Firenze 4 Giugno 2011
E-Privacy 2011

Il principio di Responsabilità
Parere 3/2010
del Gruppo ex art. 29
adottato il 13 luglio 2010 (wp 173)

Avv. Monica Gobbato

www.monicagobbato.it

Principio di Responsabilità già menzionato nel WP 168 del 1 dicembre 2009

Il Gruppo ritiene opportuno introdurre nel quadro globale **un principio di responsabilità.** In conformità a tale principio, i responsabili del trattamento sarebbero tenuti a effettuare le misure necessarie per garantire che i principi di fondo e gli obblighi della direttiva in vigore siano rispettati.. Tale disposizione permetterebbe di ampliare la necessità di porre in **atto politiche e meccanismi per rendere efficaci i principi di merito e gli obblighi della direttiva in vigore.** Inoltre, il principio di responsabilità richiede responsabili del trattamento per avere interno meccanismi necessari in atto per dimostrare la conformità alle parti interessate esterne, compresi DPA nazionale.

Effetto Diluvio

Da tempo stiamo assistendo ad un cosiddetto "**effetto diluvio",** con un continuo aumento della quantità di dati personali esistenti, elaborati e ulteriormente trasferiti. Questo fenomeno è favorito sia dai progressi tecnologici, vale a dire lo sviluppo dei sistemi di informazione e di comunicazione, sia dalla crescente capacità degli utenti di impiegare le tecnologie e interagire con esse. Con l'aumento della quantità di dati trasferiti in tutto il mondo, aumentano anche i rischi di abuso

Aumento del valore

La quantità sempre crescente di dati personali è accompagnata da un **aumento del loro valore in termini sociali, politici ed economici.** In alcuni settori, soprattutto in ambiente online, i dati personali sono diventati *de facto* la valuta di scambio per i contenuti online. Nel contempo, da un punto di vista sociale, **vi è un crescente riconoscimento della protezione dei dati come valore sociale.** In sintesi, **via via che i dati personali diventano sempre più preziosi per i responsabili del trattamento in tutti i settori, anche i cittadini, i consumatori e la società in generale sono sempre più consapevoli della loro rilevanza.** Questo fatto rafforza a sua volta la necessità di applicare misure rigorose per salvaguardarli

Conseguenze devastanti

Da quanto precede consegue che la violazione della privacy può avere notevoli ripercussioni negative per i responsabili del trattamento Potenziali anomalie nelle applicazioni di governo elettronico e di sanità elettronica avranno **conseguenze devastanti** sia in termini economici **sia, soprattutto, in termini di reputazione**. Pertanto, ridurre al minimo i rischi, costruire e mantenere una buona reputazione e garantire la fiducia dei cittadini e dei consumatori stanno diventando compiti fondamentali dei responsabili del trattamento in tutti i settori.

Ridurre al minimo rischi giuridici, economici e di reputazione

In sintesi, da quanto precede emerge l'assoluta **necessità** per i responsabili del trattamento di **applicare misure reali ed efficaci di protezione dei dati** dirette alla corretta gestione della loro protezione, **riducendo inoltre al minimo i rischi giuridici, economici e di reputazione** che possono derivare da pratiche inadeguate in materia. Come ulteriormente illustrato nel prosieguo, i meccanismi basati sulla responsabilità mirano a realizzare tali obiettivi.

Introduzione principio di responsabilita'

Una disposizione generale di questo tipo si incentrerebbe su
due elementi principali:
(i) la necessità che il responsabile del trattamento **adotti misure appropriate ed efficaci** per attuare i principi di protezione dei dati;
(ii) **la necessità di dimostrare, su richiesta, che sono state adottate misure appropriate ed efficaci.** Pertanto, il responsabile del trattamento deve fornire la prova di quanto esposto al punto (i).

Il primo elemento imporrebbe ai Titolari del trattamento di attuare misure appropriate.

L'attuazione di tali misure e processi può anche avvenire in maniera efficace attraverso **l'attribuzione di responsabilità e la formazione del personale** impegnato nelle operazioni di trattamento. In particolare, conformemente all'articolo 18 della direttiva, i responsabili del trattamento devono essere incoraggiati. Si dovrebbe caldeggiare in ogni caso **l'attribuzione di responsabilità a diversi livelli dell'organizzazione,** in modo da renderle effettive.

Verificare efficacia Misure

I Titolari dovrebbero garantire che le misure pratiche attuate siano efficaci. Nel caso di trattamenti di dati di maggiori dimensioni, più complessi o ad alto rischio, **l'efficacia delle misure adottate dovrebbe essere verificata periodicamente.** Esistono diversi modi per valutare l'efficacia (o inefficacia) delle misure: **monitoraggio, audit interni ed esterni, ecc.**

In considerazione delle osservazioni svolte finora, il Gruppo di lavoro articolo 29 ha formulato una disposizione sostanziale che potrebbe essere introdotta in un quadro legislativo globale, il cui testo recita::

Applicazione dei principi di protezione dei dati

1. Il responsabile del trattamento ***attua misure appropriate ed efficaci*** *per garantire che i principi e gli obblighi stabiliti nella direttiva siano rispettati.*

2 Su richiesta dell'autorità di vigilanza, il responsabile del trattamento ***dimostra la conformità*** *con il paragrafo 1.*

Il principio generale di responsabilità proposto evita volutamente di precisare nei dettagli il tipo di misure da attuare. Ciò solleva le seguenti due questioni fondamentali interconnesse: *(i)* quali misure comuni soddisferebbero il principio di responsabilità? *(ii)* in che modo graduare e adattare le misure a circostanze specifiche?

Le misure: descrizione

1) istituzione di procedure interne *prima* della creazione di nuove operazioni di trattamento dei dati personali (revisione interna, valutazione, ecc.);

2) **formulazione per iscritto di politiche di protezione dei dati** vincolanti da prendere in considerazione e applicare alle nuove operazioni di trattamento dei dati (ad esempio, qualità dei dati, comunicazione, principi di sicurezza, accesso, ecc.), che dovrebbero essere a disposizione degli interessati;

3) **mappatura delle procedure** per garantire la corretta identificazione di tutte le operazioni di trattamento dei dati e gestione di un inventario di dette operazioni;

Le misure: descrizione

4) **nomina di incaricati e di altri responsabili** della protezione dei dati;

5) **adeguata formazione e istruzione del personale** in materia di protezione dei dati. Il personale in questione dovrebbe includere gli incaricati (responsabili) del trattamento dei dati personali (come i direttori delle **risorse umane), ma anche dirigenti e sviluppatori in campo informatico, e direttori di unità commerciali.**

6)Dovrebbero essere **stanziate risorse sufficienti** per la gestione della privacy, ecc.;

7) creazione di **procedure trasparenti per gli interessati finalizzate alla gestione delle richieste di accesso, rettifica e cancellazione;**

8) istituzione di un **meccanismo interno di gestione dei reclami;**

Le misure: descrizione

9) **definizione di procedure interne** per la gestione e la comunicazione efficace di violazioni della sicurezza;
10) **effettuazione di valutazioni d'impatto sulla privacy,** in circostanza specifiche;
11) attuazione e controllo delle procedure di verifica per assicurare che tutte le misure esistano non solo sulla carta, ma siano applicate e funzionino nella pratica (**audit interni o esterni ecc.**).

Si potrebbe anche prevedere un approccio complementare al principio generale di responsabilità, secondo cui il quadro normativo includerebbe non solo un principio generale di responsabilità, ma anche un elenco illustrativo di misure che potrebbero essere incoraggiate a livello nazionale.

Tale elenco esemplificativo sarebbe ovviamente soltanto un complemento all'obbligo giuridico generale di adottare le misure appropriate.

Tali misure potrebbero includere:

a) ***l'attuazione di procedure di prevenzione e di individuazione delle violazioni, che potrebbero basarsi sui modelli standardizzati*** *di governance e/o di gestione della sicurezza dell'informazione;*

b) ***la nomina di uno o più Responsabili per la protezione dei dati o della privacy dotati di qualifiche, risorse e competenze adeguate a esercitare la loro funzione di sorveglianza in modo appropriato;***

Misure idonee caso per caso

Le misure da applicare **devono essere determinate in funzione dei fatti e delle circostanze di ciascun caso specifico, con particolare attenzione al rischio inerente al trattamento e al tipo di dati.** Un approccio uguale per tutti avrebbe il solo effetto di costringere i responsabili del trattamento all'interno di strutture inadatte e si rivelerebbe quindi fallimentare.

Potrebbe anche essere utile sviluppare **un *programma modello per la conformità dei dati***,

Efficacia delle Misure

Esistono vari metodi a disposizione dei responsabili del trattamento per valutare l'efficacia (o l'inefficacia) delle misure. Per il trattamento di dati di maggiori dimensioni, più complesso e ad alto rischio, gli **audit interni ed esterni** sono metodi comuni di verifica. il modo in cui un responsabile del trattamento deve assicurare l'efficacia delle misure dipende dalla sensibilità dei dati, dalla quantità dei dati trattati e dai particolari rischi che il trattamento comporta

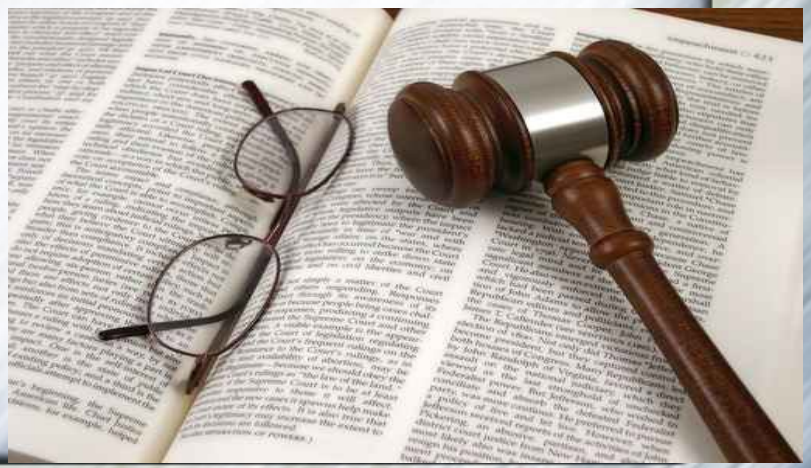
I responsabili del trattamento **dovranno essere in grado di dimostrare alle autorità se e come hanno attuato le misure. L**e autorità disporranno di informazioni altamente rilevanti in materia di conformità e **potranno in seguito utilizzare tali informazioni nel contesto delle loro azioni di verifica** dell'applicazione. **Inoltre, se tali informazioni non sono fornite su richiesta, l**e **autorità di protezione dei dati avranno un motivo per agire immediatamente contro i responsabili** del trattamento, indipendentemente dalla presunta violazione di altri principi basilari di protezione dei dati.

Persone competenti

Saranno indispensabili in questo settore persone altamente competenti, **dotate di approfondite conoscenze tecniche e giuridiche in materia di protezione dei dati, nonché di capacità di comunicare, formare il personale, elaborare e attuare politiche e svolgere audit.**

Sanzioni

Il sistema proposto può funzionare solo se le autorità di protezione dei dati sono dotate di poteri sanzionatori di una certa entità. In particolare, quando e se i responsabili del trattamento non riescono a soddisfare il principio di responsabilità, sorge la necessità di **sanzioni appropriate.**



Lo sviluppo di sistemi di certificazione

Nel lungo periodo, la disposizione sulla responsabilità potrebbe favorire lo s**viluppo di programmi o sigilli di certificazione.** Tali programmi contribuirebbero a dimostrare che un responsabile del trattamento ha rispettato la disposizione e che, quindi, ha definito e attuato misure appropriate che sono state periodicamente sottoposte a revisione. Vari fattori, illustrati di seguito, potrebbero favorire tale sviluppo.

La regolamentazione dei sistemi di certificazione

Le stesse ragioni che favoriscono lo sviluppo di servizi di certificazione avvalorano la necessità che tali servizi siano regolamentati. Infatti, se tali servizi sono intesi a fornire prove affidabili di conformità in termini di protezione dei dati (alle autorità di protezione dei dati, ai responsabili del trattamento e ai consumatori in generale) e a funzionare correttamente nel mercato interno, risultano necessarie norme disciplinanti la fornitura di tali servizi

L'obbligo di attuare tali misure dovrebbe applicarsi ai responsabili del trattamento di tutti i settori **(pubblico e privato)** ed essere adattabile, di modo che il tipo di misure sia adeguato ai rischi presentati dal trattamento e alla natura dei dati.

Grazie per l’attenzione

Avv. Monica Gobbato

gobbatomonica@tiscali.it

WWW.MONICAGOBBATO.IT