Città
metropolitana
di Milano

REGOLAMENTO DELLA CITTA' METROPOLITANA DI MILANO

PER LA PROTEZIONE DEI DATI PERSONALI

in attuazione del regolamento UE 2016/679

"*Regolamento generale per la protezione dei dati*"

INDICE

CAPO PRIMO: *PRINCIPI E ADEMPIMENTI*

Art. 1 - Oggetto e finalità pag. 3

Art. 2 - Principi pag. 3

Art. 3 - Sensibilizzazione pag. 4

Art. 4 – Titolare del trattamento pag. 4

Art. 5 - Autorizzati di 1° livello al trattamento dati personali pag. 5

Art. 6 - Responsabili esterni del trattamento pag. 6

Art. 7 - Amministratore di sistema pag. 7

Art. 8 - Responsabile della protezione dati pag. 7

Art. 9 - Sicurezza del trattamento pag. 9

Art. 10 - Pubblicazione web per obblighi di trasparenza pag. 10

Art. 11 - Registro delle attività di trattamento del Titolare pag. 10

Art. 12 - Registro delle attività di trattamento del Responsabile pag. 11

Art. 13 - Valutazione d'impatto sulla protezione dei dati pag. 11

Art. 14 - Violazione dei dati personali pag. 14

Art. 15 - Diritto di accesso pag. 15

Art. 16 - Diritto di limitazione pag. 16

Art. 17 - Diritto all'oblio pag. 16

Art. 18 - Diritto alla rettifica dei dati pag. 17

Art. 19 - Diritto di opposizione pag. 17

Art. 20 - Obbligo di informativa pag. 17

Art. 21 - Contenuto dell'informativa pag. 18

Art. 22 - Consenso pag. 18

CAPO SECONDO: ***UTILIZZO DEGLI IMPIANTI DI VIDEOSORVEGLIANZA***

Art. 23 - Oggetto pag. 19

Art. 24 - Soggetti pag. 20

Art. 25 -Trattamento dei dati personali pag. 21

Art. 26 - Misure di sicurezza pag. 23

Art. 27 - Rinvio pag. 24

CAPO PRIMO

PRINCIPI E ADEMPIMENTI

Art. 1 - Oggetto e finalità

Il presente Regolamento disciplina le misure organizzative ed i processi interni di attuazione della normativa unionale posta dal Regolamento europeo (General Data Protection Regulation del 27 aprile 2016 n. 679, di seguito indicato con RGPD, Regolamento Generale Protezione Dati) e della successiva disciplina di armonizzazione (D. Lgs n. 101 del 2018), ai fini del trattamento di dati personali per finalità istituzionali nell'Ente Città Metropolitana di Milano.

Ai fini del presente Regolamento, per funzioni istituzionali si intendono quelle:

a) previste dalla legge, dallo statuto e dai regolamenti;

b) in esecuzione di un contratto con i diretti interessati;

c) per finalità specifiche e diverse da quelle di cui ai predenti punti, purchè l'interessato esprima il consenso al trattamento.

Art. 2 - Principi

Per le finalità indicate all'articolo 1, la Città Metropolitana di Milano garantisce che il trattamento di dati si svolga nel rispetto dei diritti e delle libertà fondamentali delle persone fisiche, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale ed al diritto alla protezione dei dati personali.

La protezione delle persone fisiche, con riguardo al trattamento dei dati personali, è un diritto fondamentale, ai sensi dell'art. 8 della Carta dei diritti fondamentali dell'UE, secondo cui "*Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano*".

In attuazione a quanto previsto ai commi 1 e 2, i dati personali sono:

- trattati in conformità alle norme di legge, cioè in modo lecito e trasparente nei confronti dell'interessato;
- corretti, esatti ed aggiornati a seguito di intervenute variazioni;
- solo quelli adeguati, pertinenti e limitati a quanto necessario allo scopo specifico, con la riduzione al minimo delle informazioni identificative, il trattamento va evitato laddove lo scopo specifico può essere raggiunto tramite dati anonimi;
- conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati;
- trattati con adeguate misure di sicurezza onde evitare abusi o illeciti o perdita, distruzione o danno accidentale, in conformità ai principi di integrità e riservatezza.

Art. 3 - Sensibilizzazione

La Città Metropolitana di Milano sostiene e promuove, al suo interno, ogni strumento di sensibilizzazione che possa consolidare il pieno rispetto del diritto alla riservatezza e migliorare la qualità dei servizi offerti ai cittadini.

A tale riguardo, uno degli strumenti essenziali di sensibilizzazione è l'attività formativa del personale aziendale e l'attività informativa diretta a tutti coloro che hanno rapporti con l'Ente metropolitano.

Art. 4 -Titolare del trattamento

La Città Metropolitana di Milano è il titolare del trattamento dei dati personali raccolti in banche dati, automatizzate o cartacee, dalle strutture Organizzative dell'Ente.

Il Titolare è responsabile del rispetto dei principi stabiliti nella normativa unionale e nazionale in materia di trattamento dei dati personali ed in particolare dei seguenti principi stabiliti all'articolo 5 del Regolamento Europeo 2016/679: liceità, correttezza e trasparenza, limitazione delle finalità, minimizzazione dei dati, esattezza, limitazione della conservazione, integrità e riservatezza dei dati personali.

Il Titolare mette in atto adeguate misure tecniche ed organizzative al fine di garantire la conformità del trattamento dei dati al RGPD ed al D. Lgs. 196 del 2003, come integrato dal D. Lgs. n. 101 del 2018, e ciò deve essere dimostrabile.

Le misure sono definite fin dalla fase di progettazione e messe in atto per applicare in modo efficace i principi di protezione dati e per agevolare l'esercizio dei diritti dell'interessato stabiliti dagli art. 15 – 22 RGPD, nonchè le comunicazioni e le informazioni occorrenti per il loro esercizio.

Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare deve effettuare una valutazione dell' impatto del trattamento sulla protezione dei dati personali (di seguito indicata "DPIA") ai sensi dell'art. 35, RGDP, considerati la natura, l'oggetto, il contesto e le finalità del trattamento medesimo, tenuto conto di quanto indicato dal successivo art. 13.

Il Titolare, inoltre, provvede a:

a) nominare gli "*Autorizzati di 1° livello al trattamento dati personali*" nelle persone dei Dirigenti delle singole strutture in cui si articola l'organizzazione della Città Metropolitana, che sono preposti al trattamento dei dati contenuti nelle banche dati esistenti nelle articolazioni organizzative di loro competenza. Per il trattamento di dati il Titolare può avvalersi anche di soggetti pubblici o privati. L'elenco degli "*Autorizzati di 1° livello al trattamento dati personali*" delle strutture in cui si articola l'organizzazione dell'Ente è pubblicato nella sezione "Privacy Policy" del sito istituzionale ed aggiornato periodicamente;

b) nominare il Responsabile della protezione dati;

c) diramare le direttive necessarie per l'applicazione delle disposizioni del RGPD e del presente Regolamento, sentiti il Segretario Generale, il Responsabile della Protezione dei dati ed gli "*Autorizzati di 1° livello al trattamento dati personali*".

Nelle convenzioni, nelle concessioni, nei contratti, negli incarichi professionali o altri strumenti giuridici consentiti dalla legge con cui è affidata a soggetti esterni a Città Metropolitana la gestione di attività e servizi per conto della medesima, è prevista espressamente la nomina degli stessi soggetti affidatari quali Responsabili esterni del trattamento dei dati personali connessi alle attività istituzionali affidate.

Nel caso di esercizio associato di funzioni o servizi, nonché per i compiti la cui gestione è affidata alla Città Metropolitana da enti o organismi statali o regionali, allorchè due o più titolari determinano congiuntamente, mediante accordo, le finalità e i mezzi di trattamento, si realizza la contitolarità di cui al Capo IV Sez. I art. 26 RGPD. L'accordo definisce le responsabilità di ciascuno in merito all'osservanza degli obblighi in tema di privacy, con particolare riferimento all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli artt. 13 e 14 Capo III Sez. II del RGPD, fermo restando eventualmente quanto stabilito dalla normativa specificatamente applicabile.

La Città Metropolitana favorisce l'adesione ai codici di condotta elaborati dalle associazioni e dagli organismi di categoria rappresentativi, ovvero a meccanismi di certificazione della protezione dei dati approvati, per contribuire alla corretta applicazione del RGPD e per dimostrarne il concreto rispetto da parte del Titolare e degli "*Autorizzati di 1° livello al trattamento dati personali*".

Art. 5 - Autorizzati di 1° livello al trattamento dati personali

La Città Metropolitana si avvale obbligatoriamente di più "*Autorizzati di 1° livello al trattamento dati personali*", designati dal Sindaco con decreto di attribuzione delle funzioni dirigenziali, nel quale sono tassativamente previsti:

- la materia trattata, la durata, la natura, la finalità, i poteri e le modalità del trattamento o dei trattamenti assegnati;
- il tipo di dati personali oggetto di trattamento e le categorie di interessati;
- gli obblighi e i diritti del titolare del trattamento.

L' "*Autorizzato di 1° livello al trattamento dati personali*" deve essere in grado, anche attraverso un'adeguata preventiva formazione, di offrire garanzie sufficienti in termini di conoscenza specialistica, esperienza, capacità ed affidabilità, per mettere in atto le misure tecniche ed organizzative volte a garantire che i trattamenti siano effettuati in conformità al RGPD.

Le operazioni di trattamento possono essere effettuate solo da "*Autorizzati di 2° livello*" che operano sotto la diretta autorità dell' "*Autorizzato di 1° livello al trattamento dati personali*", attenendosi alle istruzioni loro impartite per iscritto dallo stesso, le quali individuano specificatamente l'ambito del trattamento consentito.

L' "*Autorizzato di 1° livello al trattamento dati personali*" garantisce che chiunque agisca sotto la sua autorità ed abbia accesso a dati personali sia in possesso di apposita formazione ed istruzione e sia impegnato alla riservatezza od abbia un adeguato obbligo legale di riservatezza.

L' "*Autorizzato di 1° livello al trattamento dati personali*" provvede, per il proprio ambito di competenza, a tutte le attività previste dalla legge e a tutti i compiti affidatigli dal Titolare, analiticamente specificati per iscritto nell'atto di designazione, ed in particolare provvede:

a) a tenere aggiornato il registro delle categorie di attività di trattamento svolte per conto del Titolare;

b) ad adottare misure tecniche e organizzative adeguate per garantire la sicurezza dei trattamenti;

c) ad individuare per iscritto i dipendenti appartenenti alla sua struttura autorizzando i medesimi ad accedere ai dati personali al fine di svolgerne il trattamento afferente i rispettivi compiti istituzionali;

d) alla sensibilizzazione ed alla formazione del personale di cui al punto c), fornendo le istruzioni per il corretto trattamento di dati personali nonché al successivo controllo sulle attività di trattamento, con particolare riferimento alle operazioni di comunicazione e diffusione, svolte dagli "*Autorizzati di 2° livello al trattamento dati personali*" affinchè siano conformi alle norme del RGPD;

e) a collaborare con il Titolare nella conduzione della valutazione dell'impatto sulla protezione dei dati (di seguito indicata come "DPIA") fornendo allo stesso ogni informazione di cui è in possesso;

f) ad informare il Titolare, senza ingiustificato ritardo, della conoscenza di casi di violazione dei dati personali (cd. "data breach"), informando gli interessati laddove ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà dei medesimi;

g) a curare le informative di cui agli articoli 13 e 14 del RGPD da fornire agli interessati, predisponendo la necessaria modulistica o determinando altre forme idonee di informazione inerenti i trattamenti di competenza della propria struttura organizzativa, facendo, in presenza di dati sensibili, espresso riferimento alla normativa che prevede gli obblighi o i compiti in base alla quale è effettuato il trattamento;

h) adottare le misure necessarie per facilitare l'esercizio dei diritti dell'interessato di cui agli articoli da 15 a 22 del RGPD;

i) a stipulare gli accordi con altri soggetti pubblici e privati per l'esercizio del diritto di accesso alle banche dati nei limiti previsti dalle disposizioni legislative e regolamentari;

j) ad adempiere le prescrizioni del titolare.

Art. 6 - Responsabili esterni del trattamento

I soggetti esterni che effettuano operazioni di trattamento sui dati di Città Metropolitana di Milano, per conto e nell'interesse della stessa, per finalità connesse all'esercizio delle funzioni istituzionali, sono nominati Responsabili esterni del trattamento.

A tali Responsabili esterni si applicano le disposizioni dell'articolo 28 del Regolamento Europeo.

Art. 7 - Amministratore di sistema

La Città Metropolitana di Milano si avvale obbligatoriamente di uno o più amministratori del sistema informatico al fine di assicurare che il sistema informatico dell'Ente sia strutturato e gestito in modo da garantire le misure tecniche e organizzative adeguate per la necessaria protezione dei dati personali trattati attraverso lo stesso sistema.

La Città Metropolitana applica quanto previsto *Garante per la protezione dei dati personali* con provvedimenti del 27.11.2008 e del 25.6.2009 e s.m.i..

Art. 8 - Responsabile della protezione dati

Città Metropolitana di Milano si avvale obbligatoriamente di un Responsabile della Protezione dei dati (RPD), in possesso delle qualità professionali, delle conoscenze specialistiche in materia di protezione dei dati nonché della capacità di assolvere i compiti di competenza.

Il RPD è nominato dal Titolare, con proprio atto, tra i dipendenti in servizio presso l'Ente ovvero, in mancanza di idonee figure in possesso dei requisiti prescritti, scelto all'esterno tramite procedura ad evidenza pubblica.

Il RPD è incaricato dei seguenti compiti:

a) informare e fornire consulenza al Titolare ed agli "*Autorizzati di 1° livello al trattamento dati personali*" nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal RGPD e dalle altre normative relative alla protezione dei dati. In tal senso il RPD può indicare al Titolare e/o all' "*Autorizzato di 1° livello al trattamento dati personali*" i settori funzionali ai quali riservare un audit interno o esterno in tema 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 RGPD e delle altre normative relative alla protezione dati, fermo restando le responsabilità del Titolare e degli "*Autorizzati di 1° livello al trattamento dati personali*". 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, assistenza e indirizzo nei confronti del Titolare e degli "*Autorizzati di 1° livello al trattamento dati personali*";

c) sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo poste in essere dal Titolare e dall' "*Autorizzato di 1° livello al trattamento dati personali*";

d) fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dati (DPIA) e sorvegliarne lo svolgimento. Il Titolare, in particolare, si consulta con il RPD in merito a: se condurre o meno una DPIA, quale metodologia adottare nel condurre una DPIA; se condurre la DPIA con le risorse interne ovvero esternalizzandola; quali salvaguardie applicare; comprese misure tecniche organizzative, per attenuare i rischi delle persone interessate; se la DPIA sia stata condotta correttamente o meno e se le

conclusioni raggiunte (procedere o meno con il trattamento, e quali salvaguardie applicare) siano conformi al RGPD;

e) cooperare con il *Garante per la protezione dei dati personali* e fungere da punto di contatto per detta Autorità per questioni connesse al trattamento, tra cui la consultazione preventiva di cui al Capo IV art. 36 RGPD, ed effettuare, se del caso, consultazioni relativamente a ogni altra questione.

Il Titolare ed gli "*Autorizzati di 1° livello al trattamento dati personali*" assicurano che il RPD sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali. A tal fine:

- il RPD è invitato a partecipare alle riunioni di coordinamento dei Dirigenti/Responsabili P.O. che abbiano per oggetto questioni inerenti la protezione dei dati personali;
- il RPD deve disporre tempestivamente di tutte le informazioni pertinenti sulle decisioni che impattano sulla protezione dei dati, in modo da poter rendere una consulenza idonea, scritta od orale;
- il parere del RPD sulle decisioni che impattano sulla protezione dei dati è obbligatorio ma non vincolante. Nel caso in cui la decisione assunta determina condotte difformi da quelle raccomandate dal RPD, è necessario motivare specificatamente tale decisione;
- il RPD deve essere consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente.

Nello svolgimento dei compiti affidatigli il RPD deve debitamente considerare i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo. In tal senso il RPD:

a. procede a una mappatura delle aree di attività valutandone il grado di rischio in termini di protezione dei dati;

b. propone un ordine di priorità nell'attività da svolgere sulla base dei contributi dei Dirigenti/P.O. ed in base al piano di sicurezza dell'Ente, incentrandola sulle aree di attività che presentano maggiori rischi in termini di protezione dei dati, da comunicare al Titolare ed agli "*Autorizzati di 1° livello al trattamento dati personali*".

Il RPD dispone di autonomia e risorse sufficienti a svolgere in modo efficace i compiti attribuiti, tenuto conto delle dimensioni organizzative e delle capacità di bilancio dell'Ente.

Il Titolare ed gli "*Autorizzati di 1° livello al trattamento dati personali*" forniscono al RPD le risorse necessarie per assolvere i compiti attribuiti e per accedere ai dati personali ed ai trattamenti.

In particolare è assicurato al RPD:

- supporto attivo per lo svolgimento dei compiti da parte dei Dirigenti/Responsabili P.O. e del Sindaco, anche considerando l'attuazione delle attività necessarie per la protezione dati nell'ambito della programmazione operativa;

- tempo sufficiente per l'espletamento dei compiti affidati al RPD; supporto adeguato in termini di risorse finanziarie ed infrastrutture; comunicazione ufficiale della nomina a tutto il personale, in modo da garantire che la sua presenza e le sue funzioni siano note all'interno dell' Ente;
- accesso gratuito ai settori funzionali dell'Ente così da fornirgli supporto, informazioni e input essenziali.

Il RPD opera in posizione di autonomia nello svolgimento dei compiti allo stesso attribuiti; in particolare, non deve ricevere istruzioni in merito al loro svolgimento né sull'interpretazione da dare a una specifica questione attinente alla normativa in materia di protezione dati.

Il RPD non può essere rimosso o penalizzato dal Titolare e dagli "*Autorizzati di 1° livello al trattamento dati personali*" per l'adempimento dei propri compiti.

Fermo restando l'indipendenza nello svolgimento di detti compiti, il RPD riferisce direttamente al Titolare od agli "*Autorizzati di 1° livello al trattamento dati personali*".

Nel caso in cui siano rilevate dal RPD o sottoposte alla sua attenzione decisioni incompatibili con RGPD e con le indicazioni fornite dallo stesso RPD, quest'ultimo è tenuto a manifestare il proprio dissenso motivato, comunicandolo al Titolare e agli "*Autorizzati di 1° livello al trattamento dati personali*".

Art. 9 - Sicurezza del trattamento

Il Titolare ed gli "*Autorizzati di 1° livello al trattamento dati personali*" nonché il RPD provvedono, per quanto di rispettiva competenza, all'adozione e alla dimostrazione di attuazione concreta di misure tecniche ed organizzative adeguate onde garantire un livello di sicurezza correlato al rischio tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.

Le misure tecniche ed organizzative di sicurezza da mettere in atto per ridurre i rischi del trattamento ricomprendono misure logiche e fisiche quali: la pseudonimizzazione; la minimizzazione; la cifratura dei dati personali; la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali; la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico; una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Costituiscono misure tecniche e organizzative che possono essere adottate da ciascun "*Autorizzato di 1° livello al trattamento dati personali*":

- sistemi di autenticazione; sistemi di autorizzazione; sistemi di protezione (antivirus; firewall; anti-intrusione; altro);
- misure antincendio; sistemi di rilevazione di intrusione; sistemi di sorveglianza; sistemi di protezione con videosorveglianza; registrazione accessi; porte, armadi e contenitori dotati di serrature e ignifughi; sistemi di copiatura e conservazione di archivi elettronici;

- altre misure per ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico e tecnico.

La conformità del trattamento dei dati al RGDP in materia di protezione dei dati personali è dimostrata attraverso l'adozione delle misure di sicurezza o l'adesione a codici di condotta approvati o ad un meccanismo di certificazione approvato.

il Titolare e ciascun "*Autorizzato di 1° livello al trattamento dati personali*" si impegnano ad impartire adeguate istruzioni sul rispetto delle predette misure a chiunque agisca per loro conto ed abbia accesso a dati personali.

I nominativi ed i dati di contatto del Titolare, degli "*Autorizzati di 1° livello al trattamento dati personali*" e del Responsabile della protezione dati sono pubblicati sul sito istituzionale della Città Metropolitana di Milano, sezione Amministrazione trasparente, oltre che nella sezione "Privacy Policy".

Art. 10 - Pubblicazione web per obblighi di trasparenza

La Città Metropolitana di Milano effettua il trattamento di dati personali, contenuti in atti e documenti amministrativi, che devono essere pubblicati sul web per obblighi di trasparenza previsti dalla normativa in vigore.

I documenti di cui al comma 1 sono pubblicati tempestivamente sul sito istituzionale dell'amministrazione e vanno mantenuti aggiornati.

Non possono essere resi intellegibili i dati non necessari, eccedenti o non pertinenti con la finalità di pubblicazione.

I dati idonei a rivelare origine razziale ed etnica, convinzioni religiose, filosofiche o di altro genere, opinioni politiche, adesione a partiti, sindacati, associazioni e organizzazioni a carattere filosofico, politico o sindacale possono essere diffusi solo se indispensabili; i dati relativi alla vita sessuale non possono essere diffusi per finalità di trasparenza. I dati particolari idonei a rivelare lo stato di salute non devono essere diffusi.

I dati vanno pubblicati in formato di tipo aperto ai sensi dell'art. 68, D.Lgs. n. 82/2005 e sono liberamente riutilizzabili secondo la normativa vigente.

Art. 11 - Registro delle attività di trattamento del Titolare

Il Registro delle attività di trattamento svolte dal Titolare del trattamento reca almeno le seguenti informazioni:

a) il nome ed i dati di contatto della Città Metropolitana in qualità di titolare del trattamento nonchè del Responsabile della Protezione dei Dati;

b) le finalità del trattamento;

c) la sintetica descrizione delle categorie di interessati, nonché le categorie di dati personali;

d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;

e) l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;

f) ove stabiliti, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;

g) il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate.

Ciascun "*Autorizzato di 1° livello al trattamento dati personali*" ha la responsabilità di fornire prontamente e correttamente al soggetto preposto ogni elemento necessario alla regolare tenuta ed aggiornamento del Registro.

Il Registro deve essere aggiornamento almeno annualmente.

Art. 12 - Registro delle attività di trattamento del Responsabile

Il Registro delle attività di trattamento svolte dal Responsabile reca almeno le seguenti informazioni:

a) il nome ed i dati di contatto della Città Metropolitana in qualità di Responsabile del trattamento e del Responsabile della Protezione dei Dati;

b) le categorie di trattamenti effettuati per conto di altri Titolari: raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, uso, comunicazione, raffronto, interconnessione, limitazione, cancellazione, distruzione, profilazione, pseudonimizzazione ed ogni altra operazione applicata a dati personali;

c) l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;

d) il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate.

Il predetto Registro, tenuto in formato informatico, è compreso nel Registro unitario nel quale sono annotati anche i dati del Registro delle attività di trattamento del Titolare di cui al precedente articolo.

Art. 13 - Valutazione d'impatto sulla protezione dei dati

Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare, prima di effettuare il trattamento, deve effettuare una valutazione dell' impatto del medesimo trattamento (DPIA) a sensi dell' art 35 RGDP, considerati la natura, l'oggetto, il contesto e le finalità dello stesso trattamento. La DPIA è una procedura che permette di realizzare e dimostrare la conformità alle norme del trattamento di cui trattasi.

Ai fini della decisione di effettuare o meno la DPIA si tiene conto degli elenchi delle tipologie di trattamento soggetti o non soggetti a valutazione come redatti e pubblicati dal *Garante per la protezione dei dati personali* ai sensi dell' art. 35, pp. 4-6, RGDP.

La DPIA è effettuata in presenza di un rischio elevato per i diritti e le libertà delle persone fisiche.

Fermo restando quanto indicato dall' art 35, p. 3, RGDP, i criteri in base ai quali sono evidenziati i trattamenti determinanti un rischio intrinsecamente elevato sono i seguenti:

1. trattamenti valutativi o di scoring, compresa la profilazione e attività predittive, concernenti aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l' ubicazione o gli spostamenti dell' interessato;

2. decisioni automatizzate che producono significativi effetti giuridici o di analoga natura, ossia trattamenti finalizzati ad assumere decisioni su interessati che producono effetti giuridici sulla persona fisica ovvero che incidono in modo analogo significativamente su dette persone fisiche;

3. monitoraggio sistematico, ossia trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o la sorveglianza sistematica di un' area accessibile al pubblico;

4. trattamenti di dati sensibili o dati di natura estremamente personale, ossia le categorie particolari di dati personali di cui all' art. 9 RGDP;

5. trattamenti di dati su larga scala, tenendo conto: del numero di soggetti interessati del trattamento, in termini numerici o di percentuale rispetto alla popolazione di riferimento; volume dei dati e/o ambito delle diverse tipologie di dati oggetto di trattamento; durata o persistenza dell' attività di trattamento; ambito geografico dell' attività di trattamento;

6. combinazione o raffronto di insiemi di dati, secondo modalità che esulano dalle ragionevoli aspettative dell'interessato;

7. dati relativi a interessati vulnerabili, ossia ogni interessato particolarmente vulnerabile e meritevole di specifica tutela per il quale si possa identificare una situazione di disequilibrio nel rapporto con il Titolare del trattamento, come i dipendenti dell'Ente, anziani e minori;

8. utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative;

9. tutti quei trattamenti che, di per sè, impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto.

Nel caso in cui un trattamento soddisfi almeno due dei criteri sopra indicati occorre, in via generale, condurre una DPIA, salvo che il Titolare ritenga motivatamente che non può presentare un rischio elevato; il Titolare può motivatamente ritenere che un trattamento che soddisfa solo uno dei criteri di cui sopra occorra comunque la condizione di una DPIA.

Il Titolare garantisce l'effettuazione della DPIA ed è responsabile della stessa. Il Titolare può affidare la conduzione materiale della DPIA ad un altro se oggetto, interno o esterno alla Città Metropolitana.

Il Titolare deve consultarsi con il RPD anche per assumere la decisione di effettuare o meno la DPIA; tale consultazione e le conseguenti decisioni assunte dal Titolare devono essere documentate nell'ambito della DPIA. Il RPD monitora lo svolgimento della DPIA.

Gli "*Autorizzati di 1° livello al trattamento dati personali*" collaborano e assistono il Titolare ed il RPD nella conduzione della DPIA fornendo ogni informazione necessaria.

Il RPD può proporre lo svolgimento di una DPIA in rapporto a uno specifico trattamento, collaborando al fine di mettere a punto la relativa metodologia, definire la qualità del processo di valutazione del rischio e l' accettabilità o meno del livello di rischio residuale.

La DPIA non è necessaria nei seguenti casi:

- se il trattamento non può comportare un rischio elevato per i diritti e le libertà di persone fisiche ai sensi dell' art.35, p.1, RGPD;
- se la natura, l'ambito, il contesto e le finalità del trattamento sono simili a quelli di un trattamento per il quale è già stata condotta una DPIA. In questo caso si possono utilizzare i risultati della DPIA svolta per l'analogo trattamento;
- se il trattamento è stato sottoposto a verifica da parte del *Garante per la protezione dei dati personali* prima del maggio 2018 in condizioni specifiche che non hanno subito modifiche;
- se un trattamento trova la propria base legale nella vigente legislazione che disciplina lo specifico trattamento, ed è già stata condotta una DPIA all'atto della definizione della base giuridica suddetta.

Non è necessario condurre una DPIA per quei trattamenti che siano già stati oggetto di verifica preliminare da parte del *Garante per la protezione dei dati personali* o da un RDP e che proseguano con le stesse modalità oggetto di tale verifica. Inoltre, occorre tener conto che le autorizzazioni del *Garante per la protezione dei dati personali* basate sulla direttiva 95/46/CE rimangono in vigore fino a quando non vengono modificate, sostituite od abrogate.

La DPIA è condotta prima di dar luogo al trattamento, attraverso i seguenti processi:

- descrizione sistematica del contesto, dei trattamenti previsti, delle finalità del trattamento e tenendo conto dell'osservanza di codici di condotta approvati. Sono altresì indicati: i dati personali oggetto del trattamento, i destinatari e il periodo previsto di conservazione dei dati stessi; una descrizione funzionale del trattamento; gli strumenti coinvolti nel trattamento dei dati personali (hardware, software, reti, persone, supporti cartacei o canali di trasmissione cartacei);
- valutazione della necessità e proporzionalità dei trattamenti, sulla base:
    - delle finalità' specifiche, esplicite e legittime;
    - della liceità del trattamento;
    - dei dati adeguati, pertinenti e limitati a quanto necessari;
    - del periodo limitato di conservazione;
    - delle informazioni fornite agli interessati;
    - del diritto di accesso;

- del diritto di rettifica e cancellazione, di opposizione e limitazione del trattamento;
- dei rapporti con i responsabili del trattamento;
- delle garanzie per i trasferimenti internazionali dei dati;
- consultazione preventiva del *Garante per la protezione dei dati personali*;

- valutazione dei rischi per i diritti e le libertà degli interessati, valutando la particolare probabilità e gravità dei rischi rilevati. Sono determinati l'origine, la natura, la particolarità e la gravità dei rischi o, in modo più specifico, di ogni singolo rischio (accesso illegittimo, modifiche indesiderate indisponibilità dei dati) dal punto di vista degli interessati;

- individuazione delle misure previste per affrontare ed attenuare i rischi, assicurare la protezione dei dati personali e dimostrare la conformità dl trattamento con il RGPD, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Il Titolare può raccogliere le opinioni degli interessati o dei loro rappresentanti, se gli stessi possono essere preventivamente individuati. La mancata consultazione è specificatamente motivata, così come la decisione assunta in senso difforme dall' opinione degli interessati.

Il Titolare deve consultare il *Garante per la protezione dei dati personali* prima di procedere al trattamento se le risultanze della DPIA condotta indicano l'esistenza di un rischio residuale elevato. Il Titolare consulta il *Garante per la protezione dei dati personali* anche nei casi in cui la vigente legislazione stabilisce l'obbligo di consultare e/o ottenere la previa autorizzazione della medesima autorità, per trattamenti svolti per l'esecuzione di compiti di interesse pubblico, fra cui i trattamenti connessi alla protezione sociale ed alla sanità pubblica.

La DPIA deve essere effettuata – con eventuale riesame delle valutazioni condotte – anche per i trattamenti in corso che possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, nel caso in cui siano intervenute variazioni dei rischi originari tenuto conto della natura, dell'ambito, del contesto e delle finalità del medesimo trattamento.

Art. 14 - Violazione dei dati personali

Per violazione dei dati personali (in seguito "data breach") si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati dalla Città Metropolitana.

Il Titolare, ove ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati, provvede alla notifica della violazione al *Garante per la protezione dei dati personali*. La notifica dovrà avvenire entro 72 ore e comunque senza giustificato ritardo.

Gli "*Autorizzati di 1° livello al trattamento dati personali*" ed i Responsabili del trattamento, sono obbligati a informare il Titolare, senza ingiustificato ritardo, dopo essere venuto a conoscenza della violazione.

I principali rischi per i diritti e le libertà degli interessati conseguenti ad una violazione, in conformità al considerando art. 75 del RGPD, sono i seguenti:

- danni fisici, materiali o immateriali alle persone fisiche;
- perdita di controllo dei dati personali;
- limitazione dei diritti, discriminazione;
- furto o usurpazione d'identità;
- perdite finanziarie, danno economico o sociale;
- decifratura non autorizzata della pseudonimizzazione;
- pregiudizio alla reputazione;
- perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari).

Se il Titolare ritiene che il rischio per i diritti e le libertà degli interessati conseguente alla violazione rilevata è elevato, allora deve informare questi ultimi, senza ingiustificato ritardo, con un linguaggio semplice e chiaro al fine di fare comprendere loro la natura della violazione dei dati personali verificatesi.

I rischi per i diritti e le libertà degli interessati possono essere e considerati "elevati" quando la violazione può a titolo di esempio:

- coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati;
- riguardare categorie particolari di dati personali;
- comprendere dati che possono accrescere ulteriormente i potenziali rischi (ad esempio dati di localizzazione, finanziari, relativi alle abitudini e preferenze);
- comportare rischi imminenti e con un' elevata probabilità di accadimento (ad esempio rischio di perdita finanziaria in caso di furto di dati relativi a carte di credito);
- impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (ad esempio udenti deboli, minori, soggetti indagati).

La notifica deve avere il contenuto minimo previsto dall'art. 33 RGPD, ed anche la comunicazione all'interessato deve contenere almeno le informazioni e le misure di cui al citato art. 33.

Il Titolare deve opportunamente documentare le violazioni di dati personali subite, anche se non comunicate alle autorità di controllo, nonché le circostanze ad esse relative, le conseguenze e i provvedimenti adottati o che intende adottare per porvi rimedio. Tale documentazione deve essere conservata con la massima cura e diligenza in quanto può essere richiesta dal *Garante per la protezione dei dati personali* al fine di verificare il rispetto delle disposizioni del RGPD.

Art. 15 - Diritto di accesso

L'interessato ha sempre diritto di ottenere dal Titolare del trattamento la conferma che sia in corso un trattamento dei dati personali che lo riguardano, di averne accesso e di acquisire informazioni di cui all'art. 13 del Regolamento Europeo.

La richiesta va inoltrata in forma scritta dall'interessato senza particolari formalità; in caso sia inoltrata con mezzi elettronici, salvo contraria indicazione dell'interessato, le informazioni sono fornite in formato elettronico di uso comune.

Il Titolare del trattamento deve fornire risposta entro 30 giorni dal ricevimento della richiesta.

Gli "*Autorizzati di 1° livello al trattamento dati personali*" ed i Responsabili del Trattamento, sono tenuti a collaborare per la verifica della sussistenza del diritto chiedendo informazioni all'interessato, ove necessarie, anche al fine di identificarlo e, successivamente, per consentire l'esercizio del diritto in caso di riscontro favorevole. In tale ipotesi, va rilasciata copia del documento richiesto.

Il rilascio della copia è gratuito; in caso di richiesta di copie ulteriori il rilascio può essere subordinato al pagamento di un contributo per costi amministrativi.

Il diritto alla portabilità dei dati di cui all'articolo 20 del R.G.P.D. non si applica ai trattamenti svolti dalla Città Metropolitana necessari per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito lo stesso ente.

Art. 16 - Diritto di limitazione

L'interessato, previa richiesta scritta, ha diritto ad ottenere la limitazione del trattamento:

- in caso sia contestata l'esattezza dei dati personali, per il periodo necessario alla verifica da parte della Città Metropolitana di Milano;
- in caso di trattamento illecito, se si oppone alla cancellazione dei dati chiedendo invece che ne sia limitato l'utilizzo;
- in caso di esercizio di opposizione nell'attesa della verifica dei presupposti del relativo diritto.

Il Titolare del trattamento deve fornire risposta entro 30 giorni dal ricevimento della richiesta. Gli "*Autorizzati di 1° livello al trattamento dati personali*" ed i Responsabili del Trattamento, sono tenuti a collaborare per la verifica della sussistenza del diritto chiedendo informazioni all'interessato, ove necessarie, anche al fine di identificarlo e, successivamente, per consentire l'esercizio del diritto in caso di riscontro favorevole. In caso di riscontro favorevole va comunicato all'interessato che ha ottenuto la limitazione del trattamento, senza ritardo e prima che la limitazione sia revocata.

Art. 17 - Diritto all'oblio

L'interessato ha diritto a chiedere previa richiesta scritta, al Titolare del trattamento la cancellazione dei dati personali che lo riguardano:

- se non sono più necessari per le finalità per le quali sono stati raccolti o trattati;
- se si oppone al trattamento e non sussiste motivo legittimo prevalente per procedere al trattamento;
- se i dati sono illecitamente trattati.

Il Titolare del trattamento deve fornire risposta entro 30 giorni dal ricevimento della richiesta. Gli "*Autorizzati di 1° livello al trattamento dati personali*" ed i Responsabili del Trattamento sono tenuti a collaborare per la verifica della sussistenza del diritto chiedendo informazioni all'interessato, ove necessarie, anche al fine di identificarlo e, successivamente, per consentire l'esercizio del diritto in caso di riscontro favorevole.

In caso i dati siano stati diffusi pubblicamente anche su siti web, il Titolare del trattamento, tenendo conto dei costi di attuazione, è tenuto ad informare altri titolari che trattano i medesimi dati, della richiesta di cancellazione di qualsiasi link, copia o riproduzione. In caso in cui i dati non siano diffusi pubblicamente e su siti web il Titolare del trattamento è tenuto ad avvisare i destinatari della cancellazione dei dati, salvo ciò non sia impossibile o richieda uno sforzo sproporzionato.

Art. 18 - Diritto alla rettifica dei dati

L'interessato ha diritto a chiedere la rettifica da parte della Città Metropolitana di Milano, senza ingiustificato ritardo, dei dati personali inesatti che lo riguardano. La rettifica include anche la possibile integrazione dei dati avuto riguardo alla finalità del trattamento.

Il Titolare del trattamento deve fornire risposta entro 30 giorni dal ricevimento della richiesta. Igli "*Autorizzati di 1° livello al trattamento dati personali*" ed i Responsabili del Trattamento sono tenuti a collaborare per la verifica della sussistenza del diritto chiedendo informazioni all'interessato, ove necessarie, anche al fine di identificarlo e, successivamente, per dare seguito all'esercizio del diritto dell'interessato.

Art. 19 - Diritto di opposizione

L'interessato può presentare per iscritto richiesta di opposizione al trattamento dei dati personali che lo riguardano per motivi connessi alla sua situazione particolare, inclusa la profilazione.

Il Titolare del trattamento entro trenta giorni fornisce risposta all'interessato a seguito della valutazione della situazione: è consentito l'esercizio del diritto se non esistano comprovati motivi basati su norma di legge per procedere al trattamento prevalenti sugli interessi o diritti del richiedente o negli altri casi indicati all'articolo 21 del Regolamento Europeo.

Art. 20 - Obbligo di informativa

Prima che inizi qualunque trattamento di dati personali gli "*Autorizzati di 1° livello al trattamento dati personali*" forniscono all'interessato le informazioni necessarie per consentirgli l'esercizio dei propri diritti.

L'informativa privacy deve essere fornita per iscritto in formato cartaceo o elettronico, o qualora l'interessato lo richieda espressamente, anche oralmente, previa verifica dell'identità dell'interessato.

Non è necessario fornire l'informativa:

a) nel caso in cui la comunicazione risulta impossibile o implicherebbe uno sforzo sproporzionato; in particolare per il trattamento ai fini di archiviazione nel pubblico

interesse, di ricerca scientifica o storica o a fini statistici. In tali casi il Titolare del trattamento adotta misure comunque appropriate per tutelare i diritti dell'interessato anche con pubbliche informazioni;

b) in presenza di un obbligo di legge che impone la riservatezza e segretezza dei dati personali.

Art. 21 - Contenuto dell'informativa

L'informativa è gratuita e deve essere sintetica, presentare un linguaggio chiaro e semplice ed essere in ogni caso comprensibile per l'interessato.

Essa presenta il seguente contenuto:

- indicazione dell'Ente Titolare del trattamento;
- indicazione del Responsabile della protezione dei dati;
- indicazione di ogni finalità istituzionale di trattamento e della norma giuridica di riferimento;
- indicazione di finalità aventi fondamento in contratto o in richiesta dell'interessato;
- indicazione delle modalità di trattamento evidenziando se sia un trattamento automatizzato (con eventuale possibilità di profilazione e della sua logica) o se sia un trattamento cartaceo;
- ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale;
- il periodo di conservazione dei dati personali e, se non è previsto da norma di legge, il criterio utilizzato dal Titolare per la durata del trattamento;
- l'indicazione dei diritti che l'interessato può esercitare, ovvero: accesso, integrazione e rettifica, eventuale revoca, portabilità, oblio, opposizione e reclamo;
- le conseguenze in caso di rifiuto del trattamento o di omessa comunicazione di dati.

Art. 22 - Consenso

Il consenso al trattamento dei dati non è richiesto dalla Città Metropolitana di Milano in quanto pubblica amministrazione se agisce per finalità istituzionali.

Il consenso può essere richiesto se l'ente agisce per specifiche finalità diverse da quelle istituzionali ai sensi dell'art. 1, comma 2, lett. c).

In tal caso l'"*Autorizzato di 1° livello al trattamento dati personali*" deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso.

La richiesta di consenso deve essere comprensibile, facilmente accessibile, chiara e semplice.

Il consenso può essere revocato ed in tal caso la revoca non pregiudica la liceità del trattamento già effettuato, se necessaria al caso concreto.

CAPO SECONDO

UTILIZZO DEGLI IMPIANTI DI VIDEOSORVEGLIANZA

Art. 23 - Oggetto

Il presente capo disciplina le modalità di trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza, impianti di videocontrollo e videocitofono attivati presso gli stabili o altri siti di proprietà della Città Metropolitana di Milano, che verranno individuati tramite atti dirigenziali.

La Città Metropolitana di Milano garantisce che i suddetti impianti non effettuano riprese circostanziate ai veicoli in transito nonché alle persone eventualmente in sosta, limitandosi ad effettuare una ripresa globale della situazione.

Tali impianti:

a) riprendono e/o registrano immagini in aree o zone delimitate che possono riguardare i soggetti e mezzi di trasporto che transitano nell'area interessata;

b) consentono unicamente riprese/registrazioni video senza operare algoritmi di analisi;

c) sono gestiti da Città Metropolitana di Milano.

La Città Metropolitana di Milano stabilisce che le finalità di utilizzo degli impianti di videosorveglianza sono:

a) vigilare sugli immobili e sulle relative aree di pertinenza per prevenire furti e danneggiamenti a tutela del patrimonio metropolitano e per garantire protezione e assistenza ai soggetti a vario titolo fruitori di tali spazi;

b) controllare determinate aree pubbliche di competenza della Città Metropolitana di Milano per fini istituzionali, ivi inclusa la pubblica sicurezza.

Gli impianti di videosorveglianza sono configurati in modo da raccogliere esclusivamente i dati strettamente pertinenti e limitati a quanto necessario per il raggiungimento delle finalità perseguite, registrando le sole immagini indispensabili, limitando l'angolo visuale delle riprese ed evitando, quando non indispensabili, immagini dettagliate, ingrandite o con particolari non rilevanti, non comportando lesione nei diritti e nelle libertà fondamentali degli interessati.

Ai sensi dell'articolo 4 della Legge 20 maggio 1970, n. 300 è vietato, e pertanto escluso, l'uso degli impianti di videosorveglianza per effettuare controlli a distanza sull'attività lavorativa dei dipendenti della Città Metropolitana di Milano, di altre amministrazioni pubbliche o di altri datori di lavoro, pubblici o privati.

La Città Metropolitana di Milano utilizza impianti di videosorveglianza presso le Gallerie artificiali delle strade provinciali, individuati tramite atti dirigenziali come previsto al comma 1 del presente articolo, a supporto dei sistemi di segnalazione e prevenzione incendi e allagamenti installati all'interno del manufatto. I suddetti impianti inviano le immagini presso il locale

tecnico ubicato in prossimità dei sistemi di rilevamento fumi e allagamenti, ove le stesse vengono registrate e conservate per la durata e con le modalità previste dal registro del Titolare del trattamento.

Al fine di una migliore gestione delle eventuali emergenze, il personale autorizzato, all'occorrenza, può interrogare da remoto la banca dati così alimentata mediante un sistema d'accesso protetto da algoritmi di crittografia

Art. 24 - Soggetti

La Città Metropolitana di Milano è titolare del trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza. A tal fine la Città Metropolitana di Milano è legalmente rappresentata dal Sindaco metropolitano, cui compete ogni decisione circa le modalità del trattamento, ivi compreso il profilo della sicurezza.

Il Titolare del trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza:

a) definisce le linee organizzative per l'applicazione della normativa di settore;

b) effettua le notificazioni al *Garante per la protezione dei dati personali*;

c) nomina gli "*Autorizzati di 1° livello al trattamento dati personali*", impartendo istruzioni ed assegnando compiti e responsabilità;

d) detta gli indirizzi per la sicurezza del trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza;

e) vigila sulla puntuale osservanza delle disposizioni impartite.

Gli "*Autorizzati di 1° livello al trattamento dati personali*", così individuati, ed i Responsabili del Trattamento, sono tenuti ad effettuare il trattamento nel rispetto del Regolamento (UE) 2016/679, della normativa vigente, del Provvedimento del Garante in materia di videosorveglianza del 8 aprile 2010 e delle disposizioni del presente Regolamento.

L' "*Autorizzato di 1° livello al trattamento dati personali*", in particolare:

a) organizza il trattamento delle immagini registrate e/o visualizzate tramite i sistemi di videosorveglianza;

b) adotta e rispetta le misure di sicurezza indicate dalla legge, dai provvedimenti del Garante e quelle descritte nel presente Regolamento;

c) individua gli autorizzati al trattamento dei dati, in numero sufficiente a garantire il trattamento dei dati personali acquisiti, e attribuisce ad essi diversi livelli di visibilità e trattamento delle immagini in presenza di differenti competenze specificatamente attribuite ai singoli operatori;

d) controlla che il periodo di conservazione delle immagini sia conforme a quanto previsto dalla normativa vigente per le finalità indicate dal presente Regolamento, salvo i casi di maggior durata dovuti all'intervento dell'Autorità giudiziaria;

e) vigila sulla puntuale osservanza, da parte degli autorizzati, delle istruzioni impartite e sul corretto svolgimento dei trattamenti di propria competenza;

f) aggiorna l'elenco e la descrizione degli impianti di videosorveglianza di cui all'allegato n. 1, il testo dell'Informativa nonché lo specifico modulo per l'esercizio del diritto di accesso;

g) adotta ogni altra misura prevista dalla legge o individuata dall'Ufficio del Garante a protezione delle immagini e contro accessi non autorizzati.

Sono nominati quali "*Autorizzati di 2° livello al trattamento dati personali*" i dipendenti in servizio presso la struttura tecnica preposta e/o i settori a vario titolo utilizzatori di un sistema di videosorveglianza che per la loro esperienza, capacità e affidabilità sono in grado di fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento e sicurezza dei dati.

Gli "*Autorizzati di 2° livello al trattamento dati personali*" sono a tal fine tenuti ad effettuare il trattamento attenendosi scrupolosamente alle istruzioni impartite dall' "*Autorizzato di 1° livello al trattamento dati personali*", nonché alle disposizioni di cui al presente Regolamento.

Ai soggetti esterni alla Città Metropolitana di Milano, dei quali questa si avvalga a qualsiasi titolo per lo svolgimento di servizi e attività che comportano il trattamento di dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza di cui al presente Regolamento, si applica la disposizione di cui all'articolo 28 del Regolamento (UE) 2016/679.

Art. 25 - Trattamento dei dati personali

La Città metropolitana di Milano dà atto che i dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza di cui al presente Regolamento sono:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;

b) raccolti e, laddove previsto, registrati per le finalità di cui al precedente art. 23;

c) trattati in modo pertinente, completo e non eccedente rispetto alle finalità per le quali sono raccolti;

d) conservati per un periodo non superiore a quello strettamente necessario al soddisfacimento delle finalità per le quali sono raccolti e successivamente trattati, come meglio dettagliato al successivo comma 4.

Gli impianti di videosorveglianza di cui al presente Regolamento consentono riprese video a colori in condizioni di sufficiente illuminazione naturale o artificiale, in bianco e nero in caso contrario. Non sono effettuate riprese di dettaglio dei tratti somatici delle persone, che non siano strettamente funzionali al soddisfacimento delle finalità di cui al precedente art. 23.

I segnali video delle unità di ripresa sono inviati alle centrali di controllo ubicate presso le sedi o i siti ove risiede l'impianto di videosorveglianza e connessi alla rete metropolitana a larga banda al fine di creare un sistema unico di gestione. In queste sedi le immagini sono visualizzate su monitor e registrate in modo criptato su appositi server. L'impiego del sistema di videoregistrazione è necessario per ricostruire l'evento, ai fini del soddisfacimento delle finalità di cui all'art. 1 del presente Regolamento.

I dati personali registrati mediante l'utilizzo degli impianti di videosorveglianza di cui al presente Regolamento sono conservati, ai fini della tutela del patrimonio, per un periodo di tempo non superiore di norma a 6 giorni, per armonizzarlo con gli orari di servizio ed la fine di ottemperare ad eventuali richieste dell'Autorità Giudiziaria. Decorso detto termine i dati registrati sono cancellati con modalità automatica.

La conservazione dei dati personali per un periodo di tempo superiore a quello indicato al comma 4 del presente articolo è ammessa esclusivamente su specifica richiesta della Autorità Giudiziaria o di Polizia Giudiziaria in relazione ad un'attività investigativa in corso.

Fatti salvi i casi di richiesta degli interessati, i dati personali registrati mediante l'utilizzo degli impianti di videosorveglianza di cui al presente Regolamento possono essere riesaminati, nel limite di tempo previsto al comma 4 per la conservazione, esclusivamente in caso di effettiva necessità e per il soddisfacimento delle finalità di cui al precedente art. 23.

La Città Metropolitana di Milano rende noto agli interessati il funzionamento degli impianti di videosorveglianza tramite il posizionamento di cartelli contenenti l'informativa "minima", indicante il titolare del trattamento e la finalità perseguita, di cui al punto 3.1. del Provvedimento in materia di videosorveglianza emanato dal Garante in data 8 aprile 2010.

L'informativa completa, contenente tutti gli elementi di cui all'art. 13 e 14 del Regolamento (UE) 2016/679, viene affissa in bacheche o locali attigui alle aree videosorvegliate e resa disponibile all'utenza senza oneri, nonché pubblicata sul sito internet dell'Ente.

In caso di cessazione del trattamento, i dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza vengono distrutti.

In relazione al trattamento dei dati personali l'interessato ha diritto:

a) di conoscere l'esistenza di trattamenti di dati che possano riguardarlo;

b) di essere informato sugli estremi identificativi del titolare e del responsabile oltre che sulle finalità e le modalità del trattamento cui sono destinati i dati;

c) di ottenere, da parte dell' "*Autorizzato di 1° livello al trattamento dati personali*":

   i. la conferma dell'esistenza o meno dei dati personali che lo riguardano e la comunicazione in forma intelligibile dei medesimi dati e della loro origine, nonché della logica e delle finalità su cui si basa il trattamento;

   ii. la cancellazione dei dati trattati in violazione di legge, compresi quelli di cui è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;

   iii. di opporsi in tutto o in parte, per motivi legittimi, al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta.

Le istanze degli interessati, di cui al presente articolo, devono essere indirizzate al Titolare del trattamento.

La risposta ad una richiesta di accesso a dati conservati deve riguardare tutti quelli attinenti al richiedente identificabile e può comprendere eventuali dati riferiti a terzi solo nei limiti previsti

dal Regolamento (UE) 2016/679, ovvero nei soli casi in cui la scomposizione dei dati trattati o la privazione di alcuni elementi renda incomprensibili i dati personali relativi all'interessato.

I diritti di cui al presente articolo, riferiti ai dati personali concernenti persone decedute, possono essere esercitati da chiunque vi abbia interesse.

Nel caso di esito negativo alla istanza di cui ai commi precedenti, l'interessato ha facoltà di rivolgersi al Garante.

Art. 26 - Misure di sicurezza

Ai sensi di quanto previsto dall'articolo 32 del Regolamento UE 2016/679, i dati Personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza di cui al presente Regolamento sono protetti da misure di sicurezza tali da ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato e trattamento non consentito o non conforme alle finalità di cui al precedente art. 23.

I dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza di cui al presente Regolamento sono custoditi presso le sedi o i siti ove risiede l'impianto di Videosorveglianza e connessi alla rete metropolitana a larga banda al fine di creare un sistema unico di gestione su rete privata.

L'accesso ai siti ove risiedono i server di deposito delle immagini è consentito esclusivamente al Titolare, agli "*Autorizzati di 1° livello al trattamento dati personali*" ed agli "*Autorizzati di 2° livello al trattamento dei dati personali*".

L'accesso da parte di soggetti diversi da quelli indicati al precedente comma è subordinato al rilascio, da parte del Titolare o dell' "*Autorizzato di 1° livello al trattamento dati personali*", di un'autorizzazione scritta, motivata e corredata da specifiche indicazioni in ordine ai tempi ed alle modalità dell'accesso. L'accesso avviene esclusivamente in presenza di "*Autorizzati di 1° o 2° livello al trattamento dati personali*" della Città Metropolitana di Milano.

L' "*Autorizzato di 1° livello al trattamento dati personali*" è tenuto ad impartire idonee istruzioni atte ad evitare assunzioni o rilevamenti di dati da parte dei soggetti autorizzati all'accesso per le operazioni di manutenzione degli impianti e di pulizia dei locali. I locali ove risiedono i sistemi di registrazione sono costantemente monitorati da impianto dedicato di videosorveglianza, con la finalità di monitorarne l'accesso ai fini della sicurezza dei luoghi e salvaguardia delle apparecchiature in essi presenti.

L'accesso agli impianti di videosorveglianza di cui al presente Regolamento avviene da postazioni dedicate situate in edifici costantemente presidiati o dotati di allarme, salvo i casi di preventiva autorizzazione all'accesso da remoto. L'accesso può essere effettuato esclusivamente da operatori muniti di credenziali di accesso valide e strettamente personali, rilasciate dall' "*Autorizzato di 1° livello al trattamento dati personali*".

Un file di log, generato automaticamente dal sistema informatico, consente di registrare gli accessi logici effettuati dai singoli operatori, le operazioni dagli stessi compiute sulle immagini registrate ed i relativi riferimenti temporali.

Art. 27 - Rinvio

Per tutto quanto non espressamente disciplinato con le presenti disposizioni, si applicano le disposizioni del RGPD e tutte le sue norme attuative vigenti.