

GDPR, 12 risposte per Pa e aziende sul decreto legislativo di adeguamento della normativa italiana

La tecnica di normazione utilizzata dal Governo italiano ha complicato notevolmente il lavoro di comprensione e raccordo del quadro normativo vigente. Proviamo a fare chiarezza con 12 domande e risposte.

di Stefano Mele – Avvocato specializzato di Diritto delle Tecnologie, Privacy e Cybersecurity | 12 settembre 2018, ore 09:00



Dopo un lunghissimo e tormentato *iter* di preparazione, esame e discussione, lo scorso 4 settembre, è stato finalmente pubblicato in [Gazzetta Ufficiale](#) il Decreto Legislativo 101/2018, che ha il compito di armonizzare la normativa nazionale in materia di privacy e protezione dei dati personali al Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016.

La tecnica di normazione utilizzata dal Governo italiano ha, però, complicato notevolmente il lavoro di comprensione e raccordo del quadro normativo vigente, aggiungendo complessità al già gravoso lavoro di adeguamento che le società e le pubbliche amministrazioni hanno dovuto finora approfondire per conformarsi alle richieste del legislatore europeo.

Per provare a fare un po' più di ordine e chiarezza su questo tema, senza ovviamente alcun proposito di completezza ed esaustività, di seguito vengono proposte alcune risposte alle più frequenti domande sulla nuova normativa italiana in materia di protezione dei dati personali.

Qual è la normativa che si deve applicare in Italia in caso di trattamento di dati personali?

Le norme che devono essere prese in considerazione sono quelle contenute all'interno del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, meglio noto come «GDPR», e quelle del famigerato Decreto Legislativo n. 196 del 30 giugno 2003, meglio noto come «Codice Privacy», così come novellato dal recentissimo Decreto Legislativo n. 101 del 10 agosto 2018.

Ci sono novità a seguito del Decreto Legislativo n. 101 in materia di Informativa Privacy e consenso al trattamento dei dati personali?

Nessuna novità. Per l'Informativa Privacy continuano a valere tutte le regole dettate dagli articoli 13 e 14 del GDPR. Stesso discorso per il consenso al trattamento dei dati personali, ove continuano a valere, come regole generali, quelle previste dall'art. 6, comma 1, lett. a), e dall'art. 7 del GDPR.

Qual è l'età minima per ottenere il consenso al trattamento dei dati personali direttamente dall'utente minore?

In relazione all'offerta diretta di servizi della società dell'informazione, il Decreto Legislativo n. 101 afferma che può esprimere il consenso al trattamento dei propri dati personali il minore che abbia compiuto i 14 anni di età. Questa previsione, quindi, abbassa da 16 a 14 gli anni previsti dal GDPR. Invece, il trattamento dei dati personali del minore di età inferiore a 14 anni è lecito solo nel caso in cui sia prestato da chi esercita la responsabilità genitoriale.

Un'accortezza in più dev'essere prevista dal Titolare del trattamento anche nel linguaggio che viene utilizzato per informare il minore. La normativa italiana, infatti, richiede esplicitamente che le informazioni e le comunicazioni relative al trattamento dei dati del minore siano chiare, semplici, concise, esaustive, facilmente accessibili e comprensibili.

Come fa il Titolare del trattamento a rendere l'Informativa Privacy in caso di ricezione spontanea di curriculum vitae ai propri indirizzi?

Continuano a valere le ben note regole di sempre. Infatti, specifica il Decreto Legislativo n. 101, in caso di ricezione di un curriculum spontaneamente trasmesso dall'interessato al fine dell'instaurazione di un rapporto di lavoro, l'Informativa Privacy prevista dall'art. 13 del GDPR dovrà essere fornita al momento del primo contatto utile successivamente all'invio del curriculum.

Il Titolare del trattamento può farsi supportare nelle attività di trattamento dal proprio personale interno?

Nel Decreto Legislativo n. 101 si ribadisce e si specifica quanto già previsto all'interno dell'art. 29 del GDPR. Infatti, il Decreto afferma che, nell'ambito del proprio assetto organizzativo e sotto la propria responsabilità, il Titolare del trattamento può prevedere che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche che operano sotto la sua autorità. Questi soggetti, inoltre, com'è noto, devono essere espressamente designati per tali compiti.

In tema di rapporti di lavoro, inoltre, è interessante notare come il Decreto Legislativo n. 101 abbia espressamente ribadito il divieto di controllo a distanza dei lavoratori previsto dall'art. 4 dello Statuto dei Lavoratori, confermando anche la relativa sanzione penale.

Ci sono novità a seguito del Decreto Legislativo n. 101 in materia di misure di sicurezza da applicare al trattamento di dati personali?

Il Decreto Legislativo n. 101 non apporta alcuna novità alle regole generali in materia di misure di sicurezza. Il Titolare del trattamento, pertanto, può continuare ad avere come riferimento le relative norme previste dal GDPR.

E in materia di diritti degli interessati?

Anche in questo caso il Decreto Legislativo n. 101 non apporta modifiche significative alle regole generali previste dalla normativa europea. Pertanto, il Titolare del trattamento può continuare ad avere come punto di riferimento gli articoli da 15 a 22 del GDPR.

Tuttavia, il Decreto esplicita in maniera molto puntuale i casi in cui l'esercizio dei diritti degli interessati può subire delle limitazioni. È questo il caso, ad esempio, delle richieste che possano pregiudicare i trattamenti svolti per finalità di giustizia o ledere i diritti delle persone decedute. Un'ulteriore nota di interesse, inoltre, è legata all'esplicita tutela della riservatezza dell'identità del dipendente che segnala, ai sensi della normativa sul *whistleblowing*, l'illecito di cui sia venuto a conoscenza in ragione della propria attività.

Quali sono le categorie professionali che devono guardare con maggiore attenzione il contenuto del Decreto Legislativo n. 101?

Il Decreto Legislativo 101 va a prevedere e adeguare la normativa nazionale soprattutto in quei settori dove il trattamento di dati personali risulta più delicato e complesso. È questo il caso, ad esempio, del trattamento di dati personali per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, oppure il trattamento di dati personali svolti in ambito sanitario o per l'erogazione di comunicazioni elettroniche.

Cosa ha previsto il legislatore italiano per le piccole e medie imprese (PMI)?

Effettivamente, il Decreto Legislativo 101 evidenzia con chiarezza l'esigenza di semplificare gli adempimenti per le micro, piccole e medie imprese. Il Garante per la protezione dei dati personali, pertanto, dovrà adottare delle linee guida di indirizzo riguardanti le misure organizzative e tecniche di attuazione dei principi del GDPR per il settore delle PMI, individuando delle modalità semplificate di adempimento degli obblighi del Titolare del trattamento.

Tuttavia, deve essere molto chiaro che ciò non autorizza le PMI a non adeguarsi – anzi, per essere precisi, a non essere già adeguate – al dettato del GDPR e del nostro nuovo Codice Privacy.

Cosa accade adesso per tutti quei provvedimenti emanati dal Garante per la protezione dei dati personali antecedenti al 25 maggio 2018 (come, ad esempio, quelli in materia di videosorveglianza, amministratori di sistema, marketing, ecc.)?

A decorrere dal 25 maggio 2018, tutti i provvedimenti del Garante per la protezione dei dati personali continuano ad applicarsi, in quanto compatibili con il GDPR e con le disposizioni del nuovo Codice Privacy. Discorso leggermente differente, invece, deve essere fatto per le autorizzazioni generali, per le quali il Garante dovrà pronunciarsi sulla loro compatibilità con il nuovo impianto normativo – ed eventualmente aggiornarle – entro 90 giorni dalla data di entrata in vigore del Decreto Legislativo 101.

Cosa succede se i dati personali sono trattati in violazione della disciplina vigente?

I dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati.

Oltre alle ben note sanzioni amministrative, la legislazione italiana prevede anche delle sanzioni penali per il Titolare del trattamento?

Il Decreto Legislativo n. 101, all'articolo 167 e ss., prevede alcuni illeciti penali, che si configurano soltanto nel caso in cui la condotta del Titolare del trattamento sia finalizzata a trarre per sé o per altri profitto, ovvero per arrecare danno all'interessato. Questi illeciti si riferiscono al "*Trattamento illecito di dati*" (art. 167), alla "*Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala*" (art. 167-bis) e all'"*Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala*" (art. 167-ter). Ulteriori illeciti penali sono previsti per "*Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio di poteri del Garante*" (art. 168), per l'"*Inosservanza di provvedimenti del Garante*" (art. 170) e per le "*Violazioni delle disposizioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori*" (art. 171), oltre le eventuali pene accessorie previste dall'art. 172.

Per approfondire

- [Stefano Mele \(WsW\)](https://www.key4biz.it) FONTE <https://www.key4biz.it>

