LA CASA DEI COMUNI
anci LOMBARDIA

10 mosse per la Privacy in Comune

La cooperazione intercomunale per l'adeguamento agli obblighi normativi in tema di protezione dei dati personali

Regolamento UE n. 2016/679

CONTENUTI

IL NUOVO REGOLAMENTO EUROPEO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI: DA OBBLIGO A OPPORTUNITA'

Il prossimo 25 maggio 2018 entra in vigore il Regolamento UE 79/2016 in materia di protezione dei dati personali (in seguito anche il "Regolamento") pubblicato in Gazzetta Ufficiale Europea il 4 maggio 2016.
Il Regolamento introduce tre importanti principi innovativi nel "Sistema privacy" di una organizzazione:

- "responsabilizzazione" ("accountability") che attribuisce ai titolari del trattamento l'onere di assicurare, ed essere in condizioni di comprovare, il rispetto dei principi applicabili al trattamento dei dati personali (art. 5);

- "privacy by design", in base al quale adeguate misure tecniche e organizzative devono essere adottate a partire dalla progettazione dei trattamenti;

- "privacy by default" che, ricalcando il principio di necessità previsto dall'attuale disciplina, stabilisce che i dati vengano trattati solamente per le finalità previste e per il periodo strettamente necessario a tali fini.

Inoltre, il Regolamento riconosce espressamente il "diritto all'oblio" e stabilisce il diritto alla "portabilità dei dati".

Viene introdotta una nuova figura nell'ambito dell' "organigramma Privacy": il DPO (Data Protection Officer), cui vengono assegnate specifiche attività di ausilio al titolare ed ai responsabili nell'applicazione del Regolamento, e nelle attività di controllo. L'incarico, affidabile a personale interno o esterno, deve rappresentare la principale interfaccia del nuovo sistema nei confronti: del titolare; dell'autorità garante; dei cittadini.
I responsabili del trattamento dei dati sono sottoposti a nuove sanzioni penali, amministrative e pecuniarie fissate fino a 20 milioni di euro, alle quali si potranno aggiungere gli eventuali ricorsi dei singoli cittadini per il risarcimento di eventuali danni.
Con il Nuovo Regolamento Europeo sulla Privacy tutti i comuni dovranno provvedere ad implementare le misure organizzative e tecniche necessarie per garantire la protezione dei dati personali trattati.

IL VALORE DELLA COOPERAZIONE INTERCOMUNALE

La cooperazione intercomunale rappresenta un'importante opportunità per garantire l'efficace sviluppo di progetti innovativi, quali l'applicazione del Regolamento sulla protezione dei dati personali, per risolvere le criticità e contemporaneamente e valorizzare le eccellenze che ciascuno degli enti esprime.

La ridefinizione delle "regole del gioco" in senso cooperativo consente di agire con maggiori gradi di libertà e minori vincoli per predisporre soluzioni strategiche, tecniche e organizzative che, rispetto alle gestioni singole, sono in grado potenzialmente di:

- aumentare la forza contrattuale nelle negoziazioni con altre istituzioni e fornitori;
- determinare investimenti altrimenti non compatibili con le dimensioni di singoli comuni;
- realizzare innovazioni di processo in grado di rendere più efficace ed efficiente lo svolgimento delle attività mediante una:
    - riduzione della duplicazione di tutte quelle attività della medesima specie che, nel caso di gestioni singole, sono affidate a diverse strutture organizzative;
    - una più razionale divisione del lavoro, in quanto l'aumento dei volumi delle attività da svolgere, congiuntamente a un aumento della quantità di

personale gestibile, consente di assegnare a tale personale compiti maggiormente omogenei;

- una maggiore capacità di azione su fattori quali il personale, le tecnologie e l'organizzazione.

LA NATURA E LE LOGICHE DI SVILUPPO DELL'INTERVENTO

La nascita e l'evoluzione della cooperazione, in tema di applicazione del Regolamento in tema di protezione dei dati personali, deve essere attentamente governata secondo logiche riassunte nella tabella seguente.

Contribuire a superare forme di intervento parziali e non coordinate, favorendo un approccio il più possibile globale ai problemi	Utilizzare al meglio le risorse disponibili per il cambiamento	Ottenere il massimo coinvolgimento dei Comuni interessati
Sviluppare processi di cambiamento coerenti con un quadro normativo articolato e complesso.	Diffondere le eccellenze e superare le criticità già esistenti.	Adottare un approccio sperimetale e di successivo consolidamento delle soluzioni di successo

Le fasi di sviluppo dell'iniziativa prevedono sia incontri con il personale e gli amministratori dei comuni coinvolti sia attività svolte in autonomia dal personale comunale. Lo scopo è, in primo luogo, di offrire la possibilità di acquisire nuove competenze e capacità e, in secondo luogo, di delineare indicazioni operative per l'individuazione di

concreti percorsi di applicazione del Regolamento in tema di protezione dei dati personali in ciascuno degli enti coinvolti.

Per facilitare lo svolgimento delle attività, è attivata una piattaforma di gestione della cooperazione che garantisce:

- la fornitura d'informazioni con cadenza periodica su iniziative specifiche e su scadenze relative all'attività progettuale;
- l'accesso a sistemi utilizzati per rilevare le informazioni nei singoli Comuni, utili all'applicazione del Regolamento;
- la pubblicazione degli elaborati intermedi e finali;
- l'interazione libere fra i membri della *community*.

I RUOLI DEGLI ATTORI LOCALI E DI ANCI LOMBARDIA

L'intervento prevede la costituzione di un Gruppo di lavoro operativo composto dai responsabili organizzativi dei comuni coinvolti.

I membri dei gruppo partecipano a:

- incontri di lavoro collettivi;
- attività in ogni singolo ente di rilevazione delle informazioni, analisi guidate e individuazioni delle soluzioni riguardanti lo stato e le prospettive di applicazione del Regolamento in tema di protezione dei dati personali sotto il profilo tecnologico, organizzativo e gestionale.

L'intervento è svolto secondo una logica progettuale che prevede una puntuale previsione delle fasi di lavoro, in termini di tempi, risorse e risultati attesi, e un costante monitoraggio per garantire un'efficace soddisfazione delle attese.

In tale contesto, gli esperti di Anci Lombardia contribuiscono a:

- raggiungere gli obiettivi prefissati in un tempo determinato;
- istituire momenti periodici di confronto sugli stati di avanzamento;
- coinvolgere tutti gli attori designati dalle amministrazioni comunali;
- sviluppare le professionalità interne;
- fornire strumenti per lo svolgimento delle attività.

LE FASI DEL PROGETTO

FASE 1

Sottoscrizione dell'accordo per lo svolgimento del progetto

Si tratta di sottoscrivere un accordo fra Anci Lombardia e gli enti coinvolti nel progetto per regolare i rapporti per il suo svolgimento.

FASE 2

Mappatura dei trattamenti per la redazione dei registri delle attività

L'intervento mira alla catalogazione dei trattamenti di dati svolti all'interno degli enti, al fine di redigere il registro dei trattamenti per ciascun ente come richiesto dall'articolo 30 del Regolamento Europeo. Il punto di partenza sarà l'ultima versione disponibile del Documento Programmatico sulla Sicurezza, sulla base del quale effettuare una verifica con gli uffici competenti.

Attività
• **Rilevazione dei trattamenti con le informazioni connesse** • **Analisi della completezza delle informazioni raccolte** • **Redazione dei registri dei trattamenti**

FASE 3

Analisi e revisione dei modelli di informativa ed eventuale consenso al trattamento dati personali

Al fine di adeguare la documentazione redatta dagli enti coinvolti in tema di informative al trattamento dei dati personali si tratta di raccogliere i moduli esistenti, aggiornare il loro contenuto.

Attività
• **Raccolta moduli** • **Analisi contenuto delle informative e delle formule del consenso** • **Revisione dei contenuti delle informative e delle formule del consenso**

FASE 4

Sottoscrizione di un'eventuale convenzione per la gestione associata del Regolamento sulla protezione dei dati

Nel caso in cui sia ritenuto utile, gli enti che hanno partecipato al progetto possono sottoscrivere una convenzione nella quale disciplinare le modalità di collaborazione per l'applicazione del Regolamento europeo sulla protezione dei dati personali.

Attività
• **Analisi requisiti della collaborazione** • **Sottoscrizione della convenzione**

FASE 5

Nomina del DPO e analisi e revisione degli atti giuridici che disciplina le attività dei responsabili e degli incaricati del trattamento

Una volta individuati i trattamenti, si rende necessario associarli agli uffici coinvolti di ogni sinolo Comune, al fine di costruire una matrice funzionale per definire le competenze dei singoli soggetti afferenti agli uffici. Questo consentirà di procedere alla revisione delle nomine degli incaricati del trattamento. Pur non essendo più un esplicito obbligo di legge, il Garante individua questa azione come una misura idonea di sicurezza consentendo di definire i ruoli e le attività dei soggetti coinvolti nelle fasi operative del trattamento dei dati.

Nel caso gli enti intendano istituire la figura del responsabile dei trattamenti, si deve procedere alla loro nomina. Questa attività comporta anche una ricognizione per individuare i trattamenti dei dati esternalizzati in nome e per conto dell'ente, al fine di procedere a nomine specifiche.

I Comuni sono sottoposti alla nomina obbligatoria di un Responsabile di Protezione dei Dati (DPO). Tale figura, le cui competenze, mansioni e responsabilità sono previste specificamente dagli artt. 37-39 del Regolamento Europeo 2016/679, svolge un ruolo di supporto al titolare e sorveglianza della corretta applicazione del Regolamento, oltre che da punto di contatto per l'Autorità Garante della Privacy e per i cittadini circa qualsiasi questione connessa ai trattamenti di dati effettuati dall'ente.

Il ruolo di DPO può essere assunto da soggetti interni o esterni all'ente. E' prevista, inoltre, la possibilità di costituire un ufficio strutturato per lo svolgimento dei compiti stabiliti. In ogni caso, è comunque necessario che venga sempre individuata la persona fisica che riveste il ruolo di RPD mediante specifico atto di designazione che può essere adotto da un singolo Comune o da più enti in forma associata.

Anci Lombardia garantisce il proprio apporto per individuare la più appropriata soluzione organizzativa e giuridica per la nomina dei DPO, garantendo una particolare attenzione alle specifiche problematiche che sorgano nell'ambito di una sua nomina in forma associata.

Attività
• **Raccolta informazioni** • **Stesura matrice uffici/trattamenti** • **Individuazione incaricati e responsabili del trattamento dei dati** • **Nomina del DPO** • **Formalizzazione nomine**

FASE 6

Valutazione dell’impatto sulla protezione dei dati

Il nuovo Regolamento Europeo prevede, in caso di nuovi trattamenti di dati e di trattamenti che prevedono rischi elevati, di effettuare un’analisi preliminare dell’impatto sulla protezione dei dati che tali trattamenti comportano. L’intervento prevede la redazione della necessaria documentazione per effettuare l’analisi (schede con analisi di *compliance* alla normativa) da produrre in caso di ispezione del Garante.

Attività
• **Valutazione dei rischi correlati ai trattamenti** • **Censimento dei nuovi trattamenti** • **Redazione documento di analisi dell’impatto**

FASE 7

Formazione personale sul Regolamento per la protezione dei dati personali

Sono realizzate sessioni formative d'aula e *webinar* in cui sono illustrati gli obblighi normativi e quelli relativi agli specifici comunali relativamente agli obblighi e responsabilità derivanti dal trattamento dei dati personali. E' fornito materiale specifico e sono rilasciati attestati di partecipazione.

Attività
• **Analisi dei fabbisogni formativi** • **Realizzazione sessioni formative**

FASE 8

Analisi del rischio

L'attività prevede interventi per l'individuazione delle minacce e la valutazione dell'impatto che queste possono determinare sulle risorse dell'ente, seguita da un piano dei trattamenti in cui sono indicate le misure da adottare per mitigare i rischi. Si tratta di una prima analisi finalizzata a definire gli ambiti principali di azione, che potrà successivamente essere approfondita con interventi più mirati e specifici a seconda delle necessità riscontrate.

Attività
• **Individuazione minacce correlate e valutazione di impatto** • **Piano deli interventi**

FASE 9

Processo di gestione *data breach*

L'attività prevede l'impostazione del processo di rilevazione di eventuali incidenti di sicurezza, la valutazione dell'entità degli stessi e la redazione di una procedura operativa che possa concludersi con le azioni necessarie previste dal Regolamento UE per la gestione di un *data breach* (registrazione eventi di sicurezza, eventuale notifica all'Autorità Garante e comunicazione agli interessati in caso di necessità).

Attività
• **Analisi delle procedure di gestione data breach in vigore** • **Definizione delle procedure di gestione data breach**

FASE 10

Verifica, codifica, revisione e adozione delle misure di sicurezza

Le tematiche sottoposte ad analisi allo scopo d'individuare eventuali nuove misure di sicurezza sono:

- gestione degli accessi alle risorse;
- sicurezza perimetrale e prevenzione di *malware*;
- amministrazione dei sistemi;
- gestione degli accessi remoti e utilizzo di dispositivi esterni;
- processi di *business continuity*;
- sistemi di *backup* e ripristino dei dati;
- *compliance* rispetto alle misure di sicurezza ICT per le PA.

L'elenco non è esaustivo.

Al termine dello svolgimento delle attività sarà redatto un piano di lavoro che preveda impegni, costi, tempi e priorità.

Gli interventi per la messa a norma del sistema degli enti non sono preventivamente dimensionabili, poiché dipende dalla situazione delle misure già in essere e dal livello di sicurezza che gli enti intendono raggiungere.