ORIGINALE

fascicolo _____/___/_____

CITTA' METROPOLITANA DI PALERMO

DELIBERAZIONE DEL COMMISSARIO STRAORDINARIO
in sostituzione del Consiglio Metropolitano

N. 137 del 23/12/2019

OGGETTO: Adeguamento del Regolamento per l'attuazione Regolamento U.E. 2016/679 al Decreto Legislativo n. 101 del 10.08.2018 .

L'anno duemiladiciannove, il giorno VENTITRE del mese di DICEMBRE nei locali del Palazzo della Città Metropolitana di Palermo, via Maqueda 100, il Dott. Salvatore Currao, Commissario Straordinario della Città Metropolitana di Palermo con le funzioni di Consiglio Metropolitano, giusta Decreto del Presidente della Regione Siciliana n. 574/Gab. del 01/08/2019, con la partecipazione del Segretario Generale Dott. Giuseppe Vella/ha adottato la presente deliberazione.
SA MARIANNA MIRTO

Premesso che:-

-con deliberazione del Commissario Straordinario n. 21 del 1 settembre 2018, questa Amministrazione ha approvato il Regolamento per l'attuazione del Regolamento U.E. 2016/679 ed i relativi allegati;

-al fine di dare esecuzione alle norme contenute nel Regolamento U.E , la Città Metropolitana di Palermo ha sottoscritto con il Centro Studi Enti Locali SpA di San Miniato-Pisa, a seguito di esperimento di gara sul MEPA, il contratto per l'espletamento dei servizi per l'attuazione del citato Regolamento;

Considerato che :

- con la legge 25 ottobre 2017, n. 163, il Governo è stato delegato all'emanazione di uno o piu decreti legislativi di adeguamento del quadro normativo nazionale alle disposizioni del Regolamento UE 679/2016 del Parlamento europeo;

- con il Decreto Legislativo n. 101 del 10.08.2018, attuativo della delega, sono state emanate disposizioni per l'adeguamento della normativa nazionale alle disposizioni del GDPR;

-il Responsabile Privacy del Centro Studi Enti Locali SpA di San Miniato-Pisa,, con e-mail del 2.12.2019 ha trasmesso la nuova stesura del Regolamento sulla Privacy che tiene conto delle novità introdotte dal D.Lgs101 del 10 Agosto 2018 ed ha formato oggetto di confronto con gli Uffici dell'Ente;

Ritenuto pertanto di dovere procedere all'adozione del nuovo Regolamento, da sottoporre all'apperovazione dell'organo competente, contenente gli adempimenti in applicazione del D.lgs.101/2018 secondo lo schema allegato, parte integrante della presente proposta, che andrà a sostituire Regolamento approvato con delibera commissariale n. 21 del 1.09.2018 gia citata..

Visti

il D.Lgs n. 267

/2000 e ss.mm.ii

La legge reg.le 15/2015 e ss.mm.ed ii.,

Il Dlgs 101/2018

la L.r. n.7/2019

Si propone al Commissario Straordinario con le funzioni di Consiglio Metropolitano che

1. di approvare, in sostituzione del Regolamento di cui alla Delibera del Commissario Straordinario . n.21 dell' 1 Settembre2018, il nuovo Regolamento allegato al presente atto per formarne parte integrante e sostanziale, Regolamento aggiornato alle novità introdotte dal D.Lgs101 del 10 Agosto 2018 .
2. Dare atto che dall'adozione del presente atto non scaturisce alcun onere di spesa.
3. di disporre che il suddetto Regolamento venga pubblicato all'Albo Pretorio on-line dell'Ente e sul sito istituzionale all'indirizzo www.cittametropolitana.pa.it e che entrerà in vigore il 15esimo giorno successivo alla pubblicazione dell'Albo Pretorio

Progr. 3137/19

Palermo, lì 05/12/2019

Il Responsabile del Procedimento

Si allegano:

1. schema di regolamento adeguato al Dlgs 101/2018

PARERE DI REGOLARITÀ TECNICA

Ai sensi dell'art. 147-bis del D. Lgs. 267/2000 e ss.mm.ii e del vigente Regolamento dei Controlli Interni e di Contabilità, si esprime il seguente parere di regolarità tecnica sul presente provvedimento in ordine alla legittimità, regolarità e correttezza dell'azione amministrativa e della sua conformità alla vigente normativa comunitaria, nazionale, regionale, statutaria e regolamentare:

[X] **FAVOREVOLE**
[ ] **NON FAVOREVOLE**

Per i motivi di seguito riportati:
.....
.....
.....

Si attesta, ai sensi dell'art. 183, comma 8, il preventivo accertamento della compatibilità del programma dei pagamenti conseguente al presente atto con le regole di finanza pubblica e la programmazione dei flussi di cassa.

Addì ..05/12/2019

IL DIRIGENTE
dott.ssa Marianna Mirto

PARERE DI REGOLARITÀ CONTABILE

Sul presente atto si esprime, ai sensi degli artt. 49, comma 1 e 147 bis comma 1, D. Lgs. 267/2000 e ss.mm.ii e del vigente Regolamento dei Controlli Interni e di Contabilità, il seguente parere di regolarità contabile:

[ ] FAVOREVOLE
[ ] NON FAVOREVOLE
[X] NON DOVUTO in quanto non comporta riflessi diretti o indiretti sulla situazione economico-finanziaria o sul patrimonio dell'ente.

Per i motivi di seguito riportati:
.....
.....
.....

Addì .6-12-19

IL RESPONSABILE DEI SERVIZI FINANZIARI

Il Ragioniere Generale
Dott. Massimo Bonomo

IL COMMISSARIO STRAORDINARIO

Vista la superiore proposta di deliberazione;

Visti altresì

Il Regolamento U.E. 679/2016(GDPR)

Il D.Lgs 10 agosto 2018, n. 101

Vista la L.R. n. 15 del 04/08/2015 e succ. mod. e integrazioni;

Vista la legge regionale n. 7 del/2019

DELIBERA

Approvare la proposta di deliberazione nelle risultanze di cui sopra.

Fatto e sottoscritto.

IL COMMISSARIO STRAORDINARIO
Dott. Salvatore Cutrao

IL SEGRETARIO GENERALE
dott.ssa Marianna Mirto

INIZIO PUBBLICAZIONE

Si attesta che la presente deliberazione è stata posta in pubblicazione all'Albo On Line della Città Metropolitana a far data dal _____ .

Palermo, lì _____

IL SEGRETARIO GENERALE o suo DELEGATO

_____

DICHIARAZIONE DI ESECUTIVITA'

La presente deliberazione è divenuta esecutiva il _____ .

( ) Atto dichiarato immediatamente esecutivo in sede di approvazione dall'Organo deliberante.

( ) Atto divenuto esecutivo in seguito al decorso di giorni dieci dalla data di inizio della pubblicazione all'Albo on line di questo Ente, come sopra certificato.

Palermo, lì _____

IL SEGRETARIO GENERALE o suo DELEGATO

_____

_____

CERTIFICATO DI PUBBLICAZIONE

Si certifica che la presente deliberazione è stata pubblicata all'Albo On Line della Città Metropolitana, ai sensi dell'art. 32 della L. 18 giugno 2009 n. 69 dal _____ al _____, e che, contro la stessa, non sono state prodotte opposizioni o rilievi.

Palermo, lì _____

IL SEGRETARIO GENERALE o suo DELEGATO

_____

Città Metropolitana di Palermo

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

SOMMARIO

Premesssa

Il Regolamento europeo ed il Dlgs. 101/2018 individuano diversi attori che intervengono nei trattamenti di dati personali effettuati dalle organizzazioni, ciascuno con funzioni e compiti differenti:

- il "Titolare del trattamento": la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali;
- il "Responsabile del trattamento": la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento;
- i "Soggetti designati": coloro che, sotto la responsabilità del Titolare del trattamento e nell'ambito del proprio assetto organizzativo, svolgano specifici compiti e funzioni connessi al trattamento di dati personali;
- il "Responsabile della protezione dei dati" (di seguito anche *Data Protection Officer* o DPO): figura prevista dagli artt. 37 e ss. del regolamento, che ne disciplinano compiti, funzioni e responsabilità;
- i "Soggetti autorizzati": persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile.

Art. 1
Oggetto

Con il presente Regolamento si intendono stabilire le misure procedimentali e regole di dettaglio ai fini della migliore funzionalità ed efficacia dell'attuazione del Regolamento europeo (General Data Protection Regulation del 27 aprile 2016 n. 679, di seguito indicato con "RGPD", Regolamento Generale Protezione Dati), relativo alla protezione delle persone fisiche con riguardo ai trattamenti dei dati personali, nonché alla libera circolazione di tali dati, nell'ambito dell'attività della Città Metropolitana di Palermo .

Art. 2

Titolare del trattamento

1. La Città Metropolitana di Palermo, rappresentata ai fini previsti dal RGPD dal Sindaco pro tempore, è il Titolare del trattamento dei dati personali raccolti o meno in banche dati, automatizzate o cartacee (di seguito indicato come "Titolare").

   Il Titolare del trattamento assicura il rispetto dei principi di cui al comma 2 e delle disposizioni del presente Regolamento anche mediante delega delle relative funzioni ai Dirigenti, secondo le rispettive competenze e responsabilità.
2. Il Titolare è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'art. 5 RGPD: liceità, correttezza e trasparenza; limitazione della finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza.
3. Il Titolare mette in atto misure tecniche ed organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento di dati personali è effettuato in modo conforme al RGPD. 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 RGPD, 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, 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.
4. Il Titolare adotta misure appropriate per fornire all'interessato:
   a) le informazioni indicate dall'art. 13 RGPD, qualora i dati personali siano raccolti presso lo stesso interessato;
   b) le informazioni indicate dall'art. 14 RGPD, qualora i dati personali non siano stati ottenuti presso lo stesso interessato.
5. Nel caso in cui un tipo di trattamento, specie se prevede l'uso di nuove tecnologie, presenti 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 con "DPIA") ai sensi dell'art. 35, RGDP, considerati la natura, l'oggetto, il contesto e le finalità del medesimo trattamento e tenuto conto di quanto indicato dal successivo art. 17.

6. 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 dei Responsabili del trattamento.
7. Qualora la normativa nazionale e regionale, preveda che in talune ipotesi la Città Metropolitana possa determinare unitamente e congiuntamente ad altri soggetti le finalità e i mezzi del trattamento dei dati, questi si configurano, ai sensi dell'art. 26 Reg. Ue, quali contitolari, con rispettive responsabilità da ripartire e definire in modo trasparente mediante un accordo interno.

Art.3
Finalità del trattamento

1. I trattamenti sono compiuti dalla Città Metropolitana di Palermo per le seguenti finalità:

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 amministrative che riguardano la popolazione ed il territorio, precipuamente nei settori organici dei servizi alla persona ed alla comunità, dell'assetto ed utilizzazione del territorio e dello sviluppo economico;
- l'esercizio di ulteriori funzioni amministrative per servizi di competenza statale affidate alla Città Metropolitana in base alla vigente legislazione.

La finalità del trattamento è stabilita dalla fonte normativa che lo disciplina;

b) l'adempimento di un obbligo legale al quale è soggetto la Città Metropolitana. La finalità del trattamento viene stabilita dalla fonte normativa che lo disciplina;

c) l'esecuzione di un contratto con soggetti interessati;

d) per specifiche finalità diverse da quelle di cui ai precedenti punti, purché l'interessato esprima il consenso al trattamento.

Art.4
Attribuzione di compiti a soggetti designati

1. Con proprio provvedimento, il Titolare del trattamento, nella persona del Sindaco pro-tempore, nomina delle figure di presidio interno (ai sensi dell'art. 2 *quaterdecies* del Dlgs. 101/2018), di seguito chiamate anche "Soggetti designati attuatori", da individuarsi in linea di principio nei Direttori dei

singoli servizi che, sotto la sua autorità e responsabilità, svolgano specifici compiti e funzioni connessi al trattamento di dati personali in ottemperanza dei principi dettati in materia di trattamento dei dati personali dall'Art. 5 del Regolamento con funzioni di direzione, coordinamento e vigilanza sugli incaricati sottoposti che, materialmente, procedono ai trattamenti.

In particolare ai Soggetti designati (ovvero "Soggetti designati attuatori") verranno affidati i seguenti compiti previsti dal Regolamento aventi ad oggetto:

a) la comunicazione delle informazioni nei termini indicati dall'Art. 13 del Regolamento qualora i dati personali siano raccolti presso l'interessato;

b) la comunicazione delle informazioni nei termini indicati dall'Art. 14 del Regolamento qualora i dati personali non siano stati ottenuti presso l'interessato;

c) l'esercizio del diritto di accesso dell'interessato ai sensi dell'Art. 15 del Regolamento;

d) l'esercizio del diritto di rettifica da parte dell'interessato ai sensi dell'Art. 16 del Regolamento;

e) l'esercizio del diritto alla cancellazione da parte dell'interessato ai sensi dell'Art. 17 del Regolamento;

f) l'esercizio del diritto di limitazione del trattamento da parte dell'interessato ai sensi dell'Art. 18 del Regolamento;

g) la notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento ai sensi dell'Art. 19 del Regolamento;

h) l'esercizio del diritto alla portabilità dei dati ai sensi dell'Art. 20 del Regolamento;

i) l'esercizio del diritto di opposizione ai sensi dell'Art. 21 del Regolamento;

j) l'esercizio del diritto di cui all'Art. 22 del Regolamento;

k) l'adozione, e ove necessario riesame e aggiornamento, delle misure tecniche e organizzative adeguate a garantire ed essere in grado di dimostrare che il trattamento è effettuato conformemente al Regolamento. Tali misure devono comunque essere adeguate a garantire un livello di sicurezza adeguato al rischio secondo quanto statuito dall'Art. 32 del Regolamento. Fatte salve eventuali misure particolari correlate alle specificità delle finalità del trattamento, le predette misure possono consistere in interventi conformi a linee guida e policy da applicare secondo standard comuni a tutti gli uffici dell'Amministrazione.

l) l'adozione delle misure tecniche e organizzative adeguate ad attuare in modo efficace e fin dalla progettazione i principi di protezione dei dati personali e integrare nel trattamento le garanzie per soddisfare i requisiti del Regolamento e tutelare i diritti degli interessati (*privacy by design*);

m) l'adozione delle misure tecniche e organizzative adeguate a garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari in relazione a ciascuna specifica finalità del trattamento (privacy by default);

n) lo svolgimento degli adempimenti correlati, per quanto di competenza, all'attuazione degli articoli 26 e 28 del Regolamento, concernenti, rispettivamente, gli obblighi correlati alla situazione di contitolarità del trattamento e disciplina del responsabile del trattamento;

o) la formale individuazione, nelle rispettive strutture, degli incaricati del trattamento;

p) la tenuta del registro delle attività di trattamento in modo da assicurarne, per gli aspetti di competenza, la corretta compilazione e il costante aggiornamento e revisione;

q) la rilevazione e la segnalazione al responsabile delle protezione dei dati (DPO), secondo quanto indicato nell'Art. 35 del Regolamento e nelle Linee guida adottate sul tema dal Gruppo di lavoro europeo (WP29), dei casi nei quali effettuare la valutazione d'impatto sulla protezione dei dati personali e lo svolgimento della valutazione di impatto secondo le direttive e previa consultazione del DPO, provvedendo, ove necessario anche alla consultazione preventiva ai sensi dell'Art. 36 del Regolamento.

r) la collaborazione, per quanto di competenza, con il responsabile della protezione dei dati della Città Metropolitana di Palermo, nell'esecuzione dei compiti ad esso attribuiti;

s) la cooperazione, per quanto di competenza, con l'autorità di controllo, nell'esecuzione dei compiti ad essa attribuiti.

2. Il precedente comma 1 si applica anche in caso di accordo contitolarità di cui al precedente Art.2, ultimo comma.

Art. 5
Autorizzati al trattamento dei dati

1. Sono soggetti autorizzati al trattamento i dipendenti e collaboratori che agiscono sotto la diretta autorità del Titolare del trattamento (e supervisione da parte dei "Soggetti designati attuatori"), i quali ai sensi dell'Art. 29 del Regolamento hanno accesso ai dati personali e al loro trattamento previa formale designazione e dopo essere stati debitamente istruiti e formati.

2. Il precedente comma 1 si applica anche in caso di accordo contitolarità di cui al precedente Art. 3, ultimo comma.

Art.6

Responsabile della protezione dati

Il responsabile della protezione dei dati della Città Metropolitana di Palermo, con le competenze e le prerogative previste dagli articoli 37, 38 e 39 del Regolamento, è un professionista scelto tramite procedura ad evidenza pubblica.
Il DPO è incaricato dei seguenti compiti:

a) informare e fornire consulenza al Titolare ed al Responsabile del trattamento 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 DPO può indicare al Titolare e/o al Responsabile del 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 RGPD e delle altre normative relative alla protezione dei dati, fermo restando le responsabilità del Titolare e del Responsabile del trattamento. Fanno parte di questi compiti la raccolta di informazioni per individuare i trattamenti svolti, l'analisi e la verifica dei trattamenti in termini di loro conformità, l'attività di informazione, consulenza e indirizzo nei confronti del Titolare e del Responsabile del trattamento;

c) sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo poste in essere dal Titolare e dal Responsabile del trattamento;

d) fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati (DPIA) e sorvegliarne lo svolgimento.

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'Art. 36 RGPD, ed effettuare, se del caso, consultazioni relativamente a ogni altra questione. A tali fini il nominativo del DPO è comunicato dal Titolare e/o dal Responsabile del trattamento al Garante;

2. Il Titolare ed il Responsabile del trattamento assicurano che il DPO sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.

Il Titolare del trattamento e il responsabile del trattamento sostengono il responsabile della protezione dei dati nell'esecuzione dei compiti di cui all'Art. 39 del Regolamento fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti

Art. 7

Consenso dell'Interessato

1. Il consenso al trattamento dei dati personali non verrà richiesto agli interessati allorquando il trattamento dei dati venga effettuato dalla Città metropolitana di Palermo nello svolgimento dei propri compiti istituzionali di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito dal diritto dell'Unione o dello Stato.
2. Nelle fattispecie diverse da quelle di cui al precedente comma 1, qualora il trattamento sia basato sul consenso, il Titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali.
3. Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro.
4. Prima della pubblicazione di dati personali deve essere valutato se le finalità della trasparenza e di comunicazione possono essere perseguite senza divulgare dati personali.
5. Deve essere valutato anche la possibilità di rendere pubblici atti e documenti senza indicare i dati che portino all'identificazione degli interessati.
6. Per le attività di comunicazione istituzionale che contemplino l'utilizzo di dati personali, andrà posta particolare attenzione alla necessità di fornire un'adeguata informativa relativa al trattamento e soprattutto andrà valutato se risulti necessaria l'acquisizione, anche successivo, del consenso al trattamento.
7. L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di esprimere il proprio consenso, l'interessato è informato di ciò. Il consenso è revocato con la stessa modalità con la quale è stato accordato.
8. Nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto.

Art. 8

Trattamento dei dati particolari

1. Non è consentito trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

2. Il divieto di cui al precedente comma non si applica se si verifica uno dei seguenti casi:

a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al comma 1;

b) quando il trattamento è necessario per motivi di rilevante interesse pubblico ai sensi dell'art. 9, par.1, Reg. e secondo quanto dispone l'art. 2-*sexies* Dlgs. 101/2018.

Art. 9

Trattamento dei Dati Giudiziari

1. Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'Art. 6 paragrafo 1, del RGPD deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato da norma di legge o nei casi previsti dalla legge di regolamento che prevedano garanzie appropriate per i diritti e le libertà degli interessati.

Art. 10

Trattamento di Dati Personali nei Servizi Esternalizzati

1. Nella ipotesi che a soggetti pubblici o privati esterni siano affidati tramite delega o concessione o contratto lo svolgimento di compiti e/o servizi di competenza della Città metropolitana di Palermo da cui debba conseguire il trattamento di dati personali, il provvedimento o contratto di affidamento deve prevedere norme specifiche attraverso le quali si provvede:
   - a nominare il soggetto pubblico o privato ovvero la persona fisica affidataria quale responsabile del trattamento dei dati personali per la durata dell'affidamento;
   - ad obbligare il responsabile del trattamento ad osservare le prescrizioni di cui al RGPD e alle altre fonti di diritto dell'Unione e dello Stato in materia di protezione dei dati personali;

- a consentire le verifiche sul rispetto delle predette disposizioni normative.

2. Nelle ipotesi di trattamento dei dati personali di cui al precedente comma, il Soggetto designato attuatore della struttura organizzativa della Città metropolitana competente per materia in relazione al compito e/o al servizio affidato ha il dovere di verificare che il soggetto esterno osservi le predette prescrizioni.

3. La periodicità delle predette verifiche, previste nel provvedimento o contratto di affidamento, é determinata in funzione della natura dei dati, della probabile gravità dei rischi, dei mezzi da utilizzare per il trattamento e della durata dell'affidamento.

Art. 11
Comunicazione Interna di Documenti contenenti Dati Personali

1. La comunicazione di documenti amministrativi, secondo la definizione di cui all'art. 1, comma 1, lettera a). del DPR n. 445/2000, contenenti dati personali ai componenti degli organi di governo ovvero all'interno della struttura organizzativa di questo Ente, per ragioni d'ufficio e nell'ambito delle specifiche competenze dei servizi, non è soggetta a limitazioni particolari, salvo quelle espressamente previste da leggi e regolamenti.

2. Il Soggetto designato attuatore del trattamento può tuttavia disporre, con adeguata motivazione, le misure necessarie per la protezione dei dati personali, qualora la comunicazione concerna particolari categorie di dati sensibili e/o giudiziari.

Art.12
Utilizzo di Dati da parte dei Componenti gli Organi di Governo e di Controllo Interno

1. Il Sindaco metropolitano, i Sindaci della Conferenza metropolitana, i Consiglieri metropolitani nonché i componenti degli organi di controllo interno hanno diritto di accedere a documenti amministrativi detenuti dalla Città metropolitana di Palermo nei limiti e con le modalità previsti dalle disposizioni di legge e di regolamenti.

2. Le notizie e le informazioni così acquisite devono essere utilizzate esclusivamente per le finalità pertinenti alle rispettive competenze, rispettando il divieto di divulgazione dei predetti documenti nonché l'obbligo della segretezza del loro contenuto.

Art. 13

Diritto alla cancellazione – Limitazione

1. Il "*diritto all'oblio*" attribuisce all'interessato una più ampia tutela e libertà tesa ad ottenere la cancellazione dei propri dati personali. L'interessato ha il diritto ad ottenere la cancellazione dei dati che lo riguardano, senza ingiustificato ritardo, se sussistono uno dei motivi elencati nell'art. 17 del GDPR.

2. Il Titolare e/o il Responsabile del trattamento dell'Ente se ha reso pubblici i dati personali ed è obbligato ai sensi del citato articolo 17 a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione adotta le misure ragionevoli tecniche per inibire la pubblicazione dei dati provvedendo, altresì, ad informare anche i Titolari del trattamento esterni (ai quali i dati personali da trattare sono stati trasmessi) della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali.

3. Il diritto all'oblio potrà essere limitato solo in alcuni casi specifici e, in particolare, per garantire l'esercizio di libertà di espressione e di informazione; il diritto alla difesa in sede giudiziaria; per tutelare un interesse generale (salute pubblica); quando i dati resi anonimi sono necessari per la ricerca storica o per finalità statistiche o scientifiche; per l'adempimento di un obbligo legale o per la esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il Titolare del trattamento.

Art. 14

Diritto di rettifica e integrazione

1. L'interessato ha il diritto di ottenere la rettifica dei suoi dati personali inesatti nonché, tenuto conto delle finalità del trattamento, l'integrazione dei suoi dati personali incompleti, anche fornendo una dichiarazione integrativa. L'istanza di rettifica o integrazione é formulata dall'interessato per iscritto e inviata anche tramite posta elettronica.

2. Alla rettifica ovvero all'integrazione dei dati richiesta dall'interessato provvede, senza ritardo e comunque entro cinque giorni lavorativi dalla data di arrivo della predetta istanza, il Responsabile del procedimento amministrativo cui ineriscono i dati da rettificare o integrare.

3. Dell'eseguita rettifica o integrazione ovvero della motivata inammissibilità é data tempestiva comunicazione all'interessato con raccomandata con avviso di ricevimento o con notifica a mani o tramite p.e.c..

4. Il Responsabile del procedimento relativo al trattamento dei dati oggetto della richiesta deve comunicare, con tempestività, a ciascuno dei destinatari cui sono stati trasmessi i dati personali la rettifica del trattamento effettuata, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato; e, inoltre, dà comunicazione all'interessato di tali destinatari qualora l'interessato lo richieda.

Art. 15

Sicurezza del trattamento

1. La Città Metropolitana di Palermo e ciascun Soggetto designato attuatore mettono 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, di norma: 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.

3. Costituiscono, altresì, misure tecniche ed organizzative che possono essere adottate dalla struttura cui è preposto ciascun Soggetto designato attuatore in raccordo con la Direzione Gestione Sistemi Informatici e con il Responsabile del Servizio Prevenzione e Protezione per la Sicurezza dell'Ente:

- sistemi di autenticazione; sistemi di autorizzazione; sistemi di protezione (antivirus; firewall; antintrusione; 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 o tecnico.

4. 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.

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.

5. Il Città Metropolitana di Palermo e ciascun designato si obbliga ad impartire adeguate istruzioni sul rispetto delle predette misure a chiunque agisca per loro conto ed abbia accesso a dati personali.

6. I nominativi ed i dati di contatto del Titolare, del o dei Responsabili del trattamento e del Responsabile della protezione dati sono pubblicati sul sito istituzionale della Città Metropolitana, sezione Amministrazione trasparente, sottosezione "*altri contenuti - dati ulteriori*" oltre che nella sezione "privacy" eventualmente già presente.

Art. 16
Registro delle attività di trattamento

1. 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, del Sindaco ai sensi del precedente art. 2, eventualmente del Contitolare del trattamento, 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;

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, come da precedente art.6.

2. Il Registro è tenuto dal Titolare, ovvero da uno dei soggetti eventualmente designati ai sensi del precedente Art. 4 presso gli uffici della struttura organizzativa della Città Metropolitana in forma telematica/cartacea, secondo lo schema allegato A al presente Regolamento.

3. Il Titolare del trattamento può decidere di affidare al DPO il compito di tenere il Registro, sotto la responsabilità del medesimo Titolare.

Art. 17
Registro delle categorie di attività trattate

1. Il Registro delle categorie di attività trattate da ciascun soggetto designato di cui al precedente art. 4, reca le seguenti informazioni:

a) il nome ed i dati di contatto del Responsabile del trattamento e del DPO;

b) le categorie di trattamenti effettuati da ciascun Responsabile: raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, uso, comunicazione, raffronto, interconnessione, limitazione, cancellazione, distruzione, profilazione, pseudonimizzazione, 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, come da precedente art.6.

2. Il registro è tenuto dal Responsabile del trattamento presso gli uffici della propria struttura organizzativa in forma telematica/cartacea, secondo lo schema allegato B al presente regolamento.

Art. 18
Valutazioni d'impatto sulla protezione dei dati

1. 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 attuare una valutazione dell'impatto del medesimo trattamento (DPIA) ai 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.

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 dal Garante Privacy ai sensi dell'at. 35, pp. 4-6, RGDP.

3. 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:

a) 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;

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

c) 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;

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

e) trattamenti di dati su larga scala, tenendo conto: del numero di numero di soggetti interessati dal 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;

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

g) 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, soggetti con patologie psichiatriche, richiedenti asilo, pazienti, anziani e minori;

h) utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative;

i) tutti quei trattamenti che, di per sé, 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 per un trattamento che soddisfa solo uno dei criteri di cui sopra occorra comunque la conduzione di una DPIA.

4. Il Titolare garantisce l'effettuazione della DPIA ed è responsabile della stessa. Il Titolare può affidare la conduzione materiale della DPIA ad un altro soggetto, interno o esterno alla Città Metropolitana.
   Il Titolare deve consultarsi con il DPO 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 DPO monitora lo svolgimento della DPIA. Il Responsabile del trattamento deve assistere il Titolare nella conduzione della DPIA fornendo ogni informazione necessaria.
   Il responsabile della sicurezza dei sistemi informativi, se nominato, e/o l'ufficio competente per detti sistemi, forniscono supporto al Titolare per lo svolgimento della DPIA.
5. Il DPO 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, se nominato, e/o l'ufficio competente per detti sistemi, possono proporre di condurre una DPIA in relazione a uno specifico trattamento, con riguardo alle esigenze di sicurezza od operative.
6. Con riguardo ai trattamenti svolti per l'esecuzione di un compito di interesse pubblico che possono presentare rischi elevati ai sensi dell'art. 35 del Regolamento, il Garante può, sulla base di quanto disposto dall'art. 36, paragrafo 5, del medesimo Regolamento e con provvedimenti di carattere generale adottati d'ufficio, prescrivere misure e accorgimenti a garanzia dell'interessato, che il Titolare del trattamento è tenuto ad adottare
7. 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'art. 35, p. 1, RGDP;
   - 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 Privacy 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 della Privacy o da un RDP e che proseguano con le stesse modalità

oggetto di tale verifica. Inoltre, occorre tener conto che le autorizzazioni del Garante Privacy basate sulla direttiva 95/46/CE rimangono in vigore fino a quando non vengono modificate, sostituite od abrogate.

7. 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 del Garante privacy;

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 RGPD, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

8. 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.

9. Il Titolare deve consultare il Garante Privacy prima di procedere al trattamento se le risultanze della DPIA condotta indicano l'esistenza di un rischio residuale elevato. Il Titolare consulta il Garante Privacy 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.

10. 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. 19
Violazione dei dati personali

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.

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. Il soggetto designato attuatore è obbligato ad informare il Titolare, senza ingiustificato ritardo, dopo essere venuto a conoscenza della violazione.

3. I principali rischi per i diritti e le libertà degli interessati conseguenti ad una violazione, in conformità al considerando 75 del RGPD, 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 (sanitari, giudiziari).

4. 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 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 utenti deboli, minori, soggetti indagati).

5. 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.

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 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 RGPD.

Art.20

Rinvio

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

ALLEGATI

A) Bozza Registro delle attività e delle categorie di trattamento

B) Procedura *data breach*

C) Bozza organigramma privacy

Data Breach Policy

Procedura di notifica di violazione dei dati personali

INDICE

• PREMESSA

Città Metropolitana di Palermo di seguito Città Metropolitana di Palermo ai sensi del Regolamento Europeo 2016/679 (da qui in avanti GDPR), è tenuta a mantenere sicuri i dati personali trattati nell'ambito delle proprie attività istituzionali e ad agire senza ingiustificato ritardo in caso di violazione dei dati stessi (incluse eventuali notifiche all'Autorità Garante competente ed eventuali comunicazioni agli interessati).
È di fondamentale importanza predisporre azioni da attuare nell'eventualità in cui si presentino violazioni concrete, potenziali o sospette di dati personali, ciò al fine di evitare rischi per i diritti e le libertà degli interessati, nonché danni economici all'Ente e per poter comunicare nei tempi e nei modi previsti dalla normativa europea all'Autorità Garante e/o agli interessati.

• SCOPO

Lo scopo di questa procedura è di disegnare un flusso per la gestione delle violazioni di dati personali trattati da Città Metropolitana di Palermo in qualità di Titolare del trattamento (di seguito "Titolare del trattamento").

• COS'E UNA VIOLAZIONE DEI DATI PERSONALI *(DATA BREACH)*

Una violazione di dati personali è ogni infrazione alla sicurezza degli stessi che comporti - accidentalmente o in modo illecito - la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati dal Titolare del trattamento.

Le violazioni di dati personali possono accadere per un ampio numero di ragioni che possono includere:

- Divulgazione di dati personali a soggetti non autorizzati;
- Perdita o furto di dati o di strumenti nei quali i dati sono memorizzati;
- Perdita o furto di documenti cartacei;
- Infedeltà aziendale (ad esempio: *Data Breach* causato da una persona interna che avendo autorizzazione ad accedere ai dati ne produce una copia distribuita in ambiente pubblico);
- Accesso abusivo (ad esempio: *Data Breach* causato da un accesso non autorizzato ai sistemi informatici con successiva divulgazione delle informazioni acquisite);
- Casi di pirateria informatica (usurpazione delle credenziali di accesso – fishing);
- Banche dati alterate o distrutte senza autorizzazione rilasciata dal relativo "*owner*";
- Virus o altri attacchi al sistema informatico o alla rete aziendale;
- Violazione di misure di sicurezza fisica (ad esempio: forzatura di porte o finestre di stanze di sicurezza o armadi contenenti archivi con informazioni riservate);

- Smarrimento di pc portatili, devices o attrezzature informatiche aziendali;
- Invio di e-mail contenenti dati personali e/o particolari a erroneo destinatario.

• A CHI SONO RIVOLTE QUESTE PROCEDURE?

Queste procedure sono rivolte a tutti i soggetti che a qualsiasi titolo trattano dati personali di competenza del Titolare del trattamento (meglio descritti al punto 5 della presente procedura) quali:

- I lavoratori dipendenti, nonché coloro che a qualsiasi titolo - e quindi a prescindere dal tipo di rapporto contrattuale intercorrente - abbiano accesso ai dati personali trattati nel corso delle prestazioni richieste per conto del Titolare del trattamento;
- qualsiasi soggetto (persona fisica o persona giuridica) diverso dal Destinatario interno che, in ragione del rapporto contrattuale in essere con il Titolare del trattamento abbia accesso ai suddetti dati e agisca in qualità di Responsabile del trattamento (art. 28 GDPR) o di autonomo Titolare;

Il rispetto della presente procedura è obbligatorio per tutti i soggetti coinvolti e la mancata conformità alle regole di comportamento previste dalla stessa potrà comportare provvedimenti disciplinari a carico dei dipendenti inadempienti ovvero la risoluzione dei contratti in essere con terze parti inadempienti, secondo le normative vigenti in materia.

• A QUALI TIPI DI DATI SI RIFERISCE QUESTA PROCEDURA

Queste procedure si riferiscono a:

- Dati personali trattati "da" e "per conto" del Titolare del trattamento, in qualsiasi formato (inclusi documenti cartacei) e con qualsiasi mezzo;

- Dati personali conservati o trattati a mezzo di qualsiasi altro Sistema in uso in Città Metropolitana di Palermo

Per «dato personale» si intende: 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.

• GESTIONE COMUNICAZIONE DI *DATA BREACHES*

Le violazioni di dati personali sono gestite dal Titolare del trattamento o da un Capo area sotto la supervisione del RPD.

In caso di concreta, sospetta e/o avvenuta violazione dei dati personali, è di estrema importanza assicurare che la stessa sia affrontata immediatamente e correttamente al fine di minimizzare l'impatto della violazione e prevenire che si ripeta.

Nel caso in cui uno dei Destinatari si accorga di una concreta, potenziale o sospetta violazione dei dati personali, dovrà immediatamente informare dell'incidente il Soggetto designato il quale si occuperà, senza ritardo con il supporto dei Destinatari stessi, di informare il Titolare del trattamento mediante la compilazione della scheda " Raccolta informazioni Violazione dati".

• GESTIONE DELLA

VIOLAZIONE DEI DATI PERSONALI

Per gestire una violazione dei dati personali è necessario seguire i seguenti cinque passaggi, di cui due eventuali:

Step 1: Identificazione e indagine preliminare;

Step 2: Contenimento, *recovery* e *risk assessment*;

Step 3: Notifica all'Autorità Garante (eventuale);

Step 4: Comunicazione agli interessati

(eventuale);

Step 5: Documentazione della violazione;

Step 1: Identificazione e indagine preliminare

La Sezione "Raccolta informazionecViolazione dati "debitamente compilata, permetterà al Titolare del trattamento o un Capo Area di condurre una valutazione iniziale riguardante la notizia dell'incidente occorso, ciò al fine di stabilire se si sia effettivamente verificata un'ipotesi di *Data Breach* (violazione) e se sia necessaria un'indagine più approfondita dell'accaduto, procedendo con il *risk assessment* (step 2).

Nel caso in cui si tratti di violazione di dati contenuti in un sistema informatico, il Titolare del trattamento o il capo area del settore interessato dovrà coinvolgere in tutta la procedura indicata nel presente documento anche l'amministratore di sistema

Detta valutazione iniziale sarà effettuata attraverso l'esame delle informazioni riportate nella sezione "Raccolta informazioni violazione dati", quali:

- la data di scoperta della violazione (tempestività);
- la descrizione dell'incidente (natura della violazione e dei dati coinvolti);
- la descrizione delle conseguenze dell'incidente

- le categorie e il numero approssimativo degli interessati coinvolti nella violazione;
- le banche dati o archivi anche cartacei violati;
- la descrizione di eventuali azioni già poste in essere.

Step 2: Contenimento, Recovery e risk assessment

Una volta stabilito che un *Data Breach* è avvenuto, il Titolare del trattamento e l'amministratore di sistema dovranno stabilire:

- se esistono azioni che possano limitare i danni che la violazione potrebbe causare (i.e. riparazione fisica di strumentazione; utilizzo dei file di *back up* per recuperare dati persi o danneggiati; isolamento/chiusura di un settore compromesso della rete; cambio dei codici di accesso... ecc.);

- una volta identificate tali azioni, quali siano i soggetti che devono agire per contenere la violazione;
- se sia necessario notificare la violazione all'Autorità Garante per la Protezione dei dati personali (ove sia probabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche);
- se sia necessario comunicare la violazione agli interessati (ove la violazione presenti un elevato rischio per i diritti e le libertà delle persone fisiche).

Al fine di individuare la necessità di notificazione all'Autorità Garante e di comunicazione agli interessati, il Titolare del trattamento valuterà la gravità della violazione utilizzando l'allegato A - Modulo di valutazione del Rischio connesso al *Data Breach* che dovrà essere esaminato unitamente alla scheda "raccolta informazioniViolazione dati " , tenendo, altresì, in debita considerazione i principi e le indicazioni di cui all'art. 33 GDPR .

Se, infatti, gli obblighi di notifica all'Autorità di Controllo scaturiscono dal superamento di una soglia di rischio semplice, l'art. 34 GDPR prevede, invece, che l'obbligo di comunicazione agli interessati sia innescato dal superamento di un rischio elevato.

Step 3: Notifica all'Autorità Garante competente (eventuale)

Una volta valutata la necessità di effettuare notifica della violazione dei dati subita sulla base della procedura di cui allo step 2, secondo quanto prescritto dal Regolamento (UE) 2016/679, Città Metropolitana di Palermo provvederà,

senza ingiustificato ritardo e, ove possibile entro 72 ore dal momento in cui ne è venuta a conoscenza.
Pertanto, il Titolare del trattamento individuerà la corretta modulistica da utilizzare per effettuare la notificazione e vi provvederanno.

Step 4: Comunicazione agli interessati (eventuale)

Una volta valutata la necessità di effettuare la comunicazione della violazione dei dati agli interessati, sulla base della procedura di cui allo step 2, secondo quanto prescritto dal Regolamento (UE) 2016/679, Città Metropolitana di Palermo dovrà provvedervi, senza ingiustificato ritardo.
Quanto al contenuto di tale comunicazione, il Titolare del trattamento o il Soggetto designato dovranno:

- comunicare il nome e i dati di contatto del Responsabile della protezione dei dati (RPD);
- descrivere le probabili conseguenze della violazione dei dati personali;
- descrivere le misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione dei dati personali e, se del caso, per attenuarne i possibili effetti negativi.

Quanto alle modalità di comunicazione, caso per caso, il Titolare del trattamento o il capo area dovranno sempre privilegiare la modalità di comunicazione diretta con i soggetti interessati (quali e- mail, SMS o messaggi diretti). Il messaggio dovrà essere comunicato in maniera evidente e trasparente, evitando quindi di inviare le informazioni nel contesto di update generali o newsletter, che potrebbero essere facilmente fraintesi dai lettori. Nel caso in cui la segnalazione diretta richieda uno sforzo ritenuto sproporzionato, allora si potrà utilizzare una comunicazione pubblica, che dovrà essere ugualmente efficace nel contatto diretto con l'interessato.

Step 5: Documentazione della violazione

Indipendentemente dalla valutazione circa la necessità di procedere a notificazione e/o comunicazione della violazione di *Data Breach*, ogni qualvolta si verifichi un incidente comunicato dai Destinatari attraverso l'Allegato A, Città Metropolitana di Palermo sarà tenuto a documentarlo.
Tale documentazione sarà affidata al Titolare del trattamento o all'amministratore di Sistema (qualora la violazione riguardi dati contenuti in sistemi informatici) vi provvederà mediante la tenuta del Registro dei *Data Breach*, secondo le informazioni ivi riportate.

Il Registro dei *Data Breach* deve essere continuamente aggiornato e messo a

disposizione del Garante, qualora l'Autorità chieda di accedervi.

ALLEGATO A – MODULO DI VALUTAZIONE DEL RISCHIO CONNESSO AL *DATA BREACH*

Assessment di gravità	**A cura del RPD insieme con ASICT (se del caso) e il Responsabile dell'ufficio coinvolto della violazione**
Dispositivi oggetto del *Data Breach* (computer, rete dispositivo mobile, file o parte di un file, strumento di back up, documento cartaceo, altro).	
Modalità di esposizione al rischio (tipo di violazione): lettura (presumibilmente i dati non sono stati copiati), copia (i dati sono ancora presenti sui sistemi ma del titolare), alterazione (i dati sono presenti sui sistemi ma sono stati alterati), cancellazione (i dati non sono più presenti e non li ha neppure l'autore della violazione), furto (i dati non sono più sui sistemi del titolare e li ha l'autore della violazione), altro.	
Breve descrizione dei sistemi di elaborazione o di memorizzazione dati coinvolti, con indicazione della loro ubicazione.	
Se laptop è stato perso/rubato: quando è stata l'ultima volta in cui il laptop è stato sincronizzato con il sistema IT centrale?	
Quante persone sono state colpite dalla violazione dei dati personali trattati nell'ambito della banca dati violata?	
La violazione può avere conseguenze negative in uno dei seguenti settori aziendali: operation, research, financial, legal, liability or reputation?	
Qual è la natura dei dati coinvolti? Compilare le sezioni sottostanti:	

a. Dati personali generici	

• I dati particolari (come identificati dal Regolamento (UE) 2016/679 relative ad una persona viva ed individuabile: • origine razziale o etnica; • opinion politiche, convinzioni religiose o filosofiche; • appartenenza sindacale; • dati genetici; • dati biometrici; • dati giudiziari; • relative alla salute o all'orientamento sessuale di una persona.	
c. Informazioni che possono essere utilizzate per commettere furti d'identità (i.e. dati di accesso e di identificazione, codice fiscale e copie di carta d'identità, passaporto o carte di credito);	
d. Informazioni personali relative a soggetti fragili (i.e. anziani, disabili, minori);	
e. Profili individuali che includono informazioni relative a performance lavorative, salario o stato di famiglia, sanzioni disciplinari, che potrebbero causare danni significativi alle persone;	
Altro:	
La violazione può comportare pregiudizio alla reputazione, perdita di riservatezza di dati protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro dato economico o sociale significativo?	
Gli interessati rischiano di essere privati dell'esercizio del controllo sui dati personali che li riguardano?	
Quali misure tecniche e organizzative sono adottate ai dati oggetto di violazione? (i.e. La pseudonimizzazione e la cifratura dei dati personali)	
Il Titolare del trattamento ha adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati successivamente alla violazione?	
Classificazione della violazione (1, 2 o 3) e motivazioni:	

Notificazione del *Data Breach* all'Autorità Garante	Si/NO Se sì, notificato in data: Dettagli:
Comunicazione del *Data Breach* agli interessati	Si/NO Se sì, notificato in data: Dettagli:

Comunicazione del *Data Breach* ad altri soggetti	Si/NO Se sì, notificato in data: Dettagli:

CITTÀ METROPOLITANA DI PALERMO
VIA MAQUEDA, 100
90134 - PALERMO

C. F. - P.IVA 80021470820

T. 091/6626111
F.
W. WWW.CITTAMETROPOLITANA.PA.I
CM.PA@CERT.CITTAMETROPOLITANA.
PA.IT

Registro delle attività e delle categorie di Trattamento del Titolare

Città Metropolitana di Palermo

Palermo, 11/10/2019

CITTÀ METROPOLITANA DI PALERMO
VIA MAQUEDA, 100
90134 - PALERMO

C.F. - P.IVA 80021470820

T. 091/6628111
F.
W. WWW.CITTAMETROPOLITANA.PA.I
CM.PA@CERT.CITTAMETROPOLITANA.
PA.IT

Indice

CITTÀ METROPOLITANA DI PALERMO
VIA MAQUEDA, 100
90134 - PALERMO

C.F. - P.IVA 80021470820

T. 091/6628111
F.
W. WWW.CITTAMETROPOLITANA.PA.I
CM.PA@CERT.CITTAMETROPOLITANA.
PA.IT

Introduzione

Il Registro delle attività e delle categorie di trattamento ("Registro") è previsto e disciplinato dall'art. 30 del Regolamento UE 2016/679, il quale impone al Titolare ed al Responsabile del trattamento di tracciare in questo documento tutte le attività di trattamento svolte, rispettivamente, sotto la propria responsabilità e per conto del titolare. Esso costituisce, dunque, il cuore del sistema aziendale per la protezione dei dati personali, nonché il punto di partenza della strategia di questo Ente per la messa a punto di un efficace sistema per la tutela della privacy e la protezione dei dati.

Lo scopo del presente Registro è censire le attività di trattamento effettuate da Città Metropolitana di Palermo in qualità sia di Titolare del trattamento, che di Responsabile ai sensi dell'art. 28 del Regolamento UE 2016/679.

L'art. 30 del Regolamento elenca una serie di informazioni relative alle singole attività di trattamento che il Registro deve necessariamente contenere, nonché alcune informazioni aggiuntive. Nel caso specifico, nel capitolo 4 del presente documento "Attività di trattamento", sono indicati tutti gli elementi fondamentali che costituiscono le attività di trattamento dei dati personali ed, in aggiunta, altri eventuali elementi che arricchiscono e definiscono ulteriormente una o più attività di trattamento, quali: applicativi correlati, tipologia di banca dati, eventuali referenti o designati interni. L'obiettivo perseguito con la compilazione completa del registro è quello di fornire quanti più dettagli possibili sulle attività di trattamento in ottemperanza al principio di responsabilizzazione.

Le misure di sicurezza adottate dal Titolare, utili al fine di scongiurare il verificarsi di violazioni dei dati personali, sono divise in tecniche ed organizzative. Le prime sono definite per i supporti informatici (hardware e software) utilizzati per lo svolgimento delle attività di trattamento, mentre le seconde sono definite per tutte le attività di trattamento. Per facilitare la lettura del presente registro, le misure di sicurezza sono riepilogate nel capitolo 3 "Misure di sicurezza".

Poiché tale documento è propedeutico alla valutazione dei profili di rischio e dell'analisi d'impatto sulla protezione dei dati, è necessario che lo stesso venga mantenuto costantemente aggiornato.

Il Registro è essenziale anche ai fini del rispetto dei diritti degli interessati, in quanto solo conoscendo nel dettaglio le attività di trattamento e la base giuridica su cui queste si fondano è possibile fornire risposte puntuali alle eventuali richieste di esercizio dei diritti provenienti dagli interessati stessi.

CITTÀ METROPOLITANA DI PALERMO
VIA MAQUEDA, 100
90134 - PALERMO

C.F. - P.IVA 80021470820

T. 091/6628111
F.
W. WWW.CITTAMETROPOLITANA.PA.I
CM.PA@CERT.CITTAMETROPOLITANA.
PA.IT

Identità e dati di contatto Titolare/i del trattamento e RPD

Titolare del trattamento:

Città Metropolitana di Palermo
Via Maqueda, 100 90134 Palermo
cm.pa@cert.cittametropolitana.pa.it
091/6628111

Contitolare/i del trattamento del trattamento:

Nessuno

Responsabile della protezione dei dati (RPD/DPO):

mail@dpo.com
Centro Studi Enti Locali Spa
Stefano Paoli
stefano.paoli@centrostudientilocali.it

CITTÀ METROPOLITANA DI PALERMO
VIA MAQUEDA, 100
90134 - PALERMO

C.F. - P.IVA 80021470820

T. 091/6628111
F.
W. WWW.CITTAMETROPOLITANA.PA.I
CM.PA@CERT.CITTAMETROPOLITANA.
PA.IT

Misure di sicurezza

Misure di sicurezza organizzative adottate

Categoria	Misura
Cifratura	Le chiavi private sono adeguatamente protette
Copie di sicurezza	È definito un piano formalmente approvato al fine di garantire la Continuità Operativa e il Disaster Recovery È stato redatto un manuale per la conservazione digitale Sono previste procedure di controllo al fine di garantire l'effettività delle procedure di ripristino.
Gestione utenze	È in vigore una procedura formale per il rilascio delle credenziali e per la loro cancellazione I privilegi di amministrazione vengono rilasciati ai soli utenti che abbiano le competenze adeguate e la necessità operativa. È mantenuto un inventario delle utenze amministrative. Le utenze amministrative sono formalmente autorizzate.
Misure di sicurezza analogiche	Contenitori (armadi, schedari, ecc.) muniti di serratura Chiusura a chiave dei locali Sistemi di controllo degli accessi Sistemi antincendio
Politiche, regolamenti e manuali	È stato definito un manuale per la gestione del protocollo informatico Formazione relativa al processo/applicativo in esame Formazione relativa alla normativa sulla protezione dei dati Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by design Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by default
Protezione dei Dati	Sono in vigore procedure per classificare le categorie di dati Sono in vigore procedure gestire la conservazione dei dati.

CITTÀ METROPOLITANA DI PALERMO
VIA MAQUEDA, 100
90134 - PALERMO

C.F. - P.IVA 80021470820

T. 091/6628111
F.
W. WWW.CITTAMETROPOLITANA.PA.I
CM.PA@CERT.CITTAMETROPOLITANA.
PA.IT

	Sono in vigore procedure minimizzare la conservazione dei dati. Sono in vigore procedure per notificare gli incidenti di sicurezza e le violazioni dei dati personali
Ruoli e responsabilità	Sono definiti ruoli e responsabilità interne, in ambito sicurezza ICT e protezione dei dati Sono definiti ruoli e responsabilità con terze parti, in ambito sicurezza ICT e protezione dei dati I soggetti che trattano dati personali hanno sottoscritto un accordo di riservatezza. Sono previsti specifici accordi e misure di garanzia per i dati che escano o vengano comunicati a entità stabilite fuori dallo spazio economico europeo

Misure di sicurezza tecniche adottate

Categoria	Misura
ABSC 1	1.1 - Implementare un inventario delle risorse attive collegate alla rete 3.1 - Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete. 4.1 - Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP.
ABSC 10	1.1 - Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema. 3.1 - Assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti ovvero mediante cifratura. La codifica effettuata prima della trasmissione consente la remotizzazione del backup anche nel cloud. 4.1 - Assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.

CITTÀ METROPOLITANA DI PALERMO
VIA MAQUEDA, 100
90134 PALERMO

C.F. - P.IVA 80021470820

T. 091/6628111
F.
W. WWW.CITTAMETROPOLITANA.PA.I
CM.PA@CERT.CITTAMETROPOLITANA.
PA.IT

ABSC 13	1.1 - Effettuare un'analisi dei dati per individuare quelli con particolari requisiti di riservatezza (dati rilevanti) e segnatamente quelli ai quali va applicata la protezione crittografica. 8.1 - Bloccare il traffico da e verso url presenti in una blacklist.
ABSC 2	1.1 - Stilare un elenco di software autorizzati e relative versioni necessari per ciascun tipo di sistema, compresi server, workstation e laptop di vari tipi e per diversi usi. Non consentire l'installazione di software non compreso nell'elenco. 3.1 - Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.
ABSC 3	1.1 - Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi. 1.2 - Le configurazioni sicure standard devono corrispondere alle versioni "hardened" del sistema operativo e delle applicazioni installate. La procedura di hardening comprende tipicamente: eliminazione degli account non necessari (compresi gli account di servizio), disattivazione o eliminazione dei servizi non necessari, configurazione di stack e heaps non eseguibili, applicazione di patch, chiusura di porte di rete aperte e non utilizzate. 1.3 - Assicurare con regolarità la validazione e l'aggiornamento delle immagini d'installazione nella loro configurazione di sicurezza anche in considerazione delle più recenti vulnerabilità e vettori di attacco. 2.1 - Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione. 2.2 - Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard. 3.1 - Le immagini d'installazione devono essere memorizzate offline. 4.1 - Eseguire tutte le operazioni di amministrazione remota di server, workstation, dispositivi di rete e analoghe apparecchiature per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri).

CITTÀ METROPOLITANA DI PALERMO
VIA MAQUEDA, 100
90134 - PALERMO

C.F. - P.IVA 80021470820

T. 091/6628111
F.
W. WWW.CITTAMETROPOLITANA.PA.I
CM.PA@CERT.CITTAMETROPOLITANA.
PA.IT

ABSC 4	1.1 - Ad ogni modifica significativa della configurazione eseguire la ricerca delle vulnerabilità su tutti i sistemi in rete con strumenti automatici che forniscano a ciascun amministratore di sistema report con indicazioni delle vulnerabilità più critiche. 4.1 - Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza. 5.1 - Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni. 5.2 - Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità. 7.1 - Verificare che le vulnerabilità emerse dalle scansioni siano state risolte sia per mezzo di patch, o implementando opportune contromisure oppure documentando e accettando un ragionevole rischio. 8.1 - Definire un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabi- lità , del potenziale impatto e della tipologia degli apparati (e.g. server esposti, server interni, PdL, portatili, etc.). 8.2 - Attribuire alle azioni per la risoluzione delle vulnerabilità un livello di priorità in base al ri- schio associato. In particolare applicare le patch per le vulnerabilità a partire da quelle più critiche.
ABSC 5	1.1 - Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi. 1.2 - Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato. 2.1 - Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata. 3.1 - Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso. 7.1 - Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri).

CITTÀ METROPOLITANA DI PALERMO
VIA MAQUEDA, 100
90134 - PALERMO

C.F. - P.IVA 80021470820

T. 091/6628111
F.
W. WWW.CITTAMETROPOLITANA.PA.I
CM.PA@CERT.CITTAMETROPOLITANA.
PA.IT

	7.3 - Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging). 7.4 -Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history). 10.1 - Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse. 10.2 - Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona. 10.3 - Le utenze amministrative anonime, quali "root" di UNIX o "Administrator" di Windows, debbono essere utilizzate solo per le situazioni di emergenza e le relative credenziali debbono essere gestite in modo da assicurare l'imputabilità. 11.1 - Conservare le credenziali amministrative in modo da garantirne disponibilità. 11.2 - Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.
ABSC 8	1.1 - Installare su tutti i sistemi connessi alla rete locale strumenti atti a rilevare la presenza e bloccare l'esecuzione di malware (antivirus locali). Tali strumenti sono mantenuti aggiornati in modo automatico. 1.2 - Installare su tutti i dispositivi firewall ed IPS personali. 3.1 - Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali. 7.1 - Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili. 7.2 - Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file. 7.3 - Disattivare l'apertura automatica dei messaggi di posta elettronica. 7.4 - Disattivare l'anteprima automatica dei contenuti dei file. 8.1 - Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.

CITTÀ METROPOLITANA DI PALERMO
VIA MAQUEDA, 100
90134 - PALERMO

C.F. - P.IVA 80021470820

T. 091/6628111
F.
W. WWW.CITTAMETROPOLITANA.PA.I
CM.PA@CERT.CITTAMETROPOLITANA.
PA.IT

	9.1 - Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antispam. 9.2 - Filtrare il contenuto del traffico web. 9.3 - Bloccare nella posta elettronica e nel traffico web i file la cui tipologia non è strettamente ne- cessaria per l'organizzazione ed è potenzialmente pericolosa (e.g. .cab).
Applicazione	Validazione restrittiva degli input Gestione corretta dei messaggi di errore facendo si che questi non rivelino informazioni riservate sul sistema Eventuali connessioni in entrata ed uscita effettuate tramite connessioni protette che fanno uso di protocolli intrinsecamente sicuri
Cifratura	Trasferimento dati usando SSL/TLS
Copie di sicurezza	Viene effettuata una copia di sicurezza con cadenza settimanale delle informazioni strettamente necessarie per il completo ripristino del sistema I backup sono effettuati con più di un sistema per contrastare malfunzionamenti in fase di ripristino Le copie di sicurezza sono mantenute sicure tramite misure di sicurezza fisiche Le copie di sicurezza sono isolate dal sistema
Credenziali	È garantita la qualità delle password tramite la validazione, (8 caratteri con minuscole, maiuscole, numeri e caratteri speciali) Le credenziali già utilizzate non possono essere riutilizzate a breve distanza di tempo Le credenziali soprattutto quelle delle utenze amministrative vengono sostituite con frequenza semestrale Sono utilizzati sistemi centralizzati di gestione delle password (Single Sign On) Integrazione con il Domain Controller
Gestione utenze	Implementazione del principio del privilegio minimo Disattivazione account e password predefiniti del fornitore

CITTÀ METROPOLITANA DI PALERMO
VIA MAQUEDA, 100
90134 - PALERMO

C.F. - P.IVA 80021470820

T. 091/6628111
F.
W. WWW.CITTAMETROPOLITANA.PA.I
CM.PA@CERT.CITTAMETROPOLITANA.
PA.IT

	Tutte le utenze, in particolare quelle amministrative, sono nominative e riconducibili ad una sola persona Generazione di un'allerta alla aggiunta o soppressione di un'utenza amministrativa Vengono tracciati nei log tutti i tentativi di accesso falliti delle utenze amministrative Vengono tracciate nei log tutte le azioni delle utenze amministrative
Protezione dei Dati	Analisi per identificare se e quali dati personali siano trattati Analisi per identificare se e quali dati sensibili siano trattati

CITTÀ METROPOLITANA DI PALERMO
VIA MAQUEDA, 100
90134 - PALERMO

C.F. - P.IVA 80021470820

T. 091/6628111
F.
W. WWW.CITTAMETROPOLITANA.PA.I
CM.PA@CERT.CITTAMETROPOLITANA.
PA.IT

Attività di trattamento

ID	Trattamento	Data Creazione	Data ultima modifica

Gestione degli acquisti di beni e servizi tramite affidamente secondo il Codice degli Appalti

Modalità di conservazione	
cartaceo, informatizzato	
Titolari	
Città Metropolitana di Palermo	
Responsabile Protezione dei Dati	
Non definito	
Origine dei dati	
Raccolta presso l'interessato	
Finalità	**Basi giuridiche**
	Esecuzione di un contratto di cui l'interessato è parte Adempimento di un obbligo legale del Titolare
Categorie di dati	
Personali (Identificativi, Beni/proprietà/possessi, Istruzione/Cultura, Famiglia, Lavoro, Situazione economica, Comunicazione elettronica, Giudiziari, diversi da condanne penali e reati) Giudiziari (condanne penali e reati)	
Categorie di Interessati	
Operatori economici	
Referenti interni	
Direzione - Ambiente: La Manno Giuseppe, Direzione - Edilizia e Beni culturali: Delfino Claudio, Direzione - Gare e contratti. Innovazione tecnologica: Zito Maurizio, Direzione - Patrimonio: Grigoli Giuseppa, Direzione - politiche del personale - Avvocatura: Volpe Matteo, Direzione - Ragioneria generale: Bonomo Massimo, Direzione - Sviluppo economico – Politiche del lavoro – Istruzione – Turismo – Cultura e legalità: Spallina Filippo, Direzione - Viabilità: Pampalone Salvatore, Segreteria generale e AA.GG ed istituzionali – Cerimoniale – Urp – Politiche comunitarie- Protezione civile: Mirto Marianna, Ufficio segreteria - Direzione generale: coordinamento ufficio Segretario generale: Volpe Mattea	

Destinatari	Posizione geografica	Legittimazione

CITTÀ METROPOLITANA DI PALERMO
VIA MAQUEDA, 100
90134 - PALERMO

C.F. - P.IVA 80021470820

T. 091/6628111
F.
W. WWW.CITTAMETROPOLITANA.PA.I
CM.PA@CERT.CITTAMETROPOLITANA.
PA.IT

Soggetti codice degli appalti, Regione, Comuni, agenzia delle Entrate, Ministeri, Autorità giudiziarie, Revisori dei conti	Intra UE	Nessuno
Diffusione		
Il Trattamento non comporta attività di diffusione		
Profilazione		
Il Trattamento non comporta attività di profilazione		

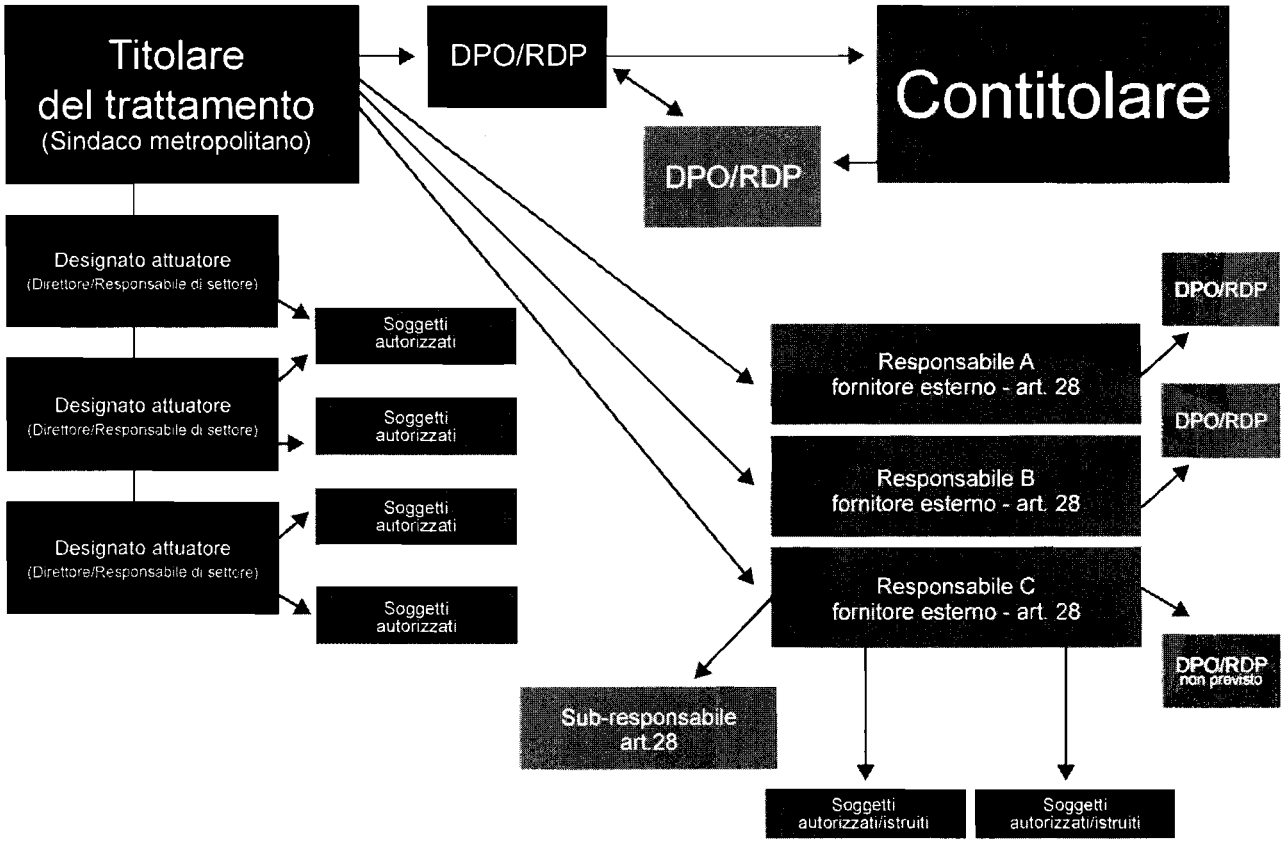
CITTÀ METROPOLITANA DI PALERMO
VIA MAQUEDA, 100
90134 - PALERMO

C.F. - P.IVA 80021470820

T. 091/6628111
F.
W. WWW.CITTAMETROPOLITANA.PA.I
CM.PA@CERT.CITTAMETROPOLITANA.
PA.IT

ID	Trattamento	Data Creazione	Data ultima modifica

ALLEGATO ALLA DELIBERA C.S Nº 137
DEL 23/12/2019



CITTÀ METROPOLITANA DI PALERMO

Proposta di Deliberazione avente per
OGGETTO: " *Adeguamento del regolamento per l'attuazione del Regolamento UE 2016/679 al Decreto legislativo n. 101 del 10.08.2018.*

IL COLLEGIO DEI REVISORI DEI CONTI

VISTA la proposta di deliberazione della Direzione Segreteria Generale - trasmessa a questo Collegio per l'acquisizione del competente parere, in data 10.12.2019 con nota prot. n.99253;

VISTO il parere "favorevole", a firma del Dirigente competente, espresso il 05.12. 2019 in ordine alla regolarità tecnica;

VISTO che in ordine alla regolarità contabile, il predetto atto non necessita del visto di regolarità, come attestato il 06.12.2019 dal Responsabile dei servizi finanziari in quanto non comporta riflessi diretti o indiretti sulla situazione economico- finanziaria dell'Ente;

PRESO ATTO che con Deliberazione del Commissario Straordinario n. 21 del 1 settembre 2018 l'Amministrazione ha approvato per l'adozione il Regolamento per l'attuazione del Regolamento UE 2016/679 ed i relativi allegati;

DATO ATTO che con la legge 25.10.2017 n.163, il Governo è stato delegato all'emanazione di uno o più decreti legislativi di adeguamento del quadro normativo nazionale alle disposizioni del Regolamento UE 679/2016 del Parlamento europeo;

CONSIDERATO che con il Decreto Legislativo n.101 del 10.08.2018, attuativo della delega, sono state emanate disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento Generale Protezione dati " RGPD";

CONSIDERATO che si rende necessario procedere all'adozione del nuovo Regolamento, contenente gli adempimenti di cui al D.lgs. 101/2018;

VISTO lo schema di " Regolamento per l'attuazione del Regolamento UE 2016/679, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali" predisposto dalla Direzione Segreteria Generale , composto da n. 20 articoli e dagli Allegati A) Bozza di registro delle attività e delle categorie di trattamento del titolare, B) Procedura data breach, C) Bozza organigramma privacy, il quale è stato redatto nel rispetto della disciplina normativa vigente;

ESAMINATA la proposta di deliberazione ed il predetto Schema di Regolamento sulla PRIVACY in essa contenuto

prende atto

della proposta di deliberazione di " *Adeguamento del regolamento per l'attuazione del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali*"nel rispetto delle norme in essa richiamate

Palermo 20.12.2019

Il Collegio dei Revisori dei conti:

dott. Salvatore Maurizio Dilena (Presidente

dott. Gioacchino Gugliotta (Componente) ASSENTE

rag. Antonino Tranchina (Componente)