Aggiornamenti REGOLAMENTO EUROPEO GDPR 2016/679

Il 19 settembre è entrato in vigore il decreto legislativo 101/2018, decreto di adeguamento della normativa nazionale alle disposizioni del GDPR. Oggi, quindi, il quadro normativo deve ritenersi più definito e **non ci sono alibi per non procedere con il necessario adeguamento**. Non si può non osservare, però, un disorientamento generale, generato da grossolani e fuorvianti titoloni su presunti esoneri generalizzati per i professionisti e sospensioni delle sanzioni di otto mesi per tutti.

Facciamo chiarezza su presunti esoneri e "periodi di grazia"

Oggi non sappiamo con certezza che tipologia di semplificazioni ci saranno per imprese o professionisti che il decreto di adeguamento rimanda a strumenti di "soft law", in mano principalmente a un Garante per la protezione dei dati personali decisamente rafforzato nelle sue funzioni di vigilanza, controllo e regolamentazione dalle modifiche normative appena entrate in vigore.

Passiamo, quindi, a questa famigerata sospensione di otto mesi (da alcuni definita "stato di grazia") di cui si è tanto parlato e scritto prima che il decreto di adeguamento al GDPR venisse finalmente pubblicato in Gazzetta Ufficiale: ora che il tanto discusso decreto c'è e finalmente è fonte di legge (e non solo fonte di diatribe dottrinali più o meno affidabili) questo "periodo di grazia" esiste o non esiste? L'art. 22 comma 13 del decreto legislativo 10 agosto 2018 n. 101 recita così: "per i primi otto mesi dalla data di entrata in vigore del presente decreto, il Garante per la protezione dei dati personali tiene conto, ai fini dell'applicazione delle sanzioni amministrative e nei limiti in cui risulti compatibile con le disposizioni del Regolamento (UE) 2016/679, della fase di prima applicazione delle disposizioni sanzionatorie".
La sospensione evidentemente non c'è, ma si rintraccia piuttosto una sorta di "preghiera" al Garante, affinché nell'applicare le sanzioni tenga conto (per un periodo di 8 mesi) della situazione di confusione in cui ancora si versa dopo più di due anni dall'entrata in vigore del GDPR.
Sì, perché – ricordiamocelo – il GDPR è in vigore dal maggio del 2016, è fonte primaria del diritto della protezione dei dati personali nel nostro Paese e chiave interpretativa sia del D.Lgs. 101/2018 che ha modificato pesantemente il Codice per la protezione dei dati personali (contenuto ancora oggi nel Decreto legislativo 196/2003, come appunto novellato e parzialmente abrogato da questa ultima riforma finalizzata a coordinarlo con il GDPR), sia di qualsiasi altra normativa nazionale che possa contenere norme rilevanti in materia di protezione dei dai personali (e loro libera circolazione).

Parola d'ordine: trasparenza

Il primo consiglio, anzi la premessa necessaria a tutto ciò che diremo successivamente, è che **ora non si può più scherzare e non ci sono alibi per non procedere con i necessari, importanti e faticosi adeguamenti**. Il GDPR c'è ed è fonte primaria (e prevede sanzioni rilevanti). È in vigore anche il decreto di adeguamento e quindi occorre applicare i principi contenuti in queste normative in modo proattivo e secondo metodi sartoriali.
La parola d'ordine da seguire – ancor prima della accountability, della privacy by design e by default – è **la trasparenza**.
Effettuare una rigorosa, efficace e trasparente mappatura di tutti i trattamenti di dati afferenti alla propria organizzazione, siano essi svolti direttamente dal Titolare o affidati all'esterno, costituisce, infatti, il presupposto necessario di ogni azione di assessment.

Del resto, come si può garantire una efficace informativa ai sensi degli artt. 13 e 14 del GDPR per gli interessati, se non si conoscono i dettagli dei trattamenti sviluppati in qualità di Titolari?
Come si possono rendere effettivi i diritti degli interessati se non si ha un controllo trasparente di sistemi informativi, database, sistemi di gestione documentale e archivi?
Come si può effettuare una esauriente analisi dei rischi ai sensi dell'art. 32 del GDPR e implementare adeguate misure di sicurezza se non si è proceduto a verificare attentamente la tipologia di dati trattati e le relative modalità di trattamento?
Come si può verificare un software o svilupparlo disegnandolo secondo i parametri di protezione delineati dal GDPR se non si conoscono nel dettaglio la natura e le finalità del trattamento dei dati e il loro ambito di circolazione?
Quindi la premessa è conoscersi in **trasparenza**. Solo dopo si può procedere in modo sostanziale e meno formale rispetto **a come abbiamo fatto sino ad oggi, cullandoci su fac simile e raffazzonati "fai da te", o da chi ne ha visto un'opportunità "commerciale" senza avere le caratteristiche di multidisciplinarietà per occuparsi di ambiti così diversi e complessi,**

Il nuovo Codice privacy e la gerarchia delle fonti

Molti oggi si stanno chiedendo cosa dice di nuovo il decreto di adeguamento (**e sono già pronti sul mercato miracolose certificazioni o software, manuali e manualini da sfogliare**). Prima di tutto questo decreto va letto con pazienza e attenzione. Il decreto infatti non è di facile comprensione e va guardato con calma. È utile anche sfogliare con impegno (magari consultando fonti autorevoli) il Codice della protezione dei dati come modificato dal decreto (oggi rubricato Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679. Ma ribadiamo **la fonte primaria rimane il GDPR.**
L'adeguamento alla normativa europea è, infatti, un percorso complesso, delicato che ha un avvio, ma che poi deve andare avanti con costanza, senza mai terminare del tutto. E infine – lo diciamo con il sorriso, ma anche con una certa dose di preoccupazione per ciò che mi capita di leggere in giro – **cercate di diffidare dei miracoli e dei bollini a buon mercato,** perché uno studio approfondito e serio della normativa e della propria organizzazione rimane la migliore soluzione per mettersi in regola.