Protezione dei dati personali

Privacy e dati personali: cosa cambia con l'arrivo delle nuove regole europee per gli Enti locali

Paolo Braccini - Dottore commercialista; Esperto in organizzazione e valutazione degli Enti locali e di Emanuele Cofanelli - Esperto in scienze giuridiche e privacy

Il 25 maggio 2018 diventerà ufficialmente operativo il nuovo Regolamento generale in materia di Protezione dei Dati personali. Il GDPR, acronimo di "General Data Protection Regulation" va ad abrogare, dopo oltre un ventennio, la cosiddetta direttiva madre n. 95/46/C, che, fino ad oggi, costituiva il quadro normativo di riferimento a livello europeo. Il nuovo Regolamento, composto da 99 articoli e 173 "considerando", costituisce, insieme alla Direttiva (UE) n. 2016/680, il "Pacchetto di protezione dei dati" elaborato ed approvato dall'Unione Europea.

Introduzione

Il Reg. (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 fa riferimento a dati concernenti persone identificate o identificabili in possesso di vari soggetti e quindi anche della Pubblica amministrazione utilizzabili per le proprie finalità istituzionali. Dati che devono essere trattati nei limiti delle funzioni dell'ente, il quale avrà anche l'obbligo di proteggerli con nuovi strumenti.

L'introduzione del GDPR viene ritenuta una riforma necessaria poiché va a definire un quadro comune europeo in materia di tutela dei dati personali, in coerenza con una più generale armonizzazione normativa europea.

L'obiettivo del legislatore europeo, infatti, è quello uniformare questa importante e delicata disciplina, eliminando le numerose barriere e disomogeneità che si erano create nel corso del tempo e che andavano ad ostacolare la libera circolazione dei dati personali all'interno dell'EU, con la conseguente penalizzazione delle attività economiche.

Le nuove regole

Il nuovo apparato normativo si regge su un nuovo principio di fondamentale importanza: la responsabilizzazione, ovvero il principio di *accountability* (nell'accezione inglese).

Tale concetto rappresenta un'assoluta novità nel campo della protezione dei dati personali, in quanto il titolare del trattamento, oltre ad avere l'esclusiva competenza per il rispetto dei principi e delle regole previste dal GDPR, deve anche essere in grado di comprovarne il corretto adempimento.

Ai titolari, altresì, viene affidato 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 indicati dal regolamento. Come specifica chiaramente l'art. 25 del GDPR, uno di quei criteri è sicuramente rappresentato dall'espressione anglofona "*data protection by default and by design*" ossia dalla necessità di configurare il trattamento prevedendo dall'inizio, ovvero fin dalla fase di progettazione, le garanzie indispensabili "al fine di soddisfare i requisiti" del regolamento 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.

Spetta dunque al titolare mettere in atto una serie di misure tecniche ed organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali strettamente necessari per ogni specifica finalità del trattamento.

Tra le nuove attività previste dal GDPR, riguardo agli obblighi dei titolari, saranno fondamentali quelle relative alla **valutazione del rischio inerente il trattamento**. Quest'ultimo è da intendersi come rischio da impatti negativi sulle libertà e sui diritti degli interessati; tali impatti dovranno essere analizzati attraverso un apposito processo di valutazione, tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) che il titolare ritiene di dover adottare per diminuirne l'impatto.
A tal proposito, possiamo prendere in considerazione un'importante procedura prevista dall'art. 35 del Regolamento: la **valutazione di impatto sulla protezione dei dati**, detta anche *DPIA*. Essa rappresenta un adempimento interno previsto quando il trattamento, in particolare se eseguito mediante l'uso di nuove tecnologie, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche. La *DPIA*, acronimo di *Data Protection Impact Assessment*, è un fondamentale strumento che realizza il principio della responsabilizzazione, in quanto aiuta il titolare a rispettare le prescrizioni del GDPR e anche ad attestare l'adozione di misure idonee a garantire il rispetto di tali prescrizioni.

Le altre novità del GDPR

Il GDPR prevede alcune nuovi principi caratteristici, quali:

PRINCIPI	CONTENUTI
Privacy by design	Obbligo di adottare fin dall'inizio del processo produttivo (tanto di un software quanto di un prodotto) comportamenti in grado di assicurare la correttezza, l'integrità, la riservatezza e la sicurezza dei dati;
Privacy by default	Adozione di strumenti e modalità di trattamento dei dati in grado di ridurre il rischio (es. ridurre i passaggi da un ufficio all'altro)
Anonimizzazione	Obbligo di tenere separato il dato dal suo identificativo, principio quasi ovvio, che pone però il problema di dotarsi di un sistema per abbinarli e ancora una volta si tratta di una questione organizzativa, più che tecnologica
Principio di accountability	Obbligo non solo di rispettare le norme del Regolamento, ma anche di mettere in pratica quanto stabilito in fase di analisi dei rischi
Sarà il titolare del trattamento a dover dimostrare, in caso di controversie, di aver adottato tutte le precauzioni previste per ridurre al minimo i rischi. Enti pubblici e imprese saranno dunque maggiormente responsabilizzati, anche attraverso sanzioni piuttosto elevate	

Novità circa gli adempimenti a carico degli Enti locali

L'approccio all'adempimento da parte degli Enti locali dovrà essere tecnologico e garantire un adeguamento della struttura organizzativa, a partire dalla nuova figura del DPO *- Data Protection Officer -*, che ricoprirà un ruolo poliedrico con competenze normative, tecniche, comunicative e una profonda conoscenza dell'organizzazione del settore in cui si trova ad operare.
Per raggiungere il risultato della responsabilizzazione, ma anche per farsi trovare pronti alla scadenza del 25 maggio, il Garante per la protezione dei dati personali ha suggerito alle PA alcuni specifici adempimenti da effettuare, con assoluta priorità (riepilogati in tavola 1), quali:
1) Designazione del responsabile della protezione dei dati (RPD o DPO nella sua accezione inglese, che sta per *Data Protection Officer*). Obbligatoria per le PA, rappresenta una figura essenziale nel nuovo quadro normativo, in quanto costituisce il fulcro del processo di attuazione del principio di responsabilizzazione. Tra le sue attività principali, vi sono sicuramente, informare e consigliare l'Ente su cosa richiede il GDPR, ma soprattutto dovrà anche sorvegliare sull'esatta esecuzione degli adempimenti previsti dalla nuova normativa in materia di protezione dei dati;
2) Istituzione del registro delle attività di trattamento. Come specifica il regolamento, esso rappresenta un documento scritto, anche in formato elettronico, nel quale sono presenti una serie di informazioni obbligatorie che riguardano le attività di trattamento eseguite dal titolare del trattamento. Il registro, indispensabile per ogni valutazione e analisi del rischio, costituisce uno strumento fondamentale non soltanto ai fini dell'eventuale supervisione da parte del Garante, ma anche allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno del soggetto pubblico.
3) La notifica delle violazioni dei dati personali (*DATA BREACH*) che, a norma di Regolamento, dovrà essere effettuata all'Autorità di controllo preposta entro 72 ore. La cosiddetta *Data breach*, definita dagli artt. 33 e 34 del Regolamento, consiste in qualunque avvenimento che potrebbe mettere a rischio i dati personali in possesso del titolare del trattamento. Estremamente importante, soprattutto nel nostro panorama attuale caratterizzato da una crescente minaccia alla sicurezza dei sistemi informativi, la pronta attuazione delle nuove regole relative alle violazioni dei dati personali, tenendo in considerazione i criteri di attenuazione del rischio e

individuando velocemente misure tecniche ed organizzative per dare attuazione alle nuove disposizioni.

Tavola 1- Adempimenti da effettuare prioritariamente

PRIORITÀ PER GLI ENTI LOCALI		
1. DESIGNAZIONE DEL RESPONSABILE DELLA PROTEZIONE DEI DATI (DPO)	2. ISTITUZIONE DEL REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO	3. NOTIFICA DELLE VIOLAZIONI DEI DATI PERSONALI (DATA BREACH)

A questi tre particolari adempimenti, possiamo sicuramente aggiungere anche quello previsto dall'art. 39 del GDPR: tra i compiti obbligatori imposti dal regolamento, infatti, è stata inserita l'attività di *formazione del personale*. Garantire la formazione sui contenuti della disciplina del trattamento dei dati personali sia dal punto di vista tecnico/organizzativo, che dal punto di vista valoriale è un'attività posta in capo al DPO, con la quale si ritiene possano essere sensibilizzati tutti gli addetti ai lavori sull'importanza di come trattare i dati altrui.

Un esempio

Un esempio di analisi che gli enti potrebbero eseguire è quello sulla gestione dei contratti di affidamento alle proprie partecipate. Una società appartenente al GAP che fornisce servizi per gestione delle entrate comunali disporrà certamente dei dati personali dei contribuenti. In questo caso la **titolarità del trattamento** sarà posta in capo al Comune (in particolare al Sindaco), mentre la **responsabilità del trattamento** sarà in capo alla società stessa. Di conseguenza il rapporto negoziale dovrà essere considerato all'interno del Registro dei trattamenti e, conseguentemente, dovranno essere dimostrate tutte le azioni poste in essere per garantire la tutela dei dati personali gestiti dalla partecipata.

Le sanzioni

Il GDPR entrerà in completa operatività il 25 maggio 2018 ed una delle più significative novità sarà rappresentata dall'elevato inasprimento delle sanzioni amministrative pecuniarie, che si applicano sino ad una somma di 10 milioni di Euro (o per le imprese, fino al 2% del fatturato annuo mondiale dell'esercizio precedente), le meno severe, o addirittura fino a 20 milioni di Euro (per le imprese, fino al 4% del fatturato annuo mondiale dell'esercizio precedente).
La competenza ad applicare tali sanzioni è attribuita alle Autorità di controllo nell'ambito del territorio del rispettivo Stato membro.
Nel caso italiano, la decisione sull'applicazione delle sanzioni spetta all'Autorità Garante per la Protezione dei Dati Personali che, nella sua valutazione, tiene conto delle circostanze del singolo caso, e comunque dei seguenti elementi:
- la natura, gravità e durata della violazione;
- il carattere doloso o colposo della violazione;
- le misure adottate per attenuare il danno subito dagli interessati;
- le eventuali precedenti violazioni commesse dal titolare del trattamento;
- il grado di cooperazione con l'autorità di controllo;
- altri eventuali fattori aggravanti o attenuanti.

Conclusioni

In via conclusiva, possiamo affermare che il GDPR porterà all'instaurazione di un nuovo "paradigma" europeo in materia di *Privacy* e trattamento di dati personali, con cui le amministrazioni pubbliche e non, dovranno immediatamente adeguarsi, nel rispetto però delle altre normative che con la *privacy* potrebbero confliggere, quali il diritto alla trasparenza e all'accesso.