



Privacy: le novità introdotte dal nuovo decreto legislativo delegato che adegua il Codice Privacy al GDPR

Il 10 agosto 2018 il decreto legislativo italiano n. 101/2018 (il "**Decreto legislativo**") che adegua la precedente normativa sulla protezione dei dati personali in vigore al Regolamento Generale sulla Protezione dei Dati ("**GDPR**") è stato finalmente approvato - dopo un lungo periodo di attesa - e entrerà in vigore il 19 settembre 2018. Il legislatore italiano ha deciso di prevedere l'abrogazione parziale e non totale del precedente Decreto Legislativo 196/2003, denominato "Codice Privacy", mantenendo le disposizioni del Codice Privacy già allineate al contenuto del GDPR.

Di seguito, una sintesi delle principali disposizioni del Decreto Legislativo n. 101/2018:

- **Sanzioni amministrative (articolo 22, §13):** per i primi 8 mesi a partire dalla data di entrata in vigore del Decreto Legislativo, l'Autorità Garante per la protezione dei dati personali adotterà un approccio graduale nell'applicazione delle sanzioni amministrative - nella misura in cui ciò sia compatibile con le disposizioni del GDPR - dato che questa sarà la prima fase di applicazione delle sanzioni;
- **Sanzioni penali (articoli 167 bis e 167 ter):** il Decreto Legislativo conferma l'importanza delle sanzioni penali previste dal Codice Privacy e introduce nuove fattispecie di reato (*e.g.* **comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala e acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala**). In particolare, mentre la comunicazione e diffusione illecita di dati personali trattati su larga scala consiste nella comunicazione o diffusione di un archivio automatizzato o di una

sua parte sostanziale, contenente dati personali trattati su larga scala al fine di trarre profitto per sé o altri o al fine di arrecare danno a terzi, l'acquisizione fraudolenta di dati personali trattati su larga scala consiste nell'acquisizione con mezzi fraudolenti di un archivio automatizzato o di una parte sostanziale di esso, contenente dati personali trattati su larga scala. Entrambi i reati sono puniti con la reclusione (per un periodo tra uno e sei anni nel caso di comunicazione e diffusione illecita di dati personali trattati su larga scala e tra un anno e quattro anni nel caso di acquisizione fraudolenta di dati personali trattati su larga scala);

- **Dati sanitari, biometrici e genetici (articolo 2 septies):** in continuità con la significativa prassi dell'Autorità Garante per la protezione dei dati (una delle più produttive in Europa), il trattamento di tali dati sarà effettuato in conformità alle misure di garanzia disposte dalla stessa Autorità con cadenza biennale. Questa disposizione è di fondamentale importanza per le società che trattano categorie particolari di dati facendo affidamento sulle precedenti autorizzazioni ai sensi del Codice Privacy. Queste società dovranno osservare le misure di sicurezza di cui sopra quando trattano categorie particolari di dati;
- **Consenso dei minori (articolo 2 quinquies):** il decreto abbassa a 14 anni l'età minima per esprimere un consenso lecito e libero in relazione all'offerta diretta di servizi della società dell'informazione ai minori. I minori di età inferiore ai 14 anni hanno bisogno del consenso di chi esercita la responsabilità genitoriale;
- **Modalità semplificate di adempimento al GDPR (articolo 154 bis,§4):** L'Autorità Garante per la protezione dei dati personali promuoverà attraverso linee guida delle disposizioni semplificate per le PMI per conformarsi al GDPR;
- **Codici deontologici e autorizzazioni (Articoli 20 e 21):** le precedenti disposizioni dei codici deontologici continueranno a produrre effetti fino alla definizione della procedura di approvazione condotta dall'Autorità Garante, mentre in relazione alle autorizzazioni generali previste dal precedente Codice Privacy il Decreto legislativo opera una chiara distinzione. Le autorizzazioni generali su materie delegate dal GDPR agli Stati Membri riguardanti il trattamento dei dati necessario per adempiere ad un obbligo legale a cui è soggetto il titolare del trattamento o per l'esecuzione di un compito di

interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare (specificamente ai sensi degli articoli 6.1 (c) ed (e) e 9.2 (b) e (4) nonché del Capitolo IX del GDPR) sono sottoposte ad una verifica di compatibilità con il GDPR e si applicheranno fino alla pubblicazione di un provvedimento da parte del Garante. Al contrario, le autorizzazioni generali diverse da quelle sopra indicate cesseranno di produrre effetti dalla data di entrata in vigore del Decreto Legislativo.

Cosa succede con i procedimenti pendenti dinanzi all'Autorità Garante per la protezione dei dati personali alla data del 25 maggio 2018 (data di applicazione del GDPR)? Il Decreto Legislativo prevede una definizione agevolata, versando due quinti della sanzione prevista precedentemente dal Codice Privacy, entro 90 giorni dalla data di entrata in vigore del Decreto Legislativo.

Alla luce di quanto sopra, suggeriamo alle società di tenere in seria considerazione le nuove disposizioni del suddetto Decreto Legislativo sulla protezione dei dati che integrano quelle previste dal GDPR. Infatti, non solo tali disposizioni sono obbligatorie, ma chiariscono e semplificano molti degli adempimenti introdotti dal GDPR. Pertanto, al fine di ottenere la piena conformità alla normativa applicabile sulla protezione dei dati applicabile, sarà necessario che il processo di adeguamento al GDPR già effettuato o intrapreso dalle aziende prima del 25 maggio 2018 tenga anche in debito conto le ulteriori disposizioni del Decreto Legislativo n.101/2018 nonché i chiarimenti, le linee guida e le misure che saranno prossimamente emanate dall'Autorità Garante per la protezione dei dati sulla base del Decreto Legislativo.

Per ulteriori approfondimenti sulle tematiche affrontate potete far riferimento all'[Avv. Carlo Impalà \(Carlo.Impala@MorriRossetti.it\)](mailto:Carlo.Impala@MorriRossetti.it), Responsabile del Dipartimento Digital-ICT e Data Protection.