Regolamento sulla protezione dei dati personali

in attuazione del regolamento UE 2016/679 "Regolamento generale per la protezione dei dati"

Sommario

Premesse e definizioni

Il Parlamento europeo e il Consiglio hanno approvato, nella seduta del 27 aprile 2016, il Regolamento 2016/679/UE (GDPR- *General Data Protection Regulation*), relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati. Detto regolamento che abroga la direttiva 95/46/CE, si applica, senza necessità di recepimento, in tutti gli Stati membri dell'Unione Europea a far data dal 25 maggio 2018.

Il Regolamento prevede che per «**dato personale**» si intenda "*qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale*".

Definisce, altresì, «**trattamento***»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di 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*".

Per rafforzare la protezione, il Regolamento UE introduce numerose e rilevanti novità partendo da un approccio, fondato sul principio di cautela, basato sul rischio del trattamento e su misure di *accountability* di titolari e responsabili (come la valutazione di impatto, il registro dei trattamenti, le misure di sicurezza, la nomina di un Responsabile della protezione dei dati).

La nuova disciplina europea pone con forza l'accento sulla "responsabilizzazione" (*accountability*) di titolari e responsabili ossia, sull'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del Regolamento. Tra i criteri che i titolari e i responsabili sono tenuti ad utilizzare nell'attuazione degli obblighi vi sono:

- il criterio del *"data protection by default and by design",* ossia la necessità di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili "al fine di soddisfare i requisiti" del regolamento e tutelare i diritti degli interessati - tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati;

- il criterio del rischio inerente al trattamento, da intendersi come rischio di impatti negativi sulle libertà e i diritti degli interessati, impatti che devono essere analizzati attraverso un apposito processo di valutazione tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) che il Titolare ritiene di dover adottare per mitigare tali rischi.

In attuazione dei principi introdotti dal GDPR i dati personali devono essere:

- 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.

Ne consegue che l'intervento delle autorità di controllo, nel nuovo impianto gestionale, è destinato a svolgersi principalmente "*ex post*", ossia a collocarsi successivamente alle determinazioni assunte autonomamente dal Titolare; ciò spiega l'abolizione, a partire dal 25 maggio 2018, di alcuni istituti previsti dalla direttiva del 1995 e dal Codice italiano, come la notifica preventiva dei trattamenti all'autorità di controllo e il cosiddetto *prior checking* (o verifica preliminare), sostituiti da obblighi di tenuta di un registro dei trattamenti e, appunto, di effettuazione di valutazioni di impatto in piena autonomia.

Con l'entrata in vigore del GDPR vengono introdotti i concetti di "dati particolari" (articolo 9) e "dati personali relativi a condanne penali e reati" (articolo 10), queste definizioni sostituiscono, ai sensi dell'articolo 22 del D.Lgs. 101 del 10 agosto 2018 le espressioni "dati sensibili" e "dati giudiziari" utilizzate ai sensi della precedente normativa in materia di privacy.

I "dati particolari" sono i dati idonei a rivelare l'origine razziale od etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, i dati relativi alla salute o alla vita sessuale, i dati genetici, i dati biometrici intesi a identificare in modo univoco una persona fisica e quelli relativi all'orientamento sessuale; "i dati relativi a condanne penali e reati" sono i dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza.

Le disposizioni del D.lgs. 196/2003 "Codice in materia di protezione dei dati personali", come modificato dal D.Lgs. 101 del 10 agosto 2018, nonché i provvedimenti di carattere generale emanati dal Garante per la protezione dei dati personali, si applicano nella misura in cui non siano in contrasto con il citato Regolamento.

Di seguito si riportano le definizioni dei soggetti che intervengono nel trattamento dei dati da parte della Città Metropolitana.

Titolare del trattamento

Il Titolare del trattamento è la Città Metropolitana di Napoli secondo le specifiche attribuzioni degli organi, come definite dalla legge e dallo Statuto, in rispetto del principio di separazione tra politica e gestione. Le funzioni e i compiti che il GDPR e la normativa nazionale attribuiscono al Titolare vengono realizzati tramite i Soggetti Attuatori.

Responsabile della protezione dei dati (RPD/DPO)

Si tratta della figura prevista dagli articoli 37 e ss. del GDPR, a cui sono assegnati compiti di consulenza e sorveglianza in possesso di idonee qualità professionali, con particolare riferimento alla comprovata conoscenza specialistica della normativa e della prassi in materia di protezione dei dati, nonché alla capacità di promuovere una cultura della protezione dati all'interno dell'organizzazione.

Soggetti Attuatori

Soggetti Attuatori sono i Dirigenti in servizio presso la Città Metropolitana di Napoli e gli organi dell'Ente, che trattano dati personali nello svolgimento delle attività di competenza.

Responsabili del trattamento

Sono tutti i soggetti esterni all'Ente che trattano dati personali per conto della Città Metropolitana di Napoli. Come previsto dall'articolo 28 del GDPR, la legittimazione al trattamento dei dati di cui è titolare la Città Metropolitana da parte di detti soggetti deve avvenire a seguito di stipula di apposito contratto, con le previsioni di cui all'articolo 28, nonché gli obblighi di cui agli articoli 30 e 33 del GDPR.

Autorizzati al trattamento

Sono tutti coloro che, all'interno delle singole unità organizzative e per le materie di competenza, effettuano trattamenti di dati personali nell'espletamento di compiti istituzionali. Tali trattamenti avvengono sotto l'autorità dei Soggetti Attuatori, i quali garantiscono adeguate istruzioni.

Articolo 1
Oggetto

1. Il presente Regolamento disciplina le misure organizzative ed i processi interni di attuazione del Regolamento europeo (*General Data Protection Regulation* del 27 aprile 2016 n. 679, di seguito indicato con "GDPR") e del Codice in materia di protezione dei dati personali (decreto legislativo 30 giugno 2003, n. 196, adeguato al GDPR con D.Lgs. n. 101 del 10 agosto 2018) nella Città Metropolitana di Napoli.

Articolo 2
Finalità del trattamento

1. I trattamenti sono compiuti dall'Ente per le finalità di seguito indicate:
a) l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri. Rientrano in questo ambito i trattamenti compiuti per:
- l'esercizio delle funzioni che la legge attribuisce alla Città Metropolitana di Napoli;
- l'esercizio di ulteriori funzioni inerenti competenze statali e/o regionali affidate alla Città Metropolitana di Napoli in base a norme di legge;

b) l'adempimento di un obbligo legale al quale è soggetto l'Ente;
c) l'esecuzione di un contratto con soggetti interessati;
d) specifiche finalità diverse da quelle di cui ai precedenti punti, purché l'interessato esprima il consenso al trattamento.

Articolo 3
Base giuridica

1. La base giuridica per il trattamento di dati personali, effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri prevista dall'articolo 6 paragrafo 3 lettera b) del GDPR, è costituita esclusivamente da una norma di legge o, nei casi previsti dalla legge, di regolamento.

2. Il GDPR non impone che vi sia un atto legislativo specifico per ogni singolo trattamento. Un atto legislativo può essere sufficiente come base per più trattamenti effettuati conformemente a un obbligo legale cui è soggetto il Titolare del trattamento o se il trattamento è necessario per l'esecuzione di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri.

3. La comunicazione fra titolari che effettuano trattamenti di dati personali, diversi da quelli ricompresi nelle particolari categorie di cui all'articolo 9 del GDPR e di quelli relativi a condanne penali e reati di cui all'articolo 10 del GDPR, per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri è ammessa se prevista ai sensi del comma 1. In mancanza di tale norma, la comunicazione è ammessa quando è comunque necessaria per lo svolgimento di compiti di interesse pubblico e lo svolgimento di funzioni istituzionali e può essere iniziata se è decorso il termine di quarantacinque giorni dalla relativa comunicazione al Garante, senza che lo stesso abbia adottato una diversa determinazione delle misure da adottarsi a garanzia degli interessati.

4. La diffusione e la comunicazione di dati personali, trattati per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, a soggetti che intendono trattarli per altre finalità sono ammesse unicamente se previste ai sensi del comma 1.

5. Si intende per:

a) "comunicazione", il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal Responsabile o dal suo rappresentante nel territorio dell'Unione europea, dai Soggetti Attuatori, dagli Autorizzati al trattamento, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione;

b) "diffusione", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Articolo 4
Titolare del trattamento

1. La Città Metropolitana di Napoli è il Titolare del trattamento dei dati personali raccolti o destinati ad essere raccolti in banche dati, sia in modalità analogica che digitale, secondo le specifiche attribuzioni degli organi, come definite dalla legge e dallo Statuto, in rispetto del principio di separazione tra politica e gestione. Le funzioni, i compiti e gli adempimenti che il GDPR, la normativa nazionale, le linee guida e i provvedimenti del Garante attribuiscono al Titolare, vengono svolte dallo stesso per il tramite dei Soggetti Attuatori di cui al successivo articolo 5.

2. Il Titolare adotta le misure tecniche ed organizzative adeguate per garantire, ed essere in grado di 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 GDPR, nonché le comunicazioni e le informazioni occorrenti per il loro esercizio. Gli interventi necessari per l'attuazione delle misure sono considerati nell'ambito della programmazione operativa (DUP), di bilancio e di PEG/PDO/PDP, 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.

3. Il Titolare, per il tramite dei propri organi, provvede a:

a) ripartire funzioni e compiti per gli adempimenti necessari ai fini della conformità dei trattamenti di dati personali effettuati dall'Ente in esecuzione del GDPR;

b) nominare il Responsabile della protezione dei dati;

4. 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 GDPR e per dimostrarne il concreto rispetto da parte del Titolare, dei Soggetti Attuatori, degli Autorizzati e dei Responsabili del trattamento.

Articolo 5
Soggetti Attuatori del trattamento

1. I Dirigenti sono individuati quali Soggetti Attuatori del trattamento dei dati personali contenuti o destinati ad essere contenuti nelle banche dati esistenti nelle articolazioni organizzative di competenza e agiscono in nome e per conto del Titolare nell'esercizio dei compiti e delle funzioni che il GDPR e la normativa nazionale attribuiscono allo stesso, secondo le modalità del presente regolamento. A tal fine devono essere in grado di offrire garanzie sufficienti in termini di conoscenza specialistica, esperienza, capacità ed affidabilità, per mettere in atto le misure tecniche e organizzative rivolte a garantire che i trattamenti siano effettuati in conformità al GDPR.

2. Ciascun Soggetto Attuatore provvede a:

a) verificare la legittimità dei trattamenti di dati personali effettuati dalla struttura di riferimento con riguardo al rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'articolo 5 GDPR: liceità, correttezza e trasparenza; limitazione della finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza;

b) disporre, in conseguenza alla verifica di cui alla lett. a) le modifiche necessarie al trattamento perché lo stesso sia conforme alla normativa vigente ovvero disporre la cessazione di qualsiasi trattamento effettuato in violazione alla stessa;

c) adottare soluzioni di *privacy by design* e *by default*, tenendo traccia del percorso logico e delle motivazioni che hanno condotto ad effettuare determinate scelte;

d) tenere costantemente aggiornato il registro delle attività di trattamento di cui al successivo articolo 13 per la struttura di competenza;

e) designare quali Responsabili del trattamento tutti i soggetti esterni all'amministrazione, pubblici o privati affidatari di attività e servizi che siano tenuti, a seguito di convenzione, contratto o altri atti ad effettuare trattamenti di dati personali per conto del Titolare; la designazione, quale atto negoziale, dovrà avvenire mediante la sottoscrizione di specifici contratti o atti integrativi di contratti in essere con i soggetti divenuti Responsabili del trattamento ai sensi e per gli effetti dell'articolo 28 del GDPR;

f) predisporre l'elenco dei Responsabili del trattamento con riferimento ai soggetti designati per la singola struttura, pubblicandolo in apposita sezione del sito istituzionale ed aggiornandolo periodicamente;

g) fornire all'interessato:

1. le informazioni indicate dall'articolo 13 GDPR, qualora i dati personali siano raccolti dallo stesso interessato;

2. le informazioni indicate dall'articolo 14 GDPR, qualora i dati personali non siano stati ottenuti dallo stesso interessato;

h) individuare i dipendenti assegnati alla struttura di competenza quali soggetti "Autorizzati al trattamento", fornendo agli stessi le direttive e le istruzioni per il corretto trattamento dei dati, sovrintendendo e vigilando sull'attuazione delle istruzioni impartite; il Soggetto Attuatore garantisce che chiunque agisca sotto la sua autorità ed abbia accesso a dati personali sia in possesso di apposita formazione ed istruzione e si sia impegnato alla riservatezza od abbia un adeguato obbligo legale di riservatezza;

i) rispondere in nome e per conto del Titolare dell'operato dell'Autorizzato anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso non gli è in alcun modo imputabile e che ha vigilato in modo adeguato sull'operato dello stesso;

l) informare il Responsabile della Protezione di dati, senza ingiustificato ritardo e comunque entro 24 ore dal momento in cui ne ha conoscenza dei casi di violazione dei dati personali (cd. "*data breach*") e provvedere alla successiva notifica della violazione all'Autorità Garante per il trattamento dei dati personali, nel caso in cui ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati;

m) effettuare la preventiva valutazione dell'impatto del trattamento sulla protezione dei dati personali (di seguito indicata con "DPIA") ai sensi dell'articolo 35, GDPR, considerati la natura, l'oggetto, il contesto e le finalità del medesimo trattamento, tenuto conto di quanto indicato dal successivo articolo 14;

n) collaborare con il Responsabile della protezione dei dati al fine di consentire allo stesso l'esecuzione dei compiti e delle funzioni assegnate.

Articolo 6
Responsabile della protezione dati

1. Il Responsabile della protezione dei dati (in seguito indicato con "RPD" o "DPO") è individuato dal Sindaco metropolitano con proprio decreto. Il Sindaco con proprio atto deliberativo, con parere tecnico reso dall'Area Risorse Umane, stabilisce gli indirizzi per l'individuazione del Responsabile e, in particolare:

a) se affidare l'incarico a personale interno o se ricorrere a soggetti esterni, come definiti nei successivi commi 2 e 3;

b) l'individuazione della struttura competente alla gestione del procedimento per l'individuazione del RDP.

2. Il RPD può essere scelto fra il personale in servizio presso la Città metropolitana, di qualifica non inferiore alla categoria D, purché in possesso di idonee qualità professionali, con particolare riferimento alla comprovata conoscenza specialistica della normativa e della prassi in materia di protezione dei dati, nonché alla capacità di promuovere una cultura della protezione dati all'interno dell'organizzazione. Il Titolare provvede affinché il RPD mantenga la propria conoscenza specialistica mediante adeguata, specifica e periodica formazione.

3. La funzione di RPD può essere esercitata anche in base ad un contratto di servizi stipulato con un soggetto esterno alla Città metropolitana in possesso dei requisiti specifici previsti dal GDPR.

4. Il RPD è incaricato di svolgere, in piena autonomia e indipendenza, i seguenti compiti:

a) informare e fornire consulenza al Titolare del trattamento, ai Soggetti Attuatori del trattamento e agli Autorizzati, in merito agli obblighi derivanti dal GDPR e dalla normativa nazionale relativi alla protezione dei dati. In tal senso il RPD/DPO può indicare ai Soggetti Attuatori e/o agli Autorizzati al trattamento i settori funzionali ai quali riservare un audit interno o esterno in tema di protezione dei dati, le attività di formazione interna per il personale che tratta dati personali e a quali trattamenti dedicare maggiori risorse e tempo in relazione al rischio riscontrato;

b) sorvegliare l'osservanza del GDPR e delle altre normative relative alla protezione dei dati, fermo restando le responsabilità dei Soggetti Attuatori e degli Autorizzati;

c) la detenzione del Registro dei trattamenti sulla base dei dati singolarmente forniti dai Soggetti Attuatori, considerato che essi andranno aggiornati ogni qualvolta cambiano le finalità, le modalità o la tipologia di trattamento dei dati;

d) vigilare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo poste dai Soggetti Attuatori;

d) fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati (DPIA) e sorvegliarne lo svolgimento. Il singolo Soggetto Attuatore, in particolare, si consulta con

il RPD in merito a: se condurre o meno una DPIA; quale metodologia adottare nel condurre una DPIA; 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 GDPR;

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 all'articolo 36 GDPR, ed effettuare, se del caso, consultazioni relativamente a ogni altra questione; a tali fini il nominativo del RPD/DPO è comunicato dal Sindaco al Garante;

f) altri compiti e funzioni, a condizione che il Titolare si assicuri che tali compiti e funzioni non diano adito a un conflitto di interessi.

5. I Soggetti Attuatori del trattamento 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 Soggetti Attuatori/Autorizzati 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 specificamente tale decisione;

- il RPD deve essere consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente (*data breach*).

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

b) definisce un ordine di priorità nell'attività da svolgere evidenziando quelle attività che presentano maggiori rischi in termini di protezione dei dati da comunicare ai Soggetti Attuatori ed agli Autorizzati al trattamento.

7. Il RPD dispone di autonomia e risorse sufficienti a svolgere in modo efficace i compiti attribuiti. In particolare è assicurato al RPD:

- supporto attivo per lo svolgimento dei compiti da parte dei Soggetti Attuatori/Autorizzati anche considerando l'attuazione delle attività necessarie per la protezione dati nell'ambito della programmazione operativa (DUP), di bilancio, di Peg/PDO/PDP;

- tempo sufficiente per l'espletamento dei compiti affidati;

- supporto adeguato in termini di risorse finanziarie, infrastrutture (sede, attrezzature, strumentazione) e personale;

- 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 garantito alle informazioni in possesso delle strutture dell'Ente, così da fornirgli supporto, informazioni e input essenziali.

8. Il RPD opera in posizione di autonomia nello svolgimento dei compiti 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. Il RPD non può essere rimosso o penalizzato dal Titolare per l'adempimento dei propri compiti. L'incarico di RPD è incompatibile con l'incarico di Responsabile per la prevenzione della corruzione e per la trasparenza.

Articolo 7
Responsabili del trattamento

1. Sono Responsabili del trattamento di dati personali i soggetti pubblici o privati esterni all'Ente affidatari di attività e servizi per conto del Titolare, relativamente ai dati personali gestiti in virtù di convenzioni, contratti, incarichi professionali o altri strumenti giuridici, consentiti dalla legge, per attività connesse alle finalità istituzionali.

2. Il Responsabile del trattamento, deve fornire garanzie sufficienti, in particolare in termini di conoscenza specialistica, esperienza, affidabilità e risorse per mettere in atto misure tecniche ed organizzative adeguate che soddisfino i requisiti del GDPR, della normativa nazionale in materia di privacy e del presente regolamento, anche per la sicurezza trattamento.

3. L'esecuzione dei trattamenti da parte del Responsabile del trattamento deve essere disciplinata da un apposito contratto o da altro atto giuridico o da clausole da inserirsi all'interno dei contratti in cui siano disciplinati la durata del trattamento, la natura e le finalità del trattamento, il tipo di dati personali e le categorie di interessati, tenendo conto dei compiti e responsabilità specifici del Responsabile nel contesto del trattamento da eseguire e del rischio in relazione ai diritti e alle libertà dell'interessato.

4. Dopo il completamento del trattamento, il Responsabile deve restituire o cancellare i dati personali detenuti, salvo che la legge non preveda diversamente.

Articolo 8
Contitolari del trattamento

1. Qualora due o più soggetti si trovino contemporaneamente, ciascuno per la propria area di competenza, ad essere e agire come Titolari del trattamento si ha una situazione di contitolarità.

2. In tal caso essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal GDPR, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14 del GDPR. Tale accordo può designare un punto di contatto per gli interessati.

3. L'accordo di cui al comma 1 riflette adeguatamente i rispettivi ruoli e i rapporti dei Contitolari con gli interessati. Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato.

4. I Soggetti Attuatori del trattamento devono valutare le possibili situazioni di contitolarità e, ove ne emergano, devono stipulare i necessari contratti di cui al comma 2.

Articolo 9
Obbligo di informativa e contenuto

1. Prima che inizi qualunque trattamento di dati personali i Soggetti Attuatori del trattamento forniscono all'interessato le informazioni necessarie per consentirgli l'esercizio dei propri diritti. L'informativa 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.

2. Non è necessario fornire l'informativa nel caso in cui la comunicazione risulti 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 Soggetto Attuatore adotta misure comunque appropriate per tutelare i diritti dell'interessato anche con informazioni di carattere generale.

3. 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 del Titolare del trattamento e del Soggetto Attuatore;
- indicazione del Responsabile della protezione dei dati;
- indicazione di ogni finalità istituzionale di trattamento e della norma giuridica di riferimento;
- 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, portabilità, oblio, opposizione e reclamo;
- le conseguenze in caso di rifiuto del trattamento o di omessa comunicazione di dati;
- la possibilità di revocare il consenso al trattamento, nei casi basati sullo stesso, ai sensi del precedente articolo 2 lett. d).

Articolo 10
Consenso

1. Il consenso al trattamento dei dati non è richiesto dalla Città Metropolitana di Napoli, 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 di cui all'articolo 2, comma 1, lett. a), b) e c). In tal caso il Soggetto Attuatore deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso.

2. 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.

Articolo 11
Pubblicazione per obblighi di trasparenza

1. La pubblicazione di dati e documenti detenuti dalle Pubbliche Amministrazioni nei siti istituzionali, in attuazione della normativa vigente in materia di pubblicità e trasparenza, integra una finalità di rilevante interesse pubblico nel rispetto della disciplina in materia di protezione dei dati personali.

2 La Città Metropolitana di Napoli effettua il trattamento di dati personali, contenuti in atti e documenti, che devono essere pubblicati sul sito istituzionale per l'adempimento degli obblighi previsti dalla normativa in vigore.

3. I documenti di cui al comma 2 sono pubblicati tempestivamente sul sito istituzionale dell'amministrazione e vanno mantenuti aggiornati per il tempo e nei modi previsti dalla legge.

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

5. I dati particolari, 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, e i dati relativi a condanne penali e reati, possono essere diffusi solo se indispensabili per le specifiche finalità di trasparenza della pubblicazione.

6. In nessun caso possono essere diffusi per finalità di trasparenza i dati relativi alla vita sessuale e quelli idonei a rivelare lo stato di salute.

7. ll Responsabile della trasparenza, nell'ambito dell'attività di controllo sull'adempimento degli obblighi di pubblicazione previsti dalla normativa vigente, segnala eventuali pubblicazioni avvenute in violazione della normativa in materia di trattamento dei dati personali, al Dirigente che le ha disposte e al RPD.

8. La diffusione dei dati in violazione delle disposizioni di cui ai commi precedenti costituisce violazione dei dati personali di cui al successivo articolo 15 (*data breach*).

Articolo12
Sicurezza del trattamento

1. I Soggetti Attuatori e gli Autorizzati al trattamento nell'ambito delle proprie attribuzioni e competenze, mettono in atto misure tecniche ed organizzative idonee a 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. L'adozione di adeguate misure di sicurezza è lo strumento fondamentale per garantire la tutela dei diritti e delle libertà delle persone fisiche. Il livello di sicurezza è valutato tenuto conto dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati. L'efficace protezione dei dati personali è perseguita sia al momento di determinare i mezzi del trattamento, fase progettuale, sia all'atto del trattamento.

3. 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 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.

4. Costituiscono, esemplificativamente, strumenti attuativi:

- sistemi di autenticazione, sistemi di autorizzazione, sistemi di protezione (antivirus, firewall, antintrusione);

- 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;

- protocollazione in modalità riservata di documenti contenenti dati particolari e giudiziari ai sensi degli articoli 9 e 10 del GDPR.

5. La conformità del trattamento dei dati al GDPR 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.

6. Ciascun Soggetto Attuatore si obbliga ad impartire adeguate istruzioni sul rispetto delle predette misure a chiunque agisca per suo conto ed abbia accesso a dati personali.

7. I nominativi ed i dati di contatto del Titolare, dei Soggetti Attuatori e dei Responsabili del trattamento, nonché del Responsabile della protezione dati sono pubblicati sul sito istituzionale dell'Ente, sezione Amministrazione trasparente, oltre che nella sezione "privacy" eventualmente già presente.

Articolo 13
Registro dei trattamenti

1. Ciascun organo dell'Amministrazione che svolga sotto la propria responsabilità attività di trattamento dei dati personali è tenuto alla compilazione del Registro dei trattamenti; tale Registro reca tutte le seguenti informazioni:

a) il nome ed i dati di contatto del Titolare del trattamento e dei Soggetti attuatori in relazione ai dati trattati ed eventualmente del Contitolare del trattamento e del Responsabile del trattamento, nonché del RPD;

b) tipologia di trattamento e dettaglio dell'attività per cui si trattano i dati;

b) le finalità del trattamento;

c) la base giuridica per il trattamento di dati effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri nel rispetto di quanto previsto, in particolare, dall'articolo 9 del GDPR;

d) la sintetica descrizione delle categorie di dati personali trattati e l'espressa indicazione dell'eventuale natura sensibile o estremamente personale dei dati ai sensi dell'articolo 9 GDPR;

e) le modalità di trattamento dei dati;

f) il termine di conservazione, ove possibile quantificarlo in giorni, mesi o anni, fermo restando il principio generale secondo il quale i dati saranno trattati per tutto il tempo necessario all'erogazione della prestazione o del servizio e, successivamente alla conclusione del procedimento o del servizio erogato, i dati saranno conservati in conformità alle norme sulla conservazione della documentazione amministrativa;

g) le categorie di interessati e se sia stata fatta o meno l'informativa;

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

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

l) l'indicazione delle categorie di soggetti autorizzati al trattamento;

m) l'indicazione dei Responsabili del trattamento;

n) il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate, come da precedente articolo 12;

o) applicativi informatici utilizzati per il trattamento;

p) eventuale effettuazione di DPIA;

q) eventuale *data breach.*

2. Il Registro, compilato a cura di ciascun organo/Soggetto Attuatore dell'Ente per ciascun procedimento di competenza che preveda il trattamento di dati personali è tenuto dal RPD in forma telematica, secondo lo schema allegato al presente Regolamento.

3. Il Registro è aggiornato a cura degli organi/Soggetti Attuatori con riferimento ai procedimenti di competenza, ogni qual volta cambino le finalità, le modalità o la tipologia di trattamento dei dati.

Articolo 14
Valutazioni d'impatto sulla protezione dei dati (DPIA)

1. Nel caso in cui un tipo di trattamento, in particolare se prevede l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, i Soggetti Attuatori prima di effettuare il trattamento, devono attuare una valutazione dell'impatto del medesimo trattamento (DPIA *Data Protection Impact Assessment*) ai sensi dell'articolo 35 GDPR, 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.

2. 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 dall'Autorità Garante per il trattamento dei dati personali ai sensi dell'articolo 35, paragrafi 4-6, GDPR.

3. Ai sensi dell'articolo 35 del GDPR la DPIA è richiesta, in particolare nei casi seguenti:

a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;

b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10 del GDPR;

c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Il Garante per la Protezione dei dati Personali, ai sensi del paragrafo 4 dell'art. 35, ha redatto un elenco delle tipologie di trattamento soggetti al requisito di valutazione di impatto sulla protezione (*doc web* 9058979 dell'11 ottobre 2018) che di seguito si riporta a titolo esemplificativo, ma non esaustivo, tenuto conto che l'elenco potrebbe essere soggetto a integrazione da parte del Garante:

a) trattamenti valutativi o di *scoring* su larga scala, nonché trattamenti che comportano la profilazione degli interessati nonché lo svolgimento di attività predittive effettuate anche on-line o attraverso app, relativi ad "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";

b) trattamenti automatizzati finalizzati ad assumere decisioni che producono "effetti giuridici" oppure che incidono "in modo analogo significativamente" sull'interessato, comprese le decisioni che impediscono di esercitare un diritto o di avvalersi di un bene o di un servizio o di continuare ad esser parte di un contratto in essere;

c) trattamenti che prevedono un utilizzo sistematico di dati per l'osservazione, il monitoraggio o il controllo degli interessati, compresa la raccolta di dati attraverso reti, effettuati anche on-line o attraverso app, nonché il trattamento di identificativi univoci in grado di identificare gli utenti di servizi della società dell'informazione inclusi servizi web, tv interattiva, ecc. rispetto alle abitudini d'uso e ai dati di visione per periodi prolungati. Rientrano in tale previsione anche i trattamenti di metadati ad es. in ambito telecomunicazioni, banche, ecc. effettuati non soltanto per profilazione, ma più in generale per ragioni organizzative, di previsioni di budget, di upgrade tecnologico, miglioramento reti, offerta di servizi antifrode, antispam, sicurezza etc.;

d) trattamenti su larga scala di dati aventi carattere estremamente personale (v. WP 248, rev. 01): si fa riferimento, fra gli altri, ai dati connessi alla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche dei quali occorre tutelare la riservatezza), o che incidono sull'esercizio di un diritto fondamentale (quali i dati sull'ubicazione, la cui raccolta mette in gioco la libertà di circolazione) oppure la cui violazione comporta un grave impatto sulla vita quotidiana dell'interessato (quali i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti;

e) trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti;

f) trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo);

g) trattamenti effettuati attraverso l'uso di tecnologie innovative, anche con particolari misure di carattere organizzativo (es. IoT, sistemi di intelligenza artificiale; utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuale; monitoraggi effettuati da dispositivi wearable; tracciamenti di prossimità come ad es. il wi-fi tracking) ogniqualvolta ricorra anche almeno un altro dei criteri individuati nel WP 248, rev. 01 h) trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche;

h) trattamenti di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedono l'incrocio dei dati di consumo di beni digitali con dati di pagamento;

i) trattamenti di categorie particolari di dati ai sensi dell'articolo 9 del GDPR oppure di dati relativi a condanne penali e a reati di cui all'articolo 10 del GDPR interconnessi con altri dati personali raccolti per finalità diverse;

l) trattamenti sistematici di dati biometrici, trattati per identificare univocamente una persona fisica, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento;

m) trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.

Si precisa che le espressioni trattamenti "sistematici" e "non occasionali" di cui ai punti precedenti sono riconducibili al criterio della "larga scala" così come espressamente illustrato al quinto criterio del *Working Party* (WP) 248 (pag. 11).

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

4. Il Soggetto Attuatore garantisce l'effettuazione della DPIA ed è responsabile della stessa. Il Soggetto Attuatore può affidare la conduzione materiale della DPIA ad un altro soggetto, interno o esterno all'Ente.
Per effettuare la DPIA può utilizzare come strumento elettronico anche il software - gratuito e liberamente scaricabile dal sito www.cnil.fr - consigliato dall'Autorità Garante nella sua pagina web.
Deve consultarsi con il RPD anche per assumere la decisione di effettuare o meno la DPIA; tale consultazione e le conseguenti decisioni assunte dal Soggetto Attuatore devono essere documentate nell'ambito della DPIA. Il RPD monitora lo svolgimento della DPIA. Il responsabile della sicurezza dei sistemi informativi fornisce supporto al Soggetto Attuatore per lo svolgimento della DPIA.

5. 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. Il responsabile della sicurezza dei sistemi informativi, può proporre di condurre una DPIA in relazione a uno specifico trattamento, con riguardo alle esigenze di sicurezza od operative.

6. La DPIA non è necessaria nei casi seguenti:

- se il trattamento non può comportare un rischio elevato per i diritti e le libertà di persone fisiche ai sensi dell'articolo 35, paragrafo 1, GDPR;
- 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 dell'Autorità Garante del trattamento 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.

7. Non è necessario condurre una DPIA per quei trattamenti che siano già stati oggetto di verifica preliminare da parte dell'Autorità Garante del trattamento 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 dell'Autorità Garante del trattamento dei dati personali basate sulla direttiva 95/46/CE rimangono in vigore fino a quando non vengono modificate, sostituite od abrogate.

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

a) 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);

b) 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 necessario;
del periodo limitato di conservazione;
delle informazioni fornite agli interessati;
del diritto di accesso e portabilità dei dati;
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 di dati;
consultazione preventiva dell'Autorità Garante del trattamento dei dati personali;

c) 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;

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

9. Il Soggetto Attuatore 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.

10. Il Soggetto Attuatore deve consultare l'Autorità Garante del trattamento 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 l'Autorità Garante 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.

11. 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.

Articolo 15
Violazione dei dati personali (*data breach*)

1. 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 di Napoli. Una violazione dei dati personali può compromettere la riservatezza, l'integrità o la disponibilità di dati personali.
Alcuni possibili esempi:
- l'accesso o l'acquisizione dei dati da parte di terzi non autorizzati;
- il furto o la perdita di dispositivi informatici contenenti dati personali;
- la deliberata alterazione di dati personali;
- l'impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, virus, malware, ecc.;
- la perdita o la distruzione di dati personali a causa di incidenti, eventi avversi, incendi o altre calamità;
- la divulgazione non autorizzata dei dati personali.

2. Il Soggetto Attuatore è obbligato ad informare il Responsabile della Protezione di dati, senza ingiustificato ritardo e comunque entro 24 ore dal momento in cui ne ha conoscenza, dei casi di violazione dei dati personali (cd. "*data breach*") nel caso in cui ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati.

3. Il Soggetto Attuatore, competente per materia, non appena viene a conoscenza di un'avvenuta violazione dei dati personali, sentito il RPD, notifica la violazione all'Autorità Garante per la protezione dei dati personali, senza giustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che non sia in grado di dimostrare che, conformemente al principio di responsabilizzazione, è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Oltre il termine di 72 ore, tale notifica dovrebbe essere corredata delle ragioni del ritardo e le informazioni potrebbero essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

4. Il Soggetto Attuatore, competente per materia, comunica all'interessato, sentito il RPD, la violazione dei dati personali senza indubbio ritardo, qualora questa violazione sia suscettibile di presentare un rischio elevato per i diritti e le libertà della persona fisica, al fine di consentirgli di prendere le precauzioni necessarie, a meno che non abbia già preso misure tali da ridurne l'impatto. La comunicazione, redatta in modo semplice e chiaro al fine di fare comprendere la natura della violazione dei dati personali verificatesi, dovrebbe descrivere la natura della violazione dei dati personali e formulare raccomandazioni per la persona fisica interessata, intese ad attenuare i potenziali effetti negativi. Tale comunicazione agli interessati dovrebbe essere effettuata non appena ragionevolmente possibile in stretta collaborazione con l'autorità di controllo e nel rispetto degli orientamenti impartiti dalle autorità competenti.

3. I rischi per i diritti e le libertà degli interessati possono essere 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;
- impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (ad esempio utenti deboli, minori, soggetti indagati).

4. I principali rischi per i diritti e le libertà degli interessati conseguenti ad una violazione sono i seguenti:
- danni fisici, materiali o immateriali alle persone fisiche;
- perdita del 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.

5. La notifica dovrà avvenire in conformità al modello predisposto dal Garante e pubblicato sul sito web dello stesso. Essa avrà il contenuto minimo previsto dall'articolo 33 GDPR; anche la comunicazione all'interessato deve contenere almeno le informazioni e le misure di cui al citato articolo 33.

6. La documentazione relativa alle violazioni di dati personali subite, le conseguenze e i provvedimenti adottati o che intende adottare, anche se non comunicate alle autorità di controllo, deve essere conservata con la massima cura e diligenza in quanto può essere richiesta dall'Autorità garante per il trattamento dei dati personali al fine di verificare il rispetto delle disposizioni del GDPR.

7. Il Garante può prescrivere misure correttive nel caso sia rilevata una violazione delle disposizioni del GDPR, anche per quanto riguarda l'adeguatezza delle misure di sicurezza tecniche e organizzative applicate ai dati oggetto di violazione. Sono previste sanzioni pecuniarie che possono arrivare fino a 10 milioni di Euro.

Articolo 16
Rinvio

1. Per tutto quanto non espressamente disciplinato con le presenti disposizioni, si applicano le disposizioni del GDPR e di tutte le sue norme attuative vigenti, quale in particolare il D.Lgs. n. 196/2003 e s.m.i., nonché le Linee guida e i provvedimenti dell'Autorità garante del trattamento dei dati personali.

Registro del Trattamento – Art. 30 GDPR

TITOLARE *	CITTA' METROPOLITANA DI NAPOLI	PIAZZA MATTEOTTI N. 1	P.IVA 01263370635	PEC: cittametropolitana.na@pec.it

RESPONSABILE PROTEZIONE DATI*	NOME	PIAZZA MATTEOTTI N. 1	PEC: cittametropolitana.na@pec.it

	DIREZIONE	
N….	**Trattamento** * (tipologia)	
	Finalità * Es. esercizio delle funzioni del Titolare	
	Base giuridica (fondamento su cui si si basa la liceità del trattamento effettuato; es. prestazione di un consenso, esecuzione di un obbligo contrattuale, adempimento di un obbligo legale)	
	Dettaglio attività Es. gestione del personale, albo di professionisti, incarichi professionali ecc.	
	Categoria di dati trattati* Es. anagrafici, contabili, societari ecc.	
	Dati sensibili: si/no	
	Modalità di trattamento Es. elettronica, cartacea	
	Termine di conservazione* (ove possibile; non superiore al perseguimento delle finalità per cui sono trattati i dati. Es. giorni/mesi/anni)	
	Categorie di interessati* Es. cittadini, dipendenti, minori, beneficiari di provvidenze, utenti ecc.	
	Informativa (si/no)	
	Destinatari * (soggetti a cui i dati sono o saranno comunicati)	
	Trasferimenti dati a paesi terzi extra UE, organizzazioni internazionali *– (si, quali/no)	
	Soggetti autorizzati al trattamento Es. dipendenti della Direzione	
	Responsabili esterni	
	Misure di sicurezza * (ove possibile, sistemi di autenticazione; sistemi di autorizzazione; sistemi di	

	protezione; antivirus; firewall; antintrusione; 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 o tecnico).	
	Applicativi utilizzati per il trattamento (software interni)	
	DPIA – si/no	
	Data Breach – si/no	
N. B. Le informazioni contrassegnate da asterisco sono obbligatorie ai sensi dell'art. 30 GDPR		