CITTÀ METROPOLITANA DI MESSINA

Decreto Sindacale

n. 97 del 31 MAG. 2019

OGGETTO: Presa d'atto della "Procedura semplificata per la gestione e la valutazione delle violazioni\data Breach" ai sensi del GDPR 2016/679 e normativa nazionale in vigore.

IL SINDACO METROPOLITANO

l'anno duemiladiciannove il giorno TRENTUNO del mese di MAGGIO, alle ore 12,15, nella sede di Palazzo dei Leoni, con l'assistenza del Segretario Generale Avv. M. A. CAPONETTI:

Vista l'allegata proposta di decreto relativo all'oggetto;
Vista la L.R. n. 15 del 04.08.2015 e successive modifiche ed integrazioni;
Viste le LL.RR. n. 48/91 e n. 30/2000 che disciplinano l'O.R.EE.LL.;
Visto il D.Lgs. n. 267/2000 e ss.mm.ii.;
Visto il D.P. della Regione Siciliana n. 576/GAB del 02/07/2018, che all'art. 2 recita: *"le funzioni del Sindaco Metropolitano e della Conferenza Metropolitana sono esercitate dal Sindaco pro-tempore del Comune di Messina On.le Cateno De Luca";*
Visti i pareri favorevoli, espressi ai sensi dell'art. 12 della L.R. n. 30 del 23.12.2000:

- per la regolarità tecnica, dal Dirigente proponente;
- per la regolarità contabile e per la copertura finanziaria della spesa, dal Dirigente della II Direzione – Servizi Finanziari;

DECRETA

APPROVARE la proposta di decreto indicata in premessa, allegata al presente atto per farne parte integrante e sostanziale, facendola propria integralmente.
DARE ATTO che il presente provvedimento è immediatamente esecutivo a norma di legge.

CITTÀ METROPOLITANA DI MESSINA

Proposta di Decreto Sindacale

della VII DIREZIONE "Affari Territoriali e Comunitari"

Servizio "Servizi Informatici"

OGGETTO: Presa d'atto della "Procedura semplificata per la gestione e la valutazione delle violazioni\data Breach" ai sensi del GDPR 2016/679 e normativa nazionale in vigore.

PREMESSO che in data 4 Maggio 2016 è stato pubblicato sulla Gazzetta Ufficiale dell'Unione Europea n. L 119/2016 il Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, indicato anche come *"General Data Protection Regulation"* (GDPR);

CHE lo stesso è stato dichiarato immediatamente esecutivo e direttamente applicabile negli ordinamenti degli Stati membri;

CHE la Città Metropolitana di Messina con il Decreto Sindacale n.161 del 16/07/2018, mediante procedura sul MEPA, ha designato quale Responsabile della Protezione dei Dati (DPO) la società "IT & T" rappresentata dall'ing. Giuseppe Bono;

EVIDENZIATO che i dati personali conservati, trattati, inviati o comunque gestiti dalle Pubbliche Amministrazioni possono essere soggetti a perdita, distruzione, manomissione, diffusione indebita anche in conseguenza di attacchi informatici, accessi abusivi, incidenti o eventi rovinosi come incendi o altre calamità, con grave pregiudizio per la privacy degli interessati cui si riferiscono i dati;

RILEVATO che i documenti già compilati dal Responsabile della Protezione dei Dati vengono integrati con la "Procedura semplificata per la gestione e la valutazione delle violazioni\data Breach" che riporta i criteri di valutazione e le azioni da intraprendere nel caso in cui si verifichi una violazione dei dati personali trasmessi, conservati o trattati nell'ambito dell'Ente;

PRESO ATTO che tali documenti sono stati visionati e personalizzati in funzione delle esigenze dell'Ente da parte dei "Servizi Informatici" della VII Direzione;

Si propone che il Sindaco Metropolitano

DECRETI

Prendere atto del documento "Procedura semplificata per la gestione e la valutazione delle violazioni\data Breach" qui allegato, che costituisceno parte integrante del presente atto.

Il Funzionario
dott. Giacomo Lucà

Il Dirigente
ing. Armando Cappadonia

SI ALLEGA IL SEGUENTI DOCUMENTO:

"Procedura semplificata per la gestione e la valutazione delle violazioni\data Breach"

oggetto: Presa d'atto della "Procedura semplificata per la gestione e la valutazione delle violazioni\data Breach" ai sensi del GDPR 2016/679 e normativa nazionale in vigore.

PARERE DI REGOLARITÀ TECNICA

Ai sensi e per gli effetti dell'art. 12 della L.R. 23-12-2000 n. 30 e ss.mm.ii., si esprime parere:

In ordine alla regolarità tecnica della superiore proposta di decreto.

Addì 30 MAG 2019

IL DIRIGENTE

ING. ARMANDO CAPPADONIA

Si dichiara che la proposta non comporta riflessi diretti o indiretti sulla situazione economico-finanziaria dell'Ente e pertanto non è dovuto il parere di regolarità contabile.

Addì 30 MAG. 2019

IL DIRIGENTE

ING. ARMANDO CAPPADONIA

PARERE DI REGOLARITÀ CONTABILE

Ai sensi e per gli effetti dell'art. 12 della L.R. 23-12-2000 n. 30 e ss.mm.ii., si esprime parere:

In ordine alla regolarità contabile della superiore proposta di decreto.

Addì_____

IL RAGIONIERE GENERALE

Ai sensi del D.Lgs 267/2000, si attesta la copertura finanziaria della superiore spesa.

Addì_____

IL RAGIONIERE GENERALE

Decreto Sindacale n. 97 **del** 31 MAG. 2019

Oggetto: PRESA D'ATTO DELLA "PROCEDURA SEMPLIFICATA PER LA GESTIONE E LA VALUTAZIONE DELLE VIOLAZIONI DATA BREACH" AI SENSI DEL GDPR 2016/679 E NORMATIVA NAZIONALE IN VIGORE

Letto, confermato e sottoscritto.

Il Sindaco Metropolitano

(Dott. On. Cateno DE LUCA)

Il Segretario Generale

Avv. M. A. CAPONETTI

CERTIFICATO DI PUBBLICAZIONE

Il sottoscritto Segretario Generale,

CERTIFICA

Che il presente decreto _____ pubblicato all'Albo on-line dell'Ente il _____ e per quindici giorni consecutivi e che contro lo stesso _____ sono stati prodotti, all'Ufficio preposto, reclami, opposizioni o richieste di controllo.

Messina, _____

IL SEGRETARIO GENERALE

_____

E' copia conforme all'originale da servire per uso amministrativo.

Messina, _____

IL SEGRETARIO GENERALE

_____

Città Metropolitana di Messina

(ai sensi della L.R. n. 15 del 4 agosto 2015)

PROCEDURA SEMPLIFICATA PER LA GESTIONE E LA VALUTAZIONE DELLE VIOLAZIONI/*DATA BREACH*

Il referente *data protection* designato nella persona di _____ nella sua qualità di soggetto preposto alla gestione delle violazioni subite dal Titolare del trattamento sotto la cui autorità opera

PRENDE ATTO DEL FATTO CHE

A. Integra una violazione (o *data breach*) ogni evento che comporta la violazione di sicurezza che può provocare 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
B. Una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata.
C. Non appena viene a conoscenza di un'avvenuta violazione dei dati personali, il titolare del trattamento dovrebbe notificare la violazione dei dati personali all'autorità di controllo competente, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che il titolare del trattamento 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.
D. 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.
E. Il titolare del trattamento dovrebbe comunicare all'interessato la violazione dei dati personali senza indebito ritardo, qualora questa violazione dei dati personali 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.
F. La comunicazione dovrebbe descrivere la natura della violazione dei dati personali e formulare raccomandazioni per la persona fisica interessata intese ad attenuare i potenziali effetti negativi. Tali comunicazioni agli interessati dovrebbero essere effettuate non appena ragionevolmente possibile e in stretta collaborazione con l'autorità di controllo e nel rispetto degli orientamenti impartiti da questa o da altre autorità competenti, quali le autorità incaricate dell'applicazione della legge. Ad esempio, la necessità di attenuare un rischio immediato di danno richiederebbe che la comunicazione agli interessati fosse tempestiva, ma la necessità di attuare

opportune misure per contrastare violazioni di dati personali ripetute o analoghe, potrebbe giustificare tempi più lunghi per la comunicazione.

G. Occorre verificare se siano state messe in atto tutte le misure tecnologiche e organizzative adeguate di protezione per stabilire immediatamente se vi sia stata violazione dei dati personali, informando tempestivamente l'autorità di controllo e l'interessato.

H. Occorre verificare che la notifica sia stata trasmessa senza ingiustificato ritardo, tenendo conto in particolare della natura e della gravità della violazione dei dati personali e delle sue conseguenze ed effetti negativi per l'interessato. Siffatta notifica può dar luogo a un intervento dell'autorità di controllo nell'ambito dei suoi compiti e poteri previsti dal presente regolamento.

I. Nella definizione delle modalità relative al formato e alle procedure applicabili alla notifica delle violazioni di dati personali, è opportuno tenere debitamente conto delle circostanze di tale violazione: ad esempio, stabilire se i dati personali fossero o meno protetti con misure tecniche adeguate atte a limitare efficacemente il rischio di furto d'identità o altre forme di abuso. Inoltre, occorre verificare se tali modalità e procedure tengano conto dei legittimi interessi delle autorità incaricate dell'applicazione della legge, qualora una divulgazione prematura possa ostacolare inutilmente l'indagine sulle circostanze di una violazione di dati personali.

E ADOTTA LA SEGUENTE PROCEDURA PER LA PREVENZIONE E PER LA GESTIONE DELLE VIOLAZIONI DEI DATI PERSONALI IN AZIENDA

Art. 1 Prevenzione delle violazioni.

Il referente *data protection*, ma anche i soggetti autorizzati e istruiti ad operare attività di trattamento sotto l'autorità, così come coloro i quali sono esclusi dalle attività di trattamento, devono adottare ogni comportamento proattivo volto a prevenire ogni possibile violazione.
In ogni caso, quando una violazione dei dati personali degli interessati viene individuata e rilevata, questa deve essere segnalata tempestivamente e senza ingiustificato ritardo al referente *data protection,* nonché al DPO ove nominato.

Art. 2 Presa di conoscenza della violazione.

Il referente generale *data protection* può prendere coscienza dell'avvenuta violazione nell'ambito dell'esercizio dei propri poteri di sorveglianza sulle misure organizzative e di sicurezza, oppure a seguito della relativa comunicazione da parte di soggetti autorizzati al trattamento o anche non autorizzati.
La data in cui il referente *data protection* prende conoscenza della violazione deve essere debitamente annotata sul registro e fa decorrere il termine di 72 (settantadue) ore per effettuare la comunicazione al Garante, ove questa sia valutata come necessaria.

2.1 Documentazione della violazione sul registro dei *data breach*.

Qualsiasi violazione, a prescindere dalla gravità della stessa, deve essere debitamente e puntualmente annotata sul registro delle violazioni (*data breach*) dal soggetto preposto, non appena ne abbia preso conoscenza, compilando debitamente ogni campo del registro utile a descriverla o indicando, comunque, ogni altro elemento utile.

Art. 3. Valutazione della violazione e della gravità della stessa.

Una volta annotata e registrata la violazione sul registro dei *data breach,* questa deve essere debitamente qualificata (art. 3.1), valutata nella sua gravità (art. 3.2) e per i rischi che presenta per i singoli interessati o le categorie di interessati coinvolte (art. 3.3).

3.1 La qualificazione della violazione:

La violazione prima di essere valutata deve essere qualificata in una delle seguenti categorie:

A. Violazione di riservatezza: quando si verifica una divulgazione o un accesso a dati personali non autorizzato o accidentale.

A.1 Comunicazione non autorizzata: i dati personali sono stati indebitamente comunicati a un numero determinato o comunque determinabile di persone fisiche non autorizzate.

A.2 Divulgazione non autorizzata: i dati personali sono stati comunicati a un numero non determinato né determinabile di soggetti non autorizzati.

B. Violazione di integrità: quando si verifica un'alterazione di dati personali non autorizzata o accidentale.

B.1 Irreparabile: i dati personali sono irrimediabilmente e totalmente alterati con conseguente impossibilità di riutilizzarli nel futuro in qualunque forma. L'unico modo per continuare a effettuare le attività di trattamento è operare sulle copie di backup.

B.2 Ripristinabile: i dati personali sono alterati solo in certe loro parti, ma il potere identificativo di questi non è integralmente annullato e i dati possono comunque essere ripristinati nella loro integrità.

C. Violazione di disponibilità: quando si verifica perdita, inaccessibilità, o distruzione accidentale o non autorizzata, di dati personali.

C.1 Indisponibilità assoluta: comporta una perdita di controllo assoluta con impossibilità di accedere ai dati personali.

C.2 Indisponibilità temporanea: comporta una perdita di controllo solo temporanea dei dati personali.

D. Violazione di altra natura: quando la stessa non rientra in alcuna delle categorie precedentemente indicate.

3.2 La valutazione della gravità della violazione.

La gravità della violazione deve essere operata caso per caso avendo riguardo:

1. del tipo di violazione (di riservatezza, di integrità o di disponibilità)

2. della natura, in ragione al carattere comune sensibile dei dati e delle informazioni violati

3. del volume dei dati personali violati

4. della facilità di riconoscimento degli interessati i cui dati personali sono stati violati (incide su questo aspetto, ad esempio, l'adozione di misure di sicurezza che diminuiscono il potere identificativo degli interessati come la criptazione o la pseudonomizzazione dei dati personali trattati)

5. della serietà delle conseguenze per le persone fisiche (ad esempio se queste possono subire un effettivo pregiudizio patrimoniale o personale, subendo, ad esempio, discriminazioni)

6. delle caratteristiche specifiche delle persone fisiche coinvolte (avendo riguardo se gli interessati coinvolti sono, ad esempio, soggetti minori, disabili, lavoratori dipendenti o altre categorie di soggetti vulnerabili)

7. della quantità di persone fisiche coinvolte

8. delle caratteristiche specifiche del titolare

Art. 3.3 La valutazione dei rischi per gli interessati che hanno subito la violazione.

Il soggetto preposto alla valutazione della violazione deve sempre valutare analiticamente anche i rischi inerenti la violazione, avendo riguardo se la violazione può comportare per gli interessati:

A. la perdita del controllo dei dati personali che li riguardano

B. la limitazione dei loro diritti

C. discriminazione

D. il furto o l'usurpazione di identità

E. perdite finanziarie

F. la decifratura non autorizzata della pseudonomizzazione

G. un pregiudizio alla reputazione

H. la perdita di riservatezza dei dati personali protetti da segreto professionale

I. qualsiasi altro danno economico o sociale significativo per la persona interessata

Art. 4 L'assegnazione di un punteggio in base alla gravità ed al rischio.

Dopo avere qualificato la violazione, occorre valutarne la gravità secondo i parametri indicati nel precedente articolo e, successivamente, operare una media fra i diversi fattori contemplati e coinvolti.
Dopo avere operato una media fra i fattori descrittivi della gravità e dei rischi per gli interessati, occorre operare una media finale fra i due valori al fine di assegnare alla violazione un punteggio finale.

La media finale è da operarsi in maniera ponderata: la gravità sul punteggio finale ha un peso pari al 25% mentre i rischi per gli interessati hanno un peso pari al 75%.
L'obbligo di notifica e quello aggiuntivo di comunicazione devono essere valutati caso per caso e presi in relazione alla gravità della violazione subita e col dovuto riguardo dei diritti e della libertà degli interessati quando la violazione sia tale da non consentire di archiviare la violazione.

La violazione può presentare una gravità:

a. bassa/trascurabile (punteggio a partire da 0 fino a 3)

b. media (punteggio a partire da 3 fino a 5)

c. alta (punteggio a partire da 5 fino a 8)

d. molto alta (punteggio a partire da 8 fino a 10)

Quando si ha il sospetto che la violazione sia di gravità non trascurabile, si deve provvedere a prendere immediatamente contatto con il Titolare del trattamento dei dati e con il DPO, se questi non risulta esserne già a conoscenza.

Art. 5 Termine per la conclusione della procedura, e per ogni sua singola fase, criterio di gestione delle violazioni sulla base del rischio e della gravità delle stesse.

La violazione dovrebbe essere annotata nel registro delle violazioni in un termine di tempo non superiore a 1 (una) ora dall'avvenuta scoperta della stessa.
Le informazioni necessarie dovrebbero essere reperite e debitamente annotate nel registro in un arco di tempo non superiore a 3 (tre) ore dal momento in cui la violazione è stata annotata sul registro.

Art. 6 Gestione di plurime violazioni.

Nel caso di plurime violazioni da gestire occorre dare precedenza alla violazione stimata di maggiore gravità, con particolare riguardo dei rischi per gli interessati.

Art. 7 L' Archiviazione della violazione.

L'archiviazione va disposta quando il Titolare è in grado di dimostrare che è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

Art. 8 La notificazione al Garante della violazione e la comunicazione della violazione agli interessati.

La Notificazione al Garante della violazione va disposta quando questa può presentare un rischio per gli interessati e provocare danni fisici, materiali o immateriali alle persone fisiche, come ad esempio, perdita del controllo dei dati personali che le riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonomizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata.

Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

Art. 9 Designazione del sostituto del referente *data protection* per la gestione delle violazione in caso di impossibilità, anche temporanea, del referente.

Nel caso in cui il referente *data protection* sia impossibilitato a provvedere alla gestione della violazione, questi deve indicare un soggetto sostituto che operi in sua vece e che svolga le sue funzioni nell'ambito della gestione del *data breach.*
Il soggetto sostituto deve essere adeguatamente formato ed istruito relativamente alla procedura di gestione della violazione