La gestione della privacy dopo l'abolizione del Dps

Pietro Gremigni *Consulente aziendale*

L'art. 45 del decreto semplificazioni dispone il venir meno, dal 10 febbraio 2012, dell'obbligo di redigere il documento programmatico per la sicurezza dei dati trattati (Dps)

Dall'entrata in vigore del decreto legge sulle semplificazioni burocratiche e amministrative e cioè dal 10 febbraio 2012 non sarà più obbligatorio redigere il Documento programmatico per la sicurezza dei dati trattati (Dps).
L'obbligo di redigere tale documento, entro il 31 marzo di ogni anno in caso di eventuali variazioni, è stato introdotto dall'articolo 34, lett. *g*, comma 1 del Codice della privacy (Dlgs n. 196/2003) che riguarda anche le misure minime di sicurezza dei dati personali trattati con strumenti elettronici, quindi in particolare i dati archiviati all'interno di strumenti elettronici come computer, pen drive, Dvd, Cd ecc.
L'articolo 45 del cd. decreto semplificazioni abroga anche il comma 1-*bis* dell'art. 34 del Codice della privacy che aveva introdotto delle semplificazioni e degli esoneri relativamente sempre al Dps, legati alla tipologia dei dati trattati e alla categoria di appartenenza (piccole e medie imprese, artigiani, professionisti).
Inoltre, dall'abrogazione dell'art. 34, comma 1, lett. *g*, cit. consegue - e ciò è espressamente previsto dall'art. 45, comma 1, lett. *d)* del decreto legge n. 5/2012 - l'abrogazione del Disciplinare tecnico di cui all'Allegato B, paragrafi da 19 a 19.8 e 26, del Codice della privacy che descrivono le modalità e i criteri di redazione del Dps.
Viene meno infine l'obbligo del titolare di riferire, nella relazione accompagnatoria del bilancio d'esercizio, se dovuta, l'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza.
L'eliminazione del Dps va indubbiamente incontro all'abolizione di un onere spesso visto dalle imprese come un gravoso impaccio burocratico, ma non elimina affatto gli altri obblighi legati alla sicurezza dei dati personali trattati dal titolare del trattamento. A parte, infatti, i trattamenti dei dati su supporti non informatici (in genere gli archivi cartacei) per i quali non è cambiato nulla, ciò che il Codice della privacy prevede per i dati trattati informaticamente rimane del tutto applicabile.
Passiamo di seguito in rassegna, pertanto, gli obblighi relativi alla sicurezza minima dei dati trattati informaticamente che restano in vigore anche dopo l'abolizione dell'obbligo di redazione del Documento programmatico di sicurezza dei dati trattati (Dps).

Trattamenti informatizzati: adempimenti generali

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 al Dlgs n. 196/2003, le seguenti misure minime (art. 34 Codice della Privacy) e cioè:
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) 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.
Tutti i predetti obblighi generali trovano poi una maggiore specificazione nell'ambito del Disciplinare tecnico di cui all'Allegato B del Codice della privacy e sono posti a carico del titolare del trattamento, del responsabile se designato e dell'incari-

Restano in vigore gli obblighi per garantire le misure minime per la privacy nel trattamento dei dati informatizzati

La tutela della privacy prima e dopo il decreto semplificazioni

Dal 10.2.2012

Obbligo di adottare le misure minime per garantire la sicurezza dei dati trattati informaticamente da parte di tutti i titolari dei trattamenti di dati comuni o sensibili/giudiziari.
Viene abolito l'obbligo di redigere in forma scritta le predette misure minime tramite il documento programmatico della sicurezza

Fino al 9.2.2012

Obbligo di garantire le misure minime per la sicurezza dei dati e di redigere il Dps (con aggiornamento entro il 31 marzo di ogni anno) per la generalità dei datori di lavoro

Per i datori di lavoro che trattavano dati diversi da quelli sensibili (salvo i dati sulla malattia o sull'adesione sindacale) al posto del Dps era possibile rilasciare un'autocertificazione. In ogni caso erano tenuti alla predisposizione delle misure minime.

Per imprese artigiane, piccole e medie imprese e professionisti gestori di dati unicamente per finalità amministrative e contabili il Dps era obbligatorio, ma redatto con modalità semplificate.
In ogni caso erano tenuti alla predisposizione delle misure minime.

cato nei limiti, per quest'ultimo degli specifici profili descritti successivamente.

Autenticazione informatica

Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti. Gli incaricati tenuti possono accedere, in virtù della loro mansione, ai dati personali solo se muniti di una credenziale di accesso (user e password).

Credenziali di accesso - Un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato (impronta digitale, riconoscimento iride ecc.), eventualmente associata a un codice identificativo o a una parola chiave.

Istruzioni

Il titolare del trattamento dei dati e il responsabile devono istruire l'incaricato di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso e a uso esclusivo dell'incaricato stesso.
Una volta impartite le necessarie istruzioni, ricade sugli incaricati la responsabilità dell'eventuale perdita o sottrazione delle credenziali.
La parola chiave per l'accesso (in genere la password) deve essere modificata al primo utilizzo e, successivamente, almeno ogni sei mesi.
In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.
Occorre poi impartire agli incaricati istruzioni circa l'obbligo di non lasciare incustodito il computer o lo strumento elettronico su sui si opera, in modo da evitare che, col semplice abbandono temporaneo del posto di lavoro, terzi non autorizzati possano accedere ai dati personali solo semplicemente consultando i *files* in dotazione.

Assenza dell'incaricato

In caso di prolungata assenza o impedimento dell'incaricato del trattamento dei dati che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, quando le uniche modalità di accesso avvengono tramite credenziali fornite agli incaricati medesimi, devono essere impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici.

In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.

Profili di autorizzazione e lettera di incarico

Secondo il Disciplinare tecnico è possibile individuare dei profili di autorizzazione per ciascun incaricato.

Il profilo di autorizzazione rappresenta l'elenco delle operazioni che l'incaricato può svolgere nell'ambito dei compiti assegnatigli.

È opportuno che i profili vengano attribuiti per iscritto in un documento nel quale ad esempio dovranno essere individuati:

- i dati trattati;
- le modalità cioè il programma con cui vengono trattati i dati;
- lo scopo ossia l'elenco ad esempio dei clienti, fornitori, dipendenti ecc.;
- le regole per il trattamento.

Protezione dei dati

I dati personali trattati con strumenti elettronici devono poi essere protetti contro il rischio di intrusione e dell'azione di programmi di cui all'articolo 615-*quinquies* del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.

Gli aggiornamenti periodici dei programmi di protezione (ad esempio antivirus) degli strumenti elettronici devono essere effettuati almeno annualmente.

In caso di trattamento di dati sensibili o giudiziari l'aggiornamento deve essere effettuato almeno semestralmente.

Il datore di lavoro o il soggetto responsabile devono impartire istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.

Trattamenti esternalizzati

Quando il titolare ossia il datore di lavoro affida all'esterno il trattamento dei dati o di alcuni dati personali, come può avvenire nel caso dell'affidamento degli adempimenti lavoristici ad un consulente, ha diritto di ricevere dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del presente disciplinare tecnico.

Si tratta pertanto di una cautela che il datore di lavoro è tenuto ad adottare (cioè farsi rilasciare una dichiarazione di conformità in modo da essere sollevato da eventuali responsabilità) ma che non esaurisce i compiti che il codice della privacy gli assegna.

Infatti lo stesso Garante della protezione deid ati personali nella *«Guida operativa per redigere il Documento programmatico sulla sicurezza»* per i «trattamenti affidati all'esterno» precisa che il titolare del trattamento affidato all'esterno deve indicare:

- la società,
- l'ente

o

- il consulente

cui è stata affidata l'attività, e il ruolo ricoperto agli effetti della disciplina sulla protezione dei dati personali (titolare o responsabile del trattamento).

Ruolo ricoperto dai soggetti esterni

Si tratta in definitiva dell'annoso problema del ruolo rivestito dai soggetti esterni a cui viene affidato il trattamento: titolare o responsabile.

Cambia moltissimo l'adozione di uno dei due criteri.

Innanzitutto la legge non prevede quale delle due ipotesi prevalga.

Allora sarà il datore di lavoro/titolare del trattamento esternalizzato ad attribuire un ruolo o l'altro.

Assegnare la funzione di semplice responsabile ad esempio ad una software house a trattare i dati per elaborare le buste paga, è operazione complicata in quanto il responsabile si muove all'interno delle istruzioni impartite in modo esplicito, al di fuori delle quali ne risponde il titolare.

Quest'ultimo però non è nella posizione di controllare l'attività dei soggetti esterni e ciò ci fa ritenere più corretto e cautelante affidare la gestione dei dati a soggetti esterni in qualità di titolari del trattamento.

In questo modo saranno i soggetti esterni a dovere adottare a loro volta le misure minime richieste dal più volte citato Disciplinare tecnico e risponderne così in prima persona.