RATIO QUOTIDIANO
Il commento e la critica delle più importanti notizie del momento

GESTIONE D'IMPRESA

di LUCA LEONI

Regolamento UE 2016/679 e il cosiddetto "approccio basato sul rischio"

L'entrata in vigore del Regolamento UE 2016/679 (RGPD o GDPR) introduce l'approccio basato sul rischio e il principio di accountability (responsabilizzazione) per i titolari e i responsabili. Vediamo di cosa si tratta.

Dalla lettura integrale del testo del RGPD emerge con forza il concetto di ***"responsabilizzazione",*** *accountability* nell'accezione inglese, in capo ai titolari e ai responsabili del trattamento. In estrema sintesi, questi due soggetti devono preoccuparsi di adottare comportamenti proattivi tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del RGPD (si vedano artt. 23-25, in particolare, e l'intero Capo IV del regolamento). Si tratta di una grande novità per la protezione dei dati in quanto **viene affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali,** nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel RGPD.

Il primo fra tali criteri è sintetizzato dall'espressione inglese *"data protection by default and by design"* (si veda art. 25), ossia la necessità di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili *"al fine di soddisfare i requisiti"* del RGPD e tutelare i diritti degli interessati, tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati. Tutto questo **deve avvenire a monte, prima di procedere al trattamento** dei dati vero e proprio *("sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso",* secondo quanto afferma l'art. 25, c. 1 del RGPD) e richiede, pertanto, un'analisi preventiva e un impegno applicativo da parte dei titolari che devono sostanziarsi in una serie di attività specifiche e dimostrabili.
Fondamentali fra tali attività sono quelle connesse al secondo criterio individuato nel RGPD rispetto alla gestione degli obblighi dei titolari, ossia il **rischio inerente al trattamento.** Quest'ultimo è da intendersi come rischio di impatti negativi sulle libertà e i diritti degli interessati (considerando 75-77); tali impatti dovranno essere analizzati attraverso un apposito processo di valutazione (v. artt. 35-36), tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) che il titolare ritiene di dover adottare per mitigare tali rischi (utili, al riguardo, le linee-guida in materia di valutazione di impatto sulla protezione dei dati pubblicate dal ex Gruppo *"Articolo 29").*
All'esito di questa valutazione di impatto il titolare potrà decidere in autonomia se iniziare il trattamento (avendo adottato le misure idonee a mitigare sufficientemente il rischio) ovvero consultare l'autorità di controllo competente per ottenere indicazioni su come gestire il rischio residuale; l'autorità non avrà il compito di *"autorizzare"* il trattamento, bensì di indicare le misure ulteriori eventualmente da implementare a cura del titolare e potrà, ove necessario, adottare tutte le misure correttive ai sensi dell'art. 58: dall'ammonimento del titolare fino alla limitazione o al divieto di procedere al trattamento.

Dunque, **l'intervento delle autorità di controllo sarà principalmente *"expost",*** ossia si collocherà successivamente alle determinazioni assunte autonomamente dal titolare; ciò spiega l'abolizione a partire dal 25.05.2018 di alcuni istituti previsti dalla Direttiva del 1995 e dal Codice italiano, come la notifica preventiva dei trattamenti all'autorità di controllo e il cosiddetto *priori checking,* o verifica preliminare ex art. 17 del Codice, sostituiti da **obblighi di tenuta di un registro dei trattamenti** da parte del titolare/responsabile e, appunto, di effettuazione di valutazioni di impatto in piena autonomia, con eventuale successiva consultazione del Garante, tranne per alcune specifiche situazioni di trattamento (art. 36, par. 5 del RGPD).