronte alla legge

la legge individua (art. 4 co.1) **le seguenti categorie di dati, alle quali sono riservate particolari forme di tutela:**

- **dati personali,** (elencati nella lettera b)
- **dati sensibili,** (elencati nella lettera d)
- **dati giudiziari,** (descritti nella lettera e)

DATI personali, sensibili e giudiziari

dati personali: qualunque informazione relativa a persona fisica identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale; *

* Novità introdotta dal d.l. 6 Dicembre 2011, n.201 (c.d. decreto salva Italia)

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;

Il concetto di TRATTAMENTO

Il trattamento dei dati personali è qualunque operazione o complesso di operazioni svolte con o senza l'ausilio di strumenti elettronici, che concerne le operazioni di: raccolta dei dati, registrazione, organizzazione, conservazione, consultazione, elaborazione, blocco, modificazione, utilizzo, interconnessione, comunicazione, diffusione, cancellazione, distruzione, selezione, estrazione, raffronto.

TITOLO I Principi generali della norma

Art. 1 (Diritto alla protezione dei dati personali)
[1] Chiunque ha diritto alla protezione dei dati personali che lo riguardano.

Art. 3 (Principio di necessità nel trattamento dei dati)
[1] I sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.

Relazione: L'art. 3 introduce il "principio di necessità" nel trattamento dei dati personali, [….]. Il principio introdotto integra e completa, con riferimento alla configurazione stessa dell'ambiente in cui i dati sono trattati, il principio di pertinenza e non eccedenza dei dati trattati già operante in relazione al trattamento dei medesimi dati (art. 11, già art. 9, Legge n. 675/1996).

TITOLO II Diritti dell'Interessato

L'interessato è la persona fisica cui si riferiscono i dati personali*

* Novità introdotta dal d.l. 6 Dicembre 2011, n.201 (c.d. decreto salva Italia)

Art. 7 (Diritto di accesso ai dati personali ed altri diritti) **NUOVO CODICE**
[1] L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile.

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

TITOLO II Diritti dell'Interessato

Diritto di conoscere

quali dati personali sul proprio conto il titolare possieda.

Il titolare deve dare riscontro all'interessato entro quindici giorni dal ricevimento della richiesta (art. 146, comma 2 del Codice). Se le operazioni necessarie per un integrale riscontro alla richiesta sono di particolare complessità, ovvero ricorre altro giustificato motivo, il titolare o il responsabile ne danno comunicazione all'interessato. In tal caso, il termine per l'integrale riscontro è di trenta giorni dal ricevimento della richiesta medesima (art. 146, comma 3 del Codice).

TITOLO II Diritti dell'Interessato

diritto di certificare e controllare

L'interessato ha inoltre diritto di chiedere:

- **l'aggiornamento e la rettifica dei dati, qualora essi siano inesatti**
- **la loro integrazione, qualora vi abbia interesse**
- **la legge prevede che il titolare debba portare l'aggiornamento, la rettifica o l'integrazione a conoscenza dell'interessato**
- **diritto di ottenere la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge**

TITOLO III principi

Art. 11 (Modalità del trattamento e requisiti dei dati)
[1] I dati personali oggetto di trattamento sono: a) trattati in modo lecito e secondo correttezza; b) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi; c) esatti e, se necessario, aggiornati; d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati; e) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

ART 13 INFORMATIVA

"DIRITTO DI CIASCUNO AD AVERE IL CONTROLLO DELLE PROPRIE INFORMAZIONI"

L'Informativa è il primo e più generalizzato adempimento, imposto a tutti i soggetti che trattano i dati personali, sia pubblici che privati

Obbligo di informare il soggetto interessato che si raccolgono e trattano dati sul suo conto

Nel sistema privacy, l'informativa è un adempimento propedeutico a tutte le operazioni di trattamento dei dati personali del soggetto interessato, che si intende porre in essere

CONTENUTO DELL'INFORMATIVA

Devono essere rese le informazioni su:

a) le finalità e le modalità del trattamento cui sono destinati i dati
b) la natura obbligatoria o facoltativa del conferimento dei dati
c) le conseguenze di un eventuale rifiuto di rispondere
d) i soggetti o le categorie di soggetti ai quali i dati possono essere comunicati, o che possono venirne a conoscenza in qualità di membri della *filiera del trattamento* del titolare (responsabili e incaricati) e l'ambito di diffusione dei dati medesimi
e) i diritti dell'interessato, di cui all'articolo 7 – *Diritto di accesso ai dati personali ed altri diritti*
f) gli estremi identificativi:
   - del titolare, del rappresentante nel territorio dello Stato, in caso di titolare residente in Paesi extra – Ue
   - di almeno un responsabile, se designato

Il titolare che informative potrà trattare ?

- **Informativa CLIENTI / FORNITORI**
  (dipende se i clienti sono persone fisiche o meno)
  Novità introdotta dal d.l. 6 Dicembre 2011, n.201 (c.d. decreto salva Italia)
- **Informativa DIPENDENTI / COLLABORATORI**
- **Informativa CURRICULA**
  ART 13 comma 5-bis: L'informativa di cui al comma 1 non è dovuta in caso di ricezione di curricula spontaneamente trasmessi dagli interessati ai fini dell'eventuale instaurazione di un rapporto di lavoro. Al momento del primo contatto successivo all'invio del curriculum, il titolare è tenuto a fornire all'interessato, anche oralmente, una informativa breve contenente almeno gli elementi di cui al comma 1, lettere a), d) ed f). (Novità introdotta dalla legge 12 luglio 2011, n. 106)

CONSENSO

Il consenso è la libera manifestazione della volontà con la quale l'interessato accetta – in modo espresso e, se vi sono dati sensibili, per iscritto - un determinato trattamento di dati che lo riguardano, sul quale è stato preventivamente informato da chi utilizza i dati.

CONSENSO

TRATTAMENTO DI SOLI DATI PERSONALI COMUNI

Impresa che tratta dati personali comuni unicamente per scopi contrattuali, contabili, fiscali o comunque derivanti da leggi o regolamenti.

NON NECESSARIO

CONSENSO

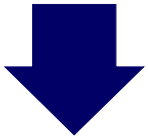
TRATTAMENTO DI SOLI DATI PERSONALI COMUNI

Impresa che tratta dati personali comuni per scopi diversi da quelli contrattuali, contabili, fiscali o comunque derivanti da leggi o regolamenti.
Es: Comunicazione a terzi per finalità commerciali

NECESSARIO

CONSENSO

TRATTAMENTO che contempla dati sensibili



SEMPRE NECESSARIO

(salvo rare eccezioni)

SANZIONI

VIOLAZIONI AMMINISTRATIVE	Sanzioni Amministrative
Art. 161 Omessa o inidonea informativa	Sanzione da 6.000 € a 36.000 €
Art. 162 c.2 ter Inosservanza dei provvedimenti del Garante (ai sensi all'art 154, c. 1, lettere c e d)	**Sanzione da 30.000 € a 180.000 €**
Art. 163 Omessa o incompleta notificazione al Garante	Sanzione da 20.000 € a 120.000 €
Art. 164 Omessa informazione o esibizione dei documenti	Sanzione da 10.000 € a 60.000 €
ILLECITI PENALI	**Sanzioni Penali**
Art. 167 Trattamento illecito di dati personali	Reclusione da 6 mesi a 3 anni.
Art. 168 Falsità nelle dichiarazioni e notificazioni al Garante	Reclusione da 6 mesi a 3 anni
Art. 169 Omessa adozione delle misure minime di sicurezza	**Arresto fino a 2 anni** **Ravvedimento operoso (Legge 14/2009)**
Art. 170 Inosservanza dei provvedimenti del Garante (provvedimento adottato dal Garante ai sensi degli articoli 26, comma 2, 90, 150, commi 1 e 2, e 143, comma 1, lettera c),)	Reclusione da tre mesi a due anni

Art. 15
DANNI CAGIONATI PER EFFETTO DEL TRATTAMENTO

[1] Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile.

***Articolo 2050 c.c. - Responsabilità per l'esercizio di attività pericolose**: Chiunque cagiona danno ad altri nello svolgimento di un'attività pericolosa, per sua natura o per la natura dei mezzi adoperati, è tenuto al risarcimento, se non prova di avere adottato tutte le misure idonee ad evitare il danno*

DANNO PATRIMONIALE

Il richiamo all'articolo 2050 c.c. introduce altri elementi gravosi, per chi tratta i dati:

l'inversione dell'onere della prova

chi ha subito il danno **non deve provare** la responsabilità oggettiva del titolare del trattamento, ma toccherà a questi provare di avere adottato **tutte le misure idonee** ad evitare il danno

la limitazione della prova

la norma non considera sufficiente la prova di avere adottato le misure ragionevolmente imposte dalla diligenza, ma richiede la prova di avere adottato **tutte le misure di sicurezza offerte dalla tecnica**. La norma dispone quindi una responsabilità per qualsiasi **danno oggettivamente evitabile**, in base allo stato della tecnica al momento in cui l'evento che ha causato il danno si è verificato.

DANNO PATRIMONIALE

Dal tenore letterale della norma emerge che chiunque è responsabile, dei danni che ha direttamente causato trattando dati personali

La disposizione trova applicazione nei riguardi di

- **a chi tratta dati per fini esclusivamente personali**
- **Titolare**
- **Responsabili**
- **Incaricati al trattamento**

Si rendono applicabili i criteri di risarcimento previsti dall'art. 2050

ci si trova quindi nel campo della **responsabilità oggettiva**, per cui **il titolare del trattamento *non risponde solo dei danni causati direttamente*, ma anche di quelli provocati dalla sua organizzazione**

DANNO NON PATRIMONIALE

Per i trattamenti che integrano la violazione dell'articolo 11 *(modalità del trattamento e requisiti dei dati personali*) **è prevista la risarcibilità non solo del danno patrimoniale, ma anche del danno non patrimoniale sofferto dal soggetto interessato**

DANNO BIOLOGICO DI NATURA PSICHICA

Sofferenze
Patemi
Risentimento
Compressioni o turbamenti della personalità
Dolore

Attenzione !!
La tendenza giurisprudenziale è di accordare cospicui risarcimenti, a fronte dei danni non patrimoniali

TITOLO IV
SOGGETTI CHE EFFETTUANO IL TRATTAMENTO

Nell'ambito del trattamento dei dati il codice prevede le seguenti figure:

- **il titolare (articolo 28)**
- **il responsabile (articolo 29)**
- **l'incaricato (articolo 30).**

TITOLO IV
SOGGETTI CHE EFFETTUANO IL TRATTAMENTO

Art. 4 [1f "Titolare"]

Ai fini del codice privacy si intende per "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.

I compiti principali del "Titolare", decidere:

- **Su come (modalità)**
- **Sul perché (finalità) raccogliere e trattare i dati**
- **Su come organizzare il trattamento**
- **Sulle risorse (strumenti) da dedicarvi**
- **Sulle Misure sicurezza da adottare**

TITOLO IV
SOGGETTI CHE EFFETTUANO IL TRATTAMENTO

Art.4 [1g "Responsabile"] **Ai fini del codice privacy si intende per "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.**

Art.29

[1] Il responsabile è designato dal titolare facoltativamente.

- **deve procedere al trattamento sulla scorta delle istruzioni impartitegli dal titolare**
- **vigila sul rispetto delle vigenti disposizioni in materia di trattamento e sicurezza**
- **vigila sul rispetto delle disposizioni da lui impartite all'organizzazione**

TITOLO IV
SOGGETTI CHE EFFETTUANO IL TRATTAMENTO

Art.4 [1h "Incaricato"] **Ai fini del codice privacy si intende per "incaricati" le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile.**

Art. 30 "Incaricati del trattamento"
[1] Le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite.
[2] La designazione è effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito. Si considera tale anche la documentata preposizione della persona fisica ad una unità per la quale è individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima.

TITOLO IV
SOGGETTI CHE EFFETTUANO IL TRATTAMENTO

L'incaricato del trattamento PUO' ESSERE

<u>Persona fisica</u> che abbia un rapporto di:

- **lavoro subordinato col titolare**
- **di lavoro autonomo col titolare**
- **di collaborazione col titolare**
- **soggetti che dipendono da altre organizzazioni** (a condizione che agiscano sotto la diretta autorità e controllo del titolare o di un responsabile, del soggetto che ha commissionato il trattamento)

TITOLO IV
SOGGETTI CHE EFFETTUANO IL TRATTAMENTO

Predisposizione e aggiornamento del "MANSIONARIO PRIVACY"

Nella predisposizione del mansionario si può procedere anche come segue:

- **definizione di classi omogenee di incarico**
- **definizione dei profili di autorizzazione; si deve distinguere almeno tra:**
  - autorizzati ad accedere ai dati di natura comune
  - autorizzati ad accedere ai dati di natura sensibile
- **successivamente, si *domiciliano* tutti gli incaricati, ciascuno nella classe omogenea di appartenenza** (per cui, ad esempio, nella classe omogenea sopra individuata confluiranno gli *impiegati dell'ufficio personale*)
- **Periodicamente, con cadenza almeno annuale,** si dovrà verificare la parte che riguarda le autorizzazioni al trattamento al fine di verificare la sussistenza delle condizioni che giustificano tali autorizzazioni

PARTE 2

Analisi dettagliata delle misure minime di sicurezza (Allegato B)

TITOLO V
SICUREZZA DEI DATI E DEI SISTEMI

Art. 31 (Obblighi di sicurezza)

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

TITOLO V
SICUREZZA DEI DATI E DEI SISTEMI

Art. 33 (Misure Minime)

Nel quadro dei più generali obblighi di sicurezza di cui all'articolo 31, o previsti da speciali disposizioni, i titolari del trattamento sono comunque tenuti ad adottare le misure minime individuate nel presente capo o ai sensi dell'articolo 58, comma 3, volte ad assicurare un livello minimo di protezione dei dati personali.

TITOLO V
SICUREZZA DEI DATI E DEI SISTEMI

La differenza tra MISURE MINIME e MISURE IDONEE

Esistono due diversi livelli di responsabilità.
Il titolare deve individuare preventivamente misure di sicurezza che devono almeno rispettare i parametri di sicurezza minimi individuati nel Codice (articoli 33, 34, 35 e 36); se le misure di sicurezza adottate non rispettano i parametri minimi contenuti nel regolamento, scatta la responsabilità penale.

Ma l'individuazione di misure che rispettano i parametri previsti come minimi non è sufficiente a liberare da ogni responsabilità il soggetto che effettua il trattamento. Se le misure adottate non sono idonee ad evitare il danno, vi può essere comunque la responsabilità civile, anche se non ci sono gli estremi per la responsabilità penale prevista dalla legge.

TITOLO V
SICUREZZA DEI DATI E DEI SISTEMI

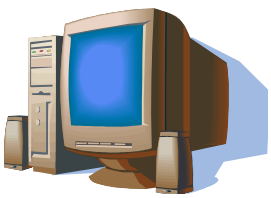
Le misure minime di sicurezza che devono essere adottate dipendono dal combinarsi di due variabili:

- **dalla natura dei dati che vengono trattati:**
  Comuni – Sensibili – Giudiziari
- **dagli strumenti che vengono utilizzati per trattare i dati:**
  - **elettronici**
  - **diversi da quelli elettronici**

Trattamenti effettuati con mezzi elettronici
Punti da 1 a 11 Disciplinare Tecnico

Punto 1.
Il trattamento di dati personali con strumenti elettronici è consentito 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.

Accesso consentito solo se si è dotati di CREDENZIALI DI AUTENTICAZIONE



Non è in alcun caso consentito che si possa accedervi liberamente

Trattamenti effettuati con mezzi elettronici
Punti da 1 a 11 Disciplinare Tecnico

Punto 3.
Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.

Ad ogni incaricato possono essere assegnate una o più chiavi, anche di natura diversa.

Non è possibile assegnare la medesima chiave a due o più incaricati

Trattamenti effettuati con mezzi elettronici
Punti da 1 a 11 Disciplinare Tecnico

Punto 5.
La parola chiave, quando è prevista dal sistema di autenticazione, è 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; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.

Password

composta da almeno otto caratteri * * * * * * * *

non deve contenere riferimenti agevolmente riconducibili all'interessato **krTT8891**

L'incaricato deve provvedere a modificare la parola chiave:

- **immediatamente, non appena la riceve per la prima volta, da chi amministra il sistema**
- **successivamente, almeno ogni sei mesi. Il termine scende a tre mesi, se la parola chiave dà accesso ad aree in cui sono contenuti dati sensibili o giudiziari**

Trattamenti effettuati con mezzi elettronici
Punti da 1 a 11 Disciplinare Tecnico

La chiave per accedere agli strumenti deve essere disattivata:

- **immediatamente, nel caso in cui l'incaricato perda la qualità, che gli consentiva di accedere allo strumento**
- **in ogni caso, entro sei mesi di mancato utilizzo, fa ovviamente eccezione il caso delle chiavi che sono state preventivamente autorizzate**
- **Si devono predisporre accorgimenti tali, per cui anche per soli pochi minuti il computer non resti incustodito e accessibile (c.d. Password di screensaver)**

Trattamenti effettuati con mezzi elettronici
Punti da 1 a 11 Disciplinare Tecnico

Punto 10.
Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o 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.
[omissis]

REGOLA GENERALE
Nessuno, (neppure il titolare del trattamento), può accedere allo strumento elettronico, utilizzando la *credenziale di autenticazione dell'incaricato*

ECCEZIONE a tale regola si ha solo se verificano congiuntamente le seguenti condizioni:
- **prolungata assenza o impedimento dell'incaricato**
- **l'intervento è indispensabile e indifferibile**
- **vi sono concrete necessità, di operatività e di sicurezza del sistema.**

Trattamenti effettuati con mezzi elettronici

Punti da 12 a 14 Disciplinare Tecnico

Sistema di AUTENTICAZIONE

Si accerta l'identità della persona

ACCESSO al sistema

Il sistema di AUTORIZZAZIONE stabilisce:

- **A quali dati è possibile accedere**
- **Quali trattamenti si possono compiere**

Trattamenti effettuati con mezzi elettronici

Punti da 16 a 18 Disciplinare Tecnico

Punto 16
I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.

Punto 20.
I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all'art. 615-ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici.

Prevenire l'attacco di "Codici nocivi"

Virus, Worm,Trojan Horse, ecc...

con l'uso di

Antivirus e Firewall (o IDS)

Trattamenti effettuati con mezzi elettronici

Punti da 16 a 18 Disciplinare Tecnico

Punto 17.
Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.

Questo significa che periodicamente vanno aggiornati i sistemi operativi e gli atri applicativi che, se obsoleti, possono creare vulnerabilità.

Punto 18.
Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.

Questo significa che almeno una volta per settimana si deve effettuare il backup di tutti i dati personali .

Misure minime di sicurezza per il trattamento cartaceo dei dati

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

È necessario che gli incaricati siano formati, mediante istruzioni fornite in forma scritta, su come trattare atti e documenti contenenti dati personali.

Misure minime di sicurezza per il trattamento cartaceo dei dati

Punto 28.
Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

Gli incaricati del trattamento devono prelevare dagli archivi i soli atti e documenti loro affidati, che devono custodire e restituire al termine delle operazioni di trattamento

Misure minime di sicurezza per il trattamento cartaceo dei dati

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

Gli archivi contenenti atti e documenti con dati sensibili e giudiziari devono essere controllati, mediante l'adozione dei seguenti accorgimenti:

- **fare in modo che agli archivi accedano solo i soggetti autorizzati:**
  - **dotare gli archivi di strumenti elettronici per il controllo degli accessi**
  - **incaricare delle persone, alla vigilanza degli archivi**
  - **nel caso in cui non venga adottata alcune delle soluzioni di cui sopra, si deve autorizzare preventivamente le persone ad accedere agli archivi**
- **per gli accessi che avvengono *dopo l'orario di chiusura*, obbligo di *identificare* e *registrare* le persone che accedono agli archivi**
- **in ogni caso, l'archivio contenente i dati in esame deve potere essere *chiuso***

SANZIONI
(art. 169 del Codice)

il mancato adeguamento alle misure minime di sicurezza costituisce reato, con la previsione della pena dell'arresto sino a 2 anni

Nuovo comma 2 (Legge 14/2009): **all'autore del reato, all'atto dell'accertamento o, nei casi complessi, anche con successivo atto del Garante, è impartita una prescrizione fissando un termine per la regolarizzazione non eccedente il periodo di tempo tecnicamente necessario, prorogabile in caso di particolare complessità o per l'oggettiva difficoltà dell'adempimento e comunque non superiore a sei mesi. Nei sessanta giorni successivi allo scadere del termine, se risulta l'adempimento alla prescrizione, l'autore del reato è ammesso dal Garante a pagare una somma pari al quarto del massimo della sanzione stabilita per la violazione amministrativa. L'adempimento e il pagamento estinguono il reato.**

Giurisprudenza
Cassazione civile - Sezione Lavoro:
licenziamento per comunicazione password per accesso alla rete aziendale (Settembre 2006)

La Beta S.r.l. ha licenziato il proprio dipendente signor Caio previa contestazione disciplinare del fatto che a partire dal mese di novembre 1999 erano state eseguite connessioni con la rete informativa interna della società utilizzando l'identificativo del Caio, e ciò anche da un'utenza telefonica del distretto di Milano, in giorni in cui il Caio era al lavoro nella sede di Avezzano; tali connessioni si erano verificate anche nei giorni 26, 27 e 28 dicembre utilizzando la password del Caio da poco sostituita.

L'impugnativa del licenziamento, accolta dal Tribunale di Avezzano, è stata respinta dalla Corte d'appello di L'Aquila con sentenza 30 ottobre 2003/8 gennaio 2004 n. 91.

Giurisprudenza

Cassazione civile - Sezione Lavoro:
licenziamento per comunicazione password per accesso alla rete aziendale (Settembre 2006)

Il giudice d'appello ha ritenuto accertate le seguenti circostanze di fatto:

1. le connessioni dall'esterno utilizzando la password del Caio sono iniziate subito dopo il licenziamento del dipendente Tizio, avvenuto il 26 ottobre 1999;

2. esse sono state eseguite in maggioranza attraverso un'utenza appartenente al distretto telefonico di Milano ed intestata alla moglie del Tizio, come da rapporto P.S.;

3. il 13 dicembre 1999 il Caio ha modificato la propria password su richiesta del sistema informatico;

4. alle ore 13.05 del giorno 24 dicembre 1999 è intercorsa una telefonata tra il Tizio ed il Caio, e dal pomeriggio dello stesso giorno sono riprese le connessioni dall'utenza telefonica intestata alla moglie del Tizio con la nuova password del Caio.

Giurisprudenza

Cassazione civile - Sezione Lavoro:
licenziamento per comunicazione password per accesso alla rete aziendale (Settembre 2006)

Caio ricorre in Cassazione ed il collegio respinge, così motivando:

"…per quanto riguarda, infine, la valutazione della gravità dell'inadempimento realizzato dal Caio, ritiene il Collegio che essa sia tale da giustificare il recesso datoriale.

Invero il comportamento del lavoratore si è concretato nella diffusione all'esterno di dati (le password personali) idonei a consentire a terzi di accedere ad una grande massa di informazioni attinenti l'attività aziendale e destinate a restare riservate.

La valutazione della proporzionalità della sanzione rispetto alla gravità della mancanza del lavoratore si risolve in un apprezzamento di fatto incensurabile in sede di legittimità ove sorretto da motivazione adeguata e logica (ex plurimis Cassazione 16628/04; 12083/03; 12001/03). La sottrazione di dati aziendali è stata ritenuta idonea ad integrare la giusta causa di licenziamento (Cassazione 2560/93)."

N/b interessante è l'equiparazione tra la comunicazione della password aziendale e la sottrazione di dati aziendali

Giurisprudenza

Cassazione civile - Sezione Lavoro:
licenziamento per comunicazione password per accesso alla rete aziendale (Settembre 2006)

A questo si aggiungono i profili penalistici (nel caso concreto non risulta denuncia/querela della azienda):

Art. 615 ter Accesso abusivo ad un sistema informatico o telematico
Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volonta' espressa o tacita di chi ha il diritto di escluderlo, e' punito con la reclusione fino a tre anni.

Art. 622 Rivelazione di segreto professionale
Chiunque, avendo notizia, per ragione del proprio stato o ufficio, o della propria professione o arte, di un segreto, lo rivela, senza giusta causa, ovvero lo impiega a proprio o altrui profitto, e' punito, se dal fatto puo' derivare nocumento, con la reclusione fino ad un anno o con la multa da lire sessantamila a un milione.

Art. 623 Rivelazione di segreti scientifici o industriali
Chiunque, venuto a cognizione per ragione del suo stato o ufficio, o della sua professione o arte, di notizie destinate a rimanere segrete, sopra scoperte o invenzioni scientifiche o applicazioni industriali, le rivela o le impiega a proprio o altrui profitto, e' punito con la reclusione fino a due anni.

Da notare che siffatta ipotesi non è riconducibile alla ipotesi di furto (624 cp) in quanto la Cassazione ha chiarito (sentenza 3449/2004) che i dati informatici (la loro duplicazione) non sono compresi nel, pur ampio, concetto di "cosa mobile".

Provvedimento in materia di videosorveglianza - 8 aprile 2010 (G.U. n. 99 del 29 aprile 2010) e problematiche connesse alla legge 300/1970

PRINCIPI GENERALI

Il Garante ha ritenuto necessario intervenire nuovamente in tale settore con il presente provvedimento generale che sostituisce quello del 29 aprile 2004.

La raccolta, la registrazione, la conservazione e, in generale, l'utilizzo di immagini configura un trattamento di dati personali (*art. 4, comma 1, lett. b), del Codice*). È considerato dato personale, infatti, qualunque informazione relativa a persona fisica identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione.

PRINCIPI GENERALI

L'installazione di sistemi di rilevazione delle immagini deve avvenire nel rispetto, oltre che della disciplina in materia di protezione dei dati personali, anche delle altre disposizioni dell'ordinamento applicabili, quali ad esempio le vigenti norme in materia di:

- interferenze illecite nella vita privata (art. 615 bis c.p.);
- controllo a distanza dei lavoratori;
- sicurezza presso stadi e impianti sportivi;
- sicurezza presso musei, biblioteche e archivi di Stato;
- navi passeggeri adibite a viaggi nazionali;
- porti, stazioni ferroviarie e linee di trasporto urbano.

PRINCIPI GENERALI

1. L'installazione di telecamere è consigliabile solo quando altre misure di sicurezza siano ritenute insufficienti o inattuabili.
2. L'eventuale registrazione e conservazione delle immagini deve essere limitata nel tempo.
3. I cittadini devono sapere sempre e comunque se un'area è sottoposta a videosorveglianza.

Prima di installare un impianto di videosorveglianza occorre valutare se la sua utilizzazione sia realmente proporzionata agli scopi perseguiti o se non sia invece superflua. Gli impianti devono cioè essere attivati solo quando altre misure (sistemi d'allarme, altri controlli fisici o logistici, misure di protezione agli ingressi ecc.) siano realmente insufficienti o inattuabili.

ADEMPIMENTI APPLICABILI A SOGGETTI PUBBLICI E PRIVATI
Informativa

Gli interessati devono essere sempre informati che stanno per accedere in una zona videosorvegliata; ciò anche nei casi di eventi e in occasione di spettacoli pubblici.

Se le immagini non sono registrate, sostituire il termine "registrazione" con quello di "rilevazione".

ADEMPIMENTI APPLICABILI A SOGGETTI PUBBLICI E PRIVATI
Informativa

Il supporto con l'informativa:

• deve essere collocato prima del raggio di azione della telecamera, anche nelle sue immediate vicinanze e non necessariamente a contatto con gli impianti;

• deve avere un formato ed un posizionamento tale da essere chiaramente visibile in ogni condizione di illuminazione ambientale, anche quando il sistema di videosorveglianza sia eventualmente attivo in orario notturno;

• può inglobare un simbolo o una stilizzazione di esplicita e immediata comprensione, eventualmente diversificati al fine di informare se le immagini sono solo visionate o anche registrate.

ADEMPIMENTI APPLICABILI A SOGGETTI PUBBLICI E PRIVATI
Informativa

Il Garante ritiene auspicabile che l'informativa, resa in forma semplificata avvalendosi del predetto modello, poi rinvii a un testo completo contenente tutti gli elementi di cui all'art. 13, comma 1, del Codice, disponibile agevolmente senza oneri per gli interessati, con modalità facilmente accessibili anche con strumenti informatici e telematici (in particolare, tramite reti Intranet o siti Internet, affissioni in bacheche o locali, avvisi e cartelli agli sportelli per gli utenti, messaggi preregistrati disponibili digitando un numero telefonico gratuito).

In ogni caso il titolare, anche per il tramite di un incaricato, ove richiesto è tenuto a fornire anche oralmente un'informativa adeguata, contenente gli elementi individuati dall'art. 13 del Codice.

ADEMPIMENTI APPLICABILI A SOGGETTI PUBBLICI E PRIVATI
Informativa

Norme specifiche sono previste per la videosorveglianza effettuata per finalità di tutela dell'ordine e della sicurezza pubblica, prevenzione, accertamento o repressione dei reati. (Forze di polizia)

Quando i soggetti privati effettuano collegamenti con le forze di polizia si deve adottare un modello differente di cartello informativo:

ADEMPIMENTI APPLICABILI A SOGGETTI PUBBLICI E PRIVATI
Verifica preliminare del Garante

Quando vi sono rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità degli interessati, in relazione alla natura dei dati o alle modalità di trattamento o agli effetti che può determinare, il Titolare del trattamento deve richiedere una verifica preliminare alla autorità Garante.

Alcuni esempi:

- sistemi di raccolta delle immagini associate a dati biometrici;
- sistemi dotati di software che permetta il riconoscimento delle persone tramite l'incrocio con altri dati personali (es: morfologia del volto);
- sistemi "intelligenti" in grado di rilevare anomalie dei comportamenti delle persone;
- sistemi che devono registrare immagini per più di 7 giorni (con esclusione delle specifiche richieste della A.G. o della P.G.).

ADEMPIMENTI APPLICABILI A SOGGETTI PUBBLICI E PRIVATI
Verifica preliminare del Garante

Il titolare del trattamento di dati personali effettuato tramite sistemi di videosorveglianza non deve richiedere una verifica preliminare purché siano rispettate tutte le seguenti condizioni:

a) il Garante si sia già espresso con un provvedimento di verifica preliminare in relazione a determinate categorie di titolari o di trattamenti;

b) la fattispecie concreta, le finalità del trattamento, la tipologia e le modalità d'impiego del sistema che si intende adottare, nonché le categorie dei titolari, corrispondano a quelle del trattamento approvato;

c) si rispettino integralmente le misure e gli accorgimenti conosciuti o concretamente conoscibili prescritti nel provvedimento di cui alla lett. a) adottato dal Garante.

ADEMPIMENTI APPLICABILI A SOGGETTI PUBBLICI E PRIVATI
Verifica preliminare del Garante

Resta inteso che il normale esercizio di un impianto di videosorveglianza, non deve essere sottoposto all'esame preventivo del Garante, sempreché il trattamento medesimo avvenga con modalità conformi al presente provvedimento.

NOTIFICAZIONE

E' regola generale che i trattamenti di dati personali devono essere notificati al Garante solo se rientrano nei casi specificamente previsti dall'*art. 37 del Codice*.

MISURE DI SICUREZZA DA APPLICARE

I dati raccolti mediante sistemi di videosorveglianza devono essere protetti con idonee e preventive misure di sicurezza, riducendo al minimo i rischi di distruzione, di perdita, anche accidentale, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità della raccolta, anche in relazione alla trasmissione delle immagini (artt. 31 e ss. del Codice).

Per siffatte misure di sicurezza si devono rispettare i seguenti principi:

- a) in presenza di differenti competenze specificatamente attribuite ai singoli operatori devono essere configurati diversi livelli di visibilità e trattamento delle immagini. Laddove tecnicamente possibile, in base alle caratteristiche dei sistemi utilizzati, i predetti soggetti, designati incaricati o, eventualmente, responsabili del trattamento, devono essere in possesso di credenziali di autenticazione che permettano di effettuare, a seconda dei compiti attribuiti ad ognuno, unicamente le operazioni di propria competenza;

- b) laddove i sistemi siano configurati per la registrazione e successiva conservazione delle immagini rilevate, deve essere altresì attentamente limitata la possibilità, per i soggetti abilitati, di visionare le immagini registrate e di effettuare sulle medesime operazioni di cancellazione o duplicazione;

MISURE DI SICUREZZA DA APPLICARE

Per siffatte misure di sicurezza si devono rispettare i seguenti principi:

- c) per quanto riguarda il periodo di conservazione delle immagini devono essere predisposte misure tecniche od organizzative per la cancellazione, anche in forma automatica, delle registrazioni, allo scadere del termine previsto;

- d) nel caso di interventi derivanti da esigenze di manutenzione, occorre adottare specifiche cautele; in particolare, i soggetti preposti alle predette operazioni possono accedere alle immagini solo se ciò si renda indispensabile;

- e) qualora si utilizzino apparati di ripresa digitali connessi a reti informatiche, gli apparati medesimi devono essere protetti contro i rischi di accesso abusivo di cui all'art. 615-*ter* del codice penale;

- f) la trasmissione tramite una rete pubblica di comunicazioni di immagini riprese da apparati di videosorveglianza deve essere effettuata previa applicazione di tecniche crittografiche che ne garantiscano la riservatezza; le stesse cautele sono richieste per la trasmissione di immagini da punti di ripresa dotati di connessioni wireless (tecnologie *wi-fi, wi-max, Gprs*).

RESPONSABILI E INCARICATI

Il titolare o il responsabile devono designare per iscritto tutte le persone fisiche, incaricate del trattamento, autorizzate sia ad accedere ai locali dove sono situate le postazioni di controllo, sia ad utilizzare gli impianti e, nei casi in cui sia indispensabile per gli scopi perseguiti, a visionare le immagini (art. 30 del Codice). Deve trattarsi di un numero delimitato di soggetti, specie quando il titolare si avvale di collaboratori esterni.

Occorre altresì individuare diversi livelli di accesso in corrispondenza delle specifiche mansioni attribuite ad ogni singolo operatore, distinguendo coloro che sono unicamente abilitati a visionare le immagini dai soggetti che possono effettuare, a determinate condizioni, ulteriori operazioni (es. registrare, copiare, cancellare, spostare l'angolo visuale, modificare lo zoom, ecc.).

E' opportuno predisporre un **REGOLAMENTO INTERNO** per la gestione del sistema di videosorveglianza, a cui si dovranno attenere il responsabile e gli incaricati designati.

DURATA DELLA CONSERVAZIONE

La conservazione deve essere limitata a poche ore o, al massimo, alle ventiquattro ore successive alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura di uffici o esercizi, nonché nel caso in cui si deve aderire ad una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria.

Solo in alcuni casi, per peculiari esigenze tecniche (mezzi di trasporto) o per la particolare rischiosità dell'attività svolta dal titolare del trattamento (ad esempio, per alcuni luoghi come le banche può risultare giustificata l'esigenza di identificare gli autori di un sopralluogo nei giorni precedenti una rapina), può ritenersi ammesso un tempo più ampio di conservazione dei dati che, sulla scorta anche del tempo massimo legislativamente posto per altri trattamenti, si ritiene non debba comunque superare la settimana.

DURATA DELLA CONSERVAZIONE

Per i comuni e nelle sole ipotesi in cui l'attività di videosorveglianza sia finalizzata alla tutela della sicurezza urbana, alla luce delle recenti disposizioni normative (art. 6, comma 8, del d.l. n. 11/2009), il termine massimo di durata della conservazione dei dati è limitato "ai sette giorni successivi alla rilevazione delle informazioni e delle immagini raccolte mediante l'uso di sistemi di videosorveglianza, fatte salve speciali esigenze di ulteriore conservazione".

In tutti i casi in cui si voglia procedere a un allungamento dei tempi di conservazione per un periodo superiore alla settimana, una richiesta in tal senso deve essere sottoposta ad una verifica preliminare del Garante, e comunque essere ipotizzato dal titolare come eccezionale nel rispetto del principio di proporzionalità.

DIRITTI DEGLI INTERESSATI

Deve essere assicurato agli interessati identificabili l'effettivo esercizio dei propri diritti in conformità al Codice, in particolare quello di accedere ai dati che li riguardano, di verificare le finalità, le modalità e la logica del trattamento (*art. 7 del Codice*).

La risposta ad una richiesta di accesso a dati conservati deve riguardare tutti quelli attinenti al richiedente identificabile e può comprendere eventuali dati riferiti a terzi solo nei limiti previsti dal Codice, ovvero nei soli casi in cui la scomposizione dei dati trattati o la privazione di alcuni elementi renda incomprensibili i dati personali relativi all'interessato (*art. 10, comma 5, del Codice*).

In riferimento alle immagini registrate non è in concreto esercitabile il diritto di aggiornamento, rettificazione o integrazione in considerazione della natura intrinseca dei dati raccolti, in quanto si tratta di immagini raccolte in tempo reale riguardanti un fatto obiettivo. Viceversa, l'interessato ha diritto di ottenere il blocco dei dati qualora essi siano trattati in violazione di legge (*art. 7, comma 3, lett. b), del Codice*).

SETTORI SPECIFICI
Rapporti di lavoro

Nuovo Art. 4 della l. n. 300/1970

SETTORI SPECIFICI
Rapporti di lavoro

COMMA 1 - Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali. In alternativa, nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale. In mancanza di accordo gli impianti e gli strumenti di cui al periodo precedente possono essere installati previa autorizzazione della Direzione territoriale del lavoro o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più Direzioni territoriali del lavoro, del Ministero del lavoro e delle politiche sociali.

SETTORI SPECIFICI
Rapporti di lavoro

COMMA 2 – La disposizione di cui al comma 1 non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze.

COMMA 3 – Le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196

SISTEMI INTEGRATI DI VIDEOSORVEGLIANZA

Per economicità delle risorse e dei mezzi impiegati, si è incrementato il ricorso a sistemi integrati di videosorveglianza tra diversi soggetti, pubblici e privati, nonché l'offerta di servizi centralizzati di videosorveglianza remota da parte di fornitori (società di vigilanza, Internet service providers, fornitori di servizi video specialistici, ecc.).

Nel caso di collegamento telematico di diversi titolari del trattamento ad un "centro" unico gestito da un soggetto terzo; tale soggetto terzo, designato responsabile del trattamento ai sensi dell'art. 29 del Codice da parte di ogni singolo titolare, deve assumere un ruolo di coordinamento e gestione dell'attività di videosorveglianza senza consentire, tuttavia, forme di correlazione delle immagini raccolte per conto di ciascun titolare;

SISTEMI INTEGRATI DI VIDEOSORVEGLIANZA

Le modalità di trattamento, per i suddetti sistemi integrati di videosorveglianza, richiedono l'adozione di specifiche misure di sicurezza ulteriori rispetto a quelle individuate in precedenza; quali :

1) adozione di sistemi idonei alla registrazione degli accessi logici degli incaricati e delle operazioni compiute sulle immagini registrate, compresi i relativi riferimenti temporali, con conservazione per un periodo di tempo congruo all'esercizio dei doveri di verifica periodica dell'operato dei responsabili da parte del titolare, comunque non inferiore a sei mesi;

2) separazione logica delle immagini registrate dai diversi titolari.

Fuori dalle predette ipotesi, in tutti i casi in cui i trattamenti effettuati tramite sistemi integrati di videosorveglianza hanno natura e caratteristiche tali per cui le misure e gli accorgimenti sopra individuati non siano integralmente applicabili, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che possono determinare, il titolare del trattamento è tenuto a richiedere una verifica preliminare al Garante.

SANZIONI

Le misure necessarie prescritte con il presente provvedimento devono essere osservate da tutti i titolari di trattamento. In caso contrario il trattamento dei dati è, a seconda dei casi, illecito oppure non corretto, ed espone:

- all'inutilizzabilità dei dati personali trattati in violazione della relativa disciplina (*art. 11, comma 2, del Codice*);
- all'adozione di provvedimenti di blocco o di divieto del trattamento disposti dal Garante (*art. 143, comma 1, lett. c*), del Codice), e di analoghe decisioni adottate dall'autorità giudiziaria civile e penale;
- all'applicazione delle pertinenti sanzioni amministrative o penali (*artt. 161 e ss. del Codice*).

SANZIONI

Art. 162.

2-ter.(3) In caso di inosservanza dei provvedimenti di prescrizione di misure necessarie o di divieto di cui, rispettivamente, all'articolo 154, comma 1, lettere c) e d), è altresì applicata in sede amministrativa, in ogni caso, la sanzione del pagamento di una somma da trentamila euro a centottantamila euro.

RIEPILOGO DOCUMENTAZIONE VIDEOSORVEGLIANZA

- Cartelli informativi
- Informativa completa
- Regolamento interno sull'utilizzo del sistema
- Designazione incaricati al trattamento
- Designazione responsabile del trattamento
- Regolare i rapporti contrattuali con l'eventuale società esterna di manutenzione
- Regolare i rapporti contrattuali con l'eventuale società di vigilanza

Lavoro: le linee guida del Garante per posta elettronica e internet

G.U. n. 58 del 10 marzo 2007

LE LINEE GUIDA DEL GARANTE PER POSTA ELETTRONICA E INTERNET

Il DISCIPLINARE INTERNO

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

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

LE LINEE GUIDA DEL GARANTE PER POSTA ELETTRONICA E INTERNET

- 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

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

LE LINEE GUIDA DEL GARANTE PER POSTA ELETTRONICA E INTERNET

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

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

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

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

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

LE LINEE GUIDA DEL GARANTE PER POSTA ELETTRONICA E 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.

LE LINEE GUIDA DEL GARANTE PER POSTA ELETTRONICA E INTERNET

La navigazione web

Il Garante "indica" le seguenti misure:

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

IL DISCIPLINARE INTERNO

- **Censimento degli strumenti: quali sono gli strumenti utilizzati in azienda ?**
- **Esiste delle della documentazione tecnica per gli strumenti censiti ?**
- **Per gli strumenti di «controllo» esistono degli accordi sindacali ?**
- **Per gli strumenti di lavoro esistono delle policy o delle istruzioni sulle modalità d'uso ?**
- **Quali sono i soggetti che possono fare i controlli ?**
- **Quali sono le modalità di realizzazione dei controlli ?**

IL DISCIPLINARE INTERNO

Alcuni consigli per la corretta stesura di un disciplinare interno:

- **Confronto con le rappresentanze sindacali**
- **Prevedere le sanzioni disciplinari**
- **Approvazione da parte del CDA**
- **Dare adeguata pubblicità interna (se possibile far firmare per presa visione e affissione in bacheca)**

IL DISCIPLINARE INTERNO

Premessa e termini utilizzati
1. Entrata in vigore del regolamento, pubblicità e campo di applicazione
2. Utilizzo delle risorse informatiche aziendali
3. Utilizzo della rete
4. Utilizzo di personal computer
5. Gestione delle credenziali di autenticazione
6. Accesso ai file su PC, dispositivi mobili e cartelle di rete
7. Assistenza tecnica e protezione da virus
8. Uso della posta elettronica
9. Gestione della posta elettronica del personale assente o cessato
10. Uso della rete internet e dei relativi servizi
11. Utilizzo dei telefoni, fax e fotocopiatrici aziendali
12. Custodia dei documenti cartacei contenenti dati personali
13. Custodia dei supporti rimovibili
14. Osservanza delle disposizioni in materia di privacy
15. Non osservanza della normativa aziendale
16. Aggiornamento e revisione

Individuazione delle modalità semplificate per fornire l'informativa e acquisire il consenso per l'uso dei cookies

(Provvedimento Garante privacy dell'8 maggio 2014)

Il nuovo regolamento privacy

Le principali novità introdotte dalla proposta di regolamento sono:

- Diritto all'oblio – Art. 17
- Diritto alla portabilità dei dati – Art. 18
- Privacy by design e privacy by default
- Valutazione di impatto sulla protezione dei dati – Art. 33
- Data breaches – Artt. 31 e 32
- Data privacy officer – Artt. 35 e ss
- Certificazione – Art. 39
- Sanzioni – Art. 79

La nuova INFORMATIVA sul trattamento dei dati personali:

- Dovrà essere indicato il fondamento legale del trattamento
- L'eventuale intenzione di trasferire dati all'estero
- La durata del trattamento

ESEMPIO DI VERBALE DI ISPEZIONE DEL 2013

Per maggiori informazioni:

Giuliano Da Valle
g.davalle@pcsystem.it

Grazie ed arrivederci