Nuovo Regolamento UE sulla Privacy: cosa cambia per le imprese?

Lo scorso 4 maggio è stato pubblicato sulla gazzetta ufficiale della Comunità Europea il "**Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE** (regolamento generale sulla protezione dei dati)" e dopo 20 giorni dalla sua pubblicazione è divenuto legge europea, pertanto a partire dal 25 maggio 2016 decorrono i due anni di transitorio per l'applicazione del nuovo Regolamento.

Nella pagina Documenti di questo sito è possibile scaricare il testo ufficiale (ora anche per gli utenti non registrati).

Il Garante per la Protezione dei dati personali ha pubblicato un'apposita guida (http://194.242.234.211/documents/10160/5184810/Guida+al+nuovo+Regolamento+europeo+in+materia+di+protezione+dati).

Rispetto al precedente articolo pubblicato su questo sito il 27/04/2016, basato sulla traduzione della proposta di Regolamento approvata dal Parlamento Europeo a dicembre 2015, di cui il presente articolo costituisce un aggiornamento, si rilevano alcune differenze nella traduzione del testo originale inglese in lingua italiana, rispetto all'attuale Codice privacy D.Lgs 196/2003:

- Viene mantenuto il "Titolare del trattamento" (*Data Controller*);
- Viene mantenuto il "Responsabile del Trattamento" (*Data processor*);
- Viene abolito l'Incaricato del trattamento.

Il nuovo Regolamento introdurrà una legislazione in materia di protezione dati uniforme e valida in tutta Europa, affrontando temi innovativi – come il diritto all'oblio e alla portabilità dei dati – e stabilendo anche criteri che da una parte responsabilizzano maggiormente imprese ed enti rispetto alla protezione dei dati personali e, dall'altra, introducono notevoli semplificazioni e sgravi dagli adempimenti per chi rispetta le regole. Il Regolamento UE 679/2016, però, non sarà l'unica fonte legislativa per regolamentare la protezione dei dati personali, infatti le Autorità dei singoli Stati Membri – e quindi il Garante della Privacy per l'Italia – potranno integrare i contenuti del Regolamento dettagliando meglio alcuni aspetti che al momento appaiono poco chiari, introdurre linee guida generali e di settore, regolamentare aspetti particolari, ecc.

A tal proposito occorre ricordare che, con l'uscita del Regolamento 679 non vengono aboliti i provvedimenti del nostro Garante su Videosorveglianza, Amministratori di Sistema, fidelity card, biometria, tracciamento flussi bancari, ecc. Tali provvedimenti probabilmente verranno modificati e/o integrati dal Garante Privacy per aggiornarli ed eventualmente adeguarli alle prescrizioni del Regolamento Europeo 679.

Il Garante Privacy italiano potrà inoltre integrare il Regolamento UE 679 per disciplinare il trattamento di dati personali effettuato per adempiere obblighi di legge italiana e in particolari ambiti, ad esempio quello dei dati sanitari, oppure per definire in modo più dettagliato gli obblighi per le PMI (ovvero per le organizzazioni che occupano meno di 250 dipendenti, per le quali il regolamento 679 ha stabilito delle semplificazioni).

Ma quali sono le principali novità per le imprese nella gestione della privacy a fronte del Regolamento UE?

L'aspetto più significativo è sicuramente il cambio di approccio rispetto al Codice Privacy attualmente in vigore in Italia, ed in particolare all'Allegato B, ovvero al Disciplinare Tecnico delle Misure Minime di Sicurezza. Il nuovo Regolamento Europeo sulla privacy, infatti, non definisce requisiti specificati in termini precisi, come avviene per l'attuale normativa italiana sulla privacy, ma sposta la responsabilità di definire le misure di sicurezza idonee a garantire la privacy dei dati personali trattati sul titolare o responsabile del trattamento, dopo un'attenta analisi dei rischi.

Dunque non ci sono più misure minime, ma solo misure di sicurezza adeguate, progettate dal titolare o responsabile del trattamento dopo aver effettuato l'analisi dei rischi che incombono sui dati personali che si intende trattare. Sottolineiamo quest'ultimo aspetto: le misure di prevenzione vanno poste in atto prima di iniziare il trattamento.

Poiché a livello nazionale la legislazione italiana ed il Garante per la Protezione dei Dati Personali hanno seguito il percorso europeo, a partire dalla Direttiva Europea 46/95, a livello di principi sulla privacy non ci sono differenze significative tra normativa italiana e Regolamento Europeo. Infatti, alcune regole già imposte dal Codice Privacy e dalle successive disposizioni del Garante restano valide, anche se con contorni un po' meno definiti da criteri oggettivi. In sostanza:

- Viene regolamentato solo il trattamento di dati personali di persone fisiche (non giuridiche) per scopi diversi dall'uso personale.
- Resta una distinzione fra trattamento di dati personali comuni e trattamento di dati c.d. sensibili, anche se la definizione del D.lgs 196/2003 non viene utilizzata nel Regolamento UE 679, lasciando però la possibilità agli Stati membri di stabilire una disciplina particolare in merito.

- Restano gli obblighi di informare l'interessato sull'uso che verrà fatto dei suoi dati personali.
- Restano gli obblighi di ottenere il consenso per i trattamenti non necessari o per i trattamenti di particolari tipi di dati, ad esempio quelli idonei a rivelare lo stato di salute delle persone, le origini razziali, le idee religiose, ecc.

Tra gli elementi che cambiano vi sono sicuramente:

- La denominazione ed i ruoli degli attori: il titolare del trattamento rimane tale, **il responsabile del trattamento è ora responsabile in solido con il titolare per i danni derivanti da un trattamento non corretto**, l'incaricato rimane il soggetto che fisicamente tratta i dati, ma tale ruolo non è delegabile, se non attraverso uno specifico accordo contrattuale. Il responsabile può individuare un proprio rappresentante.
- I dati personali trattati devono essere protetti con misure organizzative e tecniche adeguate a garantirne la riservatezza e l'integrità.
- I diritti dell'interessato sono più ampi e maggiormente tutelati.
- Il responsabile del trattamento deve mettere in atto **misure tecniche ed organizzative** tali da consentirgli di dimostrare che tratta i dati personali in conformità al Regolamento. Tali misure devono seguire lo stato dell'arte e devono derivare dall'analisi dei rischi che incombono sui dati, secondo relativa gravità e probabilità.
- **Privacy by default**: devono essere trattati "per default" solo i dati necessari a perseguire le finalità del trattamento posto in essere dal responsabile dello stesso, ovvero non devono essere trattati dati in eccesso senza che una persona fisica autorizzata lo consenta.
- **Privacy by design**: ogni nuovo trattamento di dati personali dovrà essere progettato in modo da garantire la sicurezza richiesta in base ai rischi a cui è sottoposto prima di essere implementato. Anche i sistemi informatici dovranno essere progettati secondo tale principio.
- Possono esserci più responsabili per un medesimo trattamento che risulteranno, pertanto, corresponsabili di eventuali trattamenti non conformi, ma dovranno stabilire congiuntamente le rispettive responsabilità.
- Le imprese **con sede al di fuori dell'Unione Europea**, che trattano dati personali di interessati residenti nella UE dovranno eleggere una propria organizzazione o entità all'interno della UE che sarà responsabile di tali trattamenti.
- Devono essere mantenuti **registri dei trattamenti** di dati effettuati con le informazioni pertinenti e le relative responsabilità. Tali registri non sono obbligatori per organizzazioni con meno di 250 dipendenti salvo che non trattino dati sensibili (secondo la definizione del Codice della Privacy attualmente in vigore) o giudiziari. Tale discriminante potrà essere meglio specificata da appositi provvedimenti del nostro Garante.
- Il responsabile del trattamento deve notificare all'autorità competente – e, in casi gravi, anche all'interessato – ogni **violazione dei dati** (*data breach*) trattati entro 72 ore dall'evento.

- Quando un trattamento presenta dei rischi elevati per i dati personali degli interessati (i casi specifici dovranno essere esplicitati dall'Autorità Garante), il responsabile del trattamento deve effettuare una **valutazione di impatto preventiva**, prima di iniziare il trattamento.
- Viene introdotta la **certificazione** del sistema di gestione della privacy (le cui modalità dovranno essere meglio definite tramite gli Organismi di Accreditamento Europei, ACCREDIA per l'Italia)..
- È richiesta la designazione di un **Responsabile della Protezione dei Dati** (*Data Protection Officer*) nelle Aziende Pubbliche e nelle organizzazioni che trattano dati sensibili o giudiziari su larga scala oppure che la tipologia di dati trattati e la loro finalità richieda il controllo degli incaricati al trattamento su larga scala.

Proprio quest'ultimo punto, variato rispetto alle precedenti versioni del Regolamento, farà molto discutere, poiché non stabilisce criteri precisi ed oggettivi (cosa significa "su larga scala"?) per l'adozione di tale figura professionale, di competenze adeguate a garantire una corretta applicazione della normativa sulla privacy. Il Responsabile per la Protezione dei Dati dovrà essere correttamente informato dal Responsabile del Trattamento su tutte le attività che riguardano la privacy e dovrà disporre di risorse adeguate per svolgere il proprio compito e mantenere le sue competenze adeguate al ruolo che ricopre. Egli dovrà inoltre essere indipendente dalle altre funzioni dell'organizzazione e riferire solamente all'alta direzione.

La sicurezza dei dati – in termini di riservatezza, integrità e disponibilità – deve essere garantita in funzione del rischio che corrono i dati stessi, dei costi delle misure di sicurezza e dello stato dell'arte della tecnologia. Pertanto le password di almeno 8 caratteri variate almeno trimestralmente, l'antivirus aggiornato, il firewall e l'aggiornamento del sistema operativo potrebbero essere misure adeguate per determinati trattamenti, ma non per altri, oppure in determinate organizzazioni, ma non in altre, in ogni caso lo potrebbero essere oggi, ma non domani quando il progresso tecnologico (anche degli hacker e di coloro che minacciano i nostri dati) potrebbe renderle insufficienti.

Lasciando per il momento stare gli impatti che il nuovo Regolamento UE sulla privacy potrà avere per i colossi del web, quali Facebook, Google, ecc., è opportuno osservare che per le piccole e medie imprese italiane dovrà cambiare l'approccio

alla privacy, soprattutto per quelle organizzazioni che trattano dati sensibili o giudiziari. Occorrerà un cambio di mentalità: non serve più un po' di carte (informative, consensi, lettere di incarico, …) ed alcune misure minime di sicurezza specifiche (password, antivirus,…) per garantire il rispetto della legge. Poiché molti imprenditori vedono la privacy solo come un disturbo da gestire soltanto per non incorrere in sanzioni e, quindi, come una pratica da sbrigare nel modo più indolore possibile, ecco che il passaggio al nuovo Regolamento – che dovrà avvenire nei prossimi due anni – non sarò proprio una passeggiata.

Le responsabilità in capo al responsabile del trattamento (ex titolare del trattamento) sono maggiori e comunque più impegnative da gestire, soprattutto laddove il trattamento di dati venga delegato a fornitori (es. consulenti del lavoro, consulenti fiscali e legali, strutture esterne, ecc.) che dovranno inevitabilmente essere tenuti sotto controllo.

Non è che taluni principi fossero assenti dalla normativa italiana del 2003, ma – complice la crisi e le semplificazioni adottate da precedenti governi, soprattutto l'abolizione del DPS – hanno un po' sminuito l'importanza della privacy in azienda, anche perché – si sa come siamo fatti noi italiani – senza sanzioni esemplari non ci preoccupiamo di nulla… e sono stati molto rare le sanzioni comminate alle aziende, anche perché i controlli sono stati molto poco frequenti.

Paradossalmente ha spaventato di più la disposizione sui *cookie* perché la sua mancata applicazione è di fatto pubblica, mentre altre regole di fatto trascurate rimangono tra le muar delle organizzazioni di ogni dimensione.

L'indeterminatezza di alcune regole potrà essere colmata da disposizioni specifiche dei singoli Stati membri e/o da linee guida di settori specifici che potranno agevolare l'interpretazione della legge.

Ora la privacy sarà meno materia per avvocati – se non per la stesura di contratti che regolamentano i rapporti fra clienti e fornitori anche in materia di trattamento dati personali – e più materia per **esperti della sicurezza delle informazioni**. Infatti l'approccio del nuovo Regolamento Europeo sulla Privacy si avvicina, *mutatis mutandis*, a quello della norma UNI EN ISO/IEC ISO 27001 e della linea guida UNI EN ISO/IEC 27002.

L'adozione del nuovo Regolamento UE sarà, pertanto, più impegnativa per piccole organizzazioni che trattano molti dati c.d. sensibili o giudiziari, quali organizzazioni private nel campo della sanità (cliniche ed ambulatori privati, farmacie, …), studi di consulenza del lavoro, infortunistiche, studi legali, studi di consulenza fiscale, ecc., piuttosto che per aziende che trattano come unici dati sensibili i dati relativi ai propri dipendenti. Anzi saranno proprio queste ultime che dovranno pretendere da società e studi di consulenza esterna adeguate garanzie

per il trattamento dei dati di cui sono responsabili.

La privacy in Farmacia e nell'ambulatorio medico privato

La privacy dei privati cittadini utenti delle farmacie e dei piccoli ambulatori privati spesso è messa a repentaglio da una gestione non accurata delle regole stabilite dalla normativa al riguardo (D.Lgs 196/2003 – "Codice per la protezione dei dati personali") e da tutte le buone pratiche di gestione della sicurezza delle informazioni.

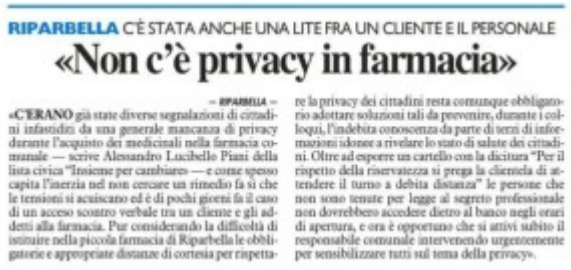
I titolari di **farmacie** ed **ambulatori medici** polifunzionali sono di fatto legali rappresentanti di imprese che, seppur di piccole dimensioni, raccolgono e gestiscono **dati personali sensibili** (in particolare dati sanitari relativi alla salute delle persone) di una **grande moltitudine di persone** fisiche e, come tali, sono tenuti a rispondere di fronte alla legge di tali gestioni.

In questi ultimi anni si è passati da una gestione prevalentemente cartacea dei dati personali sensibili raccolti da queste organizzazioni, ad una gestione elettronica di molte informazioni che riguardano la sfera privata delle persone, ovvero i **dati sanitari**.

Se pensiamo ad una farmacia moderna possiamo trovare molti **trattamenti di dati in formato digitale** che solo pochi anni fa non erano presenti: si passa dal ben noto scontrino fiscale parlante (sul quale ha molto disquisito il Garante della Privacy), generato e poi gestito da un sistema informatico, alla ricetta elettronica di recente introduzione, passando per una serie di servizi che le farmacie hanno introdotto da pochi anni: intolleranze alimentari, analisi della pelle, gestione referti esami diagnostici, preparazione di diete, fidelity card, e-commerce, ecc.. Ma anche servizi meno recenti come le prenotazioni di esami tramite CUP ASL o la Dispensazione per Conto vengono gestiti dalle farmacie, attraverso appositi portali dedicati, per conto dei clienti.

Ognuno di questi trattamenti di dati presenta vulnerabilità intrinseche per la sicurezza delle informazioni trasmesse: credenziali di accesso non sufficientemente difficili da individuare, scarsa protezione dei PC e dei Server da attacchi esterni, inadeguata protezione dei medesimi elaboratori in caso di furto e via dicendo.

Come le piccole organizzazioni di altri settori industriali o dei servizi, anche le farmacie non sono dotate di personale esperto nella gestione della sicurezza dei sistemi informatici e spesso il coinvolgimento dei fornitori esterni specializzati non è così sistemato (soprattutto per motivi di costo) da poter garantire una protezione adeguata.



RIPARBELLA C'È STATA ANCHE UNA LITE FRA UN CLIENTE E IL PERSONALE

«Non c'è privacy in farmacia»

– RIPARBELLA –

«C'ERANO già state diverse segnalazioni di cittadini infastiditi da una generale mancanza di privacy durante l'acquisto dei medicinali nella farmacia comunale — scrive Alessandro Lucibello Piani della lista civica "Insieme per cambiare» — e come spesso capita l'inerzia nel non cercare un rimedio fa sì che le tensioni si acuiscano ed è di pochi giorni fa il caso di un acceso scontro verbale tra un cliente e gli addetti alla farmacia. Pur considerando la difficoltà di istituire nella piccola farmacia di Riparbella le obbligatorie e appropriate distanze di cortesia per rispettare la privacy dei cittadini resta comunque obbligatorio adottare soluzioni tali da prevenire, durante i colloqui, l'indebita conoscenza da parte di terzi di informazioni idonee a rivelare lo stato di salute dei cittadini. Oltre ad esporre un cartello con la dicitura "Per il rispetto della riservatezza si prega la clientela di attendere il turno a debita distanza" le persone che non sono tenute per legge al segreto professionale non dovrebbero accedere dietro al banco negli orari di apertura, e ora è opportuno che si attivi subito il responsabile comunale intervenendo urgentemente per sensibilizzare tutti sul tema della privacy».

D'altro canto **dai computer delle farmacie transitano quantità di dati sensibili di gran linga superiori a quelle di altre piccole organizzazioni** e costituiscono il canale di consultazione di archivi di prenotazione di esami diagnostici di un elevatissimo numero di pazienti. Da qui la necessità di proteggere i sistemi informatici delle farmacie, sia da un punto di vista logico, sia fisico, in modo molto più attento rispetto ad un normale PC aziendale.

Anche i **piccoli ambulatori privati**, che ospitano medici che eseguono visite specialistiche ed esami diagnostici, ultimamente hanno trovato grande beneficio dall'utilizzo delle nuove tecnologie, nonostante la ritrosia all'utilizzo del computer da parte di numerosi medici. Tutto ciò, però, comporta **la necessità di proteggere adeguatamente i dati sensibili dei pazienti** che transitano in formato digitale in reti locali poco protette. In tali organizzazioni spesso non è nemmeno chiaro chi è il titolare del trattamento dati – il medico che visita il paziente o il centro medico – ed a chi vengono eventualmente delegate le responsabilità per i trattamenti delegati ad altri.

In generale, nelle farmacie e nei piccoli centri medici, tutta la "parte informatica" è delegata a **fornitori specializzati** che talvolta non conoscono in modo preciso la normativa sulla privacy e sono **negligenti nel sottoscrivere le proprie assunzioni di responsabilità** a fronte delle attività eseguite; conseguentemente **tutte le responsabilità ricadono sul titolare del trattamento**, persona fisica o giuridica avente comunque un legale rappresentante, generalmente poco avvezzo a questioni informatiche.

Dal punto di vista normativo, poi, il passaggio da una **normativa italiana** – molto completa e severa per taluni aspetti, ma ormai **obsoleta** per quanto riguarda il **disciplinare tecnico delle misure minime di sicurezza** – ad un nuovo **Regolamento Europeo in fase di approvazione**, non fa che complicare le cose per le piccole organizzazioni che finora hanno avuto regole precise (password di almeno 8 caratteri variate ogni 3 mesi se si trattano dati sensibili, backup almeno ogni 7 giorni, aggiornamenti semestrali dei programmi software, assenza di idonee dichiarazioni di conformità dei fornitori, ecc.) con le quali confrontarsi. Il nuovo Regolamento, infatti, introdurrà la necessità di **valutare i rischi che si corrono dal punto di vista della sicurezza dei dati personali** e, conseguentemente, **progettare il sistema di gestione della privacy** in funzione delle reali esigenze di riservatezza,

adottando misure di sicurezza adeguate (non solo “minime”).

Inoltre l’attuale versione del Regolamento Europeo sulla Privacy in approvazione contiene l’obbligo per i titolari di dati personali di dotarsi – entro determinate condizioni – di un “***Privacy Officer***”, ovvero di una persona, dotata di **adeguate competenze in materia di privacy e sicurezza dei dati**, **responsabile per la gestione della privacy** all’interno dell’organizzazione. Ma il limite attualmente stabilito per l’obbligo di nominare un Privacy Officer è legato al numero di dati personali gestiti (più di 5000 in un anno) che viene facilmente superato da una farmacia di medio volume di affari, ma non da numerose imprese industriali con oltre 50 dipendenti.

La ratio del nuovo Regolamento UE è evidentemente quella di **garantire migliore protezione dove esistono maggiori rischi**, sia per il numero di dati personali trattati, sia per la vulnerabilità dei sistemi.

Il **cambio di mentalità** di chi gestisce **piccole organizzazioni nel settore sanitario** non sarà facile, anche perché non ci saranno più regole precise da seguire per stare tranquilli, ma, oserei dire giustamente, **il Regolamento Europeo ribalterà la responsabilità di progettare un sistema di gestione della privacy adeguato sulle spalle degli imprenditori**. Molti di questi ultimi non saranno in grado di valutare in modo competente ed oggettivo quali misure adottare e dovranno fare attenzione a non credere alle “ricette preconfezionate” a basso costo che hanno già rovinato l’approccio alla privacy negli anni del ben noto **DPS** (Documento Programmatico sulla Sicurezza).

Già oggi il rischio di molte piccole organizzazioni del settore sanitario è quello di non essere conformi alla legislazione attuale sotto diversi aspetti (mancate nomine degli incaricati, mancanza di credenziali di autenticazione ai sistemi informatici adeguate e variate periodicamente, utilizzo troppo invasivo della videosorveglianza, archiviazione di dati privi di protezione, ecc.), figuriamoci domani se saranno i titolari del trattamento (ovvero i legali rappresentanti o direttori delle organizzazioni) a dover **decidere quali misure di sicurezza sono adeguate**! Il rischio concreto è quello di **sottovalutare il problema privacy**, come del resto è avvenuto dopo l’abolizione del DPS che non ha abolito tutti gli altri adempimenti!

Dimenticarsi di proteggere adeguatamente i dati personali dei propri clienti può comportare non solo **sanzioni civili** (e in alcuni casi anche reati penali) in caso di **ispezione da parte del nucleo Privacy della Guardia di Finanza** (oggi peraltro molto rare), ma anche, in caso di **richiesta di risarcimento danni da parte dell’interessato** i cui dati sensibili sono stati violati, ingenti perdite economiche. Talvolta, poi, la mancata diligenza del titolare del trattamento potrebbe portare anche al divieto di intraprendere relazioni commerciali con la Pubblica Amministrazione, riducendo o annullando di fatto la possibilità di operare.

Infine, oltre agli aspetti legati al rispetto della normativa cogente, esistono altri pericoli a cui è sottoposta una organizzazioni che gestisce in modo inconsapevole la sicurezza dei dati, ad esempio la **perdita di dati** e **l'indisponibilità di risorse per garantire la continuità del servizio** al cliente e, quindi, perdite economiche più o meno rilevanti in funzione della gravità dell'evento.

Altre risorse in rete:

- http://www.federfarmalombardia.it/documents/servizi/vademecum_privacy.pdf
- http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3533579
- http://www.federprivacy.it/forum/17-privacy-in-campo-sanitario/307-privacy-in-farmacia-e-negli-studi-medici.html
- http://www.federfarma.it/Edicola/Ultime-notizie/17-05-2014-07-30-18.aspx?feed=FederfarmaUltimeNotizie
- http://www.sicurezzamagazine.it/telecamere-nelle-farmacie/
- http://quellichelafarmacia.com/19493/sicurezza-farmacia-abuso-videosorveglianza-una-violazione-privacy/#sthash.RJlzvePR.dpbs

---

Le novità sulla privacy passate e future

Dall'introduzione del **D.lgs 196/2003**, noto come **Codice sulla Privacy**, sono state introdotte e modificate numerose norme nel settore della protezione dei dati personali e non. Anche il Codice Civile ed il Codice Penale hanno visto numerosi aggiornamenti, per così dire "tecnologici", relativi a comportamenti illeciti e reati perpetrati attraverso gli strumenti informatici e soprattutto via internet.

La legge sulla privacy da un lato si è dovuta adeguare alle nuove situazioni legate alla pubblicazione di altre normative legate al trattamento dei dati personali, dall'altro ha visto, nel giro di pochi mesi, ridursi gli adempimenti delle organizzazioni relativamente alla gestione dei dati personali relativi a persone giuridiche, ai trattamenti per fini amministrativo-contabili ed al decaduto obbligo di redazione ed aggiornamento del **Documento Programmatico sulla Sicurezza** (DPS).

Se escludiamo provvedimenti nati per settori specifici (*data breach* in ambito telco, tracciabilità degli accessi ai dati bancari), in attesa del **nuovo Regolamento UE**

sulla privacy che verrà emesso il prossimo anno a livello di Comunità Europea, gli adempimenti obbligatori per le aziende non sono certo aumentati, anche il **rischio D.Lgs 231** che incombeva su molte organizzazioni, relativo all'introduzione dei reati sulla privacy (trattamento illecito di dati personali), **è stato evitato**. Infatti quanto previsto dal Decreto Legge n. 93/2013 è stato convertito in Legge **eliminando la norma sull'inclusione dei reati privacy nell'elenco dei reati della 231** (la norma prevista dal D.L. 93/2013 non è stata convertita dalla legge 15 ottobre 2013, n. 119 in vigore dal 16 ottobre: il comma 2 dell'articolo 9 del DL 93/2013 è stato soppresso dalla legge di conversione 119/2013; le disposizioni prevedevano l'ingresso tra i "reati presupposto" inclusi nel D.lgs 231/2001 anche dei delitti in materia di privacym non le contravvenzioni, tra cui il trattamento illecito dei dati e le false comunicazioni al Garante).

Da ormai 10 anni a questa parte l'applicazione del codice per la protezione dei dati personali è stata vista dalle varie organizzazioni per lo più come un'incombenza burocratica, che toglie tempo e risorse alle attività cosiddette "produttive". L'unico motivo per cui applicare le misure minime di sicurezza, fornire l'informativa, nominare gli incaricati ed i responsabili del trattamento per molti imprenditori è stato quello di "essere in regola" ed evitare le possibili sanzioni legate al mancato rispetto per la privacy.

La crisi economica e la necessità, o volontà, per molte organizzazioni di ridurre i costi di struttura ha portato a **distogliere risorse dalla compliance privacy**: tagli ai costi per consulenze e servizi di assistenza informatica collegati (ad es. Amministratore di Sistema), meno tempo dedicato ad osservare gli adempimenti previsti, meno formazione del personale, ecc..

Del resto il rischio per l'organizzazione di subire impatti negativi (sanzioni, richieste di risarcimento danni, ecc.) dalla mancata applicazione rigorosa del Codice della Privacy si è via via ridotto a qualche ipotetica ispezione del famoso "Nucleo Privacy della Guardia di Finanza" oppure a denunzie di interessati i quali ritengono che i propri dati personali sono stati trattati in modo illecito.

Occorre anche sottolineare che le "**misure minime di sicurezza**" delineate dal Garante nella prima versione del D.Lgs 196/2003, nell'allegato B, non sono certo **misure adeguate** nel 2013 (si pensi all'aggiornamento dell'*anti-malware* con cadenza semestrale).

Fortunatamente chi ha applicato le misure di sicurezza le ha attuate in modo sostanzialmente corretto (ad es. ogni antivirus prevede un aggiornamento almeno settimanale dei database dei virus), anche se non è raro vedere suite di sicurezza software non configurate in modo adeguato, procedure di backup poco sicure, autenticazioni con password deboli e così via.

Per quanto riguarda il futuro prossimo, il **nuovo Regolamento UE** sarà legge immediatamente in ogni Stato della Comunità Europea ed avrà un significativo impatto

sul Codice della Privacy attualmente in vigore in Italia, in quanto le regole sulla protezione dei dati personali dovranno essere necessariamente le stesse in tutti gli Stati membri.

Alcune norme del suddetto Regolamento potranno essere abbastanza pesanti per imprese ed enti, anche se la versione attualmente in discussione non è ancora definitiva.

Vediamo alcune situazioni esemplificative:

- Viene richiesto maggior dettaglio nell'informativa al trattamento di dati personali (ad esempio l'indicazione del periodo di conservazione dei dati per ogni tipo di trattamento, possibilità di trasferire i dati ad un Paese terzo) ed alla richiesta di consenso (ogni consenso al trattamento deve essere distinguibile da altri tipi di consenso).
- L'esecuzione dei trattamenti su commissione (ovvero *l'outsourcing*, ad es. per il servizio paghe) deve essere disciplinata da un contratto o altro atto giuridico scritto che vincoli il titolare del trattamento al responsabile esterno del trattamento (si precisa che nella dizione originale del regolamento si parla di "incaricato del trattamento" al posto di r"responsabile" e "responsabile del trattamento" al posto di "titolare del trattamento", secondo la dizione italiana vigente).
- Il responsabile esterno al trattamento dei dati personali che tratta i dati conferitigli diversamente dalle istruzioni impartitegli dal titolare diviene titolare egli stesso del trattamento con le conseguenti responsabilità giuridiche.
- Dovranno essere attuati adempimenti molto dettagliati sulla documentazione da conservare relativa ai trattamenti di dati personali, sia per il titolare che per il responsabile del trattamento (non è una documentazione come quella contenuta nel DPS ma si avvicina molto ad esso).
- Le misure di sicurezza adottate dovranno essere appropriate ai rischi che incombono sui dati ed alla natura dei dati trattati; è peraltro richiesta una valutazione dei rischi.
- L'obbligo di comunicazione, sempre, all'Autorità di Controllo (Garante Privacy in Italia) ed agli interessati, quando richiesto, di violazioni di dati personali (*data breach*) incombe su tutti i titolari e responsabili di trattamento e per tutti i tipi di trattamento.
- È richiesta una valutazione dell'impatto del trattamento sulla protezione dei dati personali in caso di trattamenti particolari su cui incombono rischi specifici.
- C'è l'obbligo di nomina di un **responsabile della protezione dei dati** (con un profilo professionale abbastanza definito) per imprese che trattino dati di almeno 500 interessati (in certi settori B2C praticamente tutte le organizzazioni) ed in caso di profilazione dei dati; tale responsabile avrà il compito di garantire il rispetto di requisiti normativi specifici.

Infine il Regolamento fissa le sanzioni amministrative previste, ma non quelle

penali la cui definizione è riservata agli Stati membri.

Altri provvedimenti recenti del Garante della Privacy hanno riguardato lo *spam*, o meglio le **comunicazioni commerciali con finalità di marketing** che possono essere indesiderate da chi le riceve e la **privacy nel Condominio** (che aggiunge nuovi adempimenti per gli Amministratori di Condominio che sono stati recentemente interessati alla Riforma del Condominio).

Infine occorre portare particolare attenzione all'ambito **videosorveglianza e controllo dei lavoratori**, che, sebbene la normativa non sia sostanzialmente cambiata (vedasi art. 4 dello Statuto dei Lavoratori), grazie alla diffusione di nuovi strumenti elettronici (sistemi di sorveglianza sempre più evoluti gestiti da software accessibili anche dal web, *internet content filtering*, sistemi di controllo accessi anche con caratteristiche biometriche quali impronte digitali, log di accessi ai sistemi informatici, ecc.), vede la casistica di possibili violazioni molto più estesa che in passato ed è opportuno consultare le sentenze passate in giudicato per dirimere questioni sempre più complesse. In particolare il giusto equilibrio fra difesa dei diritti dei lavoratori a non essere controllati ed i cosiddetti "controlli difensivi" va comunque valutato di caso in caso, anche in funzione dei possibili illeciti o reati che si vuole prevenire o scoprire.

Linee guida in materia di attività promozionale e contrasto allo spam – 4 luglio 2013 [2542348]

Vademecum – Il condominio e la privacy – versione pagina singola

CloudWatch

Pubblicato il codice della privacy aggiornato

Sono state convertite in legge le modifiche apportate al codice per la protezione dei dati personali dal D.L. del 9 febbraio 2012, n. 5, convertito, con modificazioni, dalla legge 4 aprile 2012, n. 35.

Codice della privacy

Si allega il testo aggiornato del Codice della Privacy nel quale viene confermata l'abrogazione del comma g) dell'articolo 34 che prevedeva la tenuta di un documento programmatico sulla sicurezza aggiornato.

Modifiche al Codice della privacy: niente più DPS!

Con il Decreto Legge n. 5 del 9 febbraio 2012 (il c.d. Decreto "semplificazioni e sviluppo"), all'art. 45, il Governo Monti ha abrogato la lettera g) del comma 1 dell'articolo 44 del D.Lgs 196/2003 e s.m.i. (il c.d. "Codice della Privacy"), eliminando di fatto la necessità di redazione (od aggiornamento) del Documento Programmatico sulla Sicurezza (D.P.S.) da parte di tutti i tipi di imprese e liberi professionisti, indipendentemente dal tipo di dati trattati.

Premesso che si tratta di un Decreto Legge e, come tale, dovrà essere convertito in legge entro 60 giorni altrimenti decadrà automaticamente e la sua conversione in legge potrebbe avvenire con modifiche, si precisa quanto segue.

La soppressione dell'onere di redigere ed aggiornare il DPS entro il 31 marzo di ogni anno non abroga tutti gli altri adempimenti della privacy e l'applicazione stessa della legge. Ricordiamo che gli adempimenti ed il campo di applicazione della legge sulla privacy erano già stati ridotti con i provvedimenti emanati dal precedente Governo per le organizzazioni che non trattano dati sensibili eccetto i dati sensibili relativi ai propri dipendenti (e loro familiari) e trattano esclusivamente dati di persone giuridiche per scopi amministrativo-contabili.

Le statistiche, messe a disposizione dalla stessa Autorità dimostrano chiaramente che le multe per omessa redazione del DPS sono una percentuale numericamente minore rispetto alle altre casistiche rilevate nel corso delle ispezioni del nucleo Privacy della Guardia di Finanza. La sostanza della normativa privacy non è di fatto cambiata con l'abolizione del DPS e rimangono le stesse misure di sicurezza obbligatorie (ad es. attuazione delle misure minime di sicurezza, nomina incaricati e responsabili del trattamento di dati, ecc.) ed i provvedimenti del Garante che

hanno effetto di legge (ad es. quello generale sulla videosorveglianza, quello sugli amministratori di sistema, le linee guida del Garante per posta elettronica e internet nei luoghi di lavoro) che, come atti di natura prescrittiva, se non rispettati espongono i contravventori a pesanti sanzioni.

In attesa del nuovo Regolamento europeo sulla protezione dei dati personali, che peraltro ci imporrà a breve di tornare a regole più rigide e sanzioni severe, la semplificazione attuata dal Governo, che risparmia alle imprese finora tenute l'incombenza del DPS, presenta però anche l'altra faccia della medaglia, cioè quello di essere indotti ad abolire completamente la gestione della privacy in azienda, con il potenziale rischio di rimanere "scottati" al primo imprevisto (verifiche del nucleo privacy della GdF, denunce al Garante da parte di potenziali soggetti danneggiati, perdita della sicurezza delle informazioni). La stesura del DPS, tra l'altro, era ritenuto erroneamente da molte organizzazioni una sorta di adeguamento normativo omnicomprensivo sul tema della privacy, mentre invece le dichiarazioni riportate nel DPS non hanno alcun valore se poi non sono messe in pratica.

Per questo, se un'azienda decide di continuare a redigere un disciplinare interno sulla privacy dove elencare le misure di sicurezza in essere, tutti gli interventi effettuati e la previsione di quelli da effettuare, farebbe una scelta opportuna per la gestione dei potenziali rischi derivanti dal trattamento dei dati personali.

Se il DPS non dava valore aggiunto a quelle organizzazioni, soprattutto di piccole dimensioni, che lo vedevano solo come un inutile costo è giusto sopprimerlo, a condizione che la privacy sia gestita correttamente in azienda. Allora piuttosto che sottostare al rigido schema del DPS sarebbe più utile spostare i contenuti importanti del DPS in altri documenti aziendali quali procedure, istruzioni, organigrammi e mansionari, piani di formazione, ecc..

Certamente gli obblighi della privacy – realmente abolita in toto dal precedente Governo per quelle organizzazioni che non trattano dati sensibili o giudiziari eccetto che quelli dei propri dipendenti e trattano unicamente dati di persone giuridiche per adempimenti amministrativo-contabili – potevano indurre alcune organizzazione a proteggere meglio tutte le informazioni gestite, non solo quelle dei propri clienti, fornitori e dipendenti o soggetti terzi. Oggi, infatti, è importante che le imprese capiscano l'importanza delle informazioni da esse memorizzate negli archivi cartacei e nei sistemi informatici.

Senza avere la sicurezza dei dati le organizzazioni di tutti i tipi possono subire gravi danni, sia intermini economici, sia di immagine nei confronti dei clienti e della collettività. Dove per sicurezza dei dati intendo essere adeguatamente garantiti che:

- I dati sono mantenuti adeguatamente riservati, cioè non sono conosciuti da chi, se li sapesse, potrebbe crearci qualche problema (ad es. dati commerciali,

offerte, progetti di prodotti noti a concorrenti);
- I dati sono integri, ovvero i dati che noi leggiamo nei sistemi informatici e nei documenti sono aggiornati, corretti e non sono stati alterati (ad es. dati di produzione o di vendita inesatti), dunque non possono portare a decisioni sbagliate);
- I dati sono disponibili, cioè li possiamo consultare ed utilizzare quando ne abbiamo bisogno per lavorare (ad es. documenti e dati necessari per preparare un'offerta quando sta per scadere il termine, dati in input a processi produttivi interni o necessari per svolgere un servizio).

Poiché la privacy e la sicurezza delle informazioni prevede regole che servono a minimizzare i rischi potenziali di subire danni (incorrere in sanzioni, perdere dati, far conoscere dati riservati a chi non li dovrebbe conoscere, ecc.) occorre anzitutto effettuare un'adeguata valutazione dei rischi, cosa che – in generale – ben poche imprese fanno, anche su altre tematiche.

Poi si può discutere se sia giusto abolire il DPS per "semplificare" la vita delle imprese, molte delle quali se la sono già abbastanza semplificata non curandosi di tante regole. Per quelli che sono stati finora scrupolosi ed osservanti delle leggi e lo hanno sempre redatto ed aggiornato è un po' una beffa favorire tutte quelle imprese che hanno finora trascurato la redazione del DPS in questi anni. Assomiglia un po' ad un condono fiscale o edilizio. Visto, però, che coloro che non hanno redatto il DPS finora probabilmente hanno trascurato anche altri adempimenti della privacy, il loro profilo di rischio non cambia. In sostanza non è il DPS che fa la privacy.

Non essendo più necessario redigere e, soprattutto, aggiornare il DPS a cadenza annuale, le organizzazioni che trattano dati sensibili o giudiziari di persone fisiche (clienti e fornitori) dovranno comunque continuare ad osservare alcune regole che non dovranno più essere documentate nel DPS, tra cui:

- Nominare gli incaricati al trattamento dei dati personali (dipendenti o collaboratori);
- Nominare i responsabili esterni al trattamento di dati personali (ad es. consulenti del lavoro, commercialisti, avvocati, tecnici incaricati dell'assistenza sui sistemi informatici,…);
- Nominare gli Amministratori di Sistema e verificarne periodicamente l'operato;
- Attuare idonee misure di sicurezza per la protezione dei dati (controllo degli accessi ai sistemi informatici, impiego di antimalware e firewall, effettuazione di backup dei dati informatici, ecc.);
- Rispettare le regole per la videosorveglianza;
- Verificare almeno annualmente la sussistenza dei profili di autenticazione;
- Ecc.

In questo nuovo scenario chi farà la verifica dell'osservanza delle prescrizioni stabilite dal Garante della Privacy e dalle procedure interne che la legge pone in

capo al Titolare del Trattamento o al Responsabile del Trattamento dei dati? E la verifica del comportamento degli Amministratori di Sistema?

Tali verifiche possono avvenire, in modo ottimale, attraverso un vero e proprio audit indipendente di un soggetto esterno – e quindi non coinvolto nella realtà aziendale – competente in materia.

L'audit sulla privacy dovrebbe basarsi sul controllo di informazioni contenute nel DPS e documenti interni che finora erano raccolti insieme al DPS stesso (elenco trattamenti dati personali, elenco incaricati al trattamento con relativi compiti e responsabilità, lettere di nomina incaricati e responsabili al trattamento, descrizione delle misure di protezione dei sistemi informatici, istruzioni al personale, ecc..), interviste al personale e verifica di attuazione delle misure di sicurezza delle informazioni, sia fisiche che logiche. Tale verifica deve per forza di cosa svolgersi attraverso un sopralluogo presso i luoghi dove vengono trattati dati personali (visione dei sistemi informatici e della loro ubicazione, verifica della disposizione di eventuali telecamere di videosorveglianza, archiviazione sicura dei documenti, ecc.).

Il risultato della verifica, per essere efficacemente preso in carico dai responsabili dell'organizzazione titolare del trattamento, deve essere documentato in un idoneo rapporto di audit che evidenzi le e ventuali carenze (vere e proprie non conformità rispetto alla legge), le osservazioni od opportunità di miglioramento dell'approccio alla sicurezza dei dati e le azioni correttive da intraprendere per soddisfare tutte le prescrizioni vigenti per la privacy. Tale rapporto potrà poi essere utilizzato nella verifica successiva per valutare l'efficacia delle azioni intraprese.