



DFLabs Business Security Blueprint.

A premier on IT Security Governance

Breve analisi modifiche art.34 Dlgs 196-2003

1.	Premessa.....	1
2.	Descrizione del modus operandi.....	1
3.	Alcune precisazioni preliminari.....	2
4.	Analisi generale della situazione.....	5
5.	Possibili rischi.....	8
6.	Conclusioni.....	9

1. Premessa

In questa sintesi verrà analizzata, in via sintetica, la reale portata delle modifiche recentemente introdotte all'art.34 del D.Lgs. n.196/2003, anche alla luce delle varie notizie riportate dai media.

La questione fondamentale è quella della applicabilità della modifica non solamente ai soggetti organizzati in maniera semplice e di dimensioni piccole e medio piccole, ma – se del caso – anche a soggetti di dimensioni maggiori e comunque più articolati da un punto di vista organizzativo.

L'analisi si baserà fondamentalmente sul dettato della normativa

2. Descrizione del modus operandi

Fermo restando quanto in precedenza scritto, la posizione assunta è, in linea di massima, quella del consulente che, in "scienza e coscienza", debba consigliare ad un proprio Cliente, se adottare o meno la dichiarazione sostitutiva prevista dalla normativa così come modificata, ovvero continuare ad agire come se la modifica non fosse avvenuta.

Ovviamente una cosa è valutare il rapporto costi/benefici, nel senso che nel prosieguo verrà meglio spiegato (rapporto tra omissioni / risparmio organizzativo / costo delle sanzioni pecuniarie / costo delle sanzioni non pecuniarie / danni di immagine indiretti).

3. Alcune precisazioni preliminari

Per una completa comprensione del presente documento si presuppone la conoscenza dei concetti di base collegati alla applicazione dell'art.34 del D.Lgs. n.196/2003, alle responsabilità connesse alla mancata adozione delle regole da esso poste, sia in sede civile, sia in sede penale, sia in sede "amministrativa", intendendo in questo caso le responsabilità amministrative nei confronti del Garante.

Per comodità di lettura, riporto qui di seguito il testo degli articoli ai quali fa riferimento la norma in esame:

D.Lgs. n.196/2003 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 autorizzazione;*
- 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, il ripristino 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 l'unico dato sensibile e' costituito dallo stato di salute o malattia dei propri dipendenti senza indicazione della relativa diagnosi, l'obbligo di cui alla lettera g) del comma 1 e di cui al

punto 19 dell'Allegato B e' sostituito dall'autocertificazione, resa dal titolare del trattamento ai sensi dell'articolo 47 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, di trattare soltanto dati personali non sensibili, che l'unico dato sensibile e' costituito dallo stato di salute o malattia dei propri dipendenti senza indicazione della relativa diagnosi, e che il trattamento di tale ultimo dato e' stato eseguito in osservanza delle misure di sicurezza richieste dal presente codice nonche' dall'Allegato B).».

2. Entro due mesi dall'entrata in vigore della legge di conversione del presente decreto-legge, con un aggiornamento del disciplinare tecnico adottato nelle forme del decreto del Ministro della giustizia di concerto con il Ministro per la pubblica amministrazione e l'innovazione e con il Ministro per la semplificazione normativa, ai sensi dell'articolo 36 del decreto legislativo 30 giugno 2003, n. 196, sono previste modalita' semplificate di redazione del documento programmatico per la sicurezza di cui alla lettera g) del comma 1 dell'articolo 34 e di cui al punto 19 dell'Allegato B al decreto legislativo 30 giugno 2003, n. 196 per le correnti finalita' amministrative e contabili.

3. Qualora il decreto di cui al comma 2 non venga adottato entro il termine ivi indicato, la disciplina di cui al comma 1 si applica a tutti i soggetti di cui al comma 2.

D.Lgs. n.196/2003 – Punto 19 dell'allegato B

19. Entro il 31 marzo di ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari redige anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza contenente idonee informazioni riguardo:

19.1. l'elenco dei trattamenti di dati personali;

19.2. la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;

19.3. l'analisi dei rischi che incombono sui dati;

19.4. le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;

19.5. la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui al successivo punto 23;

19.6. la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di

mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;

19.7. la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;

19.8. per i dati personali idonei a rivelare lo stato di salute e la vita sessuale di cui al punto 24, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

D.P.R. 445/2000 - Articolo 47 (R) Dichiarazioni sostitutive dell'atto di notorietà

1. L'atto di notorietà concernente stati, qualità personali o fatti che siano a diretta conoscenza dell'interessato è sostituito da dichiarazione resa e sottoscritta dal medesimo con la osservanza delle modalità di cui all'articolo 38. (R)

2. La dichiarazione resa nell'interesse proprio del dichiarante può riguardare anche stati, qualità personali e fatti relativi ad altri soggetti di cui egli abbia diretta conoscenza. (R)

3. Fatte salve le eccezioni espressamente previste per legge, nei rapporti con la pubblica amministrazione e con i concessionari di pubblici servizi, tutti gli stati, le qualità personali e i fatti non espressamente indicati nell'articolo 46 sono comprovati dall'interessato mediante la dichiarazione sostitutiva di atto di notorietà. (R)

4. Salvo il caso in cui la legge preveda espressamente che la denuncia all'Autorità di Polizia Giudiziaria è presupposto necessario per attivare il procedimento amministrativo di rilascio del duplicato di documenti di riconoscimento o comunque attestanti stati e qualità personali dell'interessato, lo smarrimento dei documenti medesimi è comprovato da chi ne richiede il duplicato mediante dichiarazione sostitutiva. (R)

D.P.R. 445/2000 - Articolo 76 (L) Norme penali

1. Chiunque rilascia dichiarazioni mendaci, forma atti falsi o ne fa uso nei casi previsti dal presente testo unico è punito ai sensi del codice penale e delle leggi speciali in materia.

2. L'esibizione di un atto contenente dati non più rispondenti a verità equivale ad uso di atto falso.

3. Le dichiarazioni sostitutive rese ai sensi degli articoli 46 e 47 e le dichiarazioni rese per conto delle persone indicate nell'articolo 4, comma 2, sono considerate come fatte a pubblico ufficiale.

4. Se i reati indicati nei commi 1, 2 e 3 sono commessi per ottenere la nomina ad un pubblico ufficio o l'autorizzazione all'esercizio di una professione o arte, il giudice, nei casi più

gravi, può applicare l'interdizione temporanea dai pubblici uffici o dalla professione e arte.

D.Lgs. n.196/2003 Art. 168 Falsità nelle dichiarazioni e notificazioni al Garante

1. Chiunque, nella notificazione di cui all'articolo 37 o in comunicazioni, atti, documenti o dichiarazioni resi o esibiti in un procedimento dinanzi al Garante o nel corso di accertamenti, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da sei mesi a tre anni.

D.Lgs. n.196/2003 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 o con l'ammenda da diecimila euro a cinquantamila euro.

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 dell'ammenda stabilita per la contravvenzione. 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.

4. Analisi generale della situazione

In linea di principio, il combinato disposto degli articoli appena riportati può essere sinteticamente letto nel seguente modo “*Se il titolare tratta soltanto dati personali non sensibili e l'unico dato sensibile e' costituito dallo stato di salute o malattia dei propri dipendenti senza indicazione della relativa diagnosi, può non redigere il documento programmatico della sicurezza e sostituire tale redazione con una autodichiarazione effettuata ai sensi dell'art.47 del DPR 445/2000*”

Pertanto, dovranno ricorrere contemporaneamente e contestualmente le seguenti condizioni affinché la norma possa essere applicabile:

- a. Il titolare, direttamente ovvero attraverso i responsabili del trattamento, deve trattare esclusivamente dati non sensibili (ma non “non giudiziari”);
- b. l'unico dato sensibile e' costituito dallo stato di salute o malattia dei propri dipendenti senza indicazione della relativa diagnosi

Si tratta ora di analizzare quali potrebbero essere le categorie dei soggetti che possano usufruire della “semplificazione”, mentre nel prosieguo si effettueranno dei cenni alle conseguenze di una errata analisi della propria situazione; l'analisi e le relative esemplificazioni si baseranno oltre che sui dati comunemente reperibili anche sulla personale esperienza del sottoscritto.

La premessa indispensabile è che il titolare che decida di accedere alla procedura di semplificazione sia ben a conoscenza dei dati trattati dalla propria organizzazione.

A. PROFESSIONI LIBERALI:

- a. Medici ed assimilabili: esclusi per definizione
- b. Ingegneri / Architetti / Geometri: potrebbero usufruire della semplificazione a patto di rispettare pienamente il disposto della norma (in sostanza, solamente per i propri dipendenti e purché, per esempio, non trattino anche dati giudiziari [esclusi dalla semplificazione])
- c. Commercialisti / Consulenti del Lavoro / ecc.: potrebbero usufruire della semplificazione solamente per i propri dipendenti e purché, per esempio, non trattino anche dati giudiziari [esclusi dalla semplificazione]. Ovviamente potranno, in proprio, accedere alla semplificazione solamente dopo aver accertato che anche le tipologie di dati trattati per conto dei terzi (i propri clienti) siano totalmente e pienamente contenuti nella previsione normativa
- d. Avvocati: esclusi per definizione
- e. Consulenti in generale: potrebbero usufruire della semplificazione a patto di rispettare pienamente il disposto della norma (in sostanza, solamente per i propri dipendenti e purché, per esempio, non trattino anche dati giudiziari [esclusi dalla semplificazione])

B. IMPRESE:

- a. Artigiane: potrebbero usufruire della semplificazione a patto di rispettare pienamente il disposto della norma (in sostanza, solamente per i propri dipendenti e purché, per esempio, non trattino anche dati giudiziari [esclusi dalla semplificazione])
- b. Piccole imprese (sino a 15 dipendenti): potrebbero usufruire della semplificazione a patto di rispettare pienamente il disposto della norma (in sostanza, solamente per i propri dipendenti e purché, per esempio, non trattino anche dati giudiziari [esclusi dalla semplificazione])
- c. Medie imprese: a causa della complessità organizzativa ben difficilmente potranno ricadere nell'ipotesi prevista per le piccole imprese;
- d. Grandi imprese: a causa della complessità organizzativa ben difficilmente potranno ricadere nell'ipotesi prevista per le piccole imprese;
- e. Imprese emanazione di soggetti giuridici non italiani: esclusi per definizione

C. ASSOCIAZIONI:

- a. Onlus ed assimilabili: in linea di massima escluse per definizione (potrebbero usufruire della semplificazione a patto di rispettare pienamente il disposto della norma in sostanza, solamente per i propri dipendenti e purché, per esempio, non trattino anche dati giudiziari [esclusi dalla semplificazione])
- b. Associazioni ex art.36 C.C.: in linea di massima escluse per definizione (potrebbero usufruire della semplificazione a patto di rispettare pienamente il disposto della norma in sostanza, solamente per i propri dipendenti e purché, per esempio, non trattino anche dati giudiziari [esclusi dalla semplificazione])
- c. Partiti politici: in linea di massima esclusi per definizione (potrebbero usufruire della semplificazione a patto di rispettare pienamente il disposto della norma in sostanza, solamente per i propri dipendenti e purché, per esempio, non trattino anche dati giudiziari [esclusi dalla semplificazione])
- d. Altre tipologie di associazioni: in linea di massima escluse per definizione (potrebbero usufruire della

semplificazione a patto di rispettare pienamente il disposto della norma in sostanza, solamente per i propri dipendenti e purché, per esempio, non trattino anche dati giudiziari [esclusi dalla semplificazione])

Il punto sul quale occorre riflettere molto bene è l'esatta definizione e conseguentemente l'esatta portata della norma in esame; in effetti, nella vita di tutti i giorni, è ben difficile che un titolare tratti solamente dati non sensibili (in sostanza solamente dati "normali", non sensibili e non giudiziari); è sufficiente avere una foto¹ di un soggetto perché la possibilità di usufruire della semplificazione sia posta nel nulla.

Inoltre, l'unico dato sensibile del proprio dipendente deve essere necessariamente (e solamente) quello relativo *"allo stato di salute o malattia dei propri dipendenti senza indicazione della relativa diagnosi"*; conseguentemente, solamente i certificati inviati per le assenze dal lavoro (anche se materialmente detenuti dal commercialista, dal consulente del lavoro o soggetto ad essi assimilabile).

Pertanto, appare abbastanza evidente come le ipotesi di applicazione della norma in esame siano marginali o, più esattamente, limitate solamente ai soggetti con organizzazione e strutturazione estremamente semplice e con un numero comunque limitato di dipendenti.

5. Possibili rischi

Un discorso a parte merita l'analisi delle conseguenze di una eventuale errata interpretazione della propria situazione al fine di usufruire della procedura semplificata.

Come è noto, il D.P.S. è solamente uno degli obblighi relativi alla sicurezza, e la mancata o pesantemente incompleta redazione del medesimo integra, con ogni probabilità, il reato previsto dall'art. 169 del D.Lgs. n.196/2003 (Omessa adozione di misure di sicurezza), reato che, per la formulazione e per la connessione sistematica con i principi generali del diritto penale, ben a ragione può non essere limitato al solo

¹ Ricordiamo sempre la definizione di dato sensibile: *d) "dati sensibili", i dati personali idonei 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 i dati personali idonei a rivelare lo stato di salute e la vita sessuale;*

titolare ma anche a tutti i soggetti che, materialmente, abbiano concorso nella mancata adozione delle prescritte misure [*minime*] di sicurezza².

Orbene, la dichiarazione effettuata ai sensi del comma 1-bis del novellato articolo 34 del D.Lgs. n.196/2003, se scientemente effettuata, quanto meno integra i reati previsti dall'art.76 del D.P.R. 445/2000 (a causa del richiamo espresso dell'art.47 del medesimo D.P.R.) e contemporaneamente costituisce – comunque – una omessa adozione delle misure [*minime*] di sicurezza, con le conseguenze in precedenza evidenziate.

In effetti, laddove fosse accertabile (e/o accertata) la volontà di effettuare delle dichiarazioni, per così dire “non vere”, potrebbe agevolmente scattare anche il reato (probabilmente specifico rispetto a quello generale previsto dal D.P.R. 445/2000) previsto dall'art.168 del D.Lgs. n.196/2003.

In ambedue i casi saremmo nell'ipotesi di concorso di reati (con possibile concorso di più persone nella commissione di tali reati); ritengo che la conclusione sia talmente chiara che non meriti ulteriore approfondimento.

Ovviamente non è detto che le ipotesi di reato si debbano poi necessariamente “convertire” in condanne, dipende anche dall'insieme di quello che potrebbe emergere a seguito di una denuncia, una indagine, un esposto, ma è un elemento di rischio che deve necessariamente essere adeguatamente valutato.

6. Conclusioni

Come sempre, diffidare dalle soluzioni semplici ed affidarsi a soggetti di provata capacità ed esperienza e, soprattutto, con elevate capacità di visione complessiva del problema; si tratta di una materia nella quale non è assolutamente possibile inventare alcunché, ma occorre avere solide

(Avv. Luca-M. de Grazia)

² Che, si rammenta, sono da considerarsi come “misure minime di sicurezza”, e nulla hanno a che vedere con quelle previste dall'art.15 del medesimo D.Lgs. n.196/2003



*DFlabs Italy is a company specialized in Information Security Risk Management. With its three practices (Business Security, Compliance and Data Security), DFLabs is one of the most respected company at international level.
www.dflabs.com*