Volume 1 | Numero 7
06/06/2020

GDPR e Riservatezza ed Integrità.

Pillole di Privacy

Citazione

"Le cose che accadono in maniera consensuale fra persone maggiorenni e nella giusta riservatezza senza arrecare danno a nessuno, non possono interessare nessun'altro oltre a chi lo fa." *(Max Mosley- ex presidente della Federazione Internazionale dell'Automobile).*

I principi del GDPR: Riservatezza ed Integrità.

Per comprendere al meglio il senso dei principi di riservatezza ed integrità, occorre partire da un assioma: chiunque tratti i dati personali deve garantire delle misure adeguate per proteggere i dati dei privati da trattamenti illegittimi[1].

La protezione attuata è volta a tutelare la integrità dei dati la riservatezza degli stessi.

La protezione attuata dal titolare ovvero dal responsabile deve avvenire non solo in riferimento al dato in quanto tale, ma anche all'intera procedura di trattamento attinente direttamente alle tecnologie utilizzate.

La tutela dei dati, pertanto, si esplicherà in una valutazione riguardante il livello di sicurezza adottato.

Il titolare del trattamento e il responsabile del trattamento hanno l'obbligo di mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza appropriato al rischio[2].

La valutazione del rischio dovrà considerare le violazioni dovute ad accessi non autorizzati, ma anche dovute alla perdita o distruzione di dati.

In riferimento ai principi di riservatezza e integrità il GDPR non specifica analiticamente le misure di sicurezza necessarie a prevenire il rischio.

[1] Cfr. Art. 5 del GDPR 679/2016.
[2] Cfr. Art. 32 del GDPR 679/2016.

In pratica, la norma ha un solo scopo, raggiungere il risultato, senza vincolare l'operatore con misure minime, le quali, peraltro, potrebbero non essere sufficienti a garantire la protezione dei dati.

Questa carenza ha generato l'effetto positivo di tutelare anche sproporzionatamente i dati, tanto che, pur potendo scegliere qualsiasi metodologia, i titolari sempre più spesso tendono ad utilizzare misure di sicurezza molto potenti, quali la crittografia e la pseudonimizzazione.

Queste due misure sono individuate quali strumenti rilevanti per garantire un elevato livello di sicurezza[3].

Tuttavia, sarà sempre obbligo del titolare del trattamento o del responsabile[4]:

- Assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento.
- Ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico.
- Testare, verificare e valutare l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

[3] Art. 32.1 lett. A) del GDPR 679/2019.
[4] Art. 32.1 lett. B) C) D) del GDPR 679/2019.