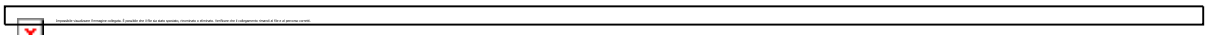
COMUNE DI CROCETTA DEL MONTELLO



TRATTAMENTO DATI PERSONALI

SOMMARIO

Allegato 1)

INDIRIZZI E LINEE GUIDA PER L'APPLICAZIONE DEL REGOLAMENTO UE 2016/679 PROTEZIONE DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI

Art. 1. TITOLARE E DESIGNATI

1. Il Comune è l'autorità pubblica titolare del trattamento dei dati ai sensi del GDPR ed esercita le proprie prerogative, poteri e doveri attraverso gli organi ed il personale dell'Ente secondo le competenze, prerogative e le responsabilità stabilite dalle disposizioni organizzative in materia ed in particolare:

- il **Sindaco pro tempore**, in quanto legale rappresentante dell'Ente, procede alla designazione e nomina degli organismi monocratici e collegiali previsti dalla normativa e rimessi alla determinazione del titolare con particolare riferimento al DPO, Responsabili esterni, Designati interni, Gruppo di Lavoro GDPR, Gruppo di Risposta alle Violazioni dei Dati ed eventuali ulteriori gruppi di lavoro o team di progetto a supporto delle attività specifiche dei quali dovesse ravvisare la necessità;
- **Il Segretario comunale e le Posizioni Organizzative**, nell'ambito delle dotazioni e risorse messe a disposizione e secondo gli indirizzi degli atti di pianificazione e programmazione dell'Ente e nel rispetto della disciplina di settore, provvedono alla corretta adozione da parte dell'Ente di tutti gli atti a rilevanza esterna, ivi compresi gli incarichi, gli affidamenti, le convenzioni e gli accordi per la corretta attuazione di quanto previsto dal GDPR;
- **il personale assegnato agli uffici e servizi** svolge le funzioni di designato del titolare in relazione ai trattamenti ed ai poteri/doveri previsti dal proprio ruolo organizzativo e nel rispetto delle indicazioni formali ed informali disposte dal Titolare e dal responsabile del servizio.

Art. 2. GRUPPO DI LAVORO GDPR

1. E' istituito un gruppo di lavoro permanente in materia di adattamento alle norme del GDPR composto da:

- segretario comunale (coordinatore e verbalizzante);
- posizioni organizzative dei servizi;
- un referente del servizio ICT del Comune o di società strumentale partecipata eventualmente invitato quale supporto tecnico per le problematiche di sicurezza tecnologica
- il DPO eventuale invitato in occasione della trattazione di particolari tematiche.

2. Le riunioni del gruppo sono tracciate, verbalizzate e conservate agli atti dell'Ente.

3. Il gruppo di lavoro definisce ed aggiorna in particolare:

- un programma permanente di informazione e formazione del personale;
- le priorità di intervento per l'adattamento al GDPR;
- le misure da adottare per il rispetto della normativa;
- la modulistica uniforme sia ad uso esterno che ad uso interno (informativa, consenso, comunicazioni, registri ecc...);
- la redazione e l'aggiornamento dell'elenco dei responsabili e dei designati.

Art. 3. GRUPPO DI RISPOSTA ALLE VIOLAZIONI DEI DATI

1. In considerazione della possibilità si verifichino eventi di cd. Data breach, viene istituito il Gruppo di Risposta alle Violazioni dei Dati che è costituito da:
- Sindaco del Comune
- Segretario comunale
- da una o più persone esperte e competenti nel settore ITC
- dalle posizioni organizzative
- dal DPO.

Per la puntuale disciplina delle attività del Gruppo si rinvia integralmente alle previsioni della "procedura di gestione della violazione dei dati" approvata con medesima deliberazione di Giunta Comunale n….del…….**Allegato 2)**

Art. 4. ACCOUNTABILITY – RESPONSABILIZZAZIONE

1. Il titolare ed i designati sono chiamati ad assicurare il rispetto dei principi previsti dal GDPR, con particolare riferimento all'art. 5 Regolamento UE 2016/679 e s.m.i..
2. A tal fine l'Amministrazione provvederà all'adozione di opportune disposizioni organizzative e procedurali per ogni fase dell'attività, procedendo all'analisi delle attività che comportano trattamento e circolazione di dati personali e, sulla base di tale valutazione, all'identificazione dei possibili rischi per i diritti e le libertà delle persone coinvolte al fine di predisporre le misure di sicurezza necessarie per porre in essere una reale protezione dei dati ed effettuare un trattamento lecito, sicuro e trasparente.
3. Il Comune si impegna quindi al rispetto dei criteri dettati dal GDPR quale guida all'applicazione della disciplina, in particolar modo nell'attuazione di una politica di "privacy by design and by default "(privacy by design è volto a tutelare il dato protetto "sin dal momento della progettazione"; mentre il principio di privacy by default è volto a tutelare la vita privata per "impostazione predefinita") nonché di minimizzazione del rischio inerente al trattamento (ovvero del rischio di conseguenze negative e della possibilità di mitigarne l'impatto sui diritti degli interessati).

Art. 5. REGISTRO DELLE ATTIVITA' DI TRATTAMENTO

1. Il Titolare, ovvero altro soggetto dal medesimo individuato, cura l'aggiornamento del registro delle attività di trattamento di cui all'art. 30 del GDPR, adeguando la versione iniziale già adottata, mediante acquisizione dai responsabili dei servizi i dati e le informazioni sulle tipologie di trattamento secondo il modello.
2. Il registro è aggiornato tempestivamente in occasione della variazione dei trattamenti e comunque almeno una volta ogni 12 mesi, senza necessità di ulteriore formale approvazione da parte della Giunta comunale, acquisendo data certa ed approvazione con la protocollazione.
3. Il registro è in formato elettronico, facilmente accessibile a tutti i soggetti autorizzati alla sua redazione ed è fruibile direttamente, senza intermediazione, da parte del DPO e dell'autorità di controllo.

Art. 6. PRINCIPIO DI COLLABORAZIONE

1. Tutto il personale coinvolto nelle procedure di trattamento dati, a qualunque livello e ruolo:

- collabora con il titolare, il DPO, l'autorità di controllo (Garante) ed eventuali ulteriori soggetti addetti alla vigilanza, controllo ed attuazione delle disposizioni in materia di trattamento dei dati fornendo la massima e tempestiva collaborazione con particolare riferimento al rispetto dei principi previsti dal GDPR
- fornisce tempestivamente informazioni su potenziali pericoli, rischi, o violazioni dei dati personali anche al fine di consentire l'esercizio dei compiti di cui all'art. 33 e 34 del GDPR (cosiddetto "data breach")
- collabora con i responsabili del trattamento, secondo le istruzioni fornite dal titolare, al fine di garantire le citate finalità e nel rispetto degli obblighi di segretezza e riservatezza.

2. Il rispetto dei principi in materia e dei compiti ed adempimenti previsti dal presente provvedimento verrà valutato in sede di raggiungimento degli obiettivi e/o negli altri casi di responsabilità del personale a vario titolo coinvolto, secondo le disposizioni normative, regolamentari e contrattuali vigenti.

Allegato 2)

PROCEDURA DI GESTIONE DELLE VIOLAZIONI DEI DATI

PREMESSA

La presente procedura, viene applicata in ottemperanza al rispetto delle misure minime di sicurezza adottate dal Comune di Crocetta del Montello.

I dati informatici devono essere contenuti in un sistema Data Base /Gestionale possibilmente criptato, con profilazione utenti e credenziali di accesso univoche per ogni utente.

Si rimanda a tal proposito al "modulo di implementazione" delle misure minime di sicurezza adottato.

1. CAMPO DI APPLICAZIONE E DESTINATARI

Scopo della presente procedura è di descrivere le attività da svolgersi in caso di violazione di dati personali (c.d. Data Breach).

La Procedura definisce i principi e le azioni generali per gestire la violazione dei dati personali e adempiere agli obblighi relativi alla notifica alle Autorità di Controllo e ai singoli individui, come richiesto dal Regolamento (UE) 2016/679 e s.m.i..

Tutto il personale a tempo indeterminato e determinato, i collaboratori e terzi che lavorino o agiscano per conto dell'Ente, devono obbligatoriamente essere a conoscenza e seguire la presente procedura in caso di violazione dei dati personali.

A tal fine l'Ente rende idonea pubblicità mediante pubblicazione del presente documento sul sito istituzionale e diffusione via email dello stesso ai propri dipendenti\consulenti\collaboratori o terzi che agiscano\lavorino per l'Ente non appena prendano servizio.

2. DOCUMENTI DI RIFERIMENTO

- Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio Europeo del 27 Aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE)
- Politica sulla Protezione dei Dati Personali;
- Guidelines on Personal data breach notification under Regulation 2016/679 - ARTICLE 29 DATA FROTECTION WORKING FARTY;
- Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche
- 2 luglio 2015 (Pubblicato sulla Gazzetta Ufficiale n. 179 del 4 agosto 2015).

3. DEFINIZIONI

Le seguenti definizioni ed i termini utilizzati in questo documento, sono tratte dall'articolo 4 del Regolamento (UE) 2016/679 ovvero afferiscono ad elementi disciplinati nel presente documento:

4. «dato personale»: 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;
5. «trattamento»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati ed applicate ai dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
6. «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; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri. Per l'Ente «titolare del trattamento» è il rappresentante legale pro tempore: il Sindaco
7. «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. Per il Comune di Crocetta del Montello «responsabile del trattamento» è la qualificazione di tutti i soggetti che trattano dati personali per conto del titolare del trattamento quali: altre autorità pubbliche, la società partecipata in house providing, le software house utilizzate, le società di elaborazione dei dati comunque denominate.
8. «DPO data protection officer» (o responsabile della protezione dei dati RDP) è un consulente tecnico designato dal Titolare del Trattamento, le cui competenze sono disciplinate dalla norma GDPR;
9. «violazione dei dati personali»: la violazione di sicurezza che comporta 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;
10. «Gruppo di Risposta alle Violazioni dei Dati»: esplica la sua funzione consultiva in caso di c.d. Data Breach ed è costituito dal Sindaco, dal Segretario Generale, dall'esperto informatico del Comune o di Società strumentale partecipata e dal DPO.
11. «autorità di controllo»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 5 1 (Garante dei dati personali)

4. GRUPPO DI RISPOSTA ALLE VIOLAZIONI DEI DATI

Il Gruppo di Risposta alle Violazioni dei Dati è costituito dal:

- Sindaco
- Segretario comunale
- persone esperte e competenti nel settore come l'esperto informatico del Comune o della Società strumentale partecipata
- DPO.

E' il Titolare del trattamento nella persona del legale rappresentante, dell'Ente che dovrà provvedere con proprio atto alla nomina dei componenti del Gruppo di Risposta alle Violazioni dei Dati. Il Gruppo deve essere nominato a prescindere dal fatto che una violazione sia avvenuta o meno.
Il Segretario comunale dirige e presiede le attività del Gruppo. In caso di assenza o impedimento ne farà le veci di lui il sostituto.
Le riunioni del gruppo possono svolgersi anche in audio\video conferenza e sono valevoli anche in assenza

di alcuni componenti.
Il gruppo può essere convocato ad esplicitare la propria funzione consultiva in ordine a qualsiasi sospetta o presunta violazione dei dati personali.
In tal senso il gruppo deve garantire la prontezza necessaria per una risposta alla violazione dei dati personali, insieme alle risorse e alla preparazione necessarie[1].
La missione del gruppo è di fornire una risposta immediata, efficace ed esperta a qualsiasi sospetta, presunta o effettiva violazione dei dati personali che riguardi l'Amministrazione.
Se ritenuto opportuno e necessario, il Segretario comunale può coinvolgere nelle attività del gruppo anche ulteriori esperti interni o esterni allo scopo di gestire una specifica violazione dei dati personali (ad esempio, un fornitore di sicurezza informatica per svolgere attività di informatica forense o un'agenzia di comunicazione esterna per assistere l'Ente in necessità di comunicazione di crisi).
Il Gruppo di Risposta alle Violazioni dei Dati, può trattare più di una violazione dei dati personali sospetta, presunta o effettiva alla volta.
Il Gruppo di Risposta alle Violazioni dei Dati presta ai sensi di legge la propria attività consulenziale in ordine a violazioni di dati personali presunte, sospette o effettive. A tal fine ciascun componente rende disponibili i propri dati, compresi quelli personali di recapito, al Segretario comunale, nonché agli altri membri del gruppo. Le informazioni di contatto acquisite verranno pertanto a tal fine archiviate ed utilizzate unicamente per lo scopo previsto.

5. COMPITI DEL GRUPPO

Il Gruppo di Risposta alle Violazioni dei Dati, coadiuva il Titolare del trattamento nella risoluzione delle questioni relative ad un evento di cd "*data breach*" sospetto, presunto o effettivo, esprimendosi in relazione ai seguenti punti (elenco esemplificativo non esaustivo) ove applicabili:

4. Determinare se la violazione di cui trattasi debba o meno essere considerata una violazione dei dati personali.
5. Convalidare / assegnare un livello di urgenza alla violazione dei dati personali;
6. Assicurare che sia avviata, condotta, documentata e conclusa un'indagine corretta e imparziale (compresa l'informatica forense, se necessario);
7. Identificare i requisiti per la risoluzione e monitorare la soluzione;
8. Coordinarsi con le autorità competenti;
9. Coordinare le comunicazioni interne ed esterne;
10. Assicurarsi che gli interessati siano adeguatamente informati.

Il Gruppo di Risposta alle Violazioni dei Dati, viene attivato a seguito di un "ammissibilità preventiva" di un potenziale "*data breach*", valutato in via informale dall'referente informatico dell'Ente congiuntamente al D.P.O

6. PROCESSO DI RISPOSTA ALLE VIOLAZIONI DEI DATI

Il Processo di Risposta alle Violazioni dei Dati viene avviato quando il dipendente viene a conoscenza che una sospetta, presunta o effettiva violazione dei dati personali si sia verificata. Di detto evento il dipendente deve dare immediata comunicazione al proprio Responsabile (Posizione Organizzativa o Dirigente utilizzando l'apposito modello allegato **All. A).**
Il Responsabile provvederà a dare comunicazione del sospetto, presunto o effettivo "*data breach*" al referente informatico dell'ente che congiuntamete al D.P.O. verificheranno l'ammissibilità preventiva del presunto "*data breach*". Qualora l'ammissibilità del presunto "*data breach*" sia positiva sarà informato il Segretario comunale che provvederà immediatamente a convocare il Gruppo di Risposta alle Violazioni dei

Dati.
Il Segretario comunale, in quanto responsabile del Gruppo di Risposta alle Violazioni dei Dati, è incaricato della raccolta delle decisioni del gruppo principale, che costituiscono documentazione che potrebbe essere esaminata dalle autorità di controllo e, in quanto tale, da redigersi in modo preciso ed accurato per garantire la tracciabilità e la responsabilizzazione, ferma restando la competenza e responsabilità del Titolare del trattamento in ordine all'assunzione della decisione definitiva.

7. FASI DEL PROCESSO

1. Il dipendente dell'Amministrazione che si accorge di una violazione o perdita dei dati (informatici o cartacei) informa immediatamente via email il suo Responsabile (Posizione Organizzativa) relazionando quanto segue:
    a. denominazione della/e banca/banche dati oggetto di "*data breach*";
    b. breve descrizione della violazione dei dati personali ivi trattati;
    c. quando si è verificata la violazione dei dati personali trattati nell'ambito della banca dati;
    d. dove è avvenuta la violazione dei dati (specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili).
2. Il Responsabile (Posizione Organizzativa) informa dell'evento il referente informatico dell'ente che congiuntamete al D.P.O. verificheranno l'ammissibilità preventiva del presunto "*data breach*". Qualora l'ammissibilità del presunto "*data breach*" sia positiva sarà informato il Segretario comunale che, assunte eventuali ulteriori informazioni qualora ritenute necessarie, convoca il Gruppo di Risposta alle Violazioni dei Dati.
3. Il Gruppo di Risposta alle Violazioni dei Dati procede tempestivamente alla seguente valutazione:
    a. Tipo di violazione
        - Lettura (presumibilmente i dati non sono stati copiati)
        - Copia (i dati sono ancora presenti sui sistemi del titolare)
        - Alterazione (i dati sono presenti sui sistemi ma sono stati alterati)
        - Cancellazione (i dati non sono più sui sistemi del titolare 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
    b. Dispositivo oggetto della violazione
        - Computer
        - Rete
        - Dispositivo mobile
        - file o parte di un file
        - Strumento di backup
        - Documento cartaceo
        - Altro da specificare
    c. Quante persone sono state colpite dalla violazione dei dati personali trattati nell'ambito della banca dati;
    d. Livello di gravità della violazione dei dati personali trattati nell'ambito della banca dati;
    e. Analisi delle misure tecniche e organizzative applicate ai dati oggetto di violazione.

4. Al termine della valutazione effettuata dal Gruppo di Risposta alle Violazioni dei Dati, il Titolare del Trattamento in persona del Sindaco quale legale rappresentante pro tempore, decide quanto segue:
    a. se comunicare o meno agli interessati l'evento di "*data breach*"

b. le misure tecnologiche e organizzative assunte o da assumere per contenere la violazione dei dati e prevenire simili violazioni future.

5. Sulla base delle indicazioni raccolte e con il supporto del DPO, il Titolare del Trattamento procede alla compilazione della modulistica prevista dall'Autorità di Controllo (Garante per la protezione dei dati), e nel tempo stabilito, invia a mezzo pec all'indirizzo databreach.pa@pec.gpdp.it le violazioni dei dati personali ("*data breach*")

8. NOTIFICA DI VIOLAZIONE DI DATI PERSONALI EFFETTUATA DAL RESPONSABILE DEL TRATTAMENTO

Qualora la violazione dei dati personali o la sospetta violazione dei dati riguardi i dati personali elaborati per conto di terzi, il Responsabile del trattamento informa il rispettivo titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza dell'evento di "*data breach*".

La notifica di cui sopra deve almeno:

a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione
b) comunicare il nome e i dati di contatto del DPO o di altro punto di contatto presso cui ottenere più informazioni
c) descrivere le probabili conseguenze della violazione dei dati personali
d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per pone rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi

Il titolare del trattamento, coadiuvato dal Segretario comunale e dal DPO, documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di porre in essere le proprie attività di verifica in ordine al rispetto dei dettami di cui al GDPR.

9. NOTIFICA DI UNA VIOLAZIONE DI DATI PERSONALI ALL'AUTORITA' DI CONTROLLO (GARANTE PER LA PROTEZIONE DEI DATI)

In caso di violazione dei dati personali, il titolare del trattamento, coadiuvato dal D.P.O., notifica all' Autorità di Controllo (Garante per la protezione dei dati) la violazione dei dati personali ("*data breach*") senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.
Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.
Nei casi più gravi, quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del trattamento è obbligato a comunicare la violazione anche alla persona a cui si riferiscono i dati (c.d. Interessato), senza ingiustificato ritardo, così come meglio di seguito disciplinato all'art. 9 del presente documento.
In caso di violazione o sospetta violazione dei dati personali trattati dall'Amministrazione, il Titolare del Trattamento, coadiuvato dal Gruppo di Risposta alle Violazioni dei Dati avente funzione tecnico-consultiva, provvederà ad assumere le seguenti decisioni:

a) stabilire se la violazione dei dati personali debba essere segnalata all'Autorità di Controllo "Garante per la protezione dei dati" ed in caso affermativo provvedere alla relativa notifica senza indebito ritardo, e non oltre le 72 ore, qualora questa violazione dei dati personali sia suscettibile di

presentare un rischio per i diritti e le libertà degli interessati colpiti dalla violazione dei dati personali.

b) stabilire, a seguito della Valutazione d'Impatto sulla Protezione dei Dati avente ad oggetto l'attività di trattamento interessata dalla violazione dei dati, se sia o meno necessario provvedere alla notifica della violazione agli interessati

La notifica deve almeno:

a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
b) comunicare il nome e i dati di contatto del DPO o di altro punto di contatto presso cui ottenere più informazioni;
c) descrivere le probabili conseguenze della violazione dei dati personali;
d) 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 anche, se del caso, per attenuarne i possibili effetti negativi;

Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite all'Autorità Garante in fasi successive senza ulteriore ingiustificato ritardo.
Il titolare del trattamento, coadiuvato dal Segretario comunale e dal DPO, documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di porre in essere le proprie attività di verifica in ordine al rispetto dei dettami di cui al GDPR.

10. COMUNICAZIONE DI VIOLAZIONE DI DATI PERSONALI: IL TITOLARE DEL TRATTAMENTO DEI DATI ALL'INTERESSATO

Il Titolare del Trattamento dei dati personali, in collaborazione con il Gruppo di Risposta alle Violazioni dei Dati Personali, deve valutare se la violazione dei dati personali può comportare un rischio elevato per i diritti e le libertà dell'interessato. In caso affermativo, il Titolare del Trattamento deve informare gli interessati senza indebito ritardo.
La comunicazione agli interessati deve essere scritta in un linguaggio chiaro e semplice e deve contenere:

a) il nome e i dati di contatto del DPO o di altro punto di contatto presso cui ottenere più informazioni;
b) la descrizione delle probabili conseguenze della violazione dei dati personali;
c) la descrizione delle le misure adottate o di cui il titolare del trattamento propone l'adozione per porre rimedio alla violazione dei dati personali e, se del caso, per attenuarne i possibili effetti negativi.

Se il numero di interessati è sproporzionatamente elevato per poter informare singolarmente tutti i soggetti in questione, il Titolare dei dati personali adotta le misure necessarie per garantire che le persone interessate siano informate utilizzando canali appropriati e pubblicamente disponibili.
Non è richiesta la comunicazione all'interessato se viene soddisfatta una delle seguenti condizioni:

a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;

c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia

11. RESPONSABILIZZAZIONE

Qualsiasi soggetto che commetta violazioni di legge in merito alla procedura descritta, sarà sottoposto alle misure disciplinari interne, sino alla risoluzione del rapporto di lavoro. Qualora si ravvisi che le sue azioni, siano in violazione di legge, potrà incorrere nelle responsabilità civili o penali previste.

12. GESTIONE DELLE REGISTRAZIONI SULLA BASE DEL PRESENTE DOCUMENTO

Nome del documento	Tempo di archiviazione
Elenchi delle persone da chiamare e sostituzioni	Permanente
Informazioni di contatto	Permanente
Decisioni documentate del Gruppo di Risposta alle Violazioni dei dati	5 anni
Comunicazione di una Violazione dei Dati	5 anni
Registro delle Violazioni di Dati	Permanente

E' istituito il Registro delle violazioni dei dati come da schema allegato al presente documento **All. B)**

13. VALIDITA' E GESTIONE DEL PRESENTE DOCUMENTO

Questo documento è stato approvato con deliberazione di Giunta Comuale n. del 6.11.2018 ed è divenuto efficace a partire dal 6.11.2018

Il responsabile per questo documento è il Titolare del trattamento, il quale deve controllare il documento con frequenza almeno annuale ed, ove necessario, provvedere alle eventuali modificazioni.

Con successivi provvedimenti sindacali si procederà alla nomina del Gruppo di lavoro GDPR e del Gruppo di risposta alla violazione dei dati come previsto dal presente atto.