REGOLAMENTO DELLA CITTÀ METROPOLITANA DI TORINO PER L'ATTUAZIONE DEL REGOLAMENTO UE 2016/679 RELATIVO ALLA PROTEZIONE DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI.

Approvato con Deliberazione del Consiglio metropolitano
n. 57/2023 del 21/12/2023

REGOLAMENTO DELLA CITTÀ METROPOLITANA DI TORINO PER L'ATTUAZIONE DEL REGOLAMENTO UE 2016/679 RELATIVO ALLA PROTEZIONE DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI

INDICE GENERALE

Articolo 1 - OGGETTO E FINALITÀ DEL TRATTAMENTO

1. Il presente Regolamento ha per oggetto misure procedimentali e regole di dettaglio ai fini della migliore funzionalità ed efficacia dell'attuazione del Regolamento europeo 679/2016 relativo alla protezione delle persone fisiche con riguardo ai trattamenti dei dati personali, nonché alla libera circolazione di tali dati (Regolamento Generale Protezione Dati o General Data Protection Regulation - GDPR del 27 aprile 2016 n. 679), nonché del D.Lgs. n. 196/2003 (Codice della Privacy) modificato dal D.Lgs. 101/2018, che si intendono integralmente richiamati, per quanto non espressamente disciplinato dal presente Regolamento.
2. Ai fini del presente Regolamento, i trattamenti sono compiuti dalla Città metropolitana di Torino per le seguenti finalità:
   a) adempimento di un obbligo legale previsto dalla legge, dallo Statuto e dai regolamenti;
   b) esecuzione di compiti di interesse pubblico o connessi all'esercizio di pubblici poteri di cui è investita la Città metropolitana di Torino;
   c) esecuzione di un contratto con i soggetti interessati;
   d) specifiche finalità diverse da quelle di cui ai precedenti punti, purché l'interessato esprima il consenso al trattamento.

Articolo 2 - DEFINIZIONI

1. Ai fini del presente Regolamento si intende per:
   a) dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile, direttamente o indirettamente. Rientrano sia i dati personali cosiddetti comuni (cognome e nome, recapiti, data e luogo di nascita, codici identificativi, targa di veicoli, foto del volto, dati finanziari e di pagamento, dati relativi a documenti d'identità, dati di geolocalizzazione) sia le categorie particolari di dati, idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, nonché i dati personali relativi a condanne penali e reati;
   b) interessato: la persona fisica a cui i dati personali si riferiscono;
   c) trattamento: qualsiasi operazione compiuta sui dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

d) titolare del trattamento: la Città metropolitana di Torino, quale autorità pubblica che singolarmente o insieme ad altri determina finalità e mezzi del trattamento di dati personali;
e) delegato del Titolare: il Dirigente che esercita le funzioni del Titolare nell'ambito dell'incarico assegnato;
f) autorizzati dal Titolare: il personale dell'Ente che, nell'ambito della struttura organizzativa di assegnazione, tratta i dati personali necessari per lo svolgimento delle funzioni istituzionali;
g) responsabile del trattamento: la persona fisica o giuridica, o l'autorità pubblica che tratta dati personali per conto della Città metropolitana di Torino;
h) autorità di controllo: l'Autorità designata anche ai fini dell'attuazione in Italia del Regolamento generale sulla protezione dei dati personali (UE) 2016/679 e denominata Garante per la protezione dei dati personali (Garante Privacy).

2. Per tutte le ulteriori definizioni ai fini del presente Regolamento si rinvia al Regolamento Europeo del 27 aprile 2016 n. 679.

Articolo 3 - TITOLARE DEL TRATTAMENTO

1. La Città metropolitana di Torino è il Titolare del trattamento dei dati personali, a cui competono le decisioni in ordine alla finalità e ai mezzi del trattamento dei dati personali raccolti o meno in banche dati, automatizzate o cartacee (di seguito indicato con "Titolare").
2. Le funzioni di Titolare del trattamento sono esercitate da ciascun Dirigente nel rispettivo ambito di competenza, in conformità all'assetto organizzativo della Città metropolitana di Torino e alle disposizioni del presente Regolamento.
3. Il Titolare è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'art. 5 del GDPR: liceità, correttezza e trasparenza; limitazione della finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza.
4. Il Titolare garantisce misure tecniche ed organizzative adeguate a dimostrare che il trattamento di dati personali è effettuato in modo conforme al GDPR. 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 articoli 15-22 del Regolamento europeo, nonché le comunicazioni e le informazioni occorrenti per il loro esercizio.
   Gli interventi necessari per l'attuazione delle misure sono considerati nell'ambito degli strumenti di programmazione previa apposita analisi preventiva della situazione in essere, tenuto conto dei costi di attuazione, della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi dallo stesso derivanti, aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche.
5. 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 DPIA – Data Protection Impact Assessment (Valutazione dell'impatto del trattamento sulla protezione dei dati) ai sensi dell'art. 35 del GDPR, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, sentito eventualmente anche il parere del DPO.

6. Il Titolare nomina il Data Protection Officer – DPO (Responsabile della Protezione dei Dati), dandone comunicazione al Garante Privacy, con le modalità stabilite dall'autorità di controllo, e con le funzioni e i compiti previsti nel successivo art. 6.
7. I dati di contatto del Titolare e del Responsabile della protezione dati sono pubblicati sul sito istituzionale dell'Ente, sezione Amministrazione trasparente, oltre che nella sezione "Privacy".
8. Il Titolare provvede inoltre a:
   a) censire e monitorare le attività di trattamento dei dati personali facenti capo alla struttura diretta, avendo cura di annotarle all'interno del Registro delle attività di trattamento;
   b) nominare quale Responsabile del trattamento i soggetti pubblici o privati affidatari, per conto dell'Ente, di attività e servizi che per la loro realizzazione rendono necessario il trattamento di dati personali, o i soggetti terzi che trattano dati sulla base di specifiche convenzioni;
   c) predisporre le informazioni agli utenti di cui all'art. 14 e curarne il costante aggiornamento;
   d) garantire l'esercizio dei diritti degli interessati previsti agli articoli da 15 a 18 e da 20 a 22 del GDPR e dar corso alle relative richieste, agevolando l'esercizio del diritto anche mediante la predisposizione di apposita modulistica disponibile sul sito Internet istituzionale, e dandone comunicazione tempestiva al DPO;
   e) verificare che in seguito a modifica, trasferimento e/o cessazione del rapporto di lavoro, gli autorizzati al trattamento alle dirette dipendenze osservino gli obblighi relativi alla riservatezza e alla comunicazione, aggiornando le relative abilitazioni;
   f) collaborare con il DPO al fine di consentire allo stesso l'esecuzione dei compiti e delle funzioni assegnate, assicurando l'accesso ai settori funzionali dell'Ente in termini di supporto, informazioni e input essenziali;
   g) notificare al Garante la violazione dei dati personali (*data breach*) e provvedere alla comunicazione della violazione agli interessati, dando informativa alla Direzione Generale;
   h) individuare, nell'ambito delle strutture dirette, uno o più Referenti privacy, che andranno a far parte del Gruppo di Lavoro Privacy di cui all'art. 8. La designazione avviene senza particolari formalità, mediante comunicazione scritta del Dirigente, anche elettronica, all'Ufficio DPO, che pubblica l'elenco aggiornato sulla Intranet aziendale.
9. Nel caso di esercizio associato di funzioni e servizi, nonché per i compiti la cui gestione è affidata alla Città metropolitana di Torino da enti ed organismi statali o regionali, allorché due o più titolari determinano congiuntamente, mediante accordo, le finalità ed i mezzi del trattamento, si realizza la contitolarità di cui all'art. 26 del GDPR. 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 del Regolamento europeo, fermo restando eventualmente quanto stabilito dalla normativa specificatamente applicabile. L'accordo può individuare un punto di contatto comune per gli interessati.

Articolo 4 - RESPONSABILE DEL TRATTAMENTO

1. Il Titolare nomina quali Responsabili del trattamento i soggetti pubblici o privati che trattano dati personali per conto della Città metropolitana di Torino, secondo quanto previsto dall'art. 28 del GDPR, a prescindere dalla forma di affidamento/incarico adottata.
2. La designazione quale Responsabile del trattamento può essere inserita all'interno dell'atto di affidamento/incarico o con atto successivo, indicando la materia, la durata, la natura e la finalità del trattamento, il tipo di dati personali, le categorie di interessati oltre agli obblighi che il Responsabile si impegna a rispettare con la sottoscrizione.
3. Il Titolare provvede a dare adeguate istruzioni per i trattamenti fin dalla fase di scelta del contraente, specificando le caratteristiche professionali e organizzative che i Responsabili devono possedere, in relazione alle peculiarità del servizio o del lavoro in affidamento.
4. Il Responsabile del trattamento può avvalersi di soggetti terzi, cosiddetti Sub-Responsabili, solo previa autorizzazione scritta del Titolare.
5. Come previsto dall'art. 30 del GDPR, il Responsabile del trattamento tiene un Registro delle attività di trattamento di dati personali effettuati per conto della Città metropolitana di Torino, secondo le indicazioni dell'art. 11, e lo mette a disposizione su richiesta.

Articolo 5 - AUTORIZZATI AL TRATTAMENTO

1. Il personale dell'Ente, nell'ambito della struttura organizzativa di assegnazione, è autorizzato in via generale al trattamento dei dati personali necessari per lo svolgimento delle funzioni istituzionali. Il trattamento deve avvenire con le seguenti modalità:
   a) accedere solo ai dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti assegnati;
   b) trattare i dati personali di cui si viene a conoscenza per l'espletamento delle proprie funzioni, in modo lecito e corretto, nel rispetto delle norme di legge, dello Statuto e dei Regolamenti che disciplinano le attività del Comune;
   c) verificare costantemente i dati, il loro aggiornamento, la loro completezza e pertinenza;

d) custodire con cura atti e documenti contenenti dati personali ricevuti in consegna per adempiere ai compiti assegnati e restituirli al termine delle operazioni affidate;
e) osservare scrupolosamente le misure di sicurezza predisposte nonché le istruzioni fornite dal Titolare anche con il supporto dell'Ufficio DPO;
f) osservare, anche in seguito a modifica, trasferimento e/o cessazione del rapporto di lavoro, gli obblighi relativi alla riservatezza e alla comunicazione.

Articolo 6 - DATA PROTECTION OFFICER - DPO

1. Il Data Protection Officer (DPO) – Responsabile della Protezione dei Dati (RPD) - è individuato dal Sindaco, fra i Dirigenti dell'Ente, in virtù dei requisiti di esperienza, capacità professionali e affidabilità con i limiti previsti dal GDPR, artt. 37-39.
2. Il Titolare assicura che il DPO sia tempestivamente e adeguatamente coinvolto e informato su tutte le questioni riguardanti la protezione dei dati personali. A tal fine:
   a) il DPO è invitato a partecipare alle riunioni di coordinamento dei Dirigenti che abbiano per oggetto questioni inerenti la protezione dei dati personali;
   b) il parere del DPO sulle decisioni che impattano sulla protezione dei dati è obbligatorio ma non vincolante. Nel caso in cui la decisione assunta dal Titolare sia difforme dalle raccomandazioni dal DPO, è necessario che tale decisione venga specificatamente motivata;
   c) il DPO deve essere consultato tempestivamente dal Titolare qualora si verifichi una violazione dei dati o un altro incidente.
3. Il DPO 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 dei dati.
4. Il DPO non può essere rimosso o penalizzato dal Titolare per l'adempimento dei propri compiti. Ferma restando l'indipendenza nello svolgimento di detti compiti, il DPO riferisce direttamente al Titolare e alla Direzione Generale.
5. 5. La figura di DPO è incompatibile con chi determina le finalità od i mezzi del trattamento; in particolare, risultano con la stessa incompatibili l'incarico di Responsabile della Prevenzione della Corruzione e della Trasparenza e di Responsabile per la transizione al Digitale.
6. 6. Il DPO è incaricato dei seguenti compiti, ai sensi dell'art. 39 del GDPR:
   a) informare e fornire consulenza al Titolare nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal Regolamento europeo e dalle altre normative relative alla protezione dei dati. In tal senso il DPO può indicare al Titolare i settori 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 GDPR e delle altre normative relative alla protezione dei dati, fermo restando le responsabilità del Titolare, con particolare riferimento alle attribuzioni delle responsabilità, alle attività di sensibilizzazione, formazione e controllo poste in essere dal Titolare;
c) supportare il Titolare nella tenuta del Registro delle attività di trattamento di cui all'articolo 12, tenuto sotto la responsabilità dei Dirigenti, che si avvalgono del Gruppo dei Referenti Privacy per l'implementazione e l'aggiornamento delle informazioni contenute, nonché nello svolgimento delle diverse attività connesse alla tutela dei dati personali, incluse le attività di informazione agli interessati, di nomina ai responsabili del trattamento e di esercizio dei diritti da parte degli interessati;
d) fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati (DPIA) e sorvegliarne l'elaborazione, come specificato nell'art. 13.
e) supportare il Titolare qualora si verifichi una violazione dei dati personali o un altro incidente;
f) cooperare con il Garante per la protezione dei dati personali e fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36 del GDPR.

7. Nello svolgimento dei compiti affidatigli il DPO 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 DPO può:
   a) procedere ad una mappatura delle aree di attività valutandone il grado di rischio in termini di protezione dei dati;
   b) definire un ordine di priorità nell'attività da svolgere, incentrandola sulle aree di attività che presentano maggiori rischi in termini di protezione dei dati, da comunicare al Titolare e alla Direzione generale.
8. Il Titolare fornisce al DPO il supporto e le risorse necessarie per assolvere i compiti attribuiti. In particolare è assicurato:
   a) supporto attivo per lo svolgimento dei compiti da parte dei Dirigenti e dell'Organo politico-esecutivo;
   b) supporto adeguato in termini di risorse finanziarie, infrastrutture (sede, attrezzature, strumentazione) e personale;
   c) 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;
   d) tempo sufficiente per l'espletamento dei compiti affidati al DPO;
   e) accesso garantito ai settori funzionali dell'Ente in modo da avere a disposizione supporto, informazioni e input essenziali.
9. Nello svolgimento dei suddetti compiti e funzioni, il DPO si avvale dell'Ufficio DPO, disciplinato dall'art. 7.

Articolo 7 - UFFICIO DPO – DATA PROTECTION OFFICER

1. E' istituito l'Ufficio DPO – Data Protection Officer, come unità specializzata, con competenze specialistiche e trasversali a tutte le strutture dell'Ente. L'ufficio funge da supporto al DPO da cui dipende funzionalmente.
2. All'ufficio sono attribuite le seguenti competenze:
   a) supporta il Titolare e i Dirigenti, anche per il tramite dei Referenti privacy o altro personale;
   b) promuove la diffusione nell'Ente di una "cultura della privacy" favorendo lo scambio di informazioni, materiali, eventi e notizie inerenti il tema della tutela dei dati personali nonché organizzando iniziative informative, formative e di sensibilizzazione in materia di privacy;
   c) cura l'aggiornamento del canale Intranet "Privacy" e della pagina Internet "Privacy" con informazioni e materiali utili al personale dell'Ente e alla cittadinanza;
   d) cura l'aggiornamento e la pubblicazione sulla Intranet aziendale della composizione del Gruppo di Lavoro Privacy di cui all'art. 8.
   e) collabora con il DPO nella definizione dei bisogni formativi in materia di tutela dei dati personali del personale dell'Ente in generale e in particolare del Gruppo di Lavoro Privacy, concordando gli interventi con l'Ufficio Formazione interna e con altre strutture eventualmente coinvolte in base alla materia trattata;
   f) supporta il DPO per le attività di consulenza al Titolare relative ai diversi adempimenti in materia di tutela dei dati personali, con particolare riferimento alla stesura del Registro delle attività di trattamento, alla predisposizione delle informative agli interessati e delle nomine a Responsabile del trattamento, all'esercizio dei diritti degli interessati, anche mediante la predisposizione di appositi modelli e modulistica.

Articolo 8 - REFERENTI PRIVACY E GRUPPO DI LAVORO PRIVACY

1. E' istituito il Gruppo di Lavoro Privacy, costituito dai Dirigenti dell'Ente e da uno o più Referenti privacy per ogni struttura, individuati dai Dirigenti.
2. La designazione in qualità di Referenti avviene obbligatoriamente mediante comunicazione scritta anche elettronica indirizzata al dipendente designato e all'Ufficio DPO, che pubblica l'elenco aggiornato sulla Intranet aziendale.
3. Il Referente privacy può essere assegnato anche a più strutture organizzative, qualora ciò sia compatibile con la complessità e l'omogeneità dei trattamenti presenti.
4. I Referenti privacy hanno i seguenti compiti:
   a) supportare il Dirigente nello svolgimento dei diversi compiti assegnati in materia di tutela dei dati personali;
   b) costituire il primo punto di riferimento delle strutture assegnate per le questioni relative alla tutela dei dati personali;

c) partecipare alle iniziative informative, formative e di sensibilizzazione in materia di protezione dei dati personali organizzate dall'Ufficio DPO al fine di accrescere la "cultura della privacy" nell'Ente.

5. Il Gruppo di Lavoro Privacy si riunisce periodicamente, sotto il coordinamento dell'Ufficio DPO, per esaminare questioni trasversali o per partecipare ad occasioni di confronto e informazione in materia di tutela dei dati personali

Articolo 9 - AMMINISTRATORE DI SISTEMA

1. La Città Metropolitana di Torino si avvale di un cosiddetto Amministratore di sistema, 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.
2. L'Amministratore di sistema viene nominato dal Dirigente responsabile dei Servizi Informativi.
3. L'Amministratore di sistema collabora con il DPO fornendo allo stesso supporto ed assistenza.

Articolo 10 - SICUREZZA DEL TRATTAMENTO

1. La Città metropolitana di Torino, anche attraverso il supporto dell'Amministratore di Sistema, mette in atto misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato 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.
2. Le misure tecniche ed organizzative di sicurezza da mettere in atto per ridurre i rischi del trattamento ricomprendono: la pseudonimizzazione; la minimizzazione; la cifratura dei dati personali; la capacità di assicurare in modo costante 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.
3. Il Titolare, con il supporto del DPO e d'intesa con il Responsabile della Transizione digitale, fa sì che chiunque agisca sotto la sua autorità e tratti dati personali sia istruito in tal senso e verifica regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
4. In particolare, il Titolare fornisce indicazioni e cautele da adottare in merito a:
   a) uso e custodia degli strumenti di lavoro, sia per le attività lavorative svolte in presenza sia per quelle svolte in modalità di lavoro agile;
   b) custodia dei documenti cartacei;
   c) memorizzazione dei dati;

d) trasferimento di documenti elettronici di grandi dimensioni;
e) pubblicazione online;
f) utilizzo della posta elettronica;
g) utilizzo di fotocopiatori e stampanti in ambienti condivisi;
h) pulizia della postazione di lavoro;
i) permessi e abilitazioni.

Articolo 11 - REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

1. Il Titolare è tenuto a compilare ed aggiornare un registro dei trattamenti di dati personali effettuati, contenente le informazioni previste dall'art. 30 del GDPR e in particolare:
   a) il nome ed i dati di contatto dell'Ente, eventualmente del Contitolare del trattamento e del DPO;
   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, inclusi eventuali Responsabili del trattamento incaricati;
   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) ove possibile, il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate, come da precedente art. 10.

   2. Il Registro è tenuto in formato elettronico e viene aggiornato dal Titolare con il supporto del DPO in modo da garantirne l'adesione alla realtà organizzativa e ai trattamenti effettuati.
   3. Anche i Responsabili del trattamento sono tenuti a conservare un Registro delle attività di trattamento di dati personali effettuati per conto della Città metropolitana di Torino, come richiamato dall'art. 4. Il Registro deve contenere le seguenti informazioni:
   a) nome e dati di contatto del Responsabile in riferimento ai trattamenti effettuati per conto di Città metropolitana di Torino;
   b) categorie di trattamento effettuati;
   c) se autorizzato, l'eventuale trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, con relativa identificazione e documentazione delle garanzie adeguate;
   d) descrizione delle misure di sicurezza tecniche ed organizzative adottate.

4, Su richiesta, il Responsabile mette il Registro a disposizione del Titolare, e il Titolare lo mette a disposizione dell'autorità di controllo.

Articolo 12 - VIOLAZIONE DEI DATI (DATA BREACH)

1. Per violazione dei dati personali ("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 dall'Ente direttamente o tramite Responsabili del trattamento.
2. 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 Privacy. La notifica dovrà avvenire entro 72 ore e comunque senza ingiustificato ritardo, e deve avere il contenuto minimo previsto dall'art. 33 del GDPR.
3. Il Responsabile del trattamento è obbligato ad informare il Titolare, senza ingiustificato ritardo, dopo essere venuto a conoscenza della violazione.
4. I principali rischi per i diritti e le libertà degli interessati conseguenti ad una violazione, sono i seguenti:
   a) danni fisici, materiali o immateriali alle persone fisiche;
   b) perdita del controllo dei dati personali;
   c) limitazione dei diritti, discriminazione;
   d) furto o usurpazione d'identità;
   e) perdite finanziarie, danno economico o sociale.
   f) decifratura non autorizzata della pseudonimizzazione;
   g) pregiudizio alla reputazione;
   h) perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari).
5. Se il Titolare ritiene che il rischio per i diritti e le libertà degli interessati conseguente alla violazione rilevata sia elevato, allora deve informare questi ultimi, senza ingiustificato ritardo, con un linguaggio semplice e chiaro. Anche la comunicazione all'interessato deve contenere almeno le informazioni e le misure di cui al citato art. 33.
6. 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, condivisa con il DPO, deve essere conservata con la massima cura e diligenza in quanto può essere richiesta dal Garante Privacy al fine di verificare il rispetto delle disposizioni del GDPR.
7. Il Titolare approva, mediante comunicazione sulla Intranet aziendale e pubblicazione nell'apposito canale Privacy, una procedura di data breach, che descrive in modo dettagliato la procedura da seguire in caso di violazione dei dati personali.

Articolo 13 - VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI (DPIA – DATA PROTECTION IMPACT ASSESSMENT)

1. Nel caso in cui un tipo di trattamento, specie se prevede 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 attuare una valutazione dell'impatto del medesimo trattamento ai sensi dell'art. 35 del GDPR, considerati la natura, l'oggetto, il contesto e le finalità dello stesso trattamento.
2. Ai fini della decisione di effettuare o meno la DPIA il Titolare tiene conto degli elenchi redatti dal Garante privacy relativi alle tipologie di trattamento soggetti o non soggetti a valutazione, ai sensi dell'art. 35, c. 4-6 del GDPR.
3. Il Titolare può consultare il DPO in merito a condurre o meno una DPIA, quale metodologia adottare, se condurre la DPIA con risorse interne ovvero esternalizzandola, quali salvaguardie applicare, comprese misure tecniche e 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 Regolamento europeo.

Articolo 14 - DIRITTI DEGLI INTERESSATI

1. Gli interessati hanno il diritto di ricevere, nel momento in cui i dati personali vengono raccolti, tutte le informazioni previste dagli artt. 13-14 in merito al trattamento dei dati personali effettuato dalla Città metropolitana di Torino (cosiddette "informative"). Tali informazioni devono essere rese in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori. Le informazioni sono fornite per iscritto o con altri mezzi, anche elettronici. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata l'identità dell'interessato.
2. Gli interessati hanno inoltre il diritto di ottenere dal Titolare del trattamento l'accesso ai dati personali trattati e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che li riguarda o di opporsi al loro trattamento, oltre al diritto della portabilità dei dati, come previsto negli articoli 15-22 del GDPR.
3. Al fine di agevolare l'esercizio da parte degli interessati dei diritti previsti dagli artt. 15-22 del Regolamento europeo, la Città metropolitana mette a disposizione sul proprio sito Internet, nella sezione "Privacy", un apposito modulo, non esclusivo.
4. L'istanza deve essere indirizzata al Titolare o al Dirigente della struttura dove sono trattati i dati, che dovranno darne tempestiva comunicazione al DPO.
5. Qualora il trattamento coinvolga altre strutture, il Dirigente ricevente l'istanza ne dà comunicazione agli altri Dirigenti che detengono i dati personali dell'interessato, informandone il DPO.

6. Se il trattamento è effettuato da soggetti terzi Responsabili del trattamento, sull'istanza è competente a rispondere il Dirigente che ha provveduto alla nomina del soggetto.
7. Il riscontro all'istanza deve essere fornito, senza ingiustificato ritardo, e comunque entro 30 giorni dalla data di ricezione della stessa. Tale termine può essere prorogato di ulteriori due mesi, se necessario, tenuto conto della complessità e del numero delle richieste, dandone in ogni caso comunicazione al richiedente con le dovute motivazioni entro trenta giorni dal ricevimento.
8. Il rilascio delle informazioni richieste è gratuito. Nel caso in cui le istanze siano chiaramente infondate, eccessive o di carattere ripetitivo, può essere addebitabile un contributo spese, il cui importo è riconducibile alle spese di rimborso fissate dalla Città metropolitana di Torino per l'esercizio del diritto di accesso agli atti; in alternativa il Dirigente può rifiutare di soddisfare la richiesta, dandone adeguata motivazione.

Articolo 15 - TRASPARENZA E TUTELA DEI DATI PERSONALI

1. La Città metropolitana di Torino presta particolare attenzione nell'effettuare un corretto bilanciamento tra le esigenze in materia di tutela dei dati personali, trasparenza amministrativa ed accesso agli atti amministrativi.
2. Su tutti i documenti oggetto di pubblicazione obbligatoria ai sensi del D.Lgs 33/2013, sugli atti pubblicati all'interno dell'Albo pretorio, nonché sugli eventuali ulteriori documenti pubblicati sul sito internet istituzionale, vengono apposti opportuni "omissis" in corrispondenza dei dati personali eccedenti, oltre alle limitazioni legate ad ulteriori interessi privati soggetti a tutela, quali ad esempio dati di natura commerciale.
3. Analoghe cautele vengono adottate per la documentazione rilasciata a seguito di istanze di accesso agli atti, nonché sui documenti pubblicati all'interno della Intranet aziendale.

Articolo 16 - OBBLIGO DI RISERVATEZZA

1. Il personale operante presso le unità organizzative dell'Ente è tenuto al segreto d'ufficio e professionale; non può trasmettere a chi non ne abbia diritto informazioni riguardanti provvedimenti od operazioni amministrative, in corso o concluse, di cui sia venuto a conoscenza a causa delle sue funzioni, al di fuori delle ipotesi e delle modalità previste dalla normativa vigente e dai Regolamenti dell'Ente

Articolo 17 - RINVIO

1. Per tutto quanto non espressamente disciplinato con le presenti disposizioni, si rimanda a quanto previsto dalla normativa vigente in materia di protezione dei dati personali e alle disposizioni contenute nei provvedimenti della Autorità Garante per la Protezione dei dati personali e del Comitato europeo per la protezione dei dati personali.