

ASSOCIAZIONE ARTIGIANI
DELLA PROVINCIA DI VICENZA



@ *Confartigianato*



SPECIALE

Il nuovo Codice della Privacy

Prima parte

**Schede riassuntive
del Decreto Legislativo n. 196 del 30 giugno 2003
(Suppl. Ord. n. 123 alla G.U. 27.07.2003, n. 174)**

IL NUOVO "CODICE DELLA PRIVACY": CHI COINVOLGE, COSA FARE, ENTRO QUANDO E PERCHÉ ADEGUARSI ALLE NORME

CHI COINVOLGE

I soggetti che devono adeguarsi rimangono, come previsto dalla precedente legge 675/96, tutti coloro che trattano dati personali, ad esempio:

- imprese individuali, società;
- società cooperative;
- professionisti;
- chiunque tratti dati personali di clienti, cittadini, dipendenti, fornitori, utenti, e così via.

COSA FARE

Chi esegue la raccolta e il trattamento dei dati, deve dare l'informativa al soggetto di cui si stanno raccogliendo le informazioni.

Ricevere da questi il consenso, che deve essere scritto, nel caso in cui si trattino dati sensibili.

Nominare eventuali figure di responsabilità interne per il trattamento e la custodia dei dati.

Attivare misure minime di sicurezza per la tutela e il trattamento dei dati per:

- impedire il trattamento non autorizzato e non consentito;
- impedire l'accesso non autorizzato;
- ridurre i rischi di perdita e/o distruzione;
- attuare, in caso di trattamento di dati sensibili il Documento Programmatico per la Sicurezza (DPS).

QUANDO ADEGUARSI

Il nuovo codice della privacy è entrato in vigore il **1° gennaio 2004**.

Le prime scadenze, valide esclusivamente per la prima fase di attivazione, sono:

- Per le società di capitale che utilizzano mezzi informatici per il trattamento di dati sensibili devono citare nella relazione accompagnatoria al bilancio l'avvenuta redazione o aggiornamento del DPS.
- **30 giugno 2004**: termine entro il quale adottare le nuove misure minime di sicurezza e per l'aggiornamento/redazione del DPS.
- **1° gennaio 2005**: su esplicita richiesta, da inoltrare al Garante sulla Privacy, da parte di quei soggetti che trattano dati e utilizzano **strumenti elettronici tecnicamente inadeguati**, può essere richiesto il differimento del termine del 30 giugno al 1° gennaio 2005 per adottare le **nuove** misure minime per la stesura del DPS.

PERCHÉ ADEGUARSI

Il testo unico sulla Privacy (che sostituisce la legge n. 675/96) innova la normativa precedente, in vigore oramai da diversi anni.

Va sottolineato che l'impianto della precedente norma non viene modificato.

Le novità sostanziali sono riconducibili soprattutto nell'applicazione delle misure minime di sicurezza, sia

nel caso in cui si utilizzino archivi cartacei o informatizzati.

Il mancato rispetto delle norme contenute nel testo unico fa scattare l'applicazione di sanzioni sia amministrative che penali che prevedono anche la reclusione.

DATI E SOGGETTI

Dati

- "**dato personale**": qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;
- "**dati identificativi**": i dati personali che permettono l'identificazione diretta dell'interessato;
- "**dati sensibili**": i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

Soggetti

- "**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.

QUALI SONO QUINDI I DATI PERSONALI?

- a) Il nome, il cognome, l'indirizzo, il numero di telefono, il codice fiscale, la Partita Iva, dati bancari...
- b) Informazioni circa la composizione del nucleo familiare, la professione esercitata da un determinato soggetto, sia fisico che giuridico, la sua formazione...

E QUELLI SENSIBILI?

- c) Fotografie, radiografie, video, suoni, impronte...
- d) Informazioni relative al profilo creditizio, alla retribuzione...
- e) Informazioni relative alla salute di un soggetto, alla vita sessuale, alla partecipazione ad associazioni di categoria, a partiti, trattenute sindacali, cartelle cliniche, rilevazioni di presenze...

CODICE DELLA PRIVACY

- **Indicazioni interpretative e applicative**
- **Collegamento tra adempimenti previsti dalla precedente legge n. 675/96 e il nuovo Codice**
- **Indicazioni sul Documento Programmatico sulla sicurezza**
- **Nuova Scadenza al 30 giugno 2004**

Con l'entrata in vigore del nuovo "Codice della Privacy" di cui al Decreto Legislativo n. 196/2003, si è riaperta una nuova fase operativa in ordine alla gestione degli adempimenti legati alla privacy.

Per agevolare le imprese nell'integrazione tra le norme della "vecchia" legge 675/96 e il nuovo ordinamento, si ritiene opportuno pubblicare un documento dedicato a ricostruire i principi applicativi cercando di correlare le vecchie prescrizioni con quelle introdotte dal nuovo codice e tentando di risolvere alcune ambiguità che possono costituire elementi di incertezza nell'orientamento dei comportamenti applicativi.

Va comunque segnalato che le nuove norme non sconvolgono profondamente l'assetto previgente, e in molti casi introducono semplificazioni considerevoli, mentre soltanto alcuni elementi costituiscono una vera novità in termini applicativi.

Di seguito, pertanto, si cercherà di ricapitolare i principi fondamentali mettendo in relazione ciò che rimane invariato e ciò che cambia.

A) Articolo 1 del Codice**Diritto alla protezione dei dati personali**

L'articolo 1 del Codice della Privacy codifica, con una definizione stringente, il diritto individuale alla protezione dei dati personali, affermando che "Chiunque ha diritto alla protezione dei dati che lo riguardano". Tale definizione semplifica il quadro di riferimento legato all'ambito di applicazione delle disposizioni normative, in quanto rende applicabili i principi di tutela in tutte le circostanze in cui chiunque, per qualsiasi fine, tratta dati personali di chiunque altro.

Il diritto garantito della protezione dei dati personali, obbliga i soggetti che li trattano, a garantirne la protezione.

Ai fini di cui sopra peraltro appare importante richiamare la disposizione di cui al comma 2 dell'articolo 2 che dispone che il trattamento dei dati personali è disciplinato assicurando un elevato livello di tutela dei diritti e delle libertà fondamentali dell'individuo nel rispetto dei principi di armonizzazione, semplificazione ed efficacia delle modalità previste per il loro esercizio da parte degli interessati, nonché l'adempimento degli obblighi da parte dei titolari del trattamento.

Si vuole richiamare queste norme introduttive a carattere generale, poiché uno dei presupposti del nuovo codice è che l'assenza di "complicazione procedurale" assume di per sé un valore di "tutela" per i soggetti di cui vengono trattati i dati personali.

B) Definizioni

In tema di definizioni generali non sono stati introdotti particolari cambiamenti. Le principali definizioni, individuate dall'articolo 4, sono:

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 modifica, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca dati.

TITOLARE DEL TRATTAMENTO

La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza. Nel caso in cui il trattamento è effettuato da una persona giuridica, da una pubblica amministrazione o da qualsiasi altro ente, associazione o organismo, il titolare del trattamento è l'entità nel suo complesso o l'unità od organismo periferico che esercita un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento, ivi compreso il profilo della sicurezza (articolo 28).

RESPONSABILE DEL TRATTAMENTO

La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali. Ricordiamo a tale proposito che il Responsabile è una figura che può essere individuata facoltativamente dal titolare e le modalità di assegnazione, nonché le caratteristiche della figura sono specificate dall'articolo 29.

INCARICATI

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

Tali soggetti devono essere individuati per iscritto (articolo 30) e sono gli unici a poter compiere operazioni di trattamento sui dati personali. Gli incaricati, inoltre, operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite.

Per quanto riguarda le definizioni dei dati oggetto di tutela, è rimasta invariata la distinzione fondamentale tra:

DATI PERSONALI

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

DATI SENSIBILI

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.

La distinzione resta di fondamentale importanza in ordine alla diversità di adempimenti che devono essere adottati dai titolari, anche ai fini della applicazione delle sanzioni previste.

C) Adempimenti

In relazione agli adempimenti da adottare i principi generali di riferimento restano sostanzialmente invariati, con l'adozione, in alcuni casi di seguito specificati, di semplificazione.

INFORMATIVA

Tutti i trattamenti, indipendentemente dalla tipologia dei dati, comportano, come per la legge n. 675/96, l'obbligo di informativa degli interessati.

L'obbligo di informativa (scritta o orale) riguarda:

- le finalità e le modalità del trattamento cui sono destinati i dati;
- la natura obbligatoria o facoltativa del conferimento dei dati;
- le conseguenze di un eventuale rifiuto di rispondere;
- i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi;
- i diritti di accesso di cui all'articolo 7 del codice;
- gli estremi identificativi del titolare e, se designati, del rappresentante nel territorio dello Stato e del responsabile.

Quando il titolare ha designato più responsabili è indicato almeno uno di essi, indicando il sito della rete di comunicazione o le modalità attraverso le quali è conoscibile in modo agevole l'elenco aggiornato dei responsabili.

Quando è stato designato un responsabile per il riscontro all'interessato in caso di esercizio dei diritti di cui all'articolo 7, è indicato tale responsabile.

L'adempimento dell'informativa di cui alla nuova norma del codice specifica anche la necessità di informare l'interessato circa i soggetti che possono venire a conoscenza dei dati, compresi gli incaricati.

Tale prescrizione aggrava notevolmente l'onere di informativa, soprattutto nel caso di trattamenti complessi. A tale proposito, peraltro, il Garante ha chiarito che, comunque, tale obbligo non riguarda i trattamenti già in corso al momento di entrata in vigore del codice, come invece poteva apparire dalla interpretazione strettamente letterale della nuove norme; ciò deve intendersi pertanto nel senso di escludere qualsiasi obbligo di integrazione per i trattamenti già in essere e per i quali l'informativa è stata già resa agli interessati sulla base delle prescrizioni della legge n. 675/96.

CONSENSO

Anche con riferimento all'obbligo di ottenere il consenso al trattamento, il nuovo codice riconferma quanto previsto dalla legge n. 675/96.

In particolare il trattamento dei dati è consentito solo con il consenso espresso dell'interessato.

Il consenso deve essere manifestato in forma scritta (mediante sottoscrizione dell'interessato) unicamente per i trattamenti di dati sensibili, mentre in tutti gli altri casi è sufficiente che il consenso espresso sia documentato per iscritto. Ciò significa che per i trattamenti di semplici dati personali è necessario unicamente che sia tenuta traccia documentale del rilascio da parte dell'interessato, secondo le modalità specifiche che la tipologia di trattamento richiede (ad esempio, nel caso di dati acquisiti mediante utilizzazione del telefono, la traccia documentale consiste nella avvenuta annotazione scritta della avvenuta manifestazione del consenso da parte dell'interessato, senza necessità di sua sottoscrizione).

NOTIFICA

L'adempimento della notifica (ovvero dell'atto con cui l'impresa, il professionista o la pubblica amministrazione segnalano al Garante i trattamenti di dati che si intendono effettuare) è l'elemento oggetto di maggiori interventi di semplificazione introdotti dal codice. L'originale impianto della legge 675/1996 (e le successive modificazioni), prevedeva che dovesse notificare i trattamenti tutti i soggetti non esplicitamente esentati.

Nel testo unico si rovescia l'impostazione e si indicano solo i pochi casi nei quali la notifica va effettuata. La notifica deve essere effettuata solo in particolari casi di trattamento di:

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

solvibilità economica, alla situazione patrimoniale, al corretto adempimento di obbligazioni, a comportamenti illeciti o fraudolenti.

Secondo tale prescrizione, pertanto, si ritengono escluse dall'obbligo di notificazione le imprese, ancorché trattino dati sensibili diversi da quelli indicati nelle lettere precedenti.

Nei casi di trattamenti che rientrano nelle lettere precedenti, invece, la notifica deve essere effettuata, anche se già effettuata in vigore della legge n. 675/96, entro il 30 aprile 04 (art. 181, comma 1, lettera c).

AUTORIZZAZIONE AL TRATTAMENTO DI DATI SENSIBILI

Il trattamento dei dati sensibili, oltre alla acquisizione del consenso dell'interessato, necessita, come nel passato, dell'autorizzazione del Garante.

Le autorizzazioni, come è noto, possono essere:

- a) **Generali**, relative cioè a determinate categorie di titolari e/o trattamenti. In tal caso il titolare del trattamento rientrante nell'ambito di applicazione di un'autorizzazione generale non deve presentare alcuna richiesta al Garante se il trattamento che intende effettuare è conforme alle prescrizioni impartite mediante detti provvedimenti generali. Le autorizzazioni generali relative ai dati sensibili e giudiziari già emanate dal Garante per la protezione dei dati personali continuano ad essere valide a seguito della proroga emanata con provvedimento in data 30 giugno 2003 sino al 30.06.04.
- b) **Su richiesta**: nei casi in cui i trattamenti di dati sensibili non rientrino nell'ambito delle autorizzazioni generali.

D) Misure di sicurezza

Il tema delle misure di sicurezza dei trattamenti è quello che ha subito le maggiori rivisitazioni a seguito della emanazione del codice della privacy.

Il principio generale, tuttavia, riconferma quanto già disposto dalla legge n. 675/96 e in particolare che i dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta. A tale proposito il codice individua misure specifiche, la cui osservanza da parte dei titolari è necessaria per adeguare i trattamenti ad un livello minimo di sicurezza, tenendo conto del fatto che comunque la valutazione del rischio di distruzione, perdita o accesso non autorizzato dovrà comunque essere effettuata discrezionalmente dal titolare, in relazione alla tipologia dei dati trattati, in modo coerente alle esigenze di tutela specifiche richieste dai trattamenti svolti (introducendo, eventualmente, misure adeguate più stringenti rispetto a quelle indicate delle norme). Il codice mantiene la distinzione fra trattamenti effettuati con e senza l'ausilio di strumenti elettronici, secondo quanto già previsto dalla legge n. 675/96 e in

particolare:

TRATTAMENTO SENZA L'AUSILIO DI STRUMENTI INFORMATICI

Le misure minime sono individuate dall'articolo 35, e riguardano:

- a) l'aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative;
- b) la previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;
- c) la previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati.

Le modalità tecniche per corrispondere a tali prescrizioni consistono in:

- a) istruzioni scritte agli incaricati finalizzate al controllo e 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;
- b) custodia e controllo di atti e i documenti contenenti dati personali sensibili o giudiziari affidata agli incaricati del trattamento per lo svolgimento dei relativi compiti, in maniera che ad essi non accedano persone prive di autorizzazione, per il tempo necessario al trattamento e fino alla restituzione al termine delle operazioni affidate;
- c) controllo degli accessi agli archivi contenenti dati sensibili o giudiziari. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, devono essere identificate e registrate;
- d) quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono devono essere preventivamente autorizzate.

TRATTAMENTO CON L'AUSILIO DI STRUMENTI INFORMATICI

Le misure minime riguardano:

- a) autenticazione informatica;
- b) adozione di procedure di gestione delle credenziali di autenticazione;
- c) utilizzazione di un sistema di autorizzazione;
- d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
- e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
- f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
- g) tenuta di un aggiornato documento programmatico sulla sicurezza;
- h) adozione di tecniche di cifratura o di codici identi-

ficativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.

Le modalità tecniche per corrispondere a tali prescrizioni sono contenute nel disciplinare tecnico, allegato B del Decreto Legislativo 196 del 30/6/2003.

Queste comunque saranno oggetto di una scheda sintetica che verrà pubblicata nei prossimi *Speciali* sulla *Privacy* allegati a InformaImpresa.

IL DOCUMENTO PROGRAMMATICO SULLA SICUREZZA (DPS)

Anche la redazione del DPS è una "misura minima". Si tratta di una misura non nuova, sebbene sia aumentato il numero dei soggetti che lo deve redigere e sia parzialmente diverso il suo contenuto.

Infatti, la precedente disciplina (la legge 675/96) prevedeva già l'obbligo di predisporre e aggiornare il DPS, almeno annualmente, in caso di trattamento di **dati sensibili** o relativi a determinati provvedimenti giudiziari effettuato mediante elaboratori accessibili mediante una rete di telecomunicazioni disponibili al pubblico. I soggetti tenuti a predisporre il DPS hanno potuto redigerlo per la prima volta entro il 29 marzo 2000 o, al più tardi, entro il 31 dicembre 2000; dovendo rispettare l'obbligo di revisione almeno annuale, hanno dovuto aggiornare il DPS negli anni successivi, anche nel 2003.

In base al nuovo Codice, la misura minima del DPS deve essere ora adottata dal titolare di un trattamento di dati sensibili o giudiziari effettuato con strumenti elettronici.

Come accennato, il DPS deve essere redatto da alcuni soggetti che non vi erano precedentemente tenuti (ad esempio, da chi trattava dati sensibili o giudiziari, ma con elaboratori non accessibili mediante una rete di telecomunicazioni disponibili al pubblico).

Infine, il contenuto stesso del DPS è arricchito da nuovi elementi che si aggiungono a quelli necessari in base alla precedente disciplina o ne specificano alcuni aspetti. Ad esempio, nel DPS occorre descrivere ora i criteri e le modalità per ripristinare la disponibilità dei dati in caso di distruzione o danneggiamento delle informazioni o degli strumenti elettronici. Benché non si tratti a rigore di una misura "nuova", è quindi legittimamente sostenibile che il DPS da redigere quest'anno per la prima volta, o da aggiornare, possa essere predisposto al più tardi entro il 30 giugno 2004, anziché necessariamente entro il 31 marzo, data che è invece prevista a regime per i prossimi anni, a partire dal 2005.

Si perviene a questa conclusione per tutti i destinatari dell'obbligo:

- a) sia per coloro che devono redigere il DPS per la prima volta nel 2004;
- b) sia per chi, già dotato di un DPS redatto o aggiornato nel 2003, ritenga necessario utilizzare un trimestre in più, rispetto al prossimo 31 marzo, per curare la stesura di un testo significativo e più impegnativo nella ricognizione dei rischi e degli interventi previsti.

RELAZIONE ACCOMPAGNATORIA AL BILANCIO D'ESERCIZIO

Il Codice della Privacy, ha introdotto una nuova regola per rendere meglio informati gli organi di vertice del titolare del trattamento e responsabilizzarli in materia di sicurezza, attraverso l'obbligo di riferire nella relazione di accompagnamento a ciascun bilancio di esercizio circa l'avvenuta redazione o aggiornamento del DPS che sia obbligatorio come misura "minima" o che sia stato comunque adottato.

Anche questo richiamo rappresenta una misura "minima" nuova, indicata tra quelle di "tutela e garanzia".

I soggetti tenuti in passato a predisporre o aggiornare il DPS, e che per il 2004 possono aggiornarlo entro il 30 giugno del presente anno, dovranno riferire già a partire dalla relazione sul bilancio di esercizio per il 2003, con riferimento al DPS già eventualmente aggiornato per il 2004, oppure menzionando l'adozione o aggiornamento avvenuto nel 2003 e indicando sinteticamente che si aggiornerà il DPS entro il 30 giugno 2004.

Le imprese tenute invece per la prima volta a redigere il DPS nel 2004 (entro il 30 giugno), non devono indicare nella relazione alcunché se il DPS 2003 o il DPS 2004 non sono stati adottati. Queste, qualora alla data in cui predispongono la predetta relazione abbiano redatto già il DPS 2004, indicheranno invece tale circostanza; potranno infine indicare facoltativamente quanto eventualmente già fatto nel 2003 e, sempre facoltativamente, l'aggiornamento 2004 in itinere.

INDICAZIONI RELATIVE A PARTICOLARI CATEGORIE DI TRATTAMENTO

TRATTAMENTI DI DATI PERSONALI EFFETTUATI DALLE IMPRESE PER ESIGENZE DI GESTIONE AMMINISTRATIVA E CONTABILE

- a) In materia di informativa e consenso non appare necessario procedere ad ulteriori adempimenti. Ricordiamo che l'informativa deve essere sempre resa e che è opportuno procedere alla raccolta del consenso degli interessati, anche soltanto documentato per iscritto;
- b) non deve essere effettuata la notifica;
- c) devono essere impartite istruzioni scritte agli incaricati;
- d) non deve essere redatto il documento programmatico per la sicurezza. E' tuttavia opportuno consigliare la redazione del Documento per la Sicurezza se vengono trattati dati sensibili, nel caso di trattamenti informatizzati.

TRATTAMENTI DI DATI PERSONALI EFFETTUATI DALLE IMPRESE CHE TRATTANO ANCHE DATI SENSIBILI

- a) In materia di informativa e consenso non appare necessario procedere ad ulteriori adempimenti. Ricordiamo che l'informativa deve essere sempre resa e che è opportuno procedere alla raccolta del consenso sottoscritto degli interessati;
- b) non deve essere effettuata la notifica;
- c) devono essere impartite istruzioni scritte agli in-

- caricati;
- d) non devono essere richieste autorizzazioni al Garante per il trattamento di dati sensibili in quanto vale l'autorizzazione generale;
- e) deve essere redatto il documento programmatico per la sicurezza.

LA TUTELA IN MATERIA DI PRIVACY

Codice in materia di protezione dei dati personali

LE NOVITA'

Principali novità del Codice Privacy rispetto alla precedente normativa:

Dichiarazione di principio

"*Chiunque ha diritto alla protezione dei dati personali che lo riguardano*" (art. 1)

La tutela riguarda singoli individui, imprese, enti e associazioni.

Nuove misure minime di sicurezza per il trattamento dei dati (art. 33).

Obbligo generalizzato di tenere un **documento programmatico sulla sicurezza** per il trattamento di dati personali con strumenti elettronici (art. 34).

Venir meno dell'obbligo generalizzato di **notifica**.

DEFINIZIONI (Art. 4)

Banca dati:

il complesso organizzato di dati personali su supporto cartaceo (in *armadi*) ovvero elettronico (su *server*, *memorie di PC*, *floppy*, *C.D. rom*).

Dato personale:

qualunque informazione relativa a persone fisiche, giuridiche, enti, associazioni o imprese che ne consentano l'identificazione diretta o indiretta (*dati di dipendenti, fornitori, clienti, soci o colleghi quali: nome, cognome, ragione sociale, telefono, fax, codice fiscale, Partita Iva, immagini, foto, dati bancari ecc.*).

Dato sensibile:

dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose o filosofiche, l'*adesione* a partiti, sindacati o *associazioni*, ovvero idonei a rivelare lo stato di salute e la vita sessuale.

REGOLE PER IL TRATTAMENTO

Informativa (Art. 13)

Contenuto obbligatorio:

- finalità del trattamento;
- natura obbligatoria o meno del consenso;
- conseguenze del rifiuto;
- diritti di accesso dell'interessato;
- estremi identificativi del titolare e del responsabile (se designato);
- indicazione di chi può venire a conoscenza dei dati (compresi gli incaricati).

Temporalità:

deve essere *rilasciata prima del trattamento*.

Forma:

orale o *scritta* (in tal caso si preconstituisce la prova dell'avvenuto adempimento).

Consenso (Artt. 23 ss.)

Il consenso dell'interessato:

- può riguardare l'intero trattamento o una o più operazioni dello stesso;
- deve essere espresso liberamente e per un trattamento individuato;
- deve essere informato;
- può essere revocato in ogni momento.

Temporalità:

il consenso espresso è necessario prima del trattamento, ai fini della sua legittimità.

Forma:

Il consenso deve essere "positivo", ossia non reso in forma implicita o in negativo.

Trattamento di *dati sensibili*: **consenso scritto**.

Trattamento di *dati comuni*: **consenso espresso** ma documentato per iscritto.

Misure minime di sicurezza (Artt. 33-35)

Complesso di misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto dalla legge.

Sono quelle misure volte a **ridurre al minimo, con idonee e preventive misure di sicurezza, i rischi** di:

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

Le misure variano a seconda delle modalità di trattamento, distinguendo tra:

- trattamenti **senza** strumenti elettronici;
- trattamenti **con** strumenti elettronici.

adeguamento:

entro il **30 giugno 2004** per le **misure minime nuove** rispetto al D.P.R. 318/99, termine prorogato al **1 gennaio 2005**, per **obiettive difficoltà tecniche**, con motivazione scritta del titolare, avente *data certa* e *conservata presso la propria sede*.

Con strumenti elettronici (Artt. 34)

Ai fini di un **trattamento lecito** le misure da adottare sono le seguenti:

- disporre di un **sistema di autenticazione degli utenti** (nel D.P.R. 318/99 si parlava solo di password, e non erano ritenute valide funzioni di autenticazione più forti, ad esempio la firma digitale o le impronte digitali);
- adottare appropriate e periodiche **procedure** per mantenere aggiornate le utenze e i relativi profili di accesso;
- definire un **sistema di autorizzazione** per abilitare gli utenti all'accesso ai dati e/o ai trattamenti;
- **proteggere strumenti elettronici e dati da accessi non autorizzati** da parte di utenti, programmi informatici e da trattamenti illeciti;
- adottare **procedure di backup, di recupero e di ripristino** della disponibilità dei sistemi e dei dati;

Venerdì 9 aprile 2004

- adottare un **documento programmatico sulla sicurezza**, in caso di trattamento di dati sensibili (ossia un resoconto delle misure di sicurezza adottate dal titolare del trattamento per ridurre al minimo ogni evento dannoso o pericoloso a carico dei dati personali trattati).

Senza strumenti elettronici (Artt. 35)

Ai fini di un **trattamento lecito** le misure da adottare sono le seguenti:

- **istruzioni scritte agli incaricati**, con la loro lista e i compiti loro assegnati sempre aggiornati;
- **definizione di opportune procedure per la custodia e il controllo dei documenti** con dati sensibili o giudiziari affidati agli incaricati;
- **controllo per l'accesso agli archivi** contenenti dati sensibili o giudiziari (con identificazione e registrazione delle persone ammesse, a qualunque titolo, dopo l'orario di chiusura);
- **preventiva autorizzazione delle persone che accedono agli archivi** quando questi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza.

Sanzioni amministrative (artt. 161 - 164)

Omessa o inadeguata informativa all'interessato:

- pagamento di una somma da 3.000 a 18.000 euro
- *se si di trattano dati sensibili o giudiziari o di maggiore pregiudizio per uno o più interessati:* da 5.000 a 30.000 euro; somma aumentabile sino al triplo quando risulti inefficace in ragione delle condizioni economiche del contravventore;

cessione dei dati in violazione del Codice o di altre disposizioni di tutela dei dati personali:

- pagamento di una somma da 5.000 a 30.000 euro

omessa o incompleta notificazione:

- pagamento di una somma da 10.000 a 60.000 euro oltre alla pubblicazione dell'ordinanza - ingiunzione, per intero o per estratto, in uno o più giornali;
- omessa informazione o esibizione di documenti al Garante:*
- pagamento di una somma da 4.000 a 24.000 euro.

Sanzioni penali (artt. 167 - 172)

Trattamento illecito di dati:

- *se da esso deriva documento*, salvo che il fatto non costituisca reato più grave: reclusione da 6 a 18 mesi;
- *se il fatto consiste nella comunicazione/diffusione:* con la reclusione da 6 a 24 mesi.

Falsità nelle dichiarazioni o notificazioni al Garante:

- salvo che il fatto non costituisca reato più grave, reclusione da 6 mesi a 3 anni.

Omessa adozione delle misure minime di sicurezza prescritte:

- arresto sino a 2 anni ovvero ammenda da 10.000 a 50.000 euro.

Inosservanza dei provvedimenti del Garante:

- sanzione della reclusione da 3 mesi a 2 anni.

Guardia di Finanza e Garante Privacy hanno siglato un accordo per regolare le reciproche forme di intesa al fine di una più intensa ed efficace attività di controllo sulla raccolta dei dati.

Fac-simile da utilizzare per l'informativa e per la raccolta del consenso. Si consiglia di compilarlo in almeno due copie, di cui una, controfirmata dal possessore dei dati nella parte relativa alla raccolta del consenso, va archiviata.

Egregio Signore/Gentile Signora

Oggetto: **informativa e raccolta del consenso**

Il sottoscritto titolare del trattamento

(*indicare la ragione sociale dell'impresa*), provvede all'informativa prevista dall'art. 13 del D.Lgs. n. 196/2003 (finalità e modalità del trattamento in materia di dati personali), garantendo, nel contempo, la sicurezza e la riservatezza dei dati, anche qualora il trattamento avvenga attraverso canali telematici o innovativi.

All'impresa può altresì rivolgersi per ottenere chiarimenti e informazioni circa le finalità e le modalità del trattamento cui sono destinati i dati e, in particolare, per ottenere la conferma circa l'esistenza o meno del trattamento, indicazioni circa l'origine, le finalità e le modalità del trattamento stesso.

Lei ha inoltre diritto di chiedere la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, nonché l'aggiornamento, la rettificazione o, se vi è interesse, l'integrazione dei dati; può altresì opporsi al trattamento a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

Ogni richiesta di informazioni in materia di protezione dei dati personali può essere rivolta:

presso la sede in:

tramite mail all'indirizzo e-mail:

per via telefonica al numero verde:

(*elencare una o più di tali opzioni*)

Formula di acquisizione del consenso

Il sottoscritto

titolare/legale rappresentante dell'impresa

(*indicare solo il nome e cognome se persona fisica*), acquisita l'informativa di cui all'art. 13 del decreto legislativo 196/2003 (finalità e modalità del trattamento), presta il proprio consenso al trattamento dei dati personali e sensibili, anche per la loro comunicazione e diffusione, ai sensi della vigente normativa in materia di protezione dei dati personali.

Data

Firma leggibile