Le risposte del Garante sul regolamento Ue. Niente sconti alle società di revisione

Privacy soft per i professionisti

Autonomi e ditte individuali senza responsabile dei dati

DI ANTONIO CICCIA MESSINA

Società di revisione, di recupero crediti e laboratori analisi mediche tenuti a nominare il Responsabile della protezione dei dati (Rpd/Dpo), previsto dal Regolamento Ue 2016/679 sulla privacy (Rgpd). Esonerato il libero professionista singolo e le imprese individuali. La lista (esemplificativa) di chi è tenuto e chi no a designare l'Rpd la fa il Garante della privacy, che offre un altro tassello di illustrazione operativa degli adempimenti imposti dal regolamento Ue, operativo dal 25 maggio 2018. Ma vediamo di illustrare le risposte del garante ai quesiti più spinosi.

CHI DEVE NOMINARLO. Sono tenuti a nominare l'Rpd, a titolo esemplificativo: istituti di credito; imprese assicurative; sistemi di informazione creditizia; società finanziarie; società di informazioni commerciali; società di revisione contabile; società di recupero crediti; istituti di vigilanza; partiti e movimenti politici; sindacati; caf e patronati; società operanti nel settore delle «utilities» (telecomunicazioni, distribuzione di energia elettrica o gas); imprese di somministrazione di lavoro e ricerca del personale; società operanti nel settore della cura della salute, della prevenzione/diagnostica sanitaria quali ospedali privati, terme, laboratori di analisi mediche e centri di riabilitazione; società di call center; società che forniscono servizi informatici; società che erogano servizi televisivi a pagamento.

CHI NON DEVE NOMINARLO. Non è obbligatoria la nomina del Rpd in relazione a trattamenti effettuati da liberi professionisti operanti in forma individuale; agenti, rappresentanti e mediatori operanti non su larga scala; imprese individuali o familiari; piccole e medie imprese, con riferimento ai trattamenti dei dati personali connessi alla gestione corrente dei rapporti con fornitori e dipendenti. La nomina anche in questi casi viene, però, raccomandata, per dimostrare di essersi responsabilizzati.

CHI NOMINARE. Il problema, che vivono le aziende, è chi nominare Rpd. Sulla carta può essere un soggetto esterno (anche una persona giuridica), ma anche un soggetto interno. Ma se è un dipendente, attenzione al conflitto di interesse. L'Rpd non può essere contemporaneamente sorvegliante e sorvegliato. Dunque meglio evitare di assegnare il ruolo di Rpd a soggetti con incarichi di alta direzione: amministratore delegato; membro del consiglio di amministrazione; direttore generale ecc.); meglio evitare di sceglierlo nell'ambito di strutture aventi potere decisionale sulle finalità e alle modalità del trattamento (direzione risorse umane, direzione marketing, direzione finanziaria, responsabile It ecc.). Timida apertura del Garante va segnalata per l'assegnazione di tale incarico ai responsabili delle funzioni di staff, come ad esempio, il responsabile della funzione legale: ma è sempre da valutare l'assenza di conflitti di interesse in base al contesto di riferimento. Aggiunge chi scrive che anche le funzioni di staff possono, in quanto chiamati a cooperare con le strutture decisionali, risultare coinvolti in decisioni su finalità e mezzi. Attenzione, dunque, a decisioni non ponderate, vista l'esposizione a sanzione amministrativa pecuniaria per cattiva scelta del Rpd.

DATI AL GARANTE. I dati di contatto del responsabile designato devono essere resi pubblici. È una buona prassi, ma non è obbligatorio, pubblicare anche il nominativo dell'Rpd: spetta all'azienda e allo stesso responsabile della protezione dei dati, valutare se sia un'informazione utile o necessaria. Il nominativo dell'Rpd e i relativi dati di contatto vanno invece comunicati al Garante della privacy, utilizzando un modello disponibile sul sito dell'autorità di controllo.

NOMINA UFFICIALE. L'Rpd interno deve essere nominato con uno specifico atto scritto di designazione, mentre con l'esterno si deve sottoscrivere un contratto di servizi.

REQUISITI. Il Garante richiama i requisiti previsti dal Regolamento Ue, i quali non sciolgono un'ambiguità di fondo: a stare aderenti alla norma l'Rpd è un tuttologo «legale-informatico-organizzativo-esperto di audit». Su questa scia, il profilo disegnato da una norma tecnica Uni riflette e amplifica le criticità della definizione dell'Rpd nel regolamento Ue. Il rischio è che di Rpd così non se ne trovi nemmeno uno. Il Garante, conscio della situazione, da un lato richiama all'alta professionalità, ma dall'altro ricorda che all'Rpd non sono richieste specifiche attestazioni formali o l'iscrizione in appositi albi.

IO ONLINE Le faq del Garante sul sito www.italiaoggi.it/documenti

LO SCHEMA DI DECRETO CHE ATTUA IL REGOLAMENTO EUROPEO 2016/679 IN VIGORE DAL 25 MAGGIO

Sconti sulle sanzioni per violazioni del vecchio codice

Privacy Ue a tinte tricolori. Il decreto legislativo di armonizzazione dell'ordinamento italiano al Regolamento Ue 2016/679 (operativo dal 25 maggio 2018) ripesca nella sostanza gran parte del Codice della Privacy (dlgs 196/2003), che formalmente è abrogato per intero. Passano il guado, tra gli altri, i regolamenti privacy per i dati sensibili del settore della pubblica amministrazione, le norme di tutela delle società e persone giuridiche contro le telefonate indesiderate; previsti, infine, sconti sulle sanzioni amministrative per le violazioni amministrative del vecchio codice.

Questo a considerare il testo provvisorio dello schema di provvedimento approvato in via preliminare dal consiglio dei ministri del 21 marzo 2018. Testo che ha importanti novità in materia di legittimo interesse (trattamenti senza bisogno di consenso), anche se proprio questo tema denuncia un andamento altalenante e confuso del legislatore: che dice e si contraddice nel giro di pochi mesi.

Ma vediamo di dare una panoramica di un testo che comunque dovrà ancora percorrere un lungo iter prima di vedere alla luce definitivamente. Non troppo a ridosso del 25 maggio 2018, si spera. Peraltro su molti settori, la nuova privacy può attendere. Lo schema di decreto rinvia al Garante della privacy, guidato da Antonello Soro, il compito di fare la cernita delle sue autorizzazioni generali, selezionando quelle che sopravvivranno e quelle che avranno cessato la loro efficacia.

Antonello Soro

RESPONSABILE INTERNO DEL TRATTAMENTO

Lo schema di decreto salva i delegati interni, anche se si guarda bene dal chiamarli «responsabili del trattamento» e questo per non creare confusione con il Regolamento Ue, che si limita a prevedere i responsabili esterni del trattamento. Quindi, compiti e funzioni possono essere attribuiti a persone fisiche espressamente designate.

Rimane, in caso di outsourcing, la possibilità di designare enti e persone giuridiche, quali responsabili esterni del trattamento ai sensi dell'articolo 28 del regolamento Ue 2016/679.

LEGITTIMO INTERESSE

Il legittimo interesse è un istituto che abilita a trattare dati senza consenso. La legge 205/2017 (commi 1022 e 1023) ha stabilito una procedura di informativa preventiva al Garante nel caso di uso di nuove tecnologie o di trattamenti automatizzati. Si tratta di una procedura che va in direzione opposta alla autodichiarazione delle aziende del proprio interesse prevalente. A rischio di violazione del Regolamento Ue, la procedura, nello schema di decreto legislativo in commento, è destinata ad essere cancellata salvo che per i trattamenti di minori on line ed è ricondotta all'istituto della consultazione preventiva (articolo 36 del Regolamento Ue). Uno stop and go, dunque. A prescindere dal merito delle questioni, aziende ed enti meritano regole certe e non altalene sconcertanti.

DATA RETENTION

Salvo ripensamenti, il testo prevede 24 mesi di conservazione del traffico telefonico e 12 mesi del traffico telematico per scopo di repressione reati. Rimane il problema di coordinare le norme sulla privacy con la legge 167/2017, articolo 24, che ha stabilito una retention molto più lunga (72 mesi).

SANZIONI AMMINISTRATIVE

Oblazione in vista per gli illeciti amministrativi anteriori al 25 maggio 2018. Non c'è un colpo di spugna, ma un forte sconto: si potrà definire la posizione pagando i due quinti del minimo entro 90 giorni dal 25 maggio 2018. Sempre in materia di sanzioni amministrative, il testo dello schema, ad oggi noto, non stabilisce i minimi edittali delle sanzioni amministrative e neppure tratta delle violazioni penali: sono due argomenti cui evidentemente è dedicato un diverso schema di decreto legislativo, considerato che sono due aspetti cruciali dell'armonizzazione della legge italiana al regolamento Ue.

MINORI

Si stabilisce a 14 anni l'età per poter dare il consenso al trattamento dei dati da parte dei social e comunque da parte dei gestori dei servizi della cosiddetta società dell'informazione.

TELEMARKETING

Il testo noto dello schema di decreto richiama la normativa sul registro delle opposizioni. Con questo viene confermato l'impianto dell'opt out per il marketing telefonico e viene confermato che la tutela riguarda tutti i contraenti, comprese le persone giuridiche. In materia si è anche in attesa del regolamento attuativo della legge 5/2018.

REGOLAMENTI DATI SENSIBILI

Nel settore della pubblica amministrazione si va verso la conferma dell'impianto dei regolamenti sul trattamento dei dati sensibili e dei dati genetici e biometrici («particolari categorie di dato personale», nel linguaggio europeo). In materia si conferma esplicitamente che le p.a. trattano dati senza il consenso dell'interessato e, quindi, esclusivamente sulla base di una legge o di un regolamento.

Antonio Ciccia Messina

IO ONLINE Lo schema di decreto sul sito www.italiaoggi.it/documenti