Comune di Modena

# MANUALE PER LA GESTIONE DI UNA VIOLAZIONE DI DATI PERSONALI ( DATA BREACH )

Approvato con deliberazione della Giunta Comunale n. 245 del 29/5/2020

## 1. FINALITA'

Il presente documento indica le opportune modalità di gestione di una violazione dei dati personali ( data breach ), al fine di limitare i rischi per i diritti e le libertà dei singoli, nella consapevolezza che l'efficacia dell'intervento dipende dalla tempestività e dall'adeguatezza delle misure adottate, nel rispetto della disposizioni normative in materia .

Nella redazione del presente Manuale si è tenuto conto, in particolare, delle indicazioni e delle disposizioni :

- del Regolamento Europeo UE 2016/679 ( d'ora innanzi " GDPR" ),
- del Dlgs. 30 giugno 2003 n.196 " Codice in materia di protezione dei dati personali" e successive modifiche ed integrazioni
- delle Linee guida sulla notifica delle violazioni di dati personali ai sensi del Regolamento UE 2016/679 WP250 rev.01 del Gruppo di lavoro Art.29 nella versione emendata e adottata il 6 febbraio 2018
- del Provvedimento del Garante del 30 luglio 2019 sulla notifica delle violazioni di dati personali.

## 2. AMBITO DI APPLICAZIONE - DESTINATARI

L'art.32 ( *" Sicurezza del trattamento* " ) del GDPR prevede che, nell'attuare misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato, occorre, tra l'altro, prendere in considerazione *" la capacità di assicurare, su base permanente, la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento"* e *" la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico "*

Il presente Manuale costituisce una guida per dirigenti, dipendenti, responsabili esterni del trattamento ed in genere per tutti i soggetti terzi autorizzati ad accedere ad archivi e a documenti cartacei, alla rete comunale e ai sistemi informatici del Comune di Modena.

La procedura di seguito indicata si applica a tutte le attività di trattamento svolte dal Comune di Modena, anche con il supporto di responsabili esterni del trattamento, con riferimento alla violazione di dati personali degli interessati ( utenti, cittadini, dipendenti, fornitori, altri soggetti terzi... ).

Le prescrizioni del presente Manuale integrano le specifiche istruzioni impartite ai responsabili e agli incaricati del trattamento in materia di privacy.

Il mancato rispetto delle istruzioni di cui al presente Manuale costituisce, per i dirigenti e dipendenti, violazione del Codice di comportamento e determina, nel rispetto dei principi di gradualità e proporzionalità, l'applicazione delle sanzioni disciplinari previste dalle disposizioni di legge e dal Contratto Collettivo Nazionale di Lavoro vigente, fatto salvo comunque il diritto del Comune al risarcimento dei danni eventualmente patiti a causa della condotta del lavoratore.

Il mancato rispetto delle regole e dei divieti del presente Manuale costituisce, per i responsabili esterni del trattamento, violazione degli obblighi contrattuali. Al momento della nomina , il responsabile esterno del trattamento dichiara di avere preso visione del presente Manuale e degli adempimenti in esso previsti.

Al presente Manuale verrà data la massima pubblicità, mediante la pubblicazione sulla intranet.

## 3 . DATO PERSONALE

Dato personale è qualsiasi informazione riguardante una persona fisica identificata o identificabile ( " interessato " ) . Si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con riferimento ad un identificativo come il nome, un numero di identificazione, un identificativo on line, dati relativi all'ubicazione o uno o più elementi della sua identità fisica, genetica, psichica, economica, culturale o sociale.

Il concetto di dato personale ricomprende qualunque contenuto che fornisca informazioni su una persona fisica. Non è unicamente un nome, un cognome, una data di nascita, un numero di telefono, l'indirizzo di posta elettronica, un dato testuale, ma, a titolo puramente esemplificativo, anche un'immagine, la registrazione di una voce, una videoripresa , un numero di targa .

## 4. VIOLAZIONE DEI DATI PERSONALI ( DATA BREACH )

La violazione della sicurezza dei dati personali comporta pertanto, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione o l'accesso non autorizzati ai dati personali trasmessi, conservati o comunque trattati.

In tal senso si ha:

- **"*distruzione* "** dei dati quando i dati non esistono più o non esistono più in una forma che sia utile al titolare del trattamento;
- ***" danno "*** quando i dati personali sono stati modificati, corrotti o non sono più completi;
- ***" perdita"*** quando il titolare ha perso il controllo o il possesso dei dati o non può più accedervi
- ***" trattamento non autorizzato o illecito "*** quando viene effettuata una divulgazione non autorizzata di dati personali, l'accesso da parte di destinatari non autorizzati a ricevere i dati o, in genere, qualsiasi forma di trattamento in violazione delle disposizioni normative o dell'Ente in materia di privacy.

Si ha

***Perdita di confidenzialità*** in caso di divulgazione o accesso non autorizzato o accidentale ai dati ( ad esempio nel caso di dati personali che, per errore o a seguito di un attacco informatico, vengono pubblicati o che vengono inviati ad un indirizzo sbagliato )

***Perdita dell'integrità*** in caso di alterazione non autorizzata o accidentale dei dati

***Perdita della disponibilità*** in caso di accidentale o non autorizzata perdita di accesso o distruzione dei dati personali ( ad esempio nel caso di dati cancellati accidentalmente o da persona non autorizzata; nel caso di interruzione di corrente significativa che comporta la perdita temporanea della disponibilità di dati personali)

Una violazione può riguardare contemporaneamente la confidenzialità, l'integrità e la disponibilità dei dati personali.

## 5. DATA BREACH PRESSO UN RESPONSABILE ESTERNO DEL TRATTAMENTO

Il soggetto che agisce in qualità di Responsabile esterno delle attività di trattamento per conto e nell'interesse del Comune di Modena, deve informare l'Ente della violazione dei dati personali, , senza ingiustificato ritardo e comunque entro 24 ore dal momento in cui ne ha conoscenza , compilando la Scheda Segnalazione ( Allegato A ) e inviandola, se possibile via Pec, al seguente indirizzo :

responsabileprotezionedati@comune.modena.it

Successivamente il Responsabile è tenuto a fornire al Comune tutta la collaborazione necessaria per consentirgli di adempiere agli obblighi previsti dalla normativa in materia di data breach.

## 6. GESTIONE DEL DATA BREACH

FASE 1 - SEGNALAZIONE AL TITOLARE

Chi, nel trattare dati personali di cui è titolare il Comune di Modena, viene a conoscenza di eventi anomali che possano determinare la violazione di dati stessi, è tenuto a segnalarlo **tempestivamente** a responsabileprotezionedati@comune.modena.it utilizzando il modello allegato A .

La segnalazione può provenire :

- da dipendenti del Comune e, in genere, da tutti i soggetti a qualunque titolo autorizzati ad accedere ad archivi e documenti cartacei, alla rete comunale e ai sistemi informatici del Comune di Modena;
- dal Responsabile esterno del trattamento :

La segnalazione può altresì provenire da soggetti esterni ( es. interessati )

FASE 2 - ANALISI DELLA SEGNALAZIONE E VALUTAZIONE DELL' EVENTO

**A ) Analisi preliminare della segnalazione**

Il Titolare e il Responsabile per la protezione dei dati ( d'ora in avanti DPO ), con la collaborazione del Responsabile del Settore a cui appartiene l'Ufficio Privacy , del Responsabile dei Settore Smart City, Servizi demografici e Partecipazione, nel caso di violazione per via informatica o telematica, e degli uffici/ servizi coinvolti dalla violazione, effettua un'analisi preliminare della segnalazione al fine di raccogliere i dati concernenti l'anomalia. Viene richiesta a tale scopo la compilazione della Parte I della Scheda Violazione - allegato B - contenente le seguenti informazioni:

- Fonte della segnalazione
- Data e ora in cui si è venuti a conoscenza della violazione
- Descrizione della violazione
- Data evento anomalo
- Luogo evento anomalo
- Tipo di violazione
- Causa della violazione
- Dispositivo oggetto della violazione
- Ubicazione del dispositivo
- Numero persone colpite dalla violazione dei dati personali
- Categorie di interessati
- Volume dei dati personali oggetto della violazione
- Categorie di dati coinvolti nella violazione
- Ulteriori soggetti coinvolti nel trattamento

**B) Verifica della segnalazione**

Il Titolare e il DPO, con la collaborazione degli uffici/ servizi coinvolti dalla violazione, del Responsabile del Settore a cui appartiene l'Ufficio Privacy, e del Responsabile dei Settore Smart City, Servizi demografici e Partecipazione, nel caso di violazione per via informatica o telematica, sulla base delle informazioni raccolte, verificano se c'è stata violazione dei dati personali. ( Parte II Scheda Violazione - all. B )

Qualora l'evento segnalato non costituisca violazione dei dati personali, la relativa motivazione viene riportata nella Scheda violazione

Nel caso si accerti l'esistenza di una violazione di dati personali, vengono esaminate le circostanze specifiche della violazione stessa per valutarne la gravità , stabilendo, in primo luogo, il tipo di violazione :

- perdita della confidenzialità ( divulgazione o accesso non autorizzato o accidentale ai dati )
- perdita dell'integrità ( alterazione non autorizzata o accidentale dei dati )
- perdita della disponibilità ( accidentale o non autorizzata perdita di accesso o distruzione dei dati personali )

Si procede successivamente alla valutazione del rischio sulla base della probabilità e della gravità dell'impatto della violazione sulle persone interessate, con particolare attenzione

1) a fattori di rischio quali:

- *Carattere particolare de dati* ( idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, i dati genetici, dati relativi alla salute o alla vita sessuale, o relative alla salute o alla vita sessuale, a condanne penali, a reati o relative misure di sicurezza, dati che riguardino valutazioni di aspetti personali quali il rendimento professionale, la situazione economica, gli interessi personali, la salute, il comportamento, l'ubicazione e gli spostamenti, al fine di creare o utilizzare profili personali);

- *Profilazione personale* ( rendimento professionale, situazione economica, interessi personali, condizioni di salute, comportamento, ubicazione, spostamenti … )

- *Quantità dei dati personali compromessi dalla violazione*

- *Numero degli interessati*

- *Facilità di identificazione degli interessati*

- *Particolarità delle conseguenze per gli interessati ( es. minori )*

- - *Gravità delle conseguenze per gli interessati (* ad esempio occorre valutare se i dati sono nella disponibilità di persone sconosciute o di persone conosciute, dalle quali il titolare può ragionevolmente aspettarsi che non li leggerà e rispetterà le istruzioni per restituirli . Si deve altresì tener conto della permanenza o della temporaneità delle conseguenze )

2) ai potenziali effetti negativi per gli interessati quali :

- *Discriminazioni*

- *Furto o usurpazione di identità*

- *Perdite finanziarie*

- *Pregiudizio alla reputazione*

- *Conoscenza da parte di terzi non autorizzati*

*- Perdita di riservatezza di dati personali protetti da segreto d'ufficio*

*- Decifratura non autorizzata della pseudonomizzazione*

*- Danno economico o sociale significativo*

*- Privazione o limitazione di diritti o di libertà*

*- Impossibilità dell'interessato di esercitare i propri diritti sul trattamento dei suoi dati personali*

*- Danni fisici, materiali o immateriali, alle persone fisiche*

Saranno inoltre valutate, come variabili qualitative dell'impatto temuto, le seguenti eventuali condizioni:

a) che si tratti di dati idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché di dati genetici, dati relativi alla salute o dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza;

b) che si tratti di dati relativi a valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di 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, al fine di creare o utilizzare profili personali;

c) che si tratti di dati di persone fisiche vulnerabili, in particolare minori;

d) che il trattamento riguardi una notevole quantità di Dati Personali;

e) che il trattamento riguardi un vasto numero di interessati.

Il livello di rischio, in relazione alla gravità del rischio e alla probabilità che il rischio si verifichi , può essere:

- trascurabile
- basso
- medio
- alto

FASE 3 - DEFINIZIONE DELLE MISURE DA ADOTTARE PER PORRE RIMEDIO ALLA VIOLAZIONE DEI DATI

Il Titolare del trattamento e il DPO e , con la collaborazione della Responsabile del Settore Risorse umane e Affari istituzionali e del Responsabile dei Settore Smart City, Servizi demografici e Partecipazione nel caso di violazione per via informatica o telematica, individuano tempestivamente le misure che consentano di minimizzare le conseguenze negative della violazione e le indicano nella Scheda Violazione ( Parte III Scheda Violazione - all. B )

FASE 4 - SEGNALAZIONE ALL'AUTORITÀ GARANTE E COMUNICAZIONE AGLI

INTERESSATI

**A ) Notifica all' Autorità Garante**

La violazione di dati personali deve essere notificata dal Titolare all'Autorità Garante ( Garante della privacy ) , senza ingiustificato ritardo e , ove possibile, entro 72 ore dal momento in cui il Titolare ne è venuto a conoscenza. ( Parte IV Scheda Violazione - all. B ) .

Si considera che il Titolare sia "a conoscenza della violazione nel momento in cui è messo a corrente del fatto che si è verificato un incidente di sicurezza che ha portato alla violazione di dati personali. Il momento esatto dipenderà dalle circostanze: in alcuni casi la violazione potrà essere evidente fin dall'inizio, in altri casi potrebbe essere necessario del tempo per stabilire se i dati personali siano stati compromessi.

E' importante porre l'accento sulla tempestività con cui deve essere effettuata l'indagine sull'incidente al fine di stabilire se c'è stata violazione dei dati personali e, in caso affermativo, prendere le misure adeguate ed effettuare, se necessario, la notifica.

Se si superano le 72 ore, la notifica deve essere corredata dalle ragioni del ritardo .

Vanno notificate unicamente le violazioni di dati personali che possono avere effetti avversi significativi sulla libertà e sui diritti degli interessati , causando danni fisici materiali o immateriali. Non è soggetta a notifica la violazione se si è in grado di dimostrare che è improbabile che la violazione stessa presenti un rischio per i diritti e le libertà delle persone fisiche ( ad esempio, la divulgazione di dati personali già oggetto di pubblicazione ) Si considera probabile il rischio relativo alla violazione di dati personali sensibili, di salute o giudiziari

In caso di dubbio è più prudente effettuare comunque la notifica.

Occorre tener presente che , anche qualora inizialmente la notifica non venga effettuata perchè si valuta che non esista un rischio probabile per i diritti e le libertà delle persone fisiche, nel caso in cui la situazione cambi nel corso del tempo , occorre rivalutare il rischio e procedere eventualmente alla notifica.

La notifica viene inviata dal Titolare all'indirizzo protocollo@pec.gpdp.it utilizzando l'apposito modello ( Allegato C ) , con firma digitale o allegando la fotocopia della carta di identità del firmatario. L'oggetto del messaggio deve necessariamente portare la dicitura " Notifica violazione dati personali " e opzionalmente la denominazione del titolare del trattamento

Se non è possibile fornire all'Autorità Garante, contestualmente alla notifica, tutte le informazioni richieste, il Titolare potrà informare quest'ultimo, indicandone le motivazioni, che non dispone ancora di tutte le informazioni e che fornirà ulteriori dettagli in un momento successivo, senza ingiustificato ritardo, non appena questi saranno disponibili.

**B) Comunicazione agli interessati**

Quando, nella Scheda Violazione ( Allegato B ) il rischio è classificato come alto, il Titolaredeve informare gli interessati della violazione in quanto quest'ultima è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

Sia nel caso in cui si provveda alla comunicazione, sia nel caso in cui non si provveda, deve essere compilata la parte relativa *( Comunicazione agli interessati )* della Parte IV della Scheda Violazione - all. B .

La comunicazione deve essere inviata all'interessato senza ingiustificato ritardo attraverso il canale ritenuto più idoneo ( e.mail, SMS, comunicato pubblicitario .. ) .

La comunicazione di Data Breach deve essere redatta utilizzando il modello allegato D e , deve

essere intellegibile, concisa e trasparente e facilmente accessibile, adottando, se possibile, la stessa lingua parlata dall'interessato.

Non è richiesta la comunicazione agli interessati se si è in grado di dimostrare che è soddisfatta una delle seguenti condizioni:

a) sono state messe in atto le misure tecniche ed organizzative adeguate di protezione dei dati e tali misure erano state applicate anche ai dati personali oggetto della violazione , in particolare quelli destinati a rendere i dati incomprensibili a chiunque non sia autorizzato ad accedervi ( sono fatti salvi i casi in cui la violazione della sicurezza ha comportato la distruzione o la perdita dei dati personali degli interessati )

b) sono state successivamente adottate misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà delle persone fisiche ( documentare le misure nella Scheda Evento )

c) la comunicazione comporterebbe sforzi sproporzionati . In tal caso si procede ad una comunicazione pubblica o a una misura simile, tramite la quale gli interessati siano informati con analoga efficacia

Se non si ha la possibilità di comunicare all'interessato la violazione, perchè non si dispone di dati sufficienti per contattarlo. l'interessato va informato non appena sia ragionevolmente possibile farlo

Va tenuto presente che, sebbene la comunicazione possa inizialmente non essere richiesta se non vi è alcun rischio per i diritti e le libertà delle persone fisiche, la situazione potrebbe cambiare nel corso del tempo e il rischio dovrebbe essere rivalutato.

## FASE 5 - REGISTRO DELLE SEGNALAZIONI E DEI DATA BREACH

Le segnalazioni vengono conservate nel rispetto delle disposizioni del presente Manuale.

Per ogni violazione segnalata, il Titolare , sulla base delle indicazioni contenute nella scheda Violazione – allegato B - compila il Registro delle violazioni secondo il modello E allegato.

Ad integrazione di quanto riportato nel Registro, il DPO raccoglie e conserva la Scheda Evento, la scheda Violazione, l'eventuale notifica all'Autorità Garante e la comunicazione agli interssati e tutti i documenti relativi ad ogni segnalazione , compresi quelli inerenti le circostanze dell'evento, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione è resa disponibile all'Autorità Garante per le verifiche di competenza.

Il Registro delle segnalazioni e la documentazione raccolta vengono conservata per 2 anni.