protiviti®
Face the Future with Confidence

Settembre
2018

19 settembre 2018: entra in vigore il decreto legislativo di adeguamento al GDPR

In data 19 settembre 2018 il tanto atteso decreto legislativo di adeguamento alle disposizioni del Regolamento Europeo in materia di protezione dei dati personali "General Data Protection Regulation" (di seguito "GDPR" o "Regolamento") è entrato ufficialmente in vigore (D. Lgs. 101/2018), essendo decorso il termine ordinario di *vacatio legis* dalla sua pubblicazione in Gazzetta Ufficiale.

In tal modo, risulta definitivamente esercitata la delega contenuta nella legge n. 163 del 25 ottobre 2017, il cui art. 13 demandava al Governo il compito di adottare i decreti legislativi necessari per adeguare entro 6 mesi la normativa nazionale al GDPR.

Il tema della protezione dei dati personali, ad oggi, risulta pertanto regolato dal GDPR e dal D. Lgs. 196/2003, così come modificato/integrato dal D. Lgs. 101/2018, che ha apportato le modifiche necessarie a rendere la disciplina vigente coerente con la normativa comunitaria. Occorre comunque tenere presente che le disposizioni in esso contenute devono essere lette in accordo con quelle del GDPR, che rimane pur sempre la fonte di rango primario.

Con questo Flash Report, Protiviti intende fornire alcuni spunti alle aziende, al fine di comprendere gli impatti che la nuova disciplina ha sulle attività di adeguamento al GDPR finora poste in essere, fermo restando che occorre tenere a mente le diverse scadenze contenute all'interno del novellato Codice Privacy.

Le principali novità

- **Consenso del minore**: in attuazione dell'art. 8 co. I del GDPR, che lascia agli Stati membri la possibilità di stabilire un'età inferiore ai 16 anni per il consenso del minore in relazione ai servizi offerti tramite Internet, l'**art. 2 – *quinquies*** del Codice Privacy prevede che il minore che abbia compiuto **14 anni** possa prestare un autonomo consenso al trattamento dei dati personali.

  A tal fine, la norma specifica espressamente che il titolare deve fornire al minore le informazioni relative al trattamento dei dati personali che lo riguardano utilizzando un linguaggio semplice, chiaro e facilmente comprensibile.

  Al di sotto di tale limite di età, il consenso deve essere necessariamente prestato da parte di chi esercita la responsabilità genitoriale.

- **Trattamento di dati genetici, biometrici e relativi alla salute**: conformemente a quanto disposto dall'art. 9 del GDPR, tali categorie di dati possono essere oggetto di trattamento purché esso avvenga nel rispetto delle condizioni previste dal medesimo articolo (consenso esplicito, assolvimento di obblighi ed esercizio di diritti in materia di diritto del lavoro e della sicurezza sociale, ecc.), oltre che in conformità alle **misure di garanzia** che verranno previste da un provvedimento *ad hoc* del **Garante Privacy**. Esso sarà aggiornato con cadenza almeno biennale e sottoposto a consultazione pubblica per un periodo non inferiore a 60 giorni.

- **Trattamento di dati relativi a condanne penali e reati ("dati giudiziari")**: l'**art. 2 – *octies*** del Codice Privacy introduce specifiche limitazioni per le ipotesi in cui tali dati non vengano trattati sotto il controllo dell'Autorità Pubblica. *In primis*, il trattamento deve essere espressamente autorizzato da una norma di legge o di regolamento riguardante, ad esempio, l'adempimento di obblighi o l'esercizio di diritti nell'ambito dei rapporti di lavoro, o l'accertamento del requisito di idoneità morale di coloro che partecipano a gare d'appalto.

  In assenza di tali norme di legge o di regolamento, il trattamento è ammesso solo se autorizzato da decreto del Ministro della Giustizia.

- **Limitazioni ai diritti degli interessati** di cui agli artt. 15 – 22 del GDPR: l'**art. 2 – *undecies*** prevede che tali diritti possano subire limitazioni qualora entrino in contrasto, ad esempio, con:

  - Disposizioni in materia di antiriciclaggio;
  - Svolgimento delle investigazioni difensive o esercizio di un diritto in sede giudiziaria;
  - Tutela dell'identità del segnalante, ai sensi della l. 179/2017 ("*whistleblowing*").

- **Diritti riguardanti le persone decedute**: l'**art. 2 – *terdecies*** detta specifiche disposizioni in ordine ai dati di **persone decedute**, stabilendo che i diritti di cui agli artt. 15 – 22 del GDPR possano essere esercitati da parte di chi ha un interesse proprio, dal mandatario o per ragioni familiari meritevoli di tutela. D'altro canto, tali diritti non possono essere esercitati se espressamente vietato dalla legge o dall'interessato, mediante una dichiarazione espressa in tal senso.

- **Persone autorizzate al trattamento dei dati personali**: l'**art. 2 – *quaterdecies*** attribuisce al titolare o al responsabile del trattamento il diritto di assegnare, a persone fisiche che operano sotto la loro autorità, specifici compiti e funzioni connessi al trattamento di dati personali. Al riguardo, si fa presente che il Garante Privacy, nella Guida all'applicazione del GDPR, aveva precisato che le disposizioni in tema di incaricati del trattamento contenute all'interno del Codice Privacy (ante D. Lgs. 101/2018) potevano ritenersi pienamente compatibili con la struttura e la filosofia del GDPR.

  Ne deriva che è rimessa al titolare/responsabile del trattamento la possibilità di individuare la modalità più idonea per attribuire le autorizzazioni citate, anche utilizzando i modelli di nomina ad incaricato del trattamento predisposti sotto la vigenza del precedente Codice Privacy.

- **Tutela amministrativa e giurisdizionale**: l'**art. 140 – *bis*** attribuisce all'interessato, che ritenga di aver subito una violazione dei propri diritti in materia di protezione dei dati personali, la possibilità di presentare alternativamente reclamo al Garante Privacy o ricorso dinanzi all'Autorità Giudiziaria Ordinaria, come era già previsto dall'art. 145 del Codice Privacy (ante D. Lgs. 101/2018), ora abrogato.

- **Semplificazioni per le micro, piccole e medie imprese**: il **co. IV** dell'**art. 154 – *bis*** attribuisce al Garante Privacy la possibilità di adottare linee guida di indirizzo che vadano a semplificare gli adempimenti previsti in capo al titolare del trattamento.

- **Sanzioni:** diverse le modifiche apportate dal D. Lgs. 101/2018 all'impianto sanzionatorio previsto dal precedente Codice Privacy. In particolare:

  - **Sanzioni amministrative pecuniarie**: l'**art. 166** contiene un nuovo procedimento per l'adozione dei provvedimenti correttivi e sanzionatori in capo al Garante Privacy;
  - **Sanzioni penali**: le fattispecie di reato attualmente previste sono di seguito riportate, ovvero:
    - **Art. 167:** trattamento illecito di dati (reclusione da 6 mesi a 1 anno e 6 mesi o da 1 a 3 anni, a seconda della tipologia di illecito posto in essere);
    - **Art. 167 – *bis*:** comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala (reclusione da 1 a 6 anni);
    - **Art. 167 – ter:** acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala (reclusione da 1 a 4 anni);
    - **Art. 168:** falsità nelle dichiarazioni al Garante o nell'interruzione dei compiti o dell'esercizio di poteri del Garante (reclusione da 6 mesi a 3 anni);
    - **Art. 170:** inosservanza di provvedimenti del Garante Privacy (reclusione da 3 mesi a 2 anni);

- **Art. 171:** violazione delle disposizioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori (ammenda da € 154 a € 1.549 o arresto da 15 giorni a 1 anno).

- **Settori specifici:** il novellato Codice Privacy contiene disposizioni relative ad ambiti specifici, di seguito riportati a titolo esemplificativo:
  - **Sanità**: sono specificate le modalità per informare l'interessato in ordine al trattamento dei dati che lo riguarda, applicabili alle strutture sanitarie pubbliche e private e agli esercenti professioni sanitarie;
  - **Trattamenti di dati personali effettuati a fini statistici o di ricerca scientifica**: essi devono avvenire nel rispetto delle regole delle regole deontologiche che verranno promosse dal Garante, e che individuino, tra le altre cose, modalità semplificate per la prestazione del consenso in relazione al trattamento di categorie particolari di dati personali;
  - **Rapporti di lavoro**: è stato introdotto il nuovo **art. 111 – *bis***, il quale specifica che, nel caso di ***curricula*** spontaneamente trasmessi dagli interessati, l'informativa andrà resa al primo contatto utile (ad es., al momento del colloquio o del primo contatto via email). Inoltre, non è necessario che il candidato inserisca all'interno del CV il consenso al trattamento dei propri dati, essendo quest'ultimo fondato sulla base giuridica di cui all'art. 6 co. I l b) del GDPR ("*esecuzione di un contratto di cui l'interessato è parte o esecuzione di misure precontrattuali*"). Tale principio era già stato ribadito dal Garante Privacy in un provvedimento risalente al 10 gennaio 2002, il quale aveva precisato che l' "autorizzazione" per il trattamento dei dati personali spesso sollecitata nei CV trasmessi dai candidati risultava essere del tutto generica e spesso slegata da un'idonea informativa**;**
  - **Comunicazioni elettroniche:** i nuovi artt. **132 *ter*** e **132 *quater*** prevedono l'obbligo in capo ai fornitori di servizi di comunicazione elettronica di adottare misure di sicurezza adeguate al rischio, oltre che di informare adeguatamente gli utenti in ordine all'eventuale sussistenza di un particolare rischio di violazione della rete.

- Infine, il D. Lgs. 101/2018 contiene alcune **disposizioni transitorie**. Ad esempio:
  - **Autorizzazioni generali del Garante Privacy:** dal 19 settembre 2018, le autorizzazioni finora adottate dal Garante Privacy cessano di produrre effetti (es. autorizzazione al trattamento dei dati sensibili nei rapporti di lavoro, dei dati genetici, dei dati a carattere giudiziario da parte di privati, enti pubblici economici e soggetti pubblici).

    D'altro canto, entro 90 giorni dalla data di entrata in vigore del D. Lgs. 101/2018, è attribuito all'Autorità il potere di emanare uno specifico provvedimento che individui le prescrizioni già adottate in merito a specifici trattamenti compatibili con le nuove disposizioni e provveda, se necessario, al loro aggiornamento;
  - I trattamenti che presentano **rischi specifici** e che siano **già in corso** alla data di entrata in vigore del Decreto, possono essere proseguiti qualora siano **autorizzati** da disposizioni di legge, ovvero siano stati sottoposti a **verifica preliminare** o **autorizzazione** del Garante Privacy;
  - **Procedimenti sanzionatori amministrativi pendenti**: entro 90 giorni dalla data di entrata in vigore del D. Lgs. 101/2018, per i procedimenti non ancora definiti con ordinanza-ingiunzione alla data del 25 maggio 2018, è ammesso il pagamento dei 2/5 del minimo edittale. Ove entro tale termine, non si proceda a questo pagamento ridotto, l'atto con il quale sono stati notificati gli estremi della violazione o l'atto di contestazione immediata assumono il valore dell'ordinanza-ingiunzione senza obbligo di ulteriore notificazione (**art. 18 co. I**);
  - L'**art. 22 co. XIII** stabilisce che il Garante Privacy terrà conto della fase di **prima applicazione delle disposizioni sanzionatorie** nei primi **8 mesi** di applicazione del decreto. Ciò, naturalmente, non contiene in alcun modo un rinvio nell'applicazione delle sanzioni previste dal GDPR e dal Codice Privacy.

Conclusioni

L'entrata in vigore del D. Lgs. 101/2018 dà avvio ad una nuova fase per quanto concerne la disciplina in materia di protezione dei dati personali.

Infatti, le singole organizzazioni avranno ora l'onere di rivedere il proprio assetto tecnico - organizzativo in tema di privacy tenendo conto non soltanto delle disposizioni emanate a livello europeo, ma altresì di quelle contenute nel decreto appena entrato in vigore.

Ad esempio, per quanto concerne il trattamento di categorie particolari di dati personali, le aziende dovranno verificare che il trattamento avvenga non soltanto nel rispetto delle condizioni previste dall'art. 9 del GDPR, ma anche in conformità alle misure di garanzia che verranno adottate dal Garante Privacy. Ancora, con riferimento ai diritti degli interessati previsti dagli artt. 15 – 22 del GDPR, il relativo esercizio dovrà essere garantito tenendo altresì conto delle limitazioni che gli stessi potrebbero dover subire, così come indicato dal nuovo Codice Privacy.

Il Garante Privacy, dal canto suo, svolge un ruolo fondamentale nell'attività di coordinamento tra le due normative: basti pensare, ad esempio, al potere allo stesso riconosciuto di adottare misure di garanzia a tutela dei dati genetici, biometrici o relativi alla salute, o ancora alla possibilità di introdurre semplificazioni per le PMI. Il novellato Codice Privacy contiene, infatti, continui rinvii al potere dell'Autorità Garante di emanare provvedimenti che vadano a specificare/attuare le disposizioni ivi contenute.

* * *

Protiviti, da anni impegnata nell'assistenza ai propri Clienti su tematiche di ***Information & Cyber Security e di Data Protection & Privacy***, è in grado di affiancare la vostra Organizzazione nell'adeguamento del proprio sistema di gestione Privacy alle evoluzioni normative e del contesto di business, fornendo anche supporto operativo nelle attività di monitoraggio e risposta in caso di data breach, nonché offrendo strumenti informatici in grado di automatizzare e tracciare i processi essenziali (gestione del registro delle attività di trattamento, gestione delle richieste di esercizio dei diritti da parte degli interessati, esecuzione Data Protection Impact Assessment, etc.)

Contatti

Enrico Ferretti – *Managing Director*

enrico.ferretti@protiviti.it
02.65506301

Andrea Gaglietto – *Manager*

andrea.gaglietto@protiviti.it
02.65506301

Stefano Micci – *Manager*

stefano.micci@protiviti.it
02.65506301

protiviti®