



Città metropolitana  
di Venezia

**Linee guida per l'organizzazione  
del sistema di tutela dei dati personali  
della Città metropolitana  
(regolamento UE n. 2016/679)**

Venezia, maggio 2018

## Premessa

- il Parlamento Europeo ed il Consiglio in data 27 aprile 2016 hanno approvato il Regolamento UE 679/2016 (GDPR – *General Data Protection Regulation*) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, che abroga la direttiva 95/46/CE e che mira a garantire una disciplina uniforme ed omogenea in tutto il territorio dell'Unione Europea;
- il testo, pubblicato nella Gazzetta Ufficiale dell'Unione Europea (GUCE) il 4 maggio 2016, diventerà definitivamente applicabile in via diretta in tutti i paesi UE a partire dal 25 maggio 2018, dopo un periodo di transizione di due anni, in quanto non richiede alcuna forma legislativa applicativa o attuativa da parte degli Stati Membri;
- il Garante per la protezione dei dati personali ha emanato una [Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali](#) che intende offrire un panorama delle principali problematiche che i soggetti pubblici, oltre alle imprese, dovranno tenere presenti in vista della piena applicazione del regolamento prevista per il 25 maggio 2018;
- ai sensi dell'art. 13 della legge n. 163/2017 il Governo è stato delegato ad adottare, entro sei mesi dalla sua entrata in vigore, uno o più decreti legislativi al fine di adeguare il quadro normativo nazionale alle disposizioni del Regolamento UE 2016/679;
- le norme introdotte dal Regolamento si traducono in obblighi organizzativi, documentali e tecnici che tutti i titolari del trattamento dei dati personali devono, fin da subito, considerare e tenere presenti per consentire la piena e consapevole applicazione del nuovo quadro normativo in materia di privacy entro il 25 maggio 2018;
- il presente documento stabilisce le modalità organizzative, le misure procedurali, finalizzate anche ad organizzare questioni interpretative, che permettano alla Città metropolitana di poter agire con adeguata funzionalità ed efficacia nell'attuazione delle disposizioni introdotte dal nuovo Regolamento UE.

## Principali novità

- l'adozione di approcci e politiche che tengano costantemente conto del rischio che un determinato trattamento di dati personali può comportare per i diritti e le libertà degli interessati;
- il principio chiave della “privacy by design”, per cui occorre garantire la protezione dei dati fin dalla fase di ideazione e progettazione di un trattamento o di un sistema, e adottare comportamenti che consentano di prevenire possibili problematiche;
- una nuova definizione di dato personale;
- nuovi compiti del titolare e del personale autorizzato al trattamento dei dati;
- un diverso approccio di valutazione dei rischi con la relativa valutazione di impatto;
- il nuovo registro dei trattamenti;
- l'adozione delle nuove misure di sicurezza;
- la nuova figura del Responsabile della Protezione dei Dati/Data Protection Officer (RPD/DPO) incaricato di assicurare una gestione corretta dei dati personali nelle imprese e negli enti;
- il diverso rapporto con l'Autorità Garante in caso di violazioni dei dati personali (data breach);

## **Principali obblighi**

- (1) l'adozione del registro dei trattamenti;*
- (2) la nomina del RPD/DPO;*
- (3) l'adozione delle misure di sicurezza basate sulla prevenzione dei rischi sulla privacy e sull'utilizzo dei dati necessari per ogni specifico trattamento (privacy by default);*

## **ORGANIZZAZIONE INTERNA - SOGGETTI E RUOLI**

Il regolamento ridisegna il ruolo, i compiti e le responsabilità del titolare e del responsabile del trattamento in relazione ai nuovi principi e strumenti introdotti dallo stesso e individua la nuova figura del “responsabile della protezione dei dati”.

### **Titolare del trattamento**

Il titolare del trattamento è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'art. 5: liceità, correttezza e trasparenza; limitazione delle finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza.

A tali fini, mette in atto misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento di dati personali sia effettuato in modo conforme al regolamento.

Le misure sono definite fin dalla fase di progettazione e messe in atto per applicare in modo efficace i principi di protezione dei dati e per agevolare l'esercizio dei diritti dell'interessato stabiliti dagli artt. 15-22 del regolamento nonché le comunicazioni occorrenti per il loro esercizio.

### **Responsabile del trattamento**

L'effettiva individuazione ed attuazione di misure tecnico – organizzative idonee a garantire il rispetto della normativa europea nel nostro Ente trova quale centro principale di responsabilità i singoli dirigenti dell'Ente nei limiti delle competenze, delle funzioni e delle materie agli stessi assegnati.

I dirigenti delle strutture in cui articola l'organizzazione della Città metropolitana, sono nominati responsabili del trattamento di tutte le banche dati personali esistenti nell'articolazione organizzativa di rispettiva competenza.

Il Responsabile deve essere in grado di offrire garanzie sufficienti in termini di conoscenza specialistica, affidabilità e risorse, per mettere in atto le misure tecniche e organizzative di cui all'art. 5 rivolte a garantire che i trattamenti siano effettuati in conformità al regolamento.

Le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità dei responsabili attenendosi alle istruzioni loro impartite per iscritto che individuano specificatamente l'ambito del trattamento consentito.

**Le funzioni dei singoli dirigenti della Città metropolitana in materia di trattamento e tutela dei dati personali, ai sensi del regolamento UE 2016/679, sono le seguenti:**

- 1) censire e monitorare costantemente le singole attività di trattamento dei dati personali facenti capo al proprio settore;
- 2) individuare eventuali attività di trattamento non previste all'interno del registro delle attività di trattamento predisposto dalla Città metropolitana al fine di consentirne il costante aggiornamento;
- 3) segnalare le fattispecie di trattamento di cui al punto precedente al responsabile della protezione dei dati (RPD-DPO) designato dalla Città metropolitana, nella sua qualità di custode del registro delle attività di trattamento;
- 4) assicurare la legittimità delle attività di trattamento dei dati personali ponendo in essere misure tecnico-organizzative di sicurezza adeguate, dimostrabili e coerenti con quanto riportato nel registro delle attività di trattamento;
- 5) individuare con apposito atto di nomina interno, prodotto dal software in uso, i dipendenti autorizzati alle attività di trattamento di dati personali;
- 6) vigilare sulla azione dei soggetti autorizzati di cui al precedente punto 5);
- 7) porre in essere adeguate azioni correttive in caso di riscontrate violazioni delle misure tecnico-organizzative di cui al precedente punto 4);
- 8) individuare gli eventuali soggetti responsabili del trattamento per conto del titolare, con conseguente definizione puntuale dei loro

- obblighi all'interno di apposito contratto/atto giuridico secondo quanto previsto dall'art. 28 del regolamento;
- 9) sollecitare l'intervento del responsabile della protezione dei dati (RPD-DPO) designato dalla Città metropolitana in tutti i casi in cui si verifichi la necessità di specifiche azioni nel suo ruolo di supervisore/consulente/garante del sistema di gestione di tutela dati;
  - 10) garantire il rispetto dei diritti del soggetto interessato e fornire adeguate informative allo stesso ai sensi degli artt. 12, 13 e 14 del regolamento;
  - 11) sollecitare e consentire idonea attività di formazione del personale autorizzato alle attività di trattamento dei dati personali;
  - 12) proporre nuove misure di sicurezza organizzative dei trattamenti;
  - 13) in aggiunta a quanto sopra, il dirigente del servizio procedure contrattuali dovrà altresì predisporre apposite clausole da inserire negli atti di gara dell'Ente, le quali andranno rese note e fruibili a tutte le strutture, in collaborazione con il Segretario generale e con il responsabile della protezione dei dati (RPD-DPO).

### **Responsabile della protezione dei dati (RPD o DPO)**

L'istituzione della nuova figura del Responsabile della protezione dei dati è la principale novità normativa del regolamento europeo che mira al potenziamento del controllo dell'efficacia e della sicurezza dei sistemi di protezione dei dati personali.

Il Responsabile della protezione dei dati è incaricato dei seguenti compiti:

- a) informare e fornire consulenza al titolare ed al responsabile nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal regolamento e dalle altre normative relative alla protezione dei dati. In tal senso il Responsabile della protezione dei dati può indicare al titolare e/o ai responsabili i settori funzionali ai quali riservare un audit interno o esterno in tema di protezione dei dati, le attività di formazione interna per il personale che tratta dati personali e a quali trattamenti dedicare maggiori risorse e tempo in relazione al rischio riscontrato;

- b) sorvegliare l'osservanza del regolamento e delle altre normative relative alla protezione dei dati, fermo restando le responsabilità del titolare e dei responsabili del trattamento. Fanno parte di questi compiti: la raccolta di informazioni per individuare i trattamenti svolti, l'analisi e la verifica dei trattamenti in termini di loro conformità, l'attività di informazione, consulenza e indirizzo nei confronti del titolare e dei responsabili del trattamento;
- c) sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo poste in essere dal titolare e dai responsabili del trattamento;
- d) fornire, su richiesta, un parere in merito alla valutazione di impatto sulla protezione dei dato e sorvegliarne lo svolgimento;
- e) cooperare con il Garante per la protezione dei dati personali e fungere da punto di contatto per detta autorità;
- f) verificare la tenuta dei registri da parte del titolare e dei responsabili dei trattamenti.

## IN SINTESI

<b>Figura</b>	<b>Norma Reg. UE 2016/679</b>	<b>Chi è / cosa fa</b>
Titolare del trattamento dei dati personali	art. 24	La Città metropolitana di Venezia, quale entità organizzativa complessiva; prende le decisioni sulle finalità; è responsabile delle misure tecniche e organizzative e dell'ottemperanza al regolamento europeo
Responsabili del trattamento	art. 28	I singoli dirigenti della Città metropolitana
Soggetti autorizzati al trattamento	art. 4 co. 1, lett. 10 e art. 29	Il dipendente autorizzato per competenza da parte dirigente al trattamento dei dati personali
Responsabili esterni del trattamento per conto del titolare	art. 28	Figura soggettiva eventuale la cui individuazione spetta al singolo dirigente con conseguente definizione puntuale degli obblighi sullo stesso gravanti all'interno di apposito contratto/atto giuridico secondo quanto previsto dall'art. 28 (Obbligo di redigere il contratto di nomina di responsabile esterno)
Responsabile della protezione dati (RPD o DPO)	Considerando 97 e art. 37 e ss	Figura soggettiva con funzioni di assistenza del titolare; verrà individuato all'esterno dell'Amministrazione nel rispetto di quanto previsto dal regolamento UE 2016/679, secondo procedura comparativa attraverso MEPA, valorizzandone la prossimità alle sedi dell'Ente al fine di consentirne il pronto intervento in caso di data breach, come raccomandato dall'art. 37, co. 2, del regolamento

## I NUOVI STRUMENTI

**Registro delle attività di trattamento** (art. 30, co. 1, del regolamento 2016/679)

Il registro dei trattamenti appartiene all'ambito oggettivo (azioni/attività) di operatività del regolamento europeo; esso costituisce una misura di adeguamento dinamico e progressivo finalizzato a dimostrare, mappare le attività di trattamento dei dati personali in capo al titolare.

La Città metropolitana, per cominciare a definire il contenuto del registro, che naturalmente sarà soggetto a costante attività di implementazione e aggiornamento, si avvarrà del software attualmente in uso.

Il registro delle attività di trattamento svolte dalla Città metropolitana quale titolare del trattamento, recherà le seguenti informazioni minime:

- a) le finalità del trattamento;
- b) una sintetica descrizione delle categorie di interessati (cittadini, residenti, utenti, dipendenti, amministratori, parti, altro), nonché le categorie di dati personali (dati identificativi, dati generici, dati biomedici, dati relativi alla salute);
- c) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati (persona fisica o giuridica; autorità pubblica; altro organismo destinatario);
- d) l'eventuale trasferimento di dati personali verso un paese terzo od organizzazione internazionale;
- e) ove stabiliti, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- f) il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate.

**Registro delle categorie di attività** (art. 30, co. 2, del regolamento 2016/679)

Il registro delle categorie di attività trattate da ciascun responsabile del trattamento recherà le seguenti informazioni:

- a) il nome ed i dati di contatto del responsabile del trattamento e del RPD;
- b) le categorie di trattamenti effettuati da ciascun responsabile: raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, uso, comunicazione, raffronto, interconnessione, limitazione, cancellazione, distribuzione;
- c) l'eventuale trasferimento di dati personali verso un paese terzo od organizzazione internazionale;
- d) il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate.

## **AZIONI IN PROGRESS**

Particolare attenzione verrà assicurata alle seguenti azioni:

1. individuazione della attività di trattamento non peculiari del singolo Servizio ma riconducibili ad attività di trattamento ritenute trasversali a tutto l'Ente;
2. analisi, in collaborazione con i diversi servizi dell'ente, della base giuridica delle attività di trattamento ai sensi dell'art. 6, par. 3 del regolamento anche al fine di definire il termine di cancellazione delle diverse categorie di dati;
3. verifica della riconducibilità del singolo trattamento anche all'utilizzo di una o più banche dati della Città metropolitana o di eventuali altre banche dati;
4. verifica delle fattispecie di trattamento in cui è rinvenibile la figura del responsabile del trattamento per conto del titolare ai sensi dell'art. 28 del regolamento.

## **AZIONI FUTURE**

Nell'ambito delle attività di implementazione delle novità del regolamento 2016/679, la Città metropolitana, seguendo l'approccio dinamico ed evolutivo indotto dalla particolarità dell'ambito di azione amministrativa che implica la materia della tutela dei dati personali, intende procedere a:

1. adeguare il presente atto ai successivi interventi del legislatore nazionale e dell'Autorità garante per la protezione dei dati personali;
2. garantire una continua ed adeguata formazione di tutto il personale dell'Ente;
3. garantire un aggiornamento costante e tempestivo del registro delle attività di trattamento;
4. assicurare la tutela dati di tutto l'Ente attraverso l'adozione di misure adeguate che garantiscano la sicurezza delle attività di trattamento.