CIRCOLARE N. 25 DEL 19 MARZO 2018

PRIVACY: AGGIORNAMENTO DEL DOCUMENTO PROGRAMMATICO

SULLA SICUREZZA (D.P.S.)

In sintesi

Il Documento Programmatico sulla Sicurezza è un documento interno che descrive il livello di implementazione della gestione della privacy aziendale, ai sensi dell'allegato B, D.Lgs. 196/2003. Seppure l'obbligo di redazione annuale del D.P.S. sia stato abrogato dal D.L. 5/2012 convertito nella L. 35/2012, sono tuttora in vigore le previsioni contenute negli articolo 33 e ss., D.Lgs. 196/2003 (Misure minime di sicurezza).

Rif. normativi e di prassi: *Regolamento UE 2016/679*

Imprese e professionisti devono strutturare la propria organizzazione aziendale al fine di rispettare le misure minime di sicurezza, riducendo i rischi di perdita, di accesso non autorizzato e di trattamento non consentito dei dati personali (anche se vengono trattati dati solo di tipo comune, non necessariamente sensibili o giudiziari). È a carico dei titolari del trattamento di dati l'obbligo di redazione di idonee informative (ai dipendenti e collaboratori; ai clienti e ai fornitori; agli utenti del sito *web*; etc.), nonché la nomina degli incaricati al trattamento dei dati personali, ed eventualmente dei responsabili, con particolare attenzione ai casi di affidamento dei dati personali in *outsourcing* o *in cloud*.

Qualora l'impresa si avvalga di amministratori di sistema, figure specificamente dedicate alla gestione dei sistemi informatici e della sicurezza, il titolare del trattamento deve valutare l'effettiva capacità ed affidabilità dei soggetti preposti e avvalersi di idonei sistemi di controllo (tramite appositi *software*) dell'attività posta in essere dagli amministratori medesimi.

Dal 25 maggio 2018 in vigore il Regolamento europeo in materia di protezione dei dati personali

Il garante della *privacy* ha elaborato e pubblicato sul sito www.garanteprivacy.it una guida (v. Allegato) utile all'applicazione del Regolamento UE 2016/679 che entrerà in vigore in Italia il **25 maggio 2018**.

Il testo della Guida è articolato in 6 sezioni tematiche:

1. fondamenti di liceità del trattamento;
2. informativa;
3. diritti degli interessati;
4. titolare, responsabile, incaricato del trattamento;
5. approccio basato sul rischio del trattamento e misure di *accountability* di titolari e responsabili;
6. trasferimenti internazionali di dati.

Attraverso raccomandazioni specifiche, vengono suggerite alcune azioni che possono essere intraprese sin d'ora perché fondate su disposizioni precise del Regolamento che non lasciano spazi a interventi del Legislatore nazionale.

Contenuti dell'informativa

I contenuti dell'informativa sono elencati in modo tassativo negli articoli 13, paragrafo 1, e 14, paragrafo 1, del regolamento e in parte sono più ampi rispetto al Codice. In particolare, il titolare deve sempre specificare i **dati di contatto del RPD-DPO** (Responsabile della protezione dei dati – Data Protection Officer), ove esistente, la base giuridica del trattamento, qual è il suo interesse legittimo se quest'ultimo costituisce la base giuridica del trattamento, nonché se trasferisce i dati personali in Paesi terzi e, in caso affermativo, attraverso quali strumenti (esempio: si tratta di un Paese terzo giudicato adeguato dalla Commissione europea; si utilizzano BCR di gruppo; sono state inserite specifiche clausole contrattuali modello, ecc.).

Il regolamento prevede anche ulteriori informazioni in quanto "necessarie per garantire un trattamento corretto e trasparente": in particolare, il titolare deve specificare il periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo di conservazione, e il diritto di presentare un reclamo all'autorità di controllo.

Se il trattamento comporta processi decisionali automatizzati (anche la profilazione), l'informativa deve specificarlo e deve indicare anche la logica di tali processi decisionali e le conseguenze previste per l'interessato.

Titolare, responsabile, incaricato del trattamento

Il regolamento:

- disciplina la contitolarità del trattamento (art. 26) 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 all'art. 29 del Codice) 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 le materie riportate al paragrafo 3 dell'art. 28 al fine di dimostrare che il responsabile fornisce "garanzie sufficienti" – quali, in particolare, 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 (si veda art. 28, paragrafo 4), 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" (si veda art. 82, paragrafo 1 e paragrafo 3);
- 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 (ex art. 30, paragrafo 2); l'adozione di idonee misure tecniche e organizzative per garantire la sicurezza dei trattamenti (ex art. 32 regolamento); la designazione di un RPD-DPO, nei casi previsti dal regolamento o dal diritto nazionale (si veda art. 37 del regolamento). Si ricorda, inoltre, che anche il responsabile non stabilito nell'Ue dovrà designare un rappresentante in Italia quando ricorrono le condizioni di cui all'art. 27, paragrafo 3, del regolamento – diversamente da quanto prevede oggi l'art. 5, comma 2, del Codice.
- definisce caratteristiche soggettive e responsabilità di titolare e responsabile del trattamento negli stessi termini di cui alla direttiva 95/46/CE e, quindi, al Codice italiano. Pur non prevedendo espressamente la figura dell'"incaricato" del trattamento (ex art. 30 Codice), il regolamento non ne esclude la presenza in quanto fa riferimento a "persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile" (si veda, in particolare, art. 4, n. 10, del regolamento).

Misure di sicurezza

Le misure di sicurezza devono "garantire un livello di sicurezza adeguato al rischio" del

trattamento (art. 32, paragrafo 1); in questo senso, la lista di cui al paragrafo 1 dell'art. 32 è una lista aperta e non esaustiva ("tra le altre, se del caso"). Per lo stesso motivo, non potranno sussistere dopo il 25 maggio 2018 obblighi generalizzati di adozione di misure "minime" di sicurezza (ex art. 33 Codice) poiché tale valutazione sarà rimessa, caso per caso, al titolare e al responsabile in rapporto ai rischi specificamente individuati come da art. 32 del regolamento. Si richiama l'attenzione anche sulla possibilità di utilizzare l'adesione a specifici codici di condotta o a schemi di certificazione per attestare l'adeguatezza delle misure di sicurezza adottate.

Tuttavia, facendo anche riferimento alle prescrizioni contenute, in particolare, nell'Allegato "B" al Codice, l'Autorità potrà valutare la definizione di linee-guida o buone prassi sulla base dei risultati positivi conseguiti in questi anni; inoltre, per alcune tipologie di trattamenti (quelli di cui all'art. 6, paragrafo 1, lettere c) ed e) del regolamento) potranno restare in vigore (in base all'art. 6, paragrafo 2, del regolamento) le misure di sicurezza attualmente previste attraverso le disposizioni di legge volta per volta applicabili: è il caso, in particolare, dei trattamenti di dati sensibili svolti dai soggetti pubblici per finalità di rilevante interesse pubblico nel rispetto degli specifici regolamenti attuativi (ex artt. 20 e 22 Codice), ove questi ultimi contengano disposizioni in materia di sicurezza dei trattamenti.

Stante la specificità dell'argomento, si invita la Gentile Clientela a voler esaminare la propria situazione specifica al fine di "garantire un livello di sicurezza adeguato al rischio", anche prendendo contatti con la propria software house e/o con la società esterna che gestisce i servizi di sicurezza.