
Privacy ed omissione delle misure minime di sicurezza dei dati e dei sistemi

di [Luigi Risolo](#)

Publicato il 18 Maggio 2010

le conseguenze del mancato rispetto delle minimali misure relative alla "privacy"

La Sicurezza dei dati e dei sistemi: premessa

Le misure minime di sicurezza, sancite nel Capo II, del Titolo V intitolato della "Sicurezza dei dati e dei sistemi", del Decreto Legislativo 30 Giugno 2003, n. 196 (Codice in materia di protezione dei dati personali), impongono in ragione della tutela dei dati personali trattati dai cosiddetti "titolari" del trattamento (ovvero tutti gli operatori economici pubblici e privati) l'adozione di idonee e preventive misure volte a contrastare 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" (art. 33 del D. Lgs. 196/2003).

La mancata adozione di tali misure comporta la reclusione fino a due anni, così come sancito dall'art. 169 del D. Lgs. 196/2003 ed in virtù delle modifiche apportate in ultimo dal Decreto Legge n. 135 del 2009, rimarcando in diritto ed in fatto la sanzione esclusivamente penale di fronte al mancato rispetto della norma. Pertanto, se nella precedente formulazione dell'art. 169, comma 1, (del decreto sulla privacy) era prevista, anche, l'ammenda, nell'attuale disposto viene sancito, in via esclusiva, quale regime sanzionatorio: la reclusione. Appare evidente, di conseguenza, l'importanza che il legislatore ha voluto attribuire agli obblighi in tema di privacy e precipuamente ai risvolti applicativi di codesta parte del "Codice in materia di protezione dei dati personali".

Misure minime di sicurezza dei dati di terzi e dei sistemi: normativa.

Le attività economiche nonché gli enti pubblici e privati che si trovano a trattare dati personali di terzi

devono adottare le misure di sicurezza così come sancito dagli articoli 33, 34, 35 e 36 del D. Lgs. n. 196/2003 e che vengono di seguito testualmente riportati:

Art. 33. Misure minime

1. Nel quadro dei più generali obblighi di sicurezza di cui all'articolo 31, o previsti da speciali disposizioni, i titolari del trattamento sono comunque tenuti ad adottare le misure minime individuate nel presente capo o ai sensi dell'articolo 58, comma 3, volte ad assicurare un livello minimo di protezione dei dati personali.

Art. 34. Trattamenti con strumenti elettronici

1. Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime: a) autenticazione informatica; b) adozione di procedure di gestione delle credenziali di autenticazione; c) utilizzazione di un sistema di autorizzazioni; 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; g) tutela 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 identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari. 1-bis. Per i soggetti che trattano soltanto dati personali non sensibili e che trattano come unici dati sensibili quelli costituiti dallo stato di salute o malattia dei propri dipendenti e collaboratori anche a progetto, senza indicazione della relativa diagnosi, ovvero dall'adesione ad organizzazioni sindacali o a carattere sindacale, la tenuta di un aggiornato documento programmatico sulla sicurezza è sostituita dall'obbligo di autocertificazione, resa dal titolare del trattamento ai sensi dell'articolo 47 del testo unico di cui al decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, di trattare soltanto tali dati in osservanza delle altre misure di sicurezza prescritte. In relazione a tali trattamenti, nonché a trattamenti comunque effettuati per correnti finalità amministrative e contabili, in particolare presso piccole e medie imprese, liberi professionisti e artigiani, il Garante, sentito il Ministro per la semplificazione normativa, individua con proprio provvedimento, da aggiornare periodicamente, modalità semplificate di applicazione del disciplinare tecnico di cui all'Allegato B) in ordine all'adozione delle misure minime di cui al comma 1.

Art. 35. Trattamenti senza l'ausilio di strumenti elettronici

1. Il trattamento di dati personali effettuato senza l'ausilio di strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime: a) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative; b) previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti; c) 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.

Art. 36. Adeguamento

1. Il disciplinare tecnico di cui all'allegato B), relativo alle misure minime di cui al presente capo, è aggiornato periodicamente con decreto del Ministro della giustizia di concerto con il Ministro per le innovazioni e le tecnologie e il Ministro per la semplificazione normativa, in relazione all'evoluzione tecnica e all'esperienza maturata nel settore.

Regime sanzionatorio in caso di mancata adozione delle misure minime di sicurezza dei dati e dei sistemi

Il regime sanzionatorio per la mancata adozione delle misure minime di sicurezza ha subito le modifiche in seguito al Decreto Legge del 30 Dicembre 2008 n. 207 – “proroga di termini previsti da disposizioni legislative e disposizioni finanziarie urgenti” -convertito con la Legge n. 14 del 27 Febbraio 2009, art. 44, avente ad oggetto “Disposizioni in materia di tutela della riservatezza”, il cui testo è in vigore dal 25 Novembre 2009 e, ancora, modificato dal Decreto Legge del 25 Settembre 2009 n. 135, di cui all’art. 20 bis, comma 9 il quale sancisce che “L'[articolo 169 del decreto legislativo 30 giugno 2003, n. 196](#), e' cosi' modificato: a) nel comma 1, sono soppresse le parole da:

“o con l'ammenda da” fino alla fine del comma; b) nel comma 2, le parole: “quarto del massimo dell'ammenda stabilita per la contravvenzione” sono sostituite dalle seguenti: “quarto del massimo della sanzione stabilita per la violazione amministrativa”.

Pertanto alla luce del nuovo disposto normativo, per chi omette di adottare le misure minime di sicurezza sarà applicato l’articolo n. 169 del D. Lgs. n. 196/2003, il quale, nella nuova formulazione così sancisce:

Art. 169. Misure di sicurezza

1. Chiunque, essendovi tenuto, omette di adottare le misure minime previste dall'articolo 33 è punito con l'arresto sino a due anni. 2. All'autore del reato, all'atto dell'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, prorogabile in caso di particolare complessità o per l'oggettiva difficoltà dell'adempimento e comunque non superiore a sei mesi. Nei sessanta giorni successivi allo scadere del termine, se risulta l'adempimento alla prescrizione, l'autore del reato è ammesso dal Garante a pagare una somma pari al quarto del massimo della sanzione stabilita per la violazione amministrativa. L'adempimento e il pagamento estinguono il reato. L'organo che impartisce la prescrizione e il pubblico ministero provvedono nei modi di cui agli articoli 21, 22, 23 e 24 del decreto legislativo 19 dicembre 1994, n. 758, e successive modificazioni, in quanto applicabili.

Considerazioni Finali

La mancata adozione delle misure minime di sicurezza implica la presunzione che le stesse non siano state eseguite praticamente o addirittura non siano nemmeno previste in quanto è possibile che non sia stato realizzato e validato il Documento Programmatico di Sicurezza; in più va rilevato che gli adempimenti previsti dal legislatore in tema di misure minime (Documento Programmatico di Sicurezza) devono avere il fine di ridurre al minimo i rischi derivanti da:

- distruzione o perdita, anche accidentale, dei dati;
- accesso non autorizzato (eseguito da soggetti estranei al trattamento dei dati) verso i dati;
- trattamento dei dati non consentito o non conforme alle finalità della raccolta;
- modifica (parziale o totale) dei dati per effetto di interventi non autorizzati o non conformi alla regole.

Del resto il confine tra la previsione nonché adozione delle suddette misure e l'adempimento del Documento programmatico di Sicurezza è assai sottile in quanto le prime sono parte integrante del DPS, e quest'ultimo è fondato proprio su di esse; una complementarità rilevante al punto che si è inteso rafforzare il regime sanzionatorio sotto il profilo penale.

18 maggio 2010 Luigi Risolo