

***A TUTTI I CLIENTI
LORO SEDI***

Milano, 1 marzo 2000

Circolare n. 3/2000

**TRATTAMENTO DI DATI PERSONALI. ADOZIONE DELLE MISURE MINIME DI
SICUREZZA INTRODOTTE CON IL D.P.R. 28 LUGLIO 1999, N. 318**

1. – Fonti normative.

Le misure minime di sicurezza per il trattamento dei dati personali sono disciplinate dai seguenti provvedimenti:

- l. 31 dicembre 1996, n. 675;
- d.p.r. 28 luglio 1999, n. 318, pubblicato in Gazzetta Ufficiale del 14 settembre 1999, n. 216 (allegato n. 1).

In particolare, l'art. 15 della citata l. n. 675/1996 dispone che:

1. *“I dati personali oggetto di trattamento devono essere custoditi e controllati, anche in relazione...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..”*
2. *“Le misure di sicurezza...sono individuate con regolamento emanato con decreto del Presidente della Repubblica”.*

Con d.p.r. 28 luglio 1999, n. 318 è stato emanato il regolamento di attuazione previsto dal suddetto art. 15, comma 2, contenente le misure minime di sicurezza che tutti i titolari di un trattamento di dati personali sono tenuti ad adottare.

A tal riguardo si richiama la definizione contenuta nell'art. 1, comma 1, lett. a) del regolamento in esame, ove si stabilisce che le suddette misure minime di sicurezza sono *“il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza, previste nel presente regolamento, che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti dall'articolo 15, comma 1, della legge (cfr. l. n. 675/1996)”*.

I rischi espressamente presi in considerazione dall'art. 15, comma 1, sono 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”*.

Si sottolinea che, secondo quanto previsto dall'art. 41 della l. n. 675/1996, le misure minime di sicurezza individuate con il predetto regolamento dovranno essere obbligatoriamente adottate entro il 28 marzo 2000 e che la mancata adozione di dette misure può comportare, come meglio si dirà in seguito, sanzioni sia di carattere civile che di carattere penale.

Si osserva, inoltre, che il regolamento in oggetto introduce, accanto a Titolare, Responsabile e Incaricato, tipizzati dalla l. n. 675/1996, due nuove figure alle quali attribuisce particolari mansioni esecutive senza specifiche responsabilità organizzative.

Le nuove figure introdotte dal suddetto regolamento sono:

- l'**amministratore di sistema**, al quale *“è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di base dati e di consentirne l'utilizzazione”* (art. 1, comma 1, lett. c);
- il **oggetto preposto alla custodia** delle *“parole chiave o che hanno accesso ad informazioni che concernono le medesime”* (art. 2, comma 1, lett. b).

2. – Trattamento di dati personali e misure minime di sicurezza.

Da un rapido esame delle disposizioni del regolamento in oggetto, si rileva anzitutto la prima fondamentale bipartizione fra:

- trattamenti di dati personali effettuati con strumenti elettronici o comunque automatizzati (cc.dd. strumenti informatici);
- trattamenti dei dati personali effettuati con strumenti non informatici.

Con particolare riferimento ai suddetti strumenti informatici, viene introdotta un'ulteriore distinzione, a seconda che il trattamento dei dati venga effettuato mediante elaboratori non accessibili in rete ovvero mediante elaboratori accessibili in rete. Il regolamento opera talune distinzioni anche tra trattamento effettuato mediante elaboratori accessibili in reti disponibili al pubblico (ad esempio, *Internet*) e trattamento effettuato mediante elaboratori accessibili in reti non disponibili al pubblico (secondo una tesi si dovrebbero considerare non disponibili al pubblico le sole reti poste all'interno di un'unica sede e prive di qualunque interconnessione con l'esterno).

Nel caso di utilizzo di elaboratori collegati in rete anche per il trattamento di dati sensibili e a carattere giudiziario, di cui rispettivamente agli artt. 22 e 24 della l. n. 675/1996, il regolamento in oggetto impone cautele aggiuntive in considerazione della particolare delicatezza delle informazioni oggetto di trattamento nonché della maggior facilità di accessi indebiti al sistema..

Inoltre laddove il trattamento venga effettuato mediante elaboratori accessibili in reti disponibili al pubblico (ad esempio, come detto, *Internet*), il suddetto regolamento prescrive l'obbligo di predisporre e aggiornare, con cadenza annuale, il "documento programmatico sulla sicurezza" il cui contenuto minimo è predeterminato dal regolamento stesso.

Da ultimo si fa, altresì, notare che il d.p.r. n. 318/1999 pone attenzione anche al trattamento dei dati personali mediante strumenti non informatici, per i quali prescrive specifiche misure di sicurezza le quali rilevano in modo particolare sotto il profilo organizzativo.

Ai fini di una migliore esposizione, si allega una tabella nella quale sono riportate, in relazione alle diverse modalità di trattamento dei dati, le misure minime di sicurezza introdotte dal regolamento in oggetto (cfr. allegato n. 2).

3. – Misure minime di sicurezza e responsabilità civile e penale.

La mancata adozione delle misure minime di sicurezza in esame, come detto in precedenza, può comportare sanzioni sia di carattere civile che di carattere penale.

Con riferimento alla responsabilità civile l'art. 18 della l. n. 675/1996 dispone che *“chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'art. 2050 del codice civile...se non prova di avere adottato tutte le misure idonee ad evitare il danno”*.

In proposito si fa notare che il riferimento all'art. 2050 c.c. comporta una inversione dell'onere della prova in quanto sarà il Titolare del trattamento a dover provare, in presenza di un danno cagionato dal trattamento di dati personali da lui effettuato, ad aver adottato tutte le misure che, in relazione al progresso tecnologico del momento, apparivano idonee in astratto a prevenire il verificarsi del danno stesso. Ove il Titolare non soddisfi il suddetto onere probatorio, opererà una presunzione di colpa a suo carico. Da quanto detto consegue che l'adozione delle misure minime di sicurezza costituisce una condizione necessaria, ma non sufficiente per l'esclusione della responsabilità civile; infatti, tali misure minime costituiscono, per l'appunto, gli strumenti minimali di sicurezza che ciascun Titolare del trattamento deve adottare in virtù dell'obbligo imposto dall'art. 15 della l. n. 675/1996 ma non costituiscono, proprio perché “misure minime”, uno strumento sufficiente a comprovare che alla condotta del Titolare non può essere mosso alcun addebito. Ai fini della prova liberatoria sarà pertanto necessario dimostrare, non solo di aver adottato le misure minime di sicurezza in parola, ma altresì di aver adottato ogni altro accorgimento possibile per evitare il danno.

Con riferimento alla responsabilità penale si osserva che la violazione dell'art. 15 della suddetta l. n. 675/1996 è richiamato dall'art. 36 della stessa legge, il quale stabilisce che *“1. Chiunque, essendovi tenuto, omette di adottare le misure necessarie a garantire la sicurezza dei dati personali, in violazione delle disposizioni dei regolamenti di cui ai commi 2 e 3 dell'articolo 15, è punito con la reclusione sino ad un anno. Se dal fatto deriva nocumento, la pena è della reclusione da due mesi a due anni. 2. Se il fatto di cui al comma 1 è commesso per colpa si applica la reclusione fino ad un anno”*.

In via preliminare, si osserva che, a differenza della responsabilità civile, l'adozione in concreto delle misure minime di sicurezza di per sé è idonea ad escludere la responsabilità penale.

In secondo luogo si fa notare che la disposizione contenuta nel citato art. 36 si riferisce, esclusivamente, al Titolare ed al Responsabile del trattamento, che sono i soggetti tenuti ad “...*adottare le misure necessarie a garantire la sicurezza dei dati personali...*”.

4. – La regolamentazione del flusso dei dati tra l'intermediario ed i collaboratori esterni.

In questa sede sembra opportuno ricordare la qualificazione giuridica dei collaboratori esterni degli intermediari ai sensi della legge sulla privacy. A tal proposito si richiama la circolare Assoreti 25 novembre 1997, n. 55, ove è stabilito che “*non vi sono ragioni di ordine concettuale che ostino all'attribuzione a tale soggetto della qualifica di incaricato rispetto all'intermediario, purché ricorrano i requisiti prescritti dall'art. 19 della l. n. 675, 31 dicembre 1996*”.

Si chiarisce inoltre che la designazione dei collaboratori esterni quali incaricati del trattamento consente di prescindere dal consenso degli interessati ai fini della comunicazione dei dati.

I requisiti richiesti dal suddetto art. 19 sono i seguenti:

- specifico conferimento per iscritto dell'incarico;
- esercizio di una “diretta autorità” del Titolare o del Responsabile sull'incaricato.

Si fa comunque presente che un ulteriore requisito, desumibile implicitamente dalla legge, è la sua natura di persona fisica.. Tale conclusione trova una conferma, oltre che nell'orientamento manifestato in più occasioni dallo stesso Garante per la protezione dei dati personali, anche nei compiti meramente materiali attribuiti all'incaricato stesso e nella circostanza che quando la l. n. 675/96 ha ritenuto che determinate funzioni potessero essere svolte anche da soggetti “non persone fisiche” (quali persone giuridiche, associazioni, ecc.) lo ha stabilito espressamente.

Sembra opportuno precisare che, con riferimento al secondo requisito, il Garante per la protezione dei dati personali ha stabilito che l'art. 19 si può riferire anche ai collaboratori

esterni. Pertanto la mancanza del vincolo di subordinazione non ostacola la formale designazione quale “incaricato del trattamento” di soggetti che non siano legati al Titolare del trattamento da un rapporto di lavoro subordinato.

Per completezza si sottolinea altresì che, secondo l’interpretazione consolidata del Garante, quando il trattamento è effettuato nell’ambito di una persona giuridica, il titolare è “l’entità nel suo complesso”, anziché taluna delle persone fisiche che operano nella relativa struttura e che concorrono, in concreto, a formarne la volontà o che sono legittimati a manifestarla all’esterno. Resta inteso, comunque, che, se titolare è la Società nel suo complesso, per essa opereranno, nelle diverse scelte che sia necessario assumere, i suoi organi, tenendo conto delle ordinarie attribuzioni previste dall’atto costitutivo e dallo statuto (ad es., il Consiglio d’Amministrazione, il Presidente, l’Amministratore Delegato, il Direttore Generale e gli altri dirigenti). Tenuto altresì conto del principio di “personalità” della responsabilità penale, delle eventuali omissioni penalmente rilevanti dovranno pertanto rispondere gli organi della società stessa.

Da ultimo si osserva che anche la responsabilità connessa con l’adozione delle misure minime di sicurezza grava sul Titolare del trattamento nonché, ove designati, sul Responsabile del trattamento al quale siano stati conferiti compiti specifici in materia. Tale responsabilità si estende, ovviamente, ai trattamenti di dati personali eseguiti dai collaboratori esterni, nella qualità di incaricati del trattamento.

5. – Conclusioni.

In relazione a quanto precede, tenuto conto delle possibili responsabilità civili e penali conseguenti alla mancata ottemperanza alle prescrizioni del regolamento, si rammenta che il termine ultimo per l’adozione delle predette misure minime di sicurezza è il 28 marzo 2000.

Peraltro, si fa notare che le citate misure di sicurezza non sono particolarmente gravose sul piano informatico, soprattutto se, dal punto di vista tecnologico, già si dispone di adeguate procedure interne di sicurezza.

L’adozione delle misure previste dal suddetto decreto può inoltre costituire l’occasione per verificare il rispetto degli adempimenti imposti dalla l. n. 675/1996 i quali, al fine di facilitare tale compito, sono sinteticamente elencati nell’allegato n. 3.

ALLEGATO 2

TRATTAMENTO DEI DATI PERSONALI E MISURE MINIME DI SICUREZZA

1. – TRATTAMENTO DEI DATI PERSONALI MEDIANTE MEZZI INFORMATICI

1.1. – TRATTAMENTO DEI DATI PERSONALI MEDIANTE ELABORATORI NON ACCESSIBILI DA ALTRI ELABORATORI O TERMINALI

| | MISURA MINIMA DA ADOTTARE | NOTE |
|----|---|---|
| 1. | <i>Prevedere una parola chiave per l'accesso ai dati, fornirla agli incaricati del trattamento e, ove tecnicamente possibile in relazione alle caratteristiche dell'elaboratore, consentirne l'autonoma sostituzione, previa comunicazione ai soggetti indicati al punto seguente (art. 2).</i> | Il legislatore non ha stabilito regole o procedure per la scelta della parola chiave (lunghezza minima, periodo di validità, ecc.). |
| 2. | <i>Individuare per iscritto, quando vi è più di un incaricato al trattamento e sono in uso più parole chiave, i soggetti preposti alla loro custodia o che hanno accesso ad informazioni che concernono le medesime (art. 2).</i> | Questa misura è prevista quando il trattamento è svolto da più incaricati ed obbliga il titolare od il responsabile ad indicare per iscritto chi ha in custodia le parole chiave. |

1.2. – TRATTAMENTO DEI DATI PERSONALI MEDIANTE ELABORATORI ACCESSIBILI IN RETE *(i.e. sistemi informativi che hanno una infrastruttura di rete locale e/o geografica) (1)*

| | MISURA MINIMA DA ADOTTARE | NOTE |
|----|--|---|
| 1. | <i>A ciascun utente o incaricato del trattamento deve essere attribuito un codice identificativo personale (c.d. user-id) per l'utilizzazione dell'elaboratore. Uno stesso codice, fatta eccezione per gli amministratori di sistema relativamente ai sistemi operativi che prevedono un unico livello di accesso per tale funzione, non può, neppure in tempi diversi, essere assegnato a persone diverse (art. 4).</i> | Questa misura viene adottata quando ci sono più incaricati o utenti e non consente l'uso di uno stesso codice da parte di più persone. |
| 2. | <i>I codici identificativi personali devono essere assegnati e gestiti in modo che ne sia prevista la disattivazione in caso di perdita della qualità che consentiva l'accesso all'elaboratore o di mancato utilizzo dei medesimi per un periodo superiore ai sei mesi (art. 4).</i> | Occorre prevedere procedure, anche automatizzate, che controllino periodicamente i codici identificativi personali e che, comunque, disattivino i codici inutilizzati o non più validi. |

| | | |
|----|---|--|
| 3. | <i>Gli elaboratori devono essere protetti contro il rischio di intrusione ad opera di programmi di cui all'art. 615 quinquies del codice penale, mediante idonei programmi, la cui efficacia ed aggiornamento sono verificati con cadenza almeno semestrale (art. 4).</i> | È necessario prevedere l'aggiornamento di programmi antivirus e la documentazione sulle attività svolte, oltre che manuali di installazione software e procedure di verifica della sua integrità. |
| 4. | <i>L'accesso per effettuare le operazioni di trattamento dei dati di cui agli artt. 22 e 24 della l. n. 675/1996 è determinato sulla base di autorizzazioni assegnate, singolarmente o per gruppi di lavoro, agli incaricati del trattamento o della manutenzione (art. 5).</i> | Da tale disposizione si evince che tutti coloro che operano sui dati sensibili e a carattere giudiziario devono essere autorizzati, singolarmente o con riferimento all'unità di appartenenza. |
| 5. | <i>Le autorizzazioni all'accesso di cui al punto precedente sono rilasciate e revocate dal titolare e, se designato, dal responsabile. Periodicamente, e comunque almeno una volta all'anno, è verificata la sussistenza delle condizioni per la loro conservazione (art. 5).</i> | Il titolare o il responsabile rilasciano e controllano le autorizzazioni per ogni trattamento di dati sensibili e a carattere giudiziario. |
| 6. | <i>L'autorizzazione al suddetto accesso deve essere limitata ai soli dati la cui conoscenza è necessaria e sufficiente per lo svolgimento delle operazioni di trattamento o di manutenzione (art. 5).</i> | Le autorizzazioni per ogni trattamento di dati sensibili e a carattere giudiziario vanno concesse solo per effettive necessità di lavoro e limitatamente ai soli dati necessari e sufficienti per le mansioni assegnate. |
| 7. | <i>La validità delle richieste di accesso ai dati personali è verificata prima di consentirne l'accesso stesso (art. 5).</i> | Misura prevista per ogni trattamento di dati sensibili e a carattere giudiziario. Il titolare o responsabile deve poter dimostrare che la misura è effettivamente implementata e impedisce in via preventiva l'accesso ai non autorizzati. |
| 8. | <i>Non è consentita la utilizzazione di un medesimo codice identificativo personale per accedere contemporaneamente alla stessa applicazione da diverse stazioni di lavoro (art. 5).</i> | Da tale disposizione si evince che, con riferimento al trattamento di dati sensibili e a carattere giudiziario, non può essere usato uno stesso <i>user-id</i> da postazioni diverse. |

**1.2.1 - TRATTAMENTO DEI DATI SENSIBILI E A CARATTERE
GIUDIZIARIO EFFETTUATO MEDIANTE UTILIZZO DI UNA RETE
DISPONIBILE AL PUBBLICO (AD ESEMPIO INTERNET) ⁽¹⁾**

| | MISURA MINIMA DA ADOTTARE | NOTE |
|-----------|---|--|
| 1. | <i>L'autorizzazione assegnata agli incaricati del trattamento o della manutenzione deve comprendere l'indicazione degli strumenti utilizzati, intesa come l'individuazione dei singoli elaboratori attraverso i quali è possibile accedere per effettuare operazioni di trattamento (art. 5).</i> | Per ogni trattamento di dati sensibili e a carattere giudiziario è sempre necessario identificare gli strumenti usati per il suddetto trattamento. |
| 2. | <i>L'autorizzazione di cui al punto precedente riguarda anche gli strumenti che possono essere utilizzati per l'interconnessione mediante reti disponibili al pubblico (art. 5).</i> | Il legislatore richiede altresì che per ogni trattamento di dati sensibili e a carattere giudiziario vengano identificati gli strumenti usati per l'interconnessione. |
| 3. | <i>Deve essere predisposto e aggiornato con cadenza annuale, un documento programmatico sulla sicurezza dei dati per definire, sulla base dell'analisi dei rischi, della distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati stessi: a. i criteri tecnici ed organizzativi per la protezione delle aree e dei locali interessati dalle misure di sicurezza nonché le procedure per controllare l'accesso delle persone autorizzate ai locali medesimi; b. i criteri e le procedure per assicurare l'integrità dei dati; c. i criteri e le procedure per la sicurezza delle trasmissioni dei dati, ivi compresi quelli per le restrizioni di accesso per via telematica; d. l'elaborazione di un piano di formazione per rendere edotti gli incaricati del trattamento dei rischi individuati e dei modi per prevenire danni (art. 6).</i> | Tale misura è prevista per ogni trattamento di dati sensibili e a carattere giudiziario. |
| 4. | <i>L'efficacia delle misure di sicurezza adottate ai sensi del punto precedente, deve essere oggetto di controlli periodici, da eseguirsi con cadenza almeno annuale (art. 6).</i> | Per ogni trattamento di dati sensibili e a carattere giudiziario occorre un <i>auditing</i> annuale, del quale avere documentazione. |
| 5. | <i>I supporti già utilizzati per il trattamento possono essere riutilizzati qualora le informazioni precedentemente contenute non siano tecnicamente recuperabili in alcun modo, altrimenti devono essere distrutti (art. 7).</i> | Nel caso di trattamento di dati sensibili e a carattere giudiziario è necessario distruggere i supporti se non si è sicuri della completa eliminazione dei dati precedentemente contenuti. |

⁽¹⁾ Si ricordi che tali misure sono previste in aggiunta a quelle prescritte per il trattamento dei dati personali mediante elaboratori non accessibili in rete.

**2. – TRATTAMENTO DEI DATI
PERSONALI MEDIANTE STRUMENTI
NON ELETTRONICI**

| | MISURA MINIMA DA ADOTTARE | NOTE |
|-----------|--|---|
| 1. | <i>Il titolare o, se nominato, il responsabile, nel designare gli incaricati del trattamento per iscritto e nell'impartire le istruzioni ai sensi degli artt. 8, comma 5, e 19, deve prescrivere che gli incaricati abbiano accesso ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati (art. 9).</i> | Occorre, quindi, limitare l'accesso degli incaricati alle sole informazioni necessarie per i compiti assegnati. |
| 2. | <i>Gli atti e i documenti contenenti i dati devono essere conservati in archivi ad accesso selezionato e, se affidati agli incaricati del trattamento, devono essere da questi ultimi conservati e restituiti al termine delle operazioni affidate (art. 9).</i> | È necessario limitare l'accesso agli archivi e la permanenza delle informazioni presso gli incaricati. |
| 3. | <i>Gli atti e i documenti contenenti dati sensibili o a carattere giudiziario affidati agli incaricati del trattamento devono essere conservati, fino alla restituzione, in contenitori muniti di serratura (art. 9).</i> | Occorre che gli incaricati conservino con cura e sotto chiave le informazioni. |
| 4. | <i>L'accesso agli archivi contenenti dati sensibili o a carattere giudiziario deve essere controllato e devono essere identificati e registrati i soggetti che vi vengono ammessi dopo l'orario di chiusura degli archivi stessi (art. 9).</i> | È necessario controllare l'accesso fisico agli archivi e limitarlo agli incaricati, aprire e conservare il registro degli ingressi. |
| 5. | <i>I supporti non informatici contenenti la riproduzione di informazioni relative al trattamento di dati sensibili o a carattere giudiziario devono essere conservati e custoditi con le modalità di cui ai punti precedenti (art. 10).</i> | Occorre conservare con cura e sotto chiave le informazioni, limitare gli accessi, ecc. |

ALLEGATO 3

ADEMPIMENTI RICHIESTI DALLA LEGGE 675/1996 PER I TRATTAMENTI DI DATI PERSONALI EFFETTUATI DA PRIVATI ED ENTI PUBBLICI ECONOMICI

1. Designazione di responsabili del trattamento.
 2. Individuazione degli incaricati del trattamento.
 3. Notificazione al Garante per la Protezione dei dati personali (da effettuare in via preventiva e per ogni modifica intervenuta rispetto ai dati precedentemente notificati).
 4. Redazione di istruzioni per i responsabili del trattamento.
 5. Redazione di istruzioni per gli incaricati del trattamento.
 6. Redazione delle informative per gli interessati.
 7. Redazione dei modelli per acquisire, ove richiesto dalla legge, il consenso al trattamento e alla comunicazione dei dati.
 8. Predisposizione di una procedura volta a soddisfare le istanze presentate ai sensi dell'art. 13 della legge 675/1996.
 9. Adozione delle misure minime di sicurezza introdotte con D.P.R. N. 318/1999.
 10. Predisposizione di procedure di verifica del rispetto delle norme in materia di trattamento dei dati personali e di report per il titolare del trattamento (al quale compete comunque il dovere di vigilare sull'operato dei responsabili e degli incaricati).
-