COMUNE DI LAMEZIA TERME
(provincia di Catanzaro)

PROCEDURA

PER LA GESTIONE DEI ***DATA BREACH***

AI SENSI DEL GDPR (REGOLAMENTO EUROPEO 679/2016)

Approvata con deliberazione di Giunta Comunale n. 74 del 07.03.2023

PREMESSA

Il Regolamento Europeo sulla protezione dei dati n. 679/2016 (di seguito "GDPR"), entrato in vigore definitivamente il 25 maggio 2018, ha introdotto l'obbligo di notificare all'Autorità di controllo nazionale (Garante Privacy) incidenti sulla sicurezza che comportino la violazione dei dati personali (data breach) e di rendere nota la violazione stessa alle persone fisiche interessate.

La violazione dei dati personali è da intendersi come 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 tale da impedire al Titolare del trattamento di garantire l'osservanza dei principi relativi al trattamento dei dati personali di cui all'articolo 5 del GDPR.

Il GDPR impone al Titolare di disporre le misure tecniche e organizzative adeguate per garantire un livello di sicurezza commisurato al rischio cui sono esposti i dati personali trattati al fine di proteggerli dalle violazioni sopra descritte.
Il presente documento si prefigge lo scopo di indicare le modalità di gestione del data breach garantendone la realizzabilità tecnica e la sostenibilità organizzativa.
La presente procedura viene approvata dalla Giunta Comunale con propria deliberazione; compete allo stesso organo definire eventuali modifiche o integrazioni.

Al fine di garantirne la massima diffusione interna ed esterna e la massima conoscibilità sulle azioni da intraprendere e sui comportamenti da adottare in caso di data breach, la presente viene pubblicata, dopo la sua approvazione, nella sezione "Amministrazione Trasparente", sottosezione di primo livello "Altri Contenuti", sottosezione di secondo livello "Privacy", nonché a garantire la conoscibilità della stessa a tutti i dipendenti dell'Ente, tramite la sua consultazione nella sezione "Amministrazione trasparente", nella sotto-sezione di primo livello "Disposizioni generali" e sotto-sezione di secondo livello "Atti generali".

NORMATIVA E DOCUMENTI DI RIFERIMENTO

- Regolamento UE 679/2016 "Regolamento generale sulla protezione dei dati personali" ("GDPR");
- D.lgs. 196/2003 "Codice in materia di protezione dei dati personali" come modificato dal D.lgs. 101/2018;
- Piano di Protezione dei dati Personali e gestione del rischio di violazione approvato con deliberazione di Giunta Municipale n. 322 del 18/12/2019;
- Art. 33 del GDPR - Notifica di una violazione dei dati personali all'Autorità di controllo;
- Art. 34 del GDPR - Comunicazione di una violazione dei dati personali all'interessato;
- le linee guida fornite dal Garante Privacy italiano raggiungibili al seguente link https://www.garanteprivacy.it/regolamentoue/databreach

GLOSSARIO E ACRONIMI

Archivio: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico.

Aree Sensibili: sono quei luoghi fisici o della Rete in cui vengono trattati dati particolari e/o dati giudiziari relativi a persone fisiche; e/o luoghi in cui vengono gestiti e consultati documenti riservati a cui è assolutamente vietato accedere se non per motivi di servizio.

Autorità di Controllo: l'Autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 GDPR.

Consenso dell'Interessato o Consenso: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'Interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

Dati Biometrici: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

Dati Comuni: sono tutti i dati personali che non appartengono alle categorie dei dati particolari e dati giudiziari;

Dati Genetici: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

Dati Giudiziari: dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza;

Dati Particolari: 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;

Dati relativi alla salute: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

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;

Destinatario/i: la persona fisica o giuridica, l'Autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le Autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate Destinatari; il trattamento di tali dati da parte di dette Autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

Device Fissi: si intendono gli strumenti informatici non facilmente removibili dal perimetro aziendale quali personal computer, server locali, stampanti affidati alle Persone Autorizzate per uso professionale;

Device Mobili: in generale si intendono quegli strumenti informatici che per loro natura sono facilmente asportabili dal perimetro aziendale quali chiavette USB, SD cards, hard disk esterni, tablet e smartphone utilizzati dalla Persone Autorizzate per uso professionale;

DPO o Data Protection Officer: è una persona fisica, nominata obbligatoriamente nei casi di cui all'art.37.1 GDPR dal Titolare o dal Responsabile del trattamento e deve possedere una conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati per assisterli nel rispetto a livello interno del GDPR;

GDPR o Regolamento: Regolamento Generale sulla Protezione dei dati personali (UE) 2016/679.

Gruppo Imprenditoriale: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;

Incaricato/i o Persona/e Autorizzata/e: si tratta dei Collaboratori autorizzati al trattamento dei dati personali sotto la diretta Autorità del Titolare e/o del Responsabile, ex artt. 4 n.10 e 29 del GDPR. Stante la definizione fornita dal Gruppo di Lavoro Articolo 29 dell'Opinione 2/2017 questa definizione ricomprende: dipendenti ed ex dipendenti, dirigenti, sindaci, collaboratori e lavoratori a partita IVA, lavoratori a chiamata, part-time, job-sharing, contratti a termine, stage, senza distinzione di ruolo, funzione e/o livello, nonché consulenti e fornitori dell'ente e, più in generale, tutti coloro che utilizzino od abbiano utilizzato Strumenti Aziendali o Strumenti Personali operino sulla Rete ovvero siano a conoscenza di informazioni aziendali rilevanti quali, a titolo esemplificativo e non esaustivo: (a) i dati personali di clienti, dipendenti e fornitori, compresi gli indirizzi di posta elettronica; (b) tutte le informazioni aventi ad oggetto informazioni confidenziali di natura commerciale, finanziaria o di strategia di business; nonché (c) i dati e le informazioni relative ai processi aziendali, inclusa la realizzazione di marchi, brevetti e diritti di proprietà industriale, la cui tutela prescinde dagli effetti pregiudizievoli che potrebbe comportare la diffusione delle medesime.

Limitazione di trattamento: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

Pseudonimizzazione: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

Responsabile del trattamento o Responsabile: la persona fisica o giuridica, l'Autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento; deve presentare garanzie sufficienti di attuare misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'interessato; nel caso specifico del Comune di Lamezia Terme, sono nominati responsabili del trattamento i dirigenti d'ufficio opportunamente individuati dal Titolare.

Rete: rappresenta il perimetro digitale dell'Ente contenente dati personali e/o informazioni riservate comprensivo della rete interna (intranet) e della rete esterna (internet) a cui ci si può collegare via rete LAN, Wi-Fi o VPN.

Strumenti Aziendali: l'insieme di Device Fissi e Device Mobili concessi in comodato d'uso dall'Ente alle Persone Autorizzate al fine di svolgere le proprie mansioni;
Strumenti Personali: i Device Mobili di proprietà delle Persone Autorizzate autorizzati ad essere impiegati per uso professionale;

Terzo: la persona fisica o giuridica, l'Autorità pubblica, il servizio o altro organismo che non sia l'interessato, il Titolare del trattamento, il Responsabile del trattamento e le Persone Autorizzate al trattamento dei dati personali sotto l'Autorità diretta del Titolare o del Responsabile;

Titolare del trattamento o Titolare: 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 o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

Trattamento o Trattato/Trattati: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

Trattamento Transfrontaliero: a) trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un Titolare del trattamento o Responsabile del trattamento nell'Unione ove il Titolare o il Responsabile siano stabiliti in più di uno Stato membro; oppure, b) trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un Titolare o Responsabile nell'Unione, ma che incide o probabilmente incide in modo sostanziale su Interessati in più di uno Stato membro;

Violazione dei dati personali ovvero Data Breach: è 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;

DEFINIZIONE DI VIOLAZIONE DEI DATI:

Classificazione delle violazioni:
Le violazioni si classificano nel seguente modo:

- Violazione della riservatezza: in caso di divulgazione dei dati personali o accesso agli stessi non autorizzati o accidentali;
- Violazione dell'integrità : in caso di modifica non autorizzata o accidentale dei dati personali;
- Violazione della disponibilità: in caso di perdita, accesso o distruzione accidentali o non autorizzati di dati personali.

La violazione può riguardare la riservatezza, l'integrità, la disponibilità dei dati personali o qualsiasi combinazione delle stesse.
Al fine di adottare le corrette procedure di segnalazione è di fondamentale importanza sapere identificare una violazione, saperne valutare la natura e le potenziali conseguenze negative.
Le violazioni dei dati personali si considerano tali se hanno un reale impatto sulla confidenzialità, integrità o disponibilità dei dati personali degli interessati (cittadini, dipendenti, soggetti terzi ecc.).

Tipologie di violazioni
All'interno della classificazione sopra indicata, quindi, si possono avere le seguenti tipologie di violazione dei dati personali:

- Distruzione: indisponibilità definitiva di dati personali con impossibilità di ripristino degli stessi. La violazione può essere determinata da una eliminazione logica (es. cancellazione dei dati) oppure fisica (es. rottura dei supporti di memorizzazione) non autorizzata e relativa impossibilità di ripristinare i dati.

- Perdita: perdita del supporto fisico di memorizzazione dei dati derivante da privazione, sottrazione, smarrimento dei dispositivi contenenti i dati degli interessati oppure dei documenti cartacei. La perdita, può riguardare anche copie od originali dei supporti contenenti i dati personali dei soggetti interessati, ed anche se temporanea può essere potenzialmente dannosa.
- Modifica: modifiche improprie dei dati degli interessati non autorizzate, effettuate al di fuori dei processi operativi di trattamento dei dati svolti dagli incaricati autorizzati, oppure modifiche con finalità fraudolente eseguite dagli incaricati autorizzati all'accesso.
- Rivelazione: distribuzione non autorizzata o impropria dei dati personali degli interessati verso terze parti (persone fisiche, persone giuridiche, gruppi di soggetti, pubblico) anche non precisamente identificabili.
- Accesso: accesso non autorizzato o improprio ai dati degli interessati. Accessi ai dati (anche in sola visualizzazione, sia in caso di accessi logici ai sistemi informatici sia agli archivi cartacei) avvenuti al di fuori dei processi operativi di trattamento dei dati previsti e autorizzati.

Esempi di eventi che possono generare violazione di dati

Al fine di facilitare l'individuazione di una possibile violazione, vengono di seguito indicati in maniera esemplificativa e non esaustiva, una serie di possibili eventi che potenzialmente possono generare violazioni dei dati personali. Pertanto si può essere in presenza di un data breach anche nel caso di un evento non compreso nell'elenco di seguito riportato, di contro il verificarsi di uno degli eventi che seguono non costituisce condizione sufficiente per stabilire l'effettivo data breach. Il Titolare deve infatti procedere sempre alle opportune valutazioni.

Eventi riguardanti trattamenti elettronici:

Eventi accidentali: eventi anomali determinati da fatti fortuiti che causano la perdita delle caratteristiche di sicurezza dei dati personali dei clienti (confidenzialità, integrità o disponibilità) in caso di trattamenti informatizzati. Rientrano in tali casistiche eventi generati nella gestione dei sistemi ICT (gestiti internamente oppure in outsourcing) quali:

- Esecuzione erronea di comandi e/o procedure per distrazione: ad esempio pubblicazione erronea delle informazioni personali (non di dominio pubblico) su portali web pubblici; erroneo invio di informazioni a enti esterni all'Ente, formattazione di dispositivi di memorizzazione, errori nell'implementazione di una policy di controllo e verifica periodica delle abilitazioni degli accessi; divulgazione accidentale di credenziali di accesso a colleghi o personale non autorizzato ecc.
- Rottura delle componenti HW: a titolo di esempio distruzione dei supporti di memorizzazione a causa di sbalzi di temperatura e di elettricità, umidità, corto circuito, caduta accidentale, eventi catastrofici/incendi, ecc.
- Malfunzionamenti Software: ad esempio esecuzione di uno script automatico non autorizzato; errori di programmazione che causano output errati, ecc.
- Visibilità errata di dati sul sito web dell'Ente: ad esempio visibilità di dati di altri utenti anche per casi di omonimia.
- Fornitura dati a persona diversa dall'Interessato: a titolo di esempio comunicazioni di dati di interessati a destinatari errati; gestione di informazioni avanzate da persone diverse dal Titolare o suo delegato;
- Guasti alla rete: a titolo di esempio caduta delle comunicazioni durante il trasferimento di dati e perdita di dati durante la trasmissione, ecc.

Eventi dolosi: eventi dolosi causati da personale interno o soggetti esterni realizzati tramite: accesso non autorizzato ai dati con lo sfruttamento di vulnerabilità dei sistemi interni e delle reti di comunicazione; compromissione o rivelazione abusiva di credenziali di autenticazione; utilizzo di

software malevolo. In tale casistica rientrano gli incidenti di sicurezza ICT che comportano la violazione dei dati personali quali:

- Furto: furto di supporti di memorizzazione e/o elaborazione contenenti dati personali dei clienti;
- Truffa informatica esterna: tutti i casi di frodi realizzate da un soggetto esterno dell'Ente rivolto a procurare a sé o ad altri un profitto o, comunque, un vantaggio in termini economici, pubblicitari, ideologici/politici, qualora tali frodi causino perdita delle caratteristiche di sicurezza dei dati personali dei soggetti interessati (confidenzialità, integrità o disponibilità) trattati dall'ente o da suoi fornitori. Ad esempio: accesso non autorizzato ed illecito alle basi dati dei sistemi contenenti i dati dei soggetti interessati tramite sfruttamento di vulnerabilità dei sistemi;
- Appropriazione dei dati di carta di credito; appropriazione (e diffusione) delle credenziali di autenticazione ai servizi dei clienti.
- Truffa informatica interna: tutti i casi di frodi realizzate da personale interno all'Ente che comportano la violazione dei dati personali. Tali eventi possono derivare dall'utilizzo illecito e/o illegittimo delle informazioni a cui un incaricato del trattamento accede anche se autorizzato.

Eventi riguardanti trattamenti cartacei

Eventi accidentali: Eventi anomali causati nell'ambito dei trattamenti non automatizzati effettuati su archivi cartacei dei dati personali dei clienti dell'ente quali:

- Distruzione accidentale di documenti: ad esempio incendio/ allagamento dei locali dove sono presenti archivi cartacei, causati da eventi fortuiti e non dolosi presso le sedi dell'ente e dei locali, degli outsourcers di archiviazione contratti, dei collaboratori cessati dai quali si attende la restituzione della documentazione contrattuale;
- Distruzione per errore di documenti originali, senza eventuale copia, da parte di dipendenti interni, di collaboratori esterni;
- Smarrimento di documenti: ad esempio perdita di documenti contenenti dati dei cittadini, degli outsourcers (es. archiviazione contratti).
- Fornitura involontaria di dati a persona diversa dal contraente: ad esempio invio lettera ad Ente senza mandato, gestione ed evasione reclami/richieste di informazioni avanzate da persone diverse dal Titolare della linea non delegato, comunicazione di dati dal subentrato al subentrante e viceversa, invio/visualizzazione di fatture a soggetti diversi dagli autorizzati.

Eventi dolosi: Comportamenti dolosi da parte di personale interno o soggetti esterni realizzati, attraverso accessi non autorizzati, nell'ambito di trattamenti effettuati su archivi cartacei di dati personali del Comune quali:

- Distruzione dolosa dei documenti: ad esempio incendio doloso provocato da personale interno o soggetti esterni che rende indisponibile in modo definitivo i documenti contenenti dati dell'utenza; accesso non autorizzato da parte di terzi ad archivi interni dell'Ente e distruzione volontaria di documenti contenenti dati dell'utenza.
- Accesso non autorizzato: ad esempio accesso non autorizzato da parte di personale interno o soggetti esterni, con lettura e/o copia dei documenti, ad archivi documentali presso le sedi dell'ente, dei collaboratori esterni. Non si verifica violazione se si ha la ragionevole certezza che non vi è stata lettura o copia dei documenti contenenti dati degli interessati.
- Furto (cartacei): furto da parte di personale interno o soggetti esterni (o non identificati) di documenti cartacei contenenti dati dei soggetti interessati.

NOTIFICA DELLA VIOLAZIONE ALL'AUTORITÀ DI CONTROLLO

Quando è richiesta la notifica

In caso di violazione dei dati personali, il Titolare del trattamento notifica la violazione all'Autorità di controllo competente a norma dell'articolo 55 del GDPR, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che la valutazione della violazione non evidenzi rischi per i diritti e le libertà delle persone fisiche.

Il Titolare del trattamento viene considerato "a conoscenza" della violazione nel momento in cui è ragionevolmente certo che si è verificato un incidente di sicurezza che ha portato alla compromissione di dati personali.

Nei casi in cui la violazione non sia evidente e chiara il Titolare è tenuto ad attivare tempestivamente le indagini finalizzate a valutare se l'incidente abbia causato una effettiva violazione di dati personali, ad adottare le dovute misure correttive e ad effettuare la notifica, se ritenuta necessaria.

La notifica all'Autorità di controllo effettuata oltre le 72 ore, deve essere corredata dai motivi del ritardo. Ogni singola violazione costituisce un incidente segnalabile con rispettiva notifica; fa eccezione il caso della notifica "cumulativa" da utilizzare in presenza di violazioni multiple riguardanti il medesimo tipo di dati personali violati nel medesimo modo ed in un lasso di tempo relativamente breve.

Contrariamente, diverse violazioni riguardanti tipi diversi di dati personali, violati in maniere diverse, costituiscono separate notifiche per ogni violazione conformemente all'articolo 33 del GDPR. L'articolo 33, paragrafo 4, afferma inoltre che "qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo".

Il Titolare quindi, a seconda della natura e delle complessità della violazione, può effettuare ulteriori accertamenti per stabilire tutti i fatti pertinenti relativi all'incidente.
In questi casi il Titolare provvede tempestivamente (entro le 72 ore) alla notifica all'Autorità riservandosi di fornire informazioni supplementari in un secondo momento, si procede pertanto ad una notifica per fasi.

Se, dopo la notifica iniziale, una successiva indagine dimostra che l'incidente di sicurezza è stato contenuto e che non si è verificata alcuna violazione il Titolare del trattamento informa l'Autorità di controllo. L'incidente, in questo caso, viene registrato come un evento che non costituisce una violazione.

<u>Quando non è richiesta la notifica</u>
Quando dalla valutazione risulti improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche il Titolare non procede né alla notifica all'Autorità di controllo né ad informare la persona interessata.
Nel caso in cui lo stato di assenza di un rischio probabile ai diritti ed alle libertà delle persone fisiche cambi nel corso del tempo si procede alla rivalutazione del rischio al fine di verificare se i nuovi elementi emersi rientrino nell'obbligo di notifica.

CONTITOLARI DEL TRATTAMENTO
Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14, a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti. Tale accordo può designare un punto di contatto per gli

interessati ed il suo contenuto è messo a disposizione dell'interessato, che può esercitare i propri diritti nei confronti di e contro ciascun titolare del trattamento. L'accordo deve contenere obbligatoriamente l'indicazione del Titolare responsabile delle violazioni e della eventuale notifica all'Autorità di controllo.

RESPONSABILE DEL TRATTAMENTO

Il Responsabile del trattamento svolge un ruolo importante nel consentire al Titolare del trattamento di adempiere ai propri obblighi in materia di notifica delle violazioni.
Il contratto, o altro atto giuridico, che disciplina il rapporto tra il Titolare ed il Responsabile del trattamento deve contenere la seguente previsione "Il responsabile del trattamento assiste il Titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento".

Se il Responsabile del trattamento viene a conoscenza di una violazione dei dati personali che sta trattando per conto del Titolare del trattamento, deve notificarla al Titolare del trattamento senza ingiustificato ritardo e comunque non oltre le 24 ore.

La valutazione del rischio derivante dalla violazione spetta al Titolare del trattamento nel momento in cui viene a conoscenza della violazione; in capo al Responsabile del trattamento insiste esclusivamente l'obbligo di verificare l'esistenza di una violazione e di notificarla tempestivamente al Titolare del trattamento nei tempi sopra indicati.

In considerazione del fatto che ai sensi del GDPR la responsabilità legale della notifica rimane sempre in capo al Titolare del trattamento, il Responsabile del trattamento può effettuare la notifica della violazione per conto del Titolare esclusivamente nel caso in cui quest'ultimo gli abbia conferito apposita autorizzazione e/o nel caso in cui tale modalità sia espressamente prevista negli accordi contrattuali tra i due soggetti.

In caso contrario è fatto obbligo al Responsabile del trattamento di informare il Titolare, nelle modalità e nei tempi di cui sopra, di ogni potenziale evento di data breach.
La segnalazione può essere trasmessa via PEC all'indirizzo protocollo@pec.comunelameziaterme.it
e per conoscenza al Responsabile della protezione dei dati personali via email ordinaria all'indirizzo dpo.comune.lamezia-terme@findata.it

Delle seguenti prescrizioni è fatta apposita menzione nel contratto, o altro atto giuridico, che disciplina il rapporto tra il Titolare ed il Responsabile del trattamento.

RESPONSABILE DELLA PROTEZIONE DATI (RPD)

Il Responsabile della Protezione dati (di seguito "RPD" o "DPO") fornisce consulenza e informazioni al Titolare del trattamento e/o al responsabile del trattamento in merito alla valutazione della necessità di notificare una violazione. L'RPD coopera inoltre con l'Autorità di controllo e funge da punto di contatto per l'Autorità di controllo e per gli eventuali interessati.

Il RPD viene informato tempestivamente dell'esistenza di una violazione e viene coinvolto nell'intera gestione delle violazioni, nonché nel processo di notifica.

Il RPD, quindi, svolge un ruolo di assistenza nella prevenzione delle violazioni, fornisce consulenza e monitora il rispetto delle norme durante il processo di gestione della violazione e assiste l'Ente nell'eventualità di successive indagini da parte dell'Autorità di controllo.

Il RPD, inoltre, su richiesta del Titolare del trattamento, esprime pareri in merito alla struttura, all'impostazione, all'amministrazione ed alla conservazione della documentazione relativa al registro delle violazioni.

CONTENUTI DELLA NOTIFICA: INFORMAZIONI OBBLIGATORIE DA FORNIRE ALL'AUTORITÀ DI CONTROLLO

La notifica all'Autorità di controllo deve obbligatoriamente contenere almeno i seguenti elementi:

- descrizione della natura della violazione dei dati personali (compresi, ove possibile, le categorie e il numero degli interessati (persone fisiche i cui dati personali sono stati oggetto di violazione) e le registrazioni dei dati personali in questione (le categorie di registrazioni dei dati personali fanno riferimento ai diversi tipi di registrazioni di cui il Titolare del trattamento può disporre, quali dati sanitari, registri didattici, informazioni sull'assistenza sociale, dettagli finanziari, numeri di conti bancari, numeri di passaporto, ecc.) ;
- comunicazione del nome e dei dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere maggiori informazioni;
- descrizione delle probabili conseguenze della violazione dei dati personali;
- descrizione delle misure adottate o da adottare 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.

L'impossibilità da parte del Titolare di disporre di informazioni precise (ad esempio il numero esatto di interessati coinvolti) non costituisce un ostacolo alla notifica tempestiva delle violazioni; in questo caso la comunicazione deve contenere un'approssimazione sul numero di persone fisiche interessate e di registrazioni dei dati personali coinvolte.
Le informazioni sopra indicate costituiscono il contenuto minimo della notifica, è facoltà del Titolare del trattamento, qualora lo ritenga necessario, fornire ulteriori informazioni.

COMUNICAZIONE ALL'INTERESSATO

Ai sensi dell'articolo 34, paragrafo 1 del GDPR "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 comunica la violazione all'Interessato senza ingiustificato ritardo".

Contenuto della comunicazione

La comunicazione di una violazione agli interessati deve avvenire senza ingiustificato ritardo e, deve descrivere con un linguaggio semplice, chiaro e trasparente la natura della violazione dei dati personali e deve contenere obbligatoriamente i seguenti contenuti minimi:

- il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto;
- una descrizione delle probabili conseguenze della violazione;
- una descrizione delle misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione e anche, se del caso, per attenuarne i possibili effetti negativi.

Modalità della comunicazione

La violazione va comunicata direttamente agli interessati coinvolti.
Nel caso la comunicazione diretta non risulta percorribile si procede ad una comunicazione pubblica o a una misura simile che permetta di informare gli interessati con analoga efficacia (articolo 34, paragrafo 3, lettera c); la misura più efficace, valutata la fattispecie concreta, viene stabilita dal Titolare. Il Titolare, può contattare l'Autorità di controllo per chiedere indicazioni ed orientamenti in

merito all'opportunità di informare gli interessati sulla violazione ai sensi dell'articolo 34, ma anche sui messaggi appropriati da inviare loro e sul modo più opportuno per contattarli. Qualora il Titolare non sia in possesso di dati sufficienti per contattare l'Interessato procede ad informarlo non appena sia ragionevolmente possibile (ad esempio può accadere che il Titolare entra in possesso di dati necessari per contattare l'Interessato nel momento in cui lo stesso esercita il proprio diritto di accesso ai dati ai sensi dell'articolo 15).

Quando la comunicazione non deve essere effettuata

La comunicazione agli interessati in caso di violazione dei dati non deve essere effettuata, ai sensi dell'articolo 34 paragrafo 3, se si verifica una delle seguenti tre condizioni:

1. Il Titolare del trattamento ha applicato misure tecniche e organizzative adeguate per proteggere i dati personali prima della violazione tali rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi (es. cifratura);
2. Subito dopo la violazione il Titolare ha adottato una serie di misure che rendano improbabile l'elevato rischio posto ai diritti e alle libertà delle persone fisiche (es. l'immediata azione nei confronti del soggetto che ha avuto accesso ai dati personali in modo da inibirne qualsiasi utilizzo);
3. Contattare gli interessati richiede uno sforzo sproporzionato. In tale circostanza il Titolare provvede ad effettuare una comunicazione pubblica o individua una misura analoga, tramite la quale gli interessati vengano informati in maniera altrettanto efficace.

Seppure la violazione inizialmente non rilevi necessità di una comunicazione all'Interessato per l'assenza di rischio per i diritti e le libertà delle persone fisiche, la situazione potrebbe nel tempo subire delle variazioni, pertanto il Titolare rivaluta il rischio e provvede all'eventuale comunicazione nelle modalità di cui sopra.

Quando la comunicazione va sempre effettuata

Il Titolare provvede in qualunque caso alla comunicazione nel caso in cui questa venga richiesta direttamente all'Autorità di controllo al fine di evitare da parte della stessa l'esercizio dei poteri sanzionatori.

VALUTAZIONE DEL RISCHIO

Non appena il Titolare del trattamento viene a conoscenza di una violazione oltre a mettere in campo tutte le azioni necessarie a contenere l'incidente, valuta anche il rischio che potrebbe derivarne.
Il rischio viene valutato in base a criteri oggettivi; i considerando 75 e 76 del GDPR stabiliscono che la valutazione deve tenere conto della probabilità e della gravità del rischio per i diritti e le libertà degli interessati.

La valutazione del rischio per i diritti e le libertà delle persone fisiche a seguito di una violazione esamina il rischio in maniera diversa rispetto alla valutazione d'impatto sulla protezione dei dati (DPIA). La valutazione di impatto prende in considerazione infatti un evento ipotetico; nel caso invece di una violazione effettiva, l'evento si è già verificato, quindi l'attenzione va concentrata esclusivamente sul rischio risultante dell'impatto di tale violazione sulle persone fisiche.

La valutazione viene effettuata tenendo conto dei seguenti criteri:

- Tipo di violazione: valutare se la violazione può influire sul livello di rischio per persone fisiche;

- Natura, carattere sensibile e volume dei dati personali: valutare il carattere, il tipo ed il volume dei dati violati;
- Facilità di identificazione delle persone fisiche: valutare la facilità con cui un soggetto che può accedere a dati personali compromessi riesce a identificare persone specifiche o ad abbinare i dati con altre informazioni per identificare persone fisiche;
- Gravità delle conseguenze per le persone fisiche: valutare il grado di gravità del danno potenziale che la violazione potrebbe creare alle persone.
- Caratteristiche particolari dell'Interessato: valutare attentamente se la violazione riguardi dati personali relativi a minori o ad altre persone fisiche vulnerabili che possono essere soggette a un rischio più elevato di danno.
- Caratteristiche particolari del Titolare del trattamento di dati: valutare la natura e il ruolo del Titolare del trattamento e delle sue attività che possono influire sul livello di rischio per le persone fisiche in seguito a una violazione.
- Numero di persone fisiche interessate : valutare il numero di persone fisiche coinvolte nella violazione.

REGISTRO DELLE VIOLAZIONI

È istituito un registro interno delle violazioni dove vengono annotate sia le violazioni non notificabili che quelle notificabili.

In ossequio al principio di responsabilizzazione di cui all'articolo 5 paragrafo 2 del GDPR, il Titolare del trattamento conserva la documentazione di tutte le violazioni come stabilito all'articolo 33, paragrafo 5: "Il Titolare del trattamento 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 verificare il rispetto del presente articolo".

Il registro deve contenere i seguenti dati:

- i dettagli relativi alla violazione (cause, fatti e dati personali interessati);
- gli effetti e le conseguenze della violazione;
- i provvedimenti adottati per porvi rimedio;
- il ragionamento alla base delle decisioni prese in risposta a una violazione (con particolare riferimento alle violazioni non notificate ed alle violazioni notificate con ritardo);

Il Titolare conserva la documentazione in conformità dell'articolo 33, paragrafo 5, anche al fine di poter fornire prontamente le prove dall'Autorità di controllo in caso di suo intervento.

GESTIONE DEL DATA BREACH

Al fine di garantire una adeguata presenza delle competenze necessarie alla gestione di eventuali data breach che potrebbero interessare il Titolare ha predisposto un gruppo di lavoro denominato DBMU (Data Breach Management Unit) formato dal Segretario Generale, dall'amministratore di sistema, dal DPO e dai dirigenti comunali interessati di volta in volta dalle violazioni dei dati. Il Sindaco resta sempre informato sulle attività del gruppo di lavoro e partecipa alle riunioni indette dallo stesso. Il Segretario Generale funge da coordinatore del gruppo.

Il Gruppo di lavoro ha lo scopo di analizzare le segnalazioni ricevute e definire le azioni da intraprendere. Nella gestione della violazione, inoltre il Gruppo si avvale durante l'intero processo anche del Responsabile del Settore a cui fa capo il dato o il gruppo di dati violati.

Al Gruppo sono assegnate le seguenti competenze:

- la predisposizione e l'invio della notifica della violazione all'Autorità di controllo utilizzando il modello messo a disposizione sul sito del Garante della Privacy all'indirizzo https://www.garanteprivacy.it o tramite PEC all'indirizzo protocollo@pec.gpdp.it
- la valutazione del rischio e l'attivazione di eventuali indagini sulla violazione;
- l'invio all'Autorità di controllo di eventuali informazioni supplementari riguardanti la segnalazione già resa;
- la comunicazione agli interessati,
- la tenuta e l'aggiornamento del Registro delle violazioni.

Il Gruppo, valutata la fattispecie concreta, individua all'occorrenza personale tecnico e/o amministrativo necessario stabilmente o episodicamente alle attività da svolgere; dell'individuazione viene dato riscontro in apposito verbale.

Tutti i dipendenti comunali autorizzati a trattare dati, possono potenzialmente venire a conoscenza di un data breach, al verificarsi di tale evento è fatto obbligo di avvisare tempestivamente il Dirigente del settore in qualità di Responsabile designato dal Titolare al trattamento dati.

Quest'ultimo, valutato l'evento alla luce delle indicazioni sopra fomite, qualora rilevi caratteristiche riconducibili ad un potenziale data breach, in considerazione dei ristretti tempi di azione e della potenziale gravità delle conseguenze, ha l'obbligo di segnalarlo tempestivamente attraverso PEC dell'indirizzo protocollo@pec.comunelameziaterme.it (C.A. Segretario Generale) e per conoscenza al Responsabile della protezione dei dati personali via email ordinaria all'indirizzo dpo.comune.lamezia-terme@findata.it

Il Gruppo di lavoro DBMU, avvalendosi del supporto del RPD, se rileva che l'episodio può essere classificato come data breach, predispone la comunicazione all'Autorità Garante, a firma del Titolare, da inviare senza ingiustificato ritardo e, ove possibile, entro 72 ore, nelle modalità sopra indicate provvedendo ad annotare sul registro le eventuali ragioni del ritardo della notifica effettuata oltre le 72 ore, nonché le motivazioni ed il ragionamento che hanno portato a non notificare una violazione.

ALLEGATI

Vengono allegati, ma non pubblicati, alla presente procedura i seguenti schemi e/o schede, predisposti per facilitare le attività in carico al Gruppo di lavoro DBMU.

A. SCHEDA EVENTO
B. SCHEDA VIOLAZIONE DATI
C. REGISTRO DEI DATA BREACH
D. MODELLO DI COMUNICAZIONE ALL'INTERESSATO DELLA VIOLAZIONE DEI DATI PERSONALI