privacy: *da maggio cambiano le regole*

di Umberto Marchi

Il prossimo 25 maggio 2018 scatterà l'ora "x" del nuovo Regolamento europeo in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (Regolamento Ue 2016/679).

Dal 25 maggio 2018 le nuove disposizioni sul trattamento dei dati personali manderanno in soffitta il vigente (e morituro) Regolamento, che a dire il vero è un po' vecchiotto, visto che risale al 2003 (un'eternità se si considerano i progressi della tecnologia, e della possibilità di trasmissione dei dati personali, intervenute nel frattempo). E chi pensa che tutto ciò sia in fondo di scarso interesse per le imprese di pulizie/ servizi integrati/ multiservizi, potrebbe essere in breve costretto a ricredersi.

Interessate anche le nostre imprese

Proprio per la natura del loro lavoro, che da un lato è altamente labour intensive, dall'altro le porta a contatto con una platea di committenze numerose, disparate ed eterogenee, più di molti altri soggetti le imprese del nostro settore hanno a che fare con messi sterminate di dati –anche sensibili- da acquisire, trattare e proteggere. E siccome i rischi sono concreti, vale la pena di mettere in atto fin da subito azioni ben precise che possono essere intraprese sin d'ora perché fondate su disposizioni del regolamento che non lasciano spazi a interventi del legislatore nazionale.

I soggetti coinvolti

Un aspetto interessante per le imprese, ad esempio, è quello relativo ai soggetti coinvolti, come titolare, responsabile, incaricato del trattamento. Il regolamento, infatti: disciplina la contitolarità del trattamento e impone ai titolari di definire specificamente (con un atto giuridicamente valido ai sensi del diritto nazionale) il rispettivo ambito di responsabilità e i compiti con particolare riguardo all'esercizio dei diritti degli interessati, che hanno comunque la possibilità di rivolgersi indifferentemente a uno qualsiasi dei titolari operanti congiuntamente; fissa più dettagliatamente rispetto alle norme ora in vigore le caratteristiche dell'atto con cui il titolare designa un responsabile del trattamento attribuendogli specifici compiti: deve trattarsi, infatti, di un contratto (o altro atto giuridico conforme al diritto nazionale) e deve disciplinare tassativamente almeno la natura, durata e finalità del trattamento o dei trattamenti assegnati, le categorie di dati oggetto di trattamento, le misure tecniche e organizzative adeguate a consentire il rispetto delle istruzioni impartite dal titolare e, in via generale, delle disposizioni contenute nel regolamento; consente la nomina di sub-responsabili del trattamento da parte di un responsabile, per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano titolare e responsabile primario; quest'ultimo risponde dinanzi al titolare dell'inadempimento dell'eventuale sub-responsabile, anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso "non gli è in alcun modo imputabile"; prevede obblighi specifici in capo ai responsabili del trattamento, in quanto distinti da quelli pertinenti ai rispettivi titolari. Ciò riguarda, in particolare, la tenuta del registro dei trattamenti svolti; l'adozione di idonee misure tecniche e organizzative per garantire la sicurezza dei trattamenti; la designazione di un RPD-DPO, nei casi previsti dal regolamento o dal diritto nazionale.

Responsabilizzazione e dintorni

Un'altra questione su cui porre l'accento è il concetto, centrale per l'Europa, di "responsabilizzazione". Il regolamento pone infatti con forza l'accento sulla "responsabilizzazione" (accountability) di titolari e responsabili – ossia, sull'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento.

I "sette passi"

Il Regolamento impone il rispetto di alcuni principi, tra cui: liceità, correttezza e trasparenza; limitazione delle finalità (determinate, esplicite e legittime); minimizzazione dei dati (adeguati, pertinenti e limitati), esattezza e aggiornamento dei dati; limitazione della conservazione per un tempo stabilito; integrità e riservatezza, responsabilizzazione.
Ed ecco una ricetta in "7 passi":
mappare i trattamenti; individuare ruoli, responsabilità e compiti; definire e attuare adempimenti per priorità d'azione; definire misure di sicurezza adeguate; definire policy e procedure organizzative; definire una procedura di data breach; documentare la conformità.

(Tratto dall'intervento di R.Cannizzaro e P.Generali di Assintel al Workshop "GDPR: cosa fare, come farlo e come gestirlo" svoltosi il 28 febbraio 2018 presso la sede di Confcommercio Milano)

Il rischio del trattamento

Fondamentali fra tali attività sono quelle connesse al secondo criterio individuato nel regolamento rispetto alla gestione degli obblighi dei titolari, ossia il rischio inerente al trattamento. Quest'ultimo è da intendersi come rischio di impatti negativi sulle libertà e i diritti degli interessati; tali impatti dovranno essere analizzati attraverso un apposito processo di valutazione tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) che il titolare ritiene di dover adottare per mitigare tali rischi.

Registro dei trattamenti

Tutti i titolari e i responsabili di trattamento, eccettuati gli organismi con meno di 250 dipendenti ma solo se non effettuano trattamenti a rischio, devono tenere un registro delle operazioni di trattamento. Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante.

Le misure di sicurezza

Le misure di sicurezza devono "garantire un livello di sicurezza adeguato al rischio" del trattamento; non potranno sussistere dopo il 25 maggio 2018 obblighi generalizzati di adozione di misure "minime" di sicurezza poiché tale valutazione sarà rimessa, caso per caso, al titolare e al responsabile in rapporto ai rischi specificamente individuati.

Segnalazione violazioni

A partire dal 25 maggio 2018, tutti i titolari – e non soltanto i fornitori di servizi di comunicazione elettronica accessibili al pubblico, come avviene oggi – dovranno notificare all'autorità di controllo le violazioni di dati personali di cui vengano a conoscenza, entro 72 ore e comunque "senza ingiustificato ritardo", ma soltanto se ritengono probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati. Pertanto, la notifica all'autorità dell'avvenuta violazione non è obbligatoria, essendo subordinata alla valutazione del rischio per gli interessati che spetta, ancora una volta, al titolare.

Responsabile protezione dati

Anche la designazione di un responsabile della protezione dati (RPD) riflette l'approccio responsabilizzante che è proprio del regolamento, essendo finalizzata a facilitare l'attuazione del regolamento da parte del titolare/responsabile. Non è un caso, infatti, che fra i compiti del RPD rientrino "la sensibilizzazione e la formazione del personale" e la sorveglianza sullo svolgimento della valutazione di impatto. La sua designazione è obbligatoria.

Le sanzioni

E infine, ma tutt'altro che "dulcis in fundo", ecco le sanzioni, che possono essere molto più severe di quelle attuali: infatti, se l'attuale Codice prevede sanzioni amministrative da 1000 a 120mila euro, con sanzioni penali qualora il fatto costituisca reato (reclusione da 6 mesi a 3 anni), con la nuova disciplina le sanzioni potranno arrivare al maggiore importo fra 20 milioni di euro e il 4% del fatturato annuo aziendale, con sanzioni penali secondo le previsioni dei singoli Stati. Non uno scherzo, insomma.