

## PRIVACY - PRIMI ADEMPIMENTI IN MATERIA DI SICUREZZA

### 1. Premessa

Il Codice in materia di protezione dei dati personali prevede numerose innovazioni in materia di misure di sicurezza nel trattamento dei dati. Le disposizioni relative alla sicurezza dei dati e dei sistemi sono contenute nel titolo V del Codice e nel disciplinare tecnico ad esso allegato.

Il Garante ha annunciato l'adozione di un *Vademecum* per fornire un'interpretazione delle regole da seguire nella predisposizione nelle nuove misure. In attesa del provvedimento del Garante, con la presente circolare si svolgono prime considerazioni in materia di sicurezza e si forniscono indicazioni in merito all'adozione del documento programmatico sulla sicurezza per il 2004.

Si allega in coda alla circolare, inoltre, un documento che descrive i principali contenuti del documento programmatico.

### 2. L'adozione del documento programmatico per l'anno in corso

Tab. 1 – L'aggiornamento del documento programmatico sulla sicurezza nel 2004

<b>I soggetti</b>	- I titolari già tenuti all'adozione del documento programmatico in base alla normativa precedente (chi tratta dati sensibili o giudiziari con elaboratori accessibili mediante una rete di telecomunicazione disponibile al pubblico)	- I titolari che trattano dati sensibili o giudiziari con elaboratore "stand alone".
<b>Il termine</b>	- Entro il 31 marzo 2004	- Entro il 31 dicembre 2004
<b>I contenuti</b>	<p>- Il documento programmatico va redatto seguendo le norme del Codice in materia di protezione dei dati personali e del disciplinare tecnico e dovrà contenere informazioni idonee circa tutte le misure di sicurezza già prescritte nel dpr 318/99.</p> <p>- Nel documento si dovrà procedere ad una descrizione degli interventi che si intende effettuare nel 2004 per adeguarsi alle nuove misure minime di sicurezza.</p> <p>- Se, in caso di difficoltà tecniche oggettive, si beneficia della proroga del termine per l'attuazione delle nuove misure minime si dovrà menzionare tale circostanza, descrivendo un piano per l'attuazione delle misure di sicurezza entro il 1 gennaio 2005</p>	<p>- Il documento programmatico va redatto seguendo le norme del Codice e del disciplinare tecnico e dovrà contenere informazioni idonee circa tutte le misure di sicurezza prescritte dal Codice.</p> <p>- Se, in caso di difficoltà tecniche oggettive, si beneficia della proroga del termine per l'attuazione delle nuove misure minime si dovrà menzionare tale circostanza, descrivendo un piano per l'attuazione delle misure di sicurezza entro il 1 gennaio 2005</p>

Tra le misure minime da adottare quando ci si avvale di strumenti elettronici il Codice menziona il documento programmatico sulla sicurezza. Si tratta di un documento che racchiude le scelte e le misure che il titolare intende adottare in materia di sicurezza dei dati quando procede al trattamento dei dati avvalendosi di strumenti elettronici.

Il disciplinare tecnico allegato al Codice dispone che **il documento programmatico debba essere adottato o aggiornato entro il 31 marzo di ogni anno.**

Il Garante ha chiarito che **il documento programmatico rappresenta misura di sicurezza minima unicamente per il trattamento di dati sensibili o giudiziari effettuato con strumenti elettronici, non per chi procede unicamente al trattamento (cartaceo o comunque anche informatico) di altri dati personali.**

*a. I soggetti obbligati*

Il Codice determina un ampliamento della categoria dei titolari tenuti all'adozione del documento programmatico. Diversamente da quanto disposto dal dpr. 318/99, infatti, la circostanza che il terminale sia isolato (elaboratore *stand alone*) non ha più alcuna rilevanza ai fini della esenzione dalla redazione del documento programmatico. **In base alle nuove regole, quindi, anche le imprese che gestiscono dati sensibili o giudiziari su di un terminale isolato dovranno redigere il documento programmatico.**

Le disposizioni transitorie suscitano alcune incertezze in merito all'individuazione dei soggetti tenuti all'adozione del documento programmatico per l'anno in corso. Non è chiaro, infatti, se tale documento sia da considerare come misura nuova o meno ai sensi della disposizione transitoria di cui all'art. 180 primo comma.

In base all'art.180, comma 1, del Codice "*Le misure minime di sicurezza di cui agli articoli da 33 a 35 e all'allegato B) che non erano previste dal D.P.R. 28 luglio 1999, n. 318, sono adottate entro il 30 giugno 2004*".

La norma transitoria, pertanto, opera solo per l'adeguamento alle "nuove misure" e conferma l'obbligo di rispettare le prescrizioni del dpr. n. 318/99 senza alcuna eccezione.

Il termine "nuove misure" minime di sicurezza deve essere inteso nel duplice significato di:

- **novità oggettiva.** Il Codice introduce una misura che non era prevista precedentemente. Si pensi, ad esempio, ai più severi requisiti previsti per l'autenticazione informatica descritti nel Disciplinare tecnico allegato al Codice;

- **novità soggettiva.** Le nuove regole ampliano il numero dei soggetti tenuti ad un determinato adempimento. La variazione rispetto alla normativa precedente è evidente: un soggetto che precedentemente non era tenuto ad adottare una certa misura minima, risulta obbligato in base alle nuove regole.

Un esempio di novità di tipo soggettivo è quello di chi non è tenuto alla redazione del documento programmatico in base alle vecchie regole (in quanto tratta dati sensibili o giudiziari con strumenti elettronici non in rete pubblica - cd. elaboratori "*stand alone*") e deve redigerlo per la prima volta.

Vi sono quindi due ipotesi:

- **chi era già tenuto all'adozione del documento programmatico in quanto trattava dati sensibili o giudiziari con "elaboratori accessibili mediante una rete di telecomunicazione disponibili al pubblico" dovrà procedere ad un aggiornamento entro il 31 marzo 2004.**

- **chi tratta dati sensibili o giudiziari con un elaboratore "*stand alone*" dovrà redigere il documento programmatico entro il 31 dicembre 2004, data in cui tutte le misure minime diventano vincolanti.**

Si ricorda, infine, che il titolare può adempiere all'obbligo di redazione del documento programmatico sulla sicurezza anche avvalendosi del responsabile.

*b. Il contenuto del documento*

Le disposizioni transitorie non chiariscono se, nel redigere il documento programmatico per l'anno in corso, si debba fare riferimento alle regole contenute nel Codice ovvero a quelle dettate dal dpr 318/99.

Si ritiene consigliabile, tuttavia, seguire lo schema di riferimento fornito dal disciplinare tecnico allegato al Codice privacy, anche se con alcune precisazioni.

Il documento programmatico, infatti, rappresenta solo una delle misure minime di sicurezza. Le "nuove" misure dovranno essere adottate entro il 30 giugno 2004. Nel documento programmatico, pertanto, si dovranno descrivere le linee di intervento che consentono di adeguarsi alle nuove regole nel corso del 2004. Si espliciteranno dunque le misure che adotteranno e le modalità con cui si intende farlo.

Di conseguenza alcune voci del documento programmatico (ad esempio le misure per il recupero dei dati sensibili o giudiziari ovvero le prescrizioni ulteriori in materia di dati relativi allo stato di salute) saranno solo accennate ovvero richiamate nella parte del documento in cui si esplicitano le linee di intervento future in conseguenza dei rischi individuati nonché delle nuove prescrizioni normative.

Inoltre, se non si posseggono strumenti idonei a supportare le nuove misure di sicurezza e si intende beneficiare della proroga prevista dal Codice, nel documento programmatico si dovrà menzionare questa circostanza, da un lato dichiarando che si provvederà all'adeguamento della strumentazione informatica e delle misure di sicurezza entro il 1 gennaio 2005, dall'altro definendo le linee ed i contenuti principali dell'intervento.

Nel caso in cui si proceda redazione del documento programmatico per la prima volta (ad esempio per le imprese di nuova costituzione) ovvero si debba procedere a significative revisioni dell'apparato di sicurezza si consiglia, ove possibile, di procedere ad un adeguamento alle nuove misure minime di sicurezza sin dal 31 marzo 2004.

In questo modo si eviterà di dover intervenire in maniera sostanziale sulle misure di sicurezza una seconda volta entro breve tempo e si avrà il vantaggio di mettersi in regola in anticipo rispetto a quanto previsto dalla legge, con ulteriori semplificazioni circa l'aggiornamento del prossimo documento programmatico.

*c. L'obbligo di menzione nella relazione sulla gestione*

Come anticipato, il titolare deve menzionare l'avvenuta adozione/aggiornamento del documento programmatico nella relazione accompagnatoria al bilancio d'esercizio, se dovuta.

La terminologia impiegata dal Codice è impropria e non è chiaro a quale comunicazione sociale ci si riferisca. Sembra corretto fare riferimento alla relazione sulla gestione, e non ad altri documenti previsti dal codice civile.

Si esclude, infatti, che il Codice privacy faccia riferimento alla nota integrativa. Tale interpretazione, infatti, priverebbe di ogni significato l'inciso "se dovuta", visto che la nota integrativa va adottata in ogni caso. Tale documento, inoltre, contiene unicamente indicazioni di tipo contabile e non è riferito ad altri aspetti della gestione, che vengono invece considerati nella relazione degli amministratori sulla gestione.

Al momento del deposito del bilancio, pertanto, gli amministratori delle società tenuti a redigere una relazione sulla gestione ai sensi dell'art. 2428 cod. civ. dovranno menzionare al suo interno la circostanza dell'avvenuta adozione/aggiornamento del documento programmatico.

Non vi è, pertanto, alcun obbligo di allegazione del documento programmatico alla relazione, né si è tenuti a descriverne il contenuto. Quanto al periodo di riferimento, come già informalmente comunicati dal Garante, sarà necessario guardare all'esercizio cui il bilancio fa riferimento e non a quello in corso.

Anche su questo tema va considerata la disciplina transitoria. La menzione nella relazione a bilancio, infatti, costituisce una "nuova" misura di sicurezza (non presente nel vecchio dpr 318/99), ed entra pertanto in vigore a partire dal 1 luglio 2004.

Secondo questa lettura, pertanto, la prima relazione sulla gestione che dovrà menzionare l'avvenuta adozione/aggiornamento sarà quella che verrà effettuata nel 2005, riguardante il bilancio d' esercizio del 2004.

Si segnala, tuttavia, la possibilità che il Garante raccomandi una lettura differente della norma, richiedendo l'obbligo di menzione sin dalla relazione adottata nel 2004. In questo caso si dovrà menzionare nella relazione di accompagnamento l'avvenuta adozione o aggiornamento del documento programmatico effettuata nel corso del 2003 in base alle regole disposizioni del dpr 318/99.

### **3. Il documento programmatico sulla sicurezza: le novità**

Il documento programmatico sulla sicurezza consiste in un insieme di indicazioni e di linee guida in materia di sicurezza nel trattamento dei dati personali effettuati con strumenti elettronici e rappresenta uno strumento utile per valutare la situazione aziendale in materia di trattamento dei dati e predisporre procedure ed azioni a garanzia della sicurezza nel trattamento.

In base al Codice il **documento programmatico sulla sicurezza costituisce misura minima nel trattamento di dati sensibili o giudiziari effettuati mediante strumenti elettronici**. La mancata adozione del documento, pertanto, comporta conseguenze di natura penale e determina la fattispecie contravvenzionale di omessa adozione di misure di sicurezza (art. 169).

Si ricorda, tuttavia, che in caso di omessa adozione delle misure di sicurezza il titolare può avvalersi della procedura di ravvedimento operoso prevista dal secondo comma dell'art. 169, in base al quale *"all'autore del reato, all'atto di accertamento o, nei casi complessi, anche con successivo atto del Garante, è impartita una prescrizione fissando un termine per la regolarizzazione non eccedente il periodo di tempo tecnicamente necessario (...) comunque non superiore a sei mesi. Nei sessanta giorni successivi allo scadere del termine, se risulta l'adempimento della prescrizione, l'autore del reato è ammesso dal Garante a pagare una somma pari al quarto del massimo dell'ammenda stabilita per la contravvenzione"*.

Pertanto per l'estinzione del reato è necessario che l'autore:

- regolarizzi la propria situazione adeguando le misure di sicurezza interne in base alle prescrizioni del Garante;
- proceda al pagamento dell'ammenda.

Il contenuto del documento programmatico in base alla normativa vigente presenta alcune novità che sono diretta conseguenza delle innovazioni in materia di sicurezza disposte dal Codice. La struttura e le funzioni del documento, tuttavia, restano inalterate rispetto al passato.

Nel nuovo documento programmatico, pertanto, dovranno essere descritti anche i criteri e le modalità previste per il **ripristino dei dati sensibili o giudiziari** in seguito a distruzione o a danneggiamento. Si dovranno inoltre specificare le misure previste per la protezione dei dati sullo stato di salute e la vita sessuale.

Anche le disposizioni circa gli **interventi formativi per gli incaricati** sono maggiormente dettagliate e devono ora riguardare:

- i rischi che incombono sui dati;

- le misure disponibili per prevenire eventi dannosi;
- i principali aspetti della disciplina sul trattamento dei dati personali in rapporto alle relative attività e responsabilità collegate al trattamento svolto;
- le modalità per aggiornarsi sulle misure minime adottate dal titolare.

Nel documento programmatico, inoltre, si prevedono **misure di tutela e garanzia** nel caso in cui i trattamenti siano affidati all'esterno della struttura.

**Si ricorda che le misure di sicurezza che il disciplinare tecnico prescrive sono quelle minime. Pertanto in casi specifici, a seconda sarà opportuno prevedere nel documento programmatico misure ulteriori, tali da poter essere considerate idonee.**

È il caso ad esempio, dei programmi antivirus, che in base al disciplinare tecnico vanno aggiornati ogni 6 mesi. È evidente che tale adempimento, per essere considerato idoneo, andrà effettuato con una frequenza ben più elevata rispetto a quanto prescritto dal disciplinare tecnico.

In altri casi, al contrario, il livello individuato come misura minima di protezione è talmente alto da poter essere considerato come misura idonea. Si pensi, a tal proposito, alle regole che dispongono l'adozione di password della grandezza minima di 8 caratteri, prescrivendo in tal modo uno standard ben più robusto rispetto a quello attualmente in uso.

#### **4. I prossimi adempimenti in materia di sicurezza**

Le nuove misure minime di sicurezza individuano uno standard di tutela più elevato rispetto al passato. Il Codice contiene disposizioni transitorie per consentire ai titolari l'adeguamento delle misure di sicurezza alle nuove prescrizioni contenute dalla legge. In base all'art. 180 del Codice, infatti, **le nuove misure minime di sicurezza devono essere adottate entro il**.

Si ricordano i prossimi adempimenti in materia di misure di sicurezza:

*Tab. 2 - Adempimenti in materia di sicurezza*

<b>31 marzo 2004</b>	Aggiornamento del documento programmatico sulla sicurezza sulla base delle misure di sicurezza già dettate dal dpr 318/99
<b>31 dicembre 2004</b>	Adozione delle misure minime di sicurezza "nuove"
<b>31 marzo 2005</b>	Adozione del documento programmatico sulla sicurezza sulla base delle nuove misure del Codice
<b>2005</b>	Obbligo di menzione nella relazione sulla gestione (riferito al bilancio 2004)

Il Codice contiene ulteriori disposizioni transitorie per i titolari che, non disponendo di adeguata strumentazione elettronica, possono avere maggiori difficoltà per l'adozione delle misure di sicurezza entro il termine previsto.

In questo caso il titolare ha la facoltà di descrivere tali ragioni in un documento a data certa. Tale documento non va inviato al Garante ma deve essere conservato presso la propria struttura ed esibito in caso di controlli e verifiche.

**È importante tenere distinta la possibilità di beneficiare di una proroga dall'obbligo di procedere alla redazione del documento programmatico sulla sicurezza. L'obbligo di adottare/aggiornare il documento programmatico, infatti, sussiste anche nel caso in cui si intenda beneficiare della proroga.**

Nella tabella successiva si ricorda la differente tempistica per chi beneficia della proroga disposta dal Codice.

*Tab. 3 - La tempistica per chi non dispone di strumentazione elettronica adeguata*

<b>31 marzo 2004</b>	Aggiornamento del documento programmatico sulla sicurezza sulla base delle misure di sicurezza già dettate dal dpr 318/99
<b>31 dicembre 2004</b>	Adozione delle possibili misure di sicurezza (tali da evitare un incremento dei rischi per i dati) da valutarsi in base agli strumenti elettronici posseduti
<b>30 giugno 2004</b>	Compilazione di un documento a data certa in cui si descrivono le ragioni tecniche che impediscono, in tutto o in parte, l'immediata attuazione delle misure minime previste dal Codice
<b>1 gennaio 2005</b>	Adeguamento degli strumenti elettronici ed adozione delle misure minime di sicurezza "nuove"
<b>31 marzo 2005</b>	Adozione del documento programmatico sulla sicurezza sulla base delle nuove misure del Codice
<b>2005</b>	Obbligo di menzione nella relazione sulla gestione (riferito al bilancio 2004)