ReteComuni

associazione nazionale comuni italiani
anci LOMBARDIA

Regolamento 2016/679/UE: Le priorità per le pubbliche amministrazioni

CENTRO COMPETENZE DIGITALI BRIANZA
TAVOLO OPERATIVO ICT - 15 NOVEMBRE 2017

REGOLAMENTO 2016/679/UE: LE PRIORITA' PER LE PA

GARANTE PRIVACY: SCHEDA INFORMATIVA

La principale novità introdotta dal regolamento è il principio di "responsabilizzazione" (cd. accountability), che attribuisce direttamente ai titolari del trattamento il compito di assicurare, ed essere in grado di comprovare, il rispetto dei principi applicabili al trattamento dei dati personali (art. 5).

In quest'ottica, la nuova disciplina impone alle amministrazioni un diverso approccio nel trattamento dei dati personali, prevede nuovi adempimenti e richiede un'intensa attività di adeguamento, preliminare alla sua definitiva applicazione a partire dal 25 maggio 2018.

Al fine di fornire un primo orientamento il Garante per la protezione dei dati personali suggerisce alle Amministrazioni pubbliche di avviare, con assoluta priorità:

1. la **designazione del Responsabile della protezione dei dati** – RPD (artt. 37-39)
2. l'**istituzione del Registro delle attività di trattamento** (art. 30 e cons. 171)
3. la **notifica delle violazioni** dei dati personali (cd. data breach, art. 33 e 34)

REGOLAMENTO 2016/679/UE: LE PRIORITA' PER LE PA

GARANTE PRIVACY: SCHEDA INFORMATIVA

1. Designazione del Responsabile della protezione dei dati – RPD (artt. 37-39)

Questa nuova figura, che il regolamento richiede sia individuata in funzione delle qualità professionali e della conoscenza specialistica della normativa e della prassi in materia di protezione dati, costituisce il fulcro del processo di attuazione del principio di "responsabilizzazione". Il diretto coinvolgimento del RPD in tutte le questioni che riguardano la protezione dei dati personali, sin dalla fase transitoria, è sicuramente garanzia di qualità del risultato del processo di adeguamento in atto. In questo ambito, sono da tenere in attenta considerazione i requisiti normativi relativamente a:

- **posizione** (riferisce direttamente al vertice),
- **indipendenza** (non riceve istruzioni per quanto riguarda l'esecuzione dei compiti)
- **autonomia** (attribuzione di risorse umane e finanziarie adeguate);

REGOLAMENTO 2016/679/UE: LE PRIORITA' PER LE PA

GARANTE PRIVACY: SCHEDA INFORMATIVA

2. Istituzione del Registro delle attività di trattamento (art. 30 e cons. 171)

Essenziale avviare quanto prima la ricognizione dei trattamenti svolti e delle loro principali caratteristiche:

- finalità del trattamento,
- descrizione delle categorie di dati e interessati,
- categorie di destinatari cui è prevista la comunicazione,
- misure di sicurezza,
- tempi di conservazione,

e ogni altra informazione che il titolare ritenga opportuna al fine di documentare le attività di trattamento svolte) funzionale all'istituzione del registro. La ricognizione sarà l'occasione per verificare anche il **rispetto dei principi fondamentali** (art. 5), la **liceità del trattamento** (verifica dell'idoneità della base giuridica, artt. 6, 9 e 10) e l'opportunità dell'introduzione di **misure a protezione dei dati** fin dalla progettazione e per impostazione (privacy by design e by default, art. 25), in modo da assicurare, entro il 25 maggio 2018, la piena conformità dei trattamenti in corso (cons. 171);

REGOLAMENTO 2016/679/UE: LE PRIORITA' PER LE PA

GARANTE PRIVACY: SCHEDA INFORMATIVA

3. Notifica delle violazioni dei dati personali (cd. data breach, art. 33 e 34)

Fondamentale appare anche, nell'attuale contesto caratterizzato da una crescente minaccia alla sicurezza dei sistemi informativi, la pronta attuazione delle nuove misure relative alle violazioni dei dati personali, tenendo in particolare considerazione i criteri di attenuazione del rischio indicati dalla disciplina e individuando quanto prima idonee procedure organizzative per dare attuazione alle nuove disposizioni.

Con il nuovo regolamento, **le Pubbliche Amministrazioni dovranno notificare la violazione dei dati personali al Garante per la Privacy entro 72 ore da quando ne vengono a conoscenza**.

Nel caso in cui la violazione dei dati personali rappresenti (o possa rappresentare) un rischio elevato per i diritti e le libertà dei soggetti coinvolti, il titolare del trattamento dovrà comunicare l'evento anche agli interessati, senza ingiustificato ritardo.

ReteComuni

associazione nazionale comuni italiani
anci LOMBARDIA

Linee-guida sui responsabili della protezione dei dati (RPD)

CENTRO COMPETENZE DIGITALI BRIANZA
TAVOLO OPERATIVO ICT - 15 NOVEMBRE 2017

Linee-guida sui responsabili della protezione dei dati (RPD)

GRUPPO DI LAVORO ARTICOLO 29
IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

16/EN
WP 243 rev. 01

Linee-guida sui responsabili della protezione dei dati (RPD)[1]

Adottate il 13 dicembre 2016
Versione emendata e adottata in data 5 aprile 2017

La scheda del Garante «Il Responsabile della protezione dei dati (RPD)»

La scheda del Garante «Il Responsabile della protezione dei dati (RPD)»

QUALI SONO I REQUISITI?

Il Responsabile della protezione dei dati, nominato dal titolare del trattamento o dal responsabile del trattamento, dovrà:

1. **possedere un'adeguata conoscenza della normativa e delle prassi di gestione dei dati personali**, anche in termini di misure tecniche e organizzative o di misure atte a garantire la sicurezza dei dati. Non sono richieste attestazioni formali o l'iscrizione ad appositi albi professionali, anche se la partecipazione a master e corsi di studio/professionali può rappresentare un utile strumento per valutare il possesso di un livello adeguato di conoscenze.
2. **adempiere alle sue funzioni in piena indipendenza e in assenza di conflitti di interesse**. In linea di principio, ciò significa che il RPD non può essere un soggetto che decide sulle finalità o sugli strumenti del trattamento di dati personali;
3. **operare alle dipendenze del titolare o del responsabile oppure sulla base di un contratto di servizio** (RPD/DPO esterno).

Il titolare o il responsabile del trattamento dovranno mettere a disposizione del Responsabile della protezione dei dati le risorse umane e finanziarie necessarie all'adempimento dei suoi compiti.

La scheda del Garante «Il Responsabile della protezione dei dati (RPD)»

QUALI SONO I COMPITI?

Il Responsabile della protezione dei dati dovrà, in particolare:

a) **sorvegliare l'osservanza del regolamento**, valutando i rischi di ogni trattamento alla luce della natura, dell'ambito di applicazione, del contesto e delle finalità;

b) **collaborare** con il titolare/responsabile, laddove necessario, nel condurre una **valutazione di impatto sulla protezione dei dati (DPIA)**;

c) **informare e sensibilizzare** il titolare o il responsabile del trattamento, nonché i dipendenti di questi ultimi, riguardo agli obblighi derivanti dal regolamento e da altre disposizioni in materia di protezione dei dati;

d) **cooperare con il Garante e fungere da punto di contatto per il Garante** su ogni questione connessa al trattamento;

e) **supportare** il titolare o il responsabile in ogni attività connessa al trattamento di dati personali, anche con riguardo alla tenuta di un **registro delle attività di trattamento**.

La scheda del Garante «Il Responsabile della protezione dei dati (RPD)»

IN QUALI CASI E' PREVISTO?

Dovranno designare obbligatoriamente un RPD:

a) amministrazioni ed enti pubblici, fatta eccezione per le autorità giudiziarie;

b) tutti i soggetti la cui attività principale consiste in trattamenti che, per la loro natura, il loro oggetto o le loro finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;

c) tutti i soggetti la cui attività principale consiste nel trattamento, su larga scala, di dati sensibili, relativi alla salute o alla vita sessuale, genetici, giudiziari e biometrici.

Anche per i casi in cui il regolamento non impone in modo specifico la designazione di un RPD, è comunque possibile una nomina su base volontaria.

Un gruppo di imprese o soggetti pubblici possono nominare un unico RPD.

Per un quadro completo: www.garanteprivacy.it/rpd

Designazione di un unico RPD per più organismi (Linee-guida)

2.3. Designazione di un unico RPD per più organismi

L'articolo 37, paragrafo 2, consente a un gruppo imprenditoriale di nominare un unico RPD a condizione che quest'ultimo sia *"facilmente raggiungibile da ciascuno stabilimento"*. Il concetto di raggiungibilità si riferisce ai compiti del RPD in quanto punto di contatto per gli interessati[19], l'autorità di controllo[20] e i soggetti interni all'organismo o all'ente, visto che uno dei compiti del RPD consiste nell'*"informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento"*.

Allo scopo di assicurare la raggiungibilità del RPD, interno o esterno, è importante garantire la disponibilità dei dati di contatto nei termini previsti dal RGPD.

[19] V. art. 38, paragrafo 4: "*Gli interessati possono contattare il responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente regolamento*."
[20] V. art. 39, paragrafo 1, lettera e): "*fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione*."

Designazione di un unico RPD per più organismi (Linee-guida)

2.3. Designazione di un unico RPD per più organismi

Il RPD, se necessario con il supporto di un *team* di collaboratori, deve essere in grado di comunicare con gli interessati in modo efficiente e di collaborare con le autorità di controllo interessate. Ciò significa, fra l'altro, che le comunicazioni in questione devono avvenire nella lingua utilizzata dalle autorità di controllo e dagli interessati volta per volta in causa. Il fatto che il RPD sia raggiungibile – vuoi fisicamente all'interno dello stabile ove operano i dipendenti, vuoi attraverso una linea dedicata o altri mezzi idonei e sicuri di comunicazione – è fondamentale al fine di garantire all'interessato la possibilità di contattare il RPD stesso.

Ai sensi dell'articolo 37, terzo paragrafo, è ammessa la designazione di un unico RPD per più autorità pubbliche o organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione. Valgono le stesse considerazioni svolte in tema di risorse e comunicazioni. Poiché il RPD è chiamato a una molteplicità di funzioni, il titolare o il responsabile deve assicurarsi che un unico RPD, se necessario supportato da un team di collaboratori, sia in grado di adempiere in modo efficiente a tali funzioni anche se designato da una molteplicità di autorità e organismi pubblici.

Fine presentazione

Maurizio Piazza
(esperto ICT per la PA Locale)
ReteComuni – ANCI Lombardia

e-mail: piazzamaurizio@gmail.com