GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

DELIBERAZIONE 24 maggio 2007.

Guida pratica e misure di semplificazione per le piccole e medie imprese. (Deliberazione n. 21).

IL GARANTE PER LA PROTEZIONE
DEI DATI PERSONALI

Nella riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vice presidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti, e del dott. Giovanni Buttarelli, segretario generale;

Visto il decreto legislativo 30 giugno 2003, n. 196 (codice in materia di protezione dei dati personali) con particolare riferimento all'art. 154, comma 1, lettera *h)*;

Esaminate le istanze provenienti da associazioni di categoria, con particolare riferimento alle piccole e medie imprese, ivi compresi gli artigiani, in materia di adempimenti derivanti dalla disciplina di protezione dei dati personali;

Ritenuta l'opportunità di indicare, a tal proposito, linee di comportamento conformi al codice e misure di semplificazione da questo previste in grado di fornire orientamenti utili per gli operatori economici nel rispetto dei diritti degli interessati;

Rilevata l'esigenza che tale quadro sia riassunto in una guida pratica, suscettibile di aggiornamento periodico e di cui verrà curata la più ampia pubblicità anche attraverso il sito Internet dell'Autorità (http://www.garanteprivacy.it);

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

Relatore il dott. Giuseppe Fortunato;

Delibera:

1. Ai sensi dell'art. 154, comma 1, lettera *h)*, del codice, di adottare il documento «Guida pratica e misure di semplificazione per le piccole e medie imprese», allegato quale parte integrante della presente deliberazione (allegato 1).

2. Ai sensi dell'art. 143, comma 2, del codice, di trasmettere copia del presente provvedimento al Ministero della giustizia - Ufficio pubblicazione leggi e decreti, unitamente alle menzionata «Guida pratica», per la pubblicazione nella *Gazzetta Ufficiale* della Repubblica italiana.

Roma, 24 maggio 2007

Il presidente
PIZZETTI

Il relatore
FORTUNATO

Il segretario generale
BUTTARELLI

ALLEGATO 1

Guida pratica e misure di semplificazione per le piccole e medie imprese

Con la disciplina contenuta nel decreto legislativo n. 196 del 2003 (*Codice in materia di protezione dei dati personali*) l'ordinamento italiano si è dotato di un quadro organico per attuare obblighi internazionali nascenti dalla Convenzione del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale (Strasburgo, 28 gennaio 1981) e per recepire direttive comunitarie (95/46/Ce e 2002/58/Ce).

Specie nello svolgimento delle ordinarie attività d'impresa, e in particolare per le realtà produttive di piccole dimensioni, alcuni adempimenti contenuti nella disciplina di protezione dei dati personali vengono reputati talvolta onerosi. Una giusta protezione dei dati personali e della riservatezza può in verità rappresentare una risorsa per l'impresa, rendendone più efficiente l'attività in modo da incrementare la fiducia di consumatori e utenti.

Questa guida intende fornire a chi opera nella realtà delle medie e piccole imprese uno strumento utile per curare gli adempimenti derivanti dalla normativa vigente, indicando le soluzioni semplificate a disposizione.

La guida, integrata da una *check list* e pubblicata sul sito *web* dell'Autorità, potrà subire aggiornamenti nel tempo [1].

(1) La guida ha mero valore indicativo ed esemplificativo rispetto al contenuto delle disposizioni normative, alla cui osservanza chiunque resta vincolato.

1. I SOGGETTI CHE EFFETTUANO IL TRATTAMENTO

Nello svolgimento dell'attività di impresa è normale che vengano trattati dati personali, vale a dire informazioni riferibili a soggetti identificati o identificabili (ad esempio, dipendenti [2], clienti e fornitori). I dati devono essere pertinenti e non eccedenti rispetto a finalità legittime, esatti e aggiornati (art. 11 del Codice). Le operazioni di trattamento (quali la raccolta, comunicazione o diffusione di dati personali) sono effettuate anche a cura del responsabile (se designato) e degli incaricati del trattamento.

1.1. *Chi è il titolare del trattamento?*

Il "titolare del trattamento", è la "[...] entità che esercita un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento, ivi compreso il profilo della sicurezza" (art. 28 del Codice). In particolare, nell'ambito dello svolgimento dell'attività economica, "titolare del trattamento" può essere la persona fisica (si pensi all'imprenditore individuale) o giuridica (ad esempio, la società) che tratta i dati (con la raccolta, la registrazione, la comunicazione o la diffusione).
Il "titolare del trattamento" è chiamato ad attuare gli obblighi in materia (riassunti nella presente *Guida*) e, se ritiene di designare uno o più responsabili del trattamento, è tenuto a vigilare sulla puntuale osservanza delle istruzioni da impartire loro.

1.2. *Chi sono i responsabili del trattamento?*

Il "responsabile del trattamento" (possono essere più d'uno), è una figura che può essere designata a propria discrezione dal titolare del trattamento con un atto scritto nel quale vanno indicati i compiti affidati. Occorre scegliere persone fisiche od organismi che per esperienza, capacità ed affidabilità, forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza (art. 29 del Codice).
Tale figura, la cui designazione da parte del "titolare del trattamento" è quindi facoltativa, ricorre frequentemente in presenza di articolazioni interne delle realtà produttive dotate di una certa autonomia (ad es., possono essere designati responsabili del trattamento i dirigenti di funzioni aziendali, quali quelle del

[2] In relazione al trattamento dei dati personali dei dipendenti si vedano altresì le "*Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati*", doc. *web* n. 1364099.

personale o del settore *marketing*) o, rispetto a soggetti esterni all'impresa, per svariate forme di *outsourcing* che comportino un trattamento di dati personali (ad es., per i centri di elaborazione dati contabili, per i servizi di postalizzazione, per le società di recupero crediti [3], etc.)

1.3. *Chi sono gli incaricati del trattamento?*

Gli "incaricati del trattamento" sono soggetti (solo persone fisiche) che effettuano materialmente le operazioni di trattamento dei dati personali e operano sotto la diretta autorità del titolare (o del responsabile) attenendosi a istruzioni scritte (art. 30 del Codice). Il "titolare del trattamento" è tenuto a designarli.
È sufficiente assegnare un dipendente ad una unità organizzativa, a condizione che risultino per iscritto le categorie di dati cui può avere accesso e gli ambiti del trattamento [4].

[3] In materia v. il provvedimento generale del 30 novembre 2005, doc. *web* n. 1213644.

[4] Così, in un'azienda nella quale ad una unità organizzativa sono stati assegnati un determinato numero di dipendenti, si potrà ovviare ad una formale designazione (ad esempio, mediante consegna di apposita comunicazione scritta), qualora si individuino gli ambiti di competenza (in ordine ai trattamenti di dati consentiti) di quella unità mediante una previsione scritta (ad es. nell'organigramma, nel contratto, nei mansionari, ecc.) e risulti inoltre che tali dipendenti sono stati assegnati stabilmente a tale unità.

2. LA NOTIFICAZIONE DEL TRATTAMENTO

La notificazione è una dichiarazione con la quale il titolare del trattamento, prima di iniziarlo, rende nota al Garante (che la inserisce nel registro pubblico dei trattamenti consultabile da chiunque sul sito *web* dell'Autorità) l'esistenza di un'attività di raccolta e di utilizzazione dei dati personali.

2.1. *È sempre necessario notificare il trattamento dei dati al Garante?*

In linea di principio i trattamenti ordinari svolti presso piccole realtà produttive non vanno notificati: si pensi ai trattamenti di dati relativi ai dipendenti, ai fornitori o alla clientela (5). In particolare, non devono essere notificati i dati relativi agli inadempimenti dei propri clienti tenuti da ciascuna impresa.
In questo quadro la notificazione deve essere effettuata in ipotesi particolari (indicate all'art. 37 del Codice). Con specifico riguardo all'attività di impresa, i trattamenti soggetti a notificazione sono quelli relativi a:

- 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; come detto, non rientrano in quest'ambito, i dati relativi agli inadempimenti dei propri clienti tenuti da ciascuna impresa.
- dati genetici [6], biometrici o dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica (ad esempio, dati trattati mediante sistemi di geolocalizzazione installati su veicoli al fine di individuarne la posizione);
- 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 (c.d. profilazione), ovvero a monitorare l'utilizzo di servizi di comunicazione elettronica con esclusione dei trattamenti tecnicamente indispensabili per fornire i servizi medesimi agli utenti;

---

5 Specifiche indicazioni sono contenute anche nel provvedimento del Garante del 31 marzo 2004 *Provvedimento relativo ai casi da sottrarre all'obbligo di notificazione*, in *G.U.* del 6 aprile 2004, n. 81 e in http://www.garanteprivacy.it, doc. *web* 852561. V. pure, *Chiarimenti sui trattamenti da notificare al Garante*, 23 aprile 2004, doc. *web*. n. 993385.

6 V. in materia Provv. 22 febbraio 2007, doc. *web* n. 1389918.

- dati sensibili registrati in banche di dati a fini di selezione del personale per conto terzi (non, quindi, quelli trattati direttamente dall'imprenditore), nonché dati sensibili utilizzati per sondaggi di opinione, ricerche di mercato e altre ricerche campionarie.

2.2. *Come si effettua la notificazione al Garante?*

Solo utilizzando l'interfaccia disponibile sul sito *web* dell'Autorità e seguendo le istruzioni ivi indicate (v. art. 38 del Codice).

2.3. *Quando occorre fare una nuova notificazione?*

Solo in caso di cessazione del trattamento o di mutamento di alcuni elementi dell'originaria notificazione.

3. L'INFORMATIVA

Chi effettua operazioni di trattamento di dati personali deve rappresentare agli interessati le caratteristiche essenziali dei trattamenti effettuati. L'informativa deve essere resa per i dati raccolti presso l'interessato e per quelli reperiti presso terzi. La disciplina prevede alcune ipotesi di semplificazione e di esonero.

3.1. Cosa è l'informativa?

L'informativa, da rendersi con chiarezza e senza inutili formalità, anche in modo sintetico e colloquiale, contiene i seguenti elementi (art. 13 del Codice):

- finalità e modalità del trattamento;
- natura obbligatoria o facoltativa del conferimento dei dati e conseguenze di un eventuale rifiuto di rispondere;
- soggetti o categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza;
- diritti riconosciuti all'interessato dall'articolo 7 del Codice;
- estremi identificativi del titolare e, se designato, del responsabile del trattamento.

Se taluno di questi elementi è già noto all'interessato, non è necessario farlo presente nuovamente.

3.2. *Quando deve essere resa l'informativa?*

In caso di dati raccolti presso l'interessato, l'informativa deve essere resa, anche in forma orale, prima delle operazioni del trattamento. Nel rapporto con fornitori, clienti, dipendenti e collaboratori non è necessario ripeterla in occasione di ogni contatto: è sufficiente fornirla con una formula generale *una tantum*, all'inizio delle operazioni di trattamento (che potranno anche protrarsi nel tempo).

L'informativa deve essere resa anche nel caso in cui i dati personali sono raccolti presso terzi; in tal caso, deve essere fornita al momento della registrazione dei dati o, se è prevista la comunicazione a terzi da parte del titolare, non oltre la prima comunicazione. Vanno indicate anche le categorie dei dati trattati.

3.3. *È possibile rendere l'informativa in una forma semplificata?*

È possibile fornire l'informativa anche oralmente, in modo sintetico e colloquiale, senza includere elementi già noti all'interessato (art. 13,

comma 2, del Codice). Si può utilizzare anche uno spazio all'interno dell'ordinario materiale cartaceo e della corrispondenza.

Inoltre la disciplina prevede margini ulteriori di semplificazione (art. 13, comma 3, del Codice), tenendo conto delle circostanze concrete da rappresentare al Garante, formulando apposita istanza, anche tramite associazioni di categoria.

3.4. *In quali casi non è necessario rendere l'informativa agli interessati?*

In relazione ai dati raccolti presso terzi, tenuto conto delle circostanze concrete, si può omettere di fornire l'informativa se i dati sono trattati (art. 13, comma 5, lett. *c*), del Codice):

- in base ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria;
- ai fini dello svolgimento delle investigazioni difensive (legge 7 dicembre 2000, n. 397) o per far valere o difendere un diritto in sede giudiziaria.

Inoltre, è prevista la possibilità di esonero totale o parziale dall'obbligo di fornire l'informativa:

- nei casi in cui renderla, a giudizio del Garante –cui può essere inviata apposita istanza–, risulti impossibile o manifestamente sproporzionato rispetto al diritto fatto valere.

4. IL CONSENSO DELL'INTERESSATO

Talora il soggetto privato che effettua operazioni di trattamento è tenuto a raccogliere il consenso dell'interessato per effettuare un trattamento di dati lecito (art. 23 del Codice). Più spesso, però, nello svolgimento dell'ordinaria attività d'impresa, il consenso dell'interessato non è necessario (art. 24 del Codice).

4.1. *Nello svolgimento dell'attività d'impresa è necessario acquisire il consenso degli interessati?*

Con particolare riferimento ai trattamenti di dati personali (non sensibili) nell'ordinaria attività d'impresa, non è necessario il consenso nei casi in cui (cfr. art. 24 del Codice):

- i dati vengono trattati nell'esecuzione di un contratto o in fase pre-contrattuale (art. 24, comma 1, lett. *b*), del Codice);
- il trattamento viene posto in essere per dare esecuzione a un obbligo legale (art. 24, comma 1, lett. *a*) del Codice);
- i dati provengono da registri ed elenchi pubblici (art. 24, comma 1, lett. *c*), del Codice);
- i dati sono relativi allo svolgimento di attività economiche da parte dell'interessato (art. 24, comma 1, lett. *d*), del Codice).

A queste macro-categorie, che comprendono larga parte dei trattamenti effettuati ordinariamente da un'impresa, devono essere aggiunte le ulteriori ipotesi di esonero enumerate all'art. 24 del Codice[7].

[7] Art. 24. *Casi nei quali può essere effettuato il trattamento senza consenso.*

1. Il consenso non è richiesto, oltre che nei casi previsti nella Parte II, quando il trattamento:

a) è necessario per adempiere ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria;

b) è necessario per eseguire obblighi derivanti da un contratto del quale è parte l'interessato o per adempiere, prima della conclusione del contratto, a specifiche richieste dell'interessato;

c) riguarda dati provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque, fermi restando i limiti e le modalità che le leggi, i regolamenti o la normativa comunitaria stabiliscono per la conoscibilità e pubblicità dei dati;

d) riguarda dati relativi allo svolgimento di attività economiche, trattati nel rispetto della vigente normativa in materia di segreto aziendale e industriale;

e) è necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo. Se la medesima finalità riguarda l'interessato e quest'ultimo non può prestare il proprio consenso per impossibilità fisica, per incapacità di agire o per incapacità di intendere o di volere, il consenso è manifestato da chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato. Si applica la disposizione di cui all'articolo 82, comma 2;

Nei casi restanti, l'interessato deve aver manifestato un consenso libero, specifico e informato in relazione al trattamento effettuato. Il consenso deve essere documentato per iscritto (art. 23 del Codice).

4.2. *Quali sono gli adempimenti da osservare per trattare dati sensibili?*

Cautele maggiori devono essere osservate nel trattamento dei dati sensibili: tali sono considerate le informazioni idonee 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 dei dati personali idonei a rivelare lo stato di salute e la vita sessuale (art. 4, comma 1, lett. *d*), del Codice).
Per il trattamento dei dati sensibili di regola è necessario il consenso scritto, oltre l'autorizzazione del Garante.

Il Garante ha rilasciato sette autorizzazioni generali che comprendono tutti i trattamenti abitualmente effettuati nell'ordinaria attività di impresa. Non vi è quindi bisogno di rivolgere una richiesta al Garante, che va presentata solo per casi del tutto eccezionali non contemplati dalle medesime autorizzazioni già rilasciate (questa ipotesi si è sinora verificata in casi rari) [8].

---

f) con esclusione della diffusione, è necessario ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento, nel rispetto della vigente normativa in materia di segreto aziendale e industriale;

g) con esclusione della diffusione, è necessario, nei casi individuati dal Garante sulla base dei princìpi sanciti dalla legge, per perseguire un legittimo interesse del titolare o di un terzo destinatario dei dati, anche in riferimento all'attività di gruppi bancari e di società controllate o collegate, qualora non prevalgano i diritti e le libertà fondamentali, la dignità o un legittimo interesse dell'interessato;

h) con esclusione della comunicazione all'esterno e della diffusione, è effettuato da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, in riferimento a soggetti che hanno con essi contatti regolari o ad aderenti, per il perseguimento di scopi determinati e legittimi individuati dall'atto costitutivo, dallo statuto o dal contratto collettivo, e con modalità di utilizzo previste espressamente con determinazione resa nota agli interessati all'atto dell'informativa ai sensi dell'articolo 13;

i) è necessario, in conformità ai rispettivi codici di deontologia di cui all'allegato *A*), per esclusivi scopi scientifici o statistici, ovvero per esclusivi scopi storici presso archivi privati dichiarati di notevole interesse storico ai sensi dell'articolo 6, comma 2, del decreto legislativo 29 ottobre 1999, n. 490, di approvazione del testo unico in materia di beni culturali e ambientali o, secondo quanto previsto dai medesimi codici, presso altri archivi privati.

[8] V., allo stato, l'Autorizzazione n. 1/2005 al trattamento dei dati sensibili nei rapporti di lavoro - 21 dicembre 2005, in *G.U.* n. 2 del 3 gennaio 2006 Suppl.

Inoltre, per i dati sensibili il Codice non richiede il consenso dell'interessato se:

- il trattamento è necessario per svolgere le investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397 o per far valere o difendere in sede giudiziaria un diritto. I dati vanno trattati solo per tali finalità e per il periodo strettamente necessario al loro perseguimento (art. 26, comma 4, lett. *c*) del Codice) (9);
- il trattamento è necessario per adempiere a specifici obblighi o compiti previsti dalla legge oppure da un regolamento o dalla normativa comunitaria per la gestione del rapporto di lavoro, anche in materia di igiene e sicurezza del lavoro e della popolazione e di previdenza e assistenza. Occorre rispettare i limiti previsti dall'autorizzazione generale del Garante (art. 26, comma 4, lett. *d*) del Codice).

Ordinario n. 1 e doc. *web* 1203930; Autorizzazione n. 2/2005 al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale - 21 dicembre 2005, in *G.U.* n. 2 del 3 gennaio 2006 Suppl. Ordinario n. 1 e doc. *web* 1203946; Autorizzazione n. 3/2005 al trattamento dei dati sensibili da parte degli organismi di tipo associativo e delle fondazioni - 21 dicembre 2005, in *G.U.* n. 2 del 3 gennaio 2006 Suppl. Ordinario n. 1 e doc. *web* n. 1203934; Autorizzazione n. 4/2005 al trattamento dei dati sensibili da parte dei liberi professionisti - 21 dicembre 2005, in *G.U.* n. 2 del 3 gennaio 2006 Suppl. Ordinario n. 1 e doc. *web* n. 1203954; Autorizzazione n. 5/2005 al trattamento dei dati sensibili da parte di diverse categorie di titolari - 21 dicembre 2005, in *G.U.* n. 2 del 3 gennaio 2006 Suppl. Ordinario n. 1 e doc. *web* n. 1203938; Autorizzazione n. 6/2005 al trattamento dei dati sensibili da parte degli investigatori privati - 21 dicembre 2005, in *G.U.* n. 2 del 3 gennaio 2006 Suppl. Ordinario n. 1 e doc. *web* n. 1203950; Autorizzazione n. 7/2005 al trattamento dei dati a carattere giudiziario da parte di privati, di enti pubblici economici e di soggetti pubblici - 21 dicembre 2005, in *G.U.* n. 2 del 3 gennaio 2006 Suppl. Ordinario n. 1 e doc. *web* n. 1203942.

9 Tuttavia "se i dati sono idonei a rivelare lo stato di salute e la vita sessuale, il diritto deve essere di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile".

5. LA SICUREZZA DEI DATI

Il profilo della sicurezza e dell'integrità delle informazioni oggetto di legittimo trattamento è un elemento qualificante delle discipline di protezione dei dati personali (artt. 31 ss. del Codice e disciplinare tecnico di cui all'All. B al Codice).

5.1. *Chi deve adottare le misure di sicurezza*

L'obbligo generale di adottare idonee misure di sicurezza è posto dal Codice. Il titolare del trattamento può adempiervi avvalendosi anche di un responsabile (art. 29, comma 2, del Codice).

5.2. *Quali misure di sicurezza devono essere adottate?*

Il titolare del trattamento è tenuto ad adottare tutte le misure idonee, valutate alla luce delle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle caratteristiche del trattamento, a ridurre i rischi di distruzione o di perdita anche accidentale dei dati o di accesso non autorizzato o non consentito ai dati (art. 31 del Codice).
In questo quadro vanno anche attuate le misure minime, applicabili a piccole e medie imprese (artt. 33-35 e all. B del Codice[10]).

5.3. *Come e quando deve essere redatto il DPS?*

In base alla vigente disciplina, in caso di trattamento di dati sensibili e giudiziari attraverso sistemi informatici deve essere redatto il documento programmatico sulla sicurezza (art. 34, comma 1, lett. *g*) e regola 19 dell'Allegato B al Codice). Si può tener conto dei suggerimenti già formulati dal Garante che –recependo le esigenze e le istanze peculiari di professionisti e piccoli operatori, con particolare riguardo alle piccole e medie imprese– ha già reso

[10] Le misure minime di sicurezza contenute nell'allegato B) del Codice riguardano anzitutto i trattamenti effettuati con strumenti elettronici: esse comprendono un sistema di autenticazione informatica con credenziali di autenticazione (cioè, un codice per l'identificazione dell'incaricato associato a una parola chiave), programmi per elaboratore volti a prevenirne la vulnerabilità (ad esempio, antivirus), procedure per realizzare il salvataggio periodico dei dati (c.d. procedure di *back up*) e la redazione di un documento programmatico sulla sicurezza in caso di trattamento di dati sensibili. Per i trattamenti effettuati senza l'ausilio di strumenti elettronici rientrano tra le misure minime le istruzioni scritte finalizzate al controllo ed alla custodia dei dati impartite agli incaricati e l'uso di contenitori o locali con idonea serratura per custodire i dati personali.

disponibile *on-line*, a far data dal 11 giugno 2004, una "*Guida operativa*".

Il Dps:

- va redatto o aggiornato entro il 31 marzo di ciascun anno;
- non deve essere comunicato al Garante, ma semplicemente conservato dal titolare presso la propria struttura per essere esibito in occasione di eventuali accertamenti ispettivi (art. 34, comma 1, lett. *g*) del Codice e regola 19 dell'Allegato B) al Codice);
- deve essere redatto dal "[...] titolare di un trattamento di dati sensibili o giudiziari anche attraverso il responsabile, se designato [...]" (regola 19 dell'All. B) cit.).

6. IL TRASFERIMENTO DI DATI PERSONALI IN PAESI TERZI

Nello svolgimento dell'attività di impresa può risultare necessario trasferire dati personali fuori dell'Unione europea (ad esempio relativi alla clientela o ai dipendenti). Il Codice prevede specifiche regole al riguardo.

6.1. *Quando si applica la disciplina del Codice in materia di trasferimento di dati fuori dall'Unione europea?*

La disciplina in materia di trasferimento di dati fuori dall'Unione europea (Ue) riguarda principalmente i flussi di dati personali verso i c.d. Paesi terzi, considerato che i Paesi situati all'interno dell'Ue hanno attuato, nei rispettivi ambiti, la direttiva 95/46/Ce, adottando specifiche normative in materia di protezione dei dati personali. Il loro rispetto è considerato idoneo per trasferire dati nell'Ue (art. 42 del Codice).

6.2. *In quali casi è consentito il trasferimento dei dati fuori dall'Unione europea?*

Il trasferimento è sempre consentito in varie ipotesi (art. 43 del Codice), tra le quali, con particolare riferimento alle attività d'impresa, possono ricordarsi i casi in cui:

- l'interessato ha manifestato il proprio consenso espresso e, se si tratta di dati sensibili, in forma scritta;
- il trasferimento è necessario per eseguire obblighi derivanti da un contratto del quale è parte l'interessato o per adempiere, prima della conclusione del contratto, a specifiche richieste dell'interessato, ovvero per la conclusione o per l'esecuzione di un contratto stipulato a favore dell'interessato;
- il trasferimento è necessario per la salvaguardia di un interesse pubblico rilevante individuato con legge o con regolamento;
- è necessario ai fini dello svolgimento delle investigazioni difensive (legge 7 dicembre 2000, n. 397), o, comunque, per far valere o difendere un diritto in sede giudiziaria;
- il trattamento concerne dati riguardanti persone giuridiche, enti o associazioni.

6.3. *Qualora non sussistano i presupposti sopra indicati, in quali circostanze il trasferimento è comunque autorizzato?*

Il trasferimento è consentito anche quando è autorizzato dal Garante in presenza di adeguate garanzie per i diritti dell'interessato:

- individuate dal Garante;
- in base alle decisioni di adeguatezza adottate dalla Commissione europea in ordine al livello di protezione dei dati garantito dall'ordinamento del Paese destinatario (artt. 25, par. 6, e 26, par. 4, della direttiva 95/46/CE) [11];
- in base alla decisione di adeguatezza delle garanzie contenute *nel Safe Harbor* per il trasferimento verso organizzazioni stabilite negli Stati Uniti d'America che ad esso aderiscono [12];
- in base all'adozione di clausole contrattuali standard tra "esportatore" e "importatore" di dati, il cui contenuto è stato ritenuto idoneo dalla Commissione europea (artt. 25, par. 6, e 26, par. 4, della direttiva 95/46/CE) [13].

---

[11] Per l'Argentina, Decisione della Commissione del 30 giugno 2003, n. 2003/490/CE; per il Canada, Decisione della Commissione del 20 dicembre 2001, n. 2002/2/CE; per il Baliato di Guernesy, Decisione della Commissione del 21 novembre 2003, n. 2003/821/CE; per l'Isola di Man, Decisione della Commissione del 28 aprile 2004, n. 2004/411/CE; per la Svizzera, Decisione della Commissione del 26 luglio 2000, n. 2000/518/CE. In relazione ad esse v., nell'ordine, le autorizzazioni rilasciate dal Garante: Autorizzazione del 9 giugno 2005 in *G.U.* del 25 luglio 2005, n. 171, doc. *web* n. 1151846; Autorizzazione del 30 aprile 2003 in *G.U.* n. 191 del 19 agosto 2003, doc. *web* n. 1075324; Autorizzazione del 7 settembre 2004 in *G.U.* del 22 luglio 2005, n. 169, doc. *web* n. 1139333; Autorizzazione del 9 giugno 2005 in *G.U.* del 25 luglio 2005, n. 171, doc. *web* n. 1151889; Autorizzazione del 17 ottobre 2001 in *G.U.* del 26 novembre 2001 n. 275 - Suppl. Ordinario n. 250, doc. *web* n. 39428.

[12] Cfr. Decisione della Commissione europea del 26 luglio 2000 n. 2000/520/CE e la correlativa l'Autorizzazione del 10 ottobre 2001 (in *G.U.* 26 novembre 2001), doc. *web* n. 39939. Le organizzazioni aderenti al *Safe Harbor* sono pubblicate sul sito *web*: http://www.export.gov/safeharbor/index.html.

[13] Cfr. Decisione della Commissione europea del 27 dicembre 2001, n. 2002/16/Ce, relativa alle clausole contrattuali tipo per il trasferimento di dati personali a "incaricati" del trattamento residenti in paesi terzi, a norma della direttiva 95/46/Ce (e correlativa deliberazione del Garante n. 3 del 10 aprile 2002, doc. web n. 1065361); Decisione della Commissione europea del 15 giugno 2001, n. 2001/497/CE, relativa alle clausole contrattuali tipo per il trasferimento di dati a carattere personale verso paesi terzi a norma della direttiva 95/46/Ce (e correlativa deliberazione del Garante del 10 ottobre 2001, doc. *web* 42156). La Commissione ha altresì individuato un modello alternativo di clausole contrattuali tipo (definito Insieme II) con la decisione del 27 dicembre 2004, n. 2004/915/Ce (e la correlativa autorizzazione del Garante del 9 giugno 2005, doc. *web* n. 1151949).

7. I DOVERI DEL TITOLARE DEL TRATTAMENTO IN CASO DI ESERCIZIO DEI DIRITTI DEGLI INTERESSATI AI SENSI DELL'ART. 7 DEL CODICE

La disciplina di protezione dei dati personali attribuisce a ciascun interessato il diritto di accedere ai dati personali a sé riferiti e di esercitare gli altri diritti previsti dall'art. 7 del Codice [14].

7.1. *Cosa si deve fare quando l'interessato esercita il diritto d'accesso?*

Se l'interessato esercita il proprio diritto d'accesso ai dati che lo riguardano o uno degli altri diritti che gli sono riconosciuti, il titolare del trattamento (o il responsabile) deve fornire riscontro (di regola) entro quindici giorni dal ricevimento dell'istanza (art. 146 del Codice).

7.2. *Quali sono le conseguenze nel caso in cui non venga fornito il riscontro all'interessato?*

In caso di omesso o incompleto riscontro, i predetti diritti possono essere fatti valere dinanzi all'autorità giudiziaria o con ricorso al Garante (art. 145 del Codice).

---

[14] Art. 7. *Diritto di accesso ai dati personali ed altri diritti.*

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.
3. L'interessato ha diritto di ottenere:
   a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati;
   b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
   c) l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.
4. L'interessato ha diritto di opporsi, in tutto o in parte:
   a) per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;
   b) al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

7.2. Quali sono le conseguenze nel caso in cui non venga fornito il riscontro all'interessato?

In caso di omesso o incompleto riscontro, i predetti diritti possono essere fatti valere dinanzi all'autorità giudiziaria o con ricorso al Garante (art. 145 del Codice).

8. *CHECK LIST*

La seguente lista di controllo è predisposta per i "titolari del trattamento"; mira a riassumere, in forma interrogativa, i punti sopra riassunti. La risposta negativa ad uno dei quesiti, denota un possibile profilo critico dal punto di vista della protezione dei dati personali.

	QUESITO	SI	NO
1.	È stata effettuata una valutazione circa le operazioni di trattamento di dati personali, anche sensibili, effettuate dall'impresa?	□	□
	I dati trattati sono pertinenti e non eccedenti rispetto alle legittime finalità del trattamento, oltre che esatti e aggiornati?	□	□
	Le persone fisiche che all'interno dell'impresa trattano dati personali sono state designate tutte quali "incaricate del trattamento"?	□	□
	Sono state fornite a tutti gli "incaricati del trattamento" istruzioni scritte circa i propri compiti?	□	□
	Se all'interno dell'impresa sono stati individuati soggetti che hanno ambiti di autonomia nel trattamento dei dati personali, sono stati designati per iscritto "responsabili del trattamento"?	□	□
	Se fuori dell'impresa enti o persone fisiche trattano dati personali nel suo interesse, obbligati a seguirne le istruzioni (come accade per i casi di *outsourcing*), sono stati designati per iscritto quali "responsabili del trattamento"?	□	□
2.	Si è verificato, prima di intraprendere operazioni di trattamento, se l'impresa effettua i trattamenti da notificare al Garante?	□	□
	Se sono intervenute modificazioni relativamente ai trattamenti già eventualmente notificati, è stato curato il loro aggiornamento in una nuova notificazione?	□	□
	Se cessano i trattamenti, ciò ha formato oggetto di specifica notificazione?	□	□
3.	È stata fornita l'informativa agli interessati in caso di dati raccolti presso di essi?	□	□
	È stata fornita l'informativa agli interessati in caso di dati raccolti presso soggetti diversi dagli interessati stessi?	□	□

4.	Il trattamento dei dati personali viene effettuato in presenza di uno dei presupposti di liceità indicati all'art. 24 del Codice?	□	□
	Se non ricorre uno dei presupposti di liceità indicati all'art. 24 del Codice, è stato raccolto il consenso dell'interessato?	□	□
	Se sono trattati dati sensibili è stato raccolto il consenso scritto degli interessati?	□	□
	Se sono trattati dati sensibili, è stato verificato se il trattamento rientra tra quelli già autorizzati dal Garante con le autorizzazioni generali?	□	□
	Se il trattamento di dati sensibili non rientra tra quelli previsti dalle autorizzazioni generali, è stata richiesta al Garante un'autorizzazione *ad hoc*?	□	□
5.	Sono state adottate idonee misure di sicurezza per proteggere i dati personali?	□	□
	Sono state adottate le misure minime di sicurezza previste per proteggere i dati personali?	□	□
	Se sono trattati dati sensibili e giudiziari, è stato redatto, quando è necessario, il documento programmatico per la sicurezza e ne vengono osservate le previsioni?	□	□
	Periodicamente, e comunque entro il 31 marzo di ciascun anno, formano oggetto di rinnovata valutazione le misure di sicurezza individuate con il documento programmatico per la sicurezza?	□	□
6.	Se i dati personali trattati dall'impresa sono soggetti a trasferimento verso Paesi terzi (esterni all'Unione europea e all'area economica europea), il trasferimento avviene: • in presenza di una delle condizioni previste dall'art. 43 del Codice? oppure • verso uno dei paesi che assicurano un livello adeguato di protezione (Svizzera, Argentina, Isola di Man, Baliato di Guernsey)? oppure • verso un'impresa statunitense che aderisce al *Safe Harbor*? oppure • in presenza di clausole contrattuali *standard* tra esportatore e importatore? oppure • in presenza di un'autorizzazione *ad hoc* da parte del Garante?	□	□
7.	In presenza dell'esercizio del diritto d'accesso, viene dato riscontro all'interessato secondo le modalità previste dalla legge?	□	□

07A05511