prorevi auditing

NOTA INFORMATIVA N. 10/2018

IL NUOVO REGOLAMENTO SULLA PRIVACY

Il nuovo regolamento sulla privacy (GDPR) entra in vigore il 25 maggio 2018 e prevede adempimenti più complessi, sanzioni più pesanti, maggiori tutele nel trattamento dei dati personali.

Il 4 maggio 2016 è stato pubblicato sulla Gazzetta Ufficiale dell'Unione Europea il Regolamento Europeo 2016/679, c.d. General Data Protection Regulation (GDPR), relativo alla protezione delle persone fisiche con riguardo al trattamento e alla libera circolazione dei dati personali, che abroga e/o sostituisce numerose disposizioni del D.Lgs 30 giugno 2003, n. 196 (il "Codice privacy"). Il Regolamento si applicherà in tutti gli Stati membri a partire dal 25 maggio 2018, termine entro il quale le imprese, i professionisti e le pubbliche amministrazioni dovranno aver allineato le proprie attività e i processi interni ai nuovi obblighi previsti dal Regolamento.

Sotto l'aspetto oggettivo, il Regolamento si applica a tutti i trattamenti di dati personali, automatizzati e non, effettuati da soggetti (titolari o responsabili del trattamento), anche non stabiliti nell'Unione Europea, in relazione a dati personali di individui che si trovano del territorio dell'Unione, indipendentemente dal luogo in cui il trattamento è effettuato.

Da un punto di vista soggettivo, gli obblighi e i principi si applicano sia ai soggetti privati (persone fisiche e/o giuridiche) sia alle Pubbliche amministrazioni, restando esclusi tutti i trattamenti effettuati da una persona fisica nell'ambito di attività a carattere esclusivamente personale o domestico.

Il **presupposto di liceità** del trattamento è sempre rappresentato dal consenso dell'interessato (preceduto dall'informativa), fatta eccezione per una serie di casi di trattamento "necessario", quali l'adempimento di un obbligo legale o contrattuale; la salvaguardia degli interessi vitali dell'interessato o di altra persona fisica; l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.

I **principi generali**, che enunciano le norme fondamentali che i titolari devono rispettare per il trattamento dei dati personali, sono i seguenti:

- ✓ *limitazione della finalità*: ciascun titolare deve individuare la finalità che intende perseguire prima di procedere al trattamento e quali dati personali deve trattare in relazione a tale finalità;
- ✓ *minimizzazione dei dati*: i dati personali oggetto di trattamento devono essere "adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati";
- ✓ *limitazione della conservazione*: i dati personali devono essere "conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati";

✓ *data protection by design and by default*: il titolare del trattamento è tenuto ad adottare misure tecniche e organizzative adeguate ad assicurare la protezione dei dati personali, la riduzione al minimo del loro trattamento, la loro sicurezza e confidenzialità fin dalla progettazione (*by design*) e a non abbandonare mai questo approccio, assicurandone l'implementazione come elemento predefinito e non derogabile del trattamento (*by default*).

In generale, l'attenzione del legislatore europeo è focalizzata sulla protezione dei dati personali e tutela delle persone fisiche (gli interessati), per rispettarne i diritti e le libertà fondamentali, in quanto la tecnologia odierna consente alle informazioni di raggiungere in pochi secondi tutti gli angoli del pianeta, col rischio di violare la libertà e la riservatezza dell'individuo a cui i dati si riferiscono.

Rilevanti sono gli **impatti sulla gestione ed organizzazione interna** dei soggetti del trattamento, al cui vertice si trova il *titolare del trattamento* o *controller* (o, se previsto, due o più *contitolari*), a cui è affidato il compito di decidere autonomamente le finalità, le modalità, le garanzie e i limiti del trattamento dei dati personali, adottando le misure di sicurezza e gli adempimenti previsti dalla normativa, ed assumendo la responsabilità del trattamento effettuato direttamente o da altri per suo conto.

Il titolare può delegare una parte delle proprie funzioni a uno o più *responsabili del trattamento* o *processor.* Alla base della piramide organizzativa si trova chi effettua il trattamento (c.d. *incaricato del trattamento*) che può essere lo stesso responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento. Altre due figure generalmente obbligatorie sono *l'amministratore di sistema* a cui è delegata la gestione e la manutenzione dei sistemi hardware e software mediante i quali sono gestiti i dati personali e il *responsabile della protezione dei dati* o *Data Protection Officer,* collocato al di fuori dell'organizzazione gerarchico-piramidale, con funzioni di supporto e di controllo sull'osservanza del Regolamento.

Per quanto riguarda gli **adempimenti**, scompare l'obbligo di procedere alla notifica dei trattamenti, sostituito dall'obbligo di tenuta del registro dei trattamenti, ed è previsto il dovere di effettuare una valutazione di impatto (*Data Protection Impact Assessment – DPIA)* quando il trattamento presenti specifici rischi per i diritti fondamentali e le libertà personali degli interessati.

Il titolare che riscontra una violazione dei dati personali (*data breach*) è tenuto a notificare la circostanza all'Autorità nazionale di controllo (Anc), a comunicarla all'interessato, adottando le misure necessarie a ridurne le conseguenze dannose, nonché ad aggiornare il registro delle violazioni. Il Regolamento raccomanda anche l'elaborazione ed approvazione di un codice di condotta e l'ottenimento di una certificazione che dimostri la conformità al Gdpr.

I titolari devono anche garantire l'esercizio dei diritti agli interessati, tra cui il diritto all'informazione, di opposizione, all'accesso ai propri dati personali, all'oblio e alla portabilità dei dati personali.

Le **sanzioni**, comminate dall'Anc, possono arrivare fino a 10 milioni di euro per le persone fisiche e al 2% del fatturato annuo dell'esercizio precedente per le imprese, in caso di violazione di obblighi del Titolare e/o Responsabile, e fino a 20

milioni di euro e al 4 % del fatturato in caso di violazione dei principi di base del Trattamento (es. condizioni relative al consenso), dei diritti degli interessati o di trasferimenti *cross-border* di dati personali. Restano ferme le responsabilità civili e penali nei casi di violazione.

15 febbraio 2018