COMUNE DI NOCERA TERINESE

(PROVINCIA DI CATANZARO)

LETTERA DI NOMINA

Responsabile del trattamento art. 28 GDPR

Nocera Terinese. 08/04/2024

SPETT.LE
MELANIDE

OGGETTO: Lettera di Nomina a Responsabile del Trattamento dei dati peri il servizio di riscossione tributi.

Il Sindaco pro-tempore Sig. Saverio Russo, in qualità di "Titolare del Trattamento" dei dati personali del Comune di Nocera Terinese, conformemente a quanto stabilito dal GDPR (UE 2016/679) e dal D. Lgs. 10.08.2018 n. 101

AFFIDA

Alla SocietàMELANIDE in persona delRappresentante legale Pro-tempore, la mansione di Responsabile del Trattamento dei dati, con l'incarico di realizzare il sistema di sicurezza e di Accountability per la Privacy inerente l'organizzazione dell'Area affidatagli, in base alle scelte e regole contenute negli Allegati "DELEGA AL RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI" e "MANSIONARIO COMPORTAMENTALE".

Ai fini suddetti il RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI dovrà, nella propria Unità Organizzativa, individuare le persone che sono autorizzate al trattamento dei dati per le attività in oggetto e ad esse afferenti.
Con la presente ricordiamo quanto sia fondamentale che l'Ente sia dotato da più Organizzazioni interne che siano di supporto al Titolare dei dati per il trattamento degli stessi in totale accordo col nuovo Regolamento europeo UE 2016/679.

Il "Responsabile del Trattamento" dichiara di essere a conoscenza di quanto stabilito dal GDPR (UE 2016/679) per l'adozione delle misure di sicurezza, nonché del D. Lgs. 196/03 e del D. Lgs. 101/18 e si impegna ad attuare le norme in esso contenute.

La Formazione sul nuovo Regolamento europeo ha l'obiettivo di garantire un'adeguata Responsabilizzazione comportamentale al riguardo della consapevolezza di trattamento dei dati.
Sarà compito del Responsabile del Trattamento dei dati assicurarsi che tutte le risorse interne e facenti parte della propria Unità Organizzativa, di supporto alle attività della propria Struttura Organizzativa, attuino le regole di sicurezza e abbiano preso parte ai corsi di formazione sul nuovo regolamento europeo UE 2016/679.

Il Titolare dei dati

(Saverio Russo)

Il Responsabile del trattamento
Firmato digitalmente da

NICOLA BEVIVINO

C = IT
(MELANIDE)

DELEGA AL RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI

TRATTAMENTO DEI DATI PERSONALI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

Per il trattamento di dati personali, effettuato con strumenti diversi da quelli elettronici o comunque automatizzati, dovrà essere richiesta almeno l'osservanza delle seguenti modalità finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento, da parte degli incaricati, nelle operazioni di trattamento, degli atti e dei documenti contenenti dati personali:

- **individuare le persone che sono autorizzate al trattamento dei dati personali** che trattano i dati del Comune di Nocera Terinese, predisporre la lista delle persone che sono autorizzate al trattamento e dei relativi profili di autorizzazione. Per ogni persona autorizzata occorre definire l'ambito del trattamento consentito e i relativi profili di autorizzazione. Provvedere con cadenza almeno annuale (o inferiore se ne ricorre il caso) all'aggiornamento della lista e delle conseguenti autorizzazioni: nell'ambito dell'aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli autorizzati al trattamento, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione;
- quando **gli atti e i documenti contenenti dati personali indicati all'art. 9 del GDPR (UE 2016/679) (intesi come sensibili o giudiziari)** saranno affidati per lo svolgimento dei relativi compiti, i medesimi atti e documenti**dovranno essere controllati e custoditi dallepersone che sono autorizzate al trattamento** fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e, al termine delle operazioni affidate, dovranno essere da questi restituiti;
- **l'accesso agli archivi contenenti dati di cui all'art. 9 del GDPR dovrà essere controllato**. Qualora le persone che sono autorizzate al trattamento di dati personali dovessero trattare documenti contenenti dati personali sensibili o giudiziari e per far ciò dovessero accedere all'archivio, gli stessi dovranno aver cura di esibire la documentazione comprovante l'autorizzazione all'accesso e al trattamento. Nel caso in cui le persone che sono autorizzate al trattamento fossero ammesse, a qualunque titolo, dopo l'orario di chiusura, dovranno dare le loro generalità in quanto vi è l'obbligo di identificare e registrare coloro che accedono agli archivi stessi. Qualora gli archivi non fossero dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, gli incaricati dovranno richiedere preventivamente l'autorizzazione all'accesso.

TRATTAMENTO DEI DATI PERSONALI CON STRUMENTI ELETTRONICI

Per il trattamento di dati personali, effettuato con strumenti elettronici, dovrà essere richiesta almeno l'osservanza delle modalità di seguito indicate.

Sistema di autenticazione informatica.

Individuare le persone che sono autorizzateal trattamento dei dati personali e predisporre la lista dellepersone autorizzate che potrà essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione. **Per ogni persona autorizzata al trattamento,** occorre definire **l'ambito del trattamento consentito e i relativi profili di autorizzazione.** Provvedere con cadenza almeno annuale (o inferiore se ne ricorre il caso) all'aggiornamento della lista e delle conseguenti autorizzazioni: nell'ambito dell'aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli autorizzati, la lista delle persone che sono autorizzate al trattamento può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

Il trattamento di dati personali con strumenti elettronici deve essere consentito alle persone autorizzate e dotate di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti. **Per le credenziali occorrerà osservare quanto disposto dal D. Lgs. 30.6.2003 n. 196, GDPR (UE 2016/679) e dal D. Lgs. 101/18.**

Ad ogni persona autorizzata devono essere assegnate o associate individualmente una o più credenziali per l'autenticazione.

Dovranno essere impartite,alle persone autorizzate, istruzioni per adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.

Deve essere previsto che:

- **le credenziali di autenticazione non utilizzate da almeno sei mesi siano disattivate**, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica;
- **le credenziali dovranno essere disattivate** anche **in caso di perdita della qualità** che consente alla persona autorizzata l'accesso ai dati personali.

Devono essere impartite istruzioni alle persone autorizzate al trattamento, per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.

Per i casi in cui l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, saranno impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto le personaautorizzata della loro custodia, la quale deve informare tempestivamente la persona autorizzata al trattamento, dell'intervento effettuato.

Sistema di autorizzazione

Nei casi in cui, per le persone autorizzate, siano individuati profili di autorizzazione di ambito diverso dovrà essere operativo un sistema di autorizzazione.

I profili di autorizzazione, per ciascunapersona autorizzata o per classi omogenee di persone autorizzate, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.

Periodicamente, e comunque almeno annualmente, dovrà essere verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione (o inferiore se ne ricorre il caso).

Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito alle persone autorizzate e addette alla gestione o alla manutenzione degli strumenti elettronici, la lista delle persone autorizzate può essere redatta anche per classi omogenee di persone autorizzate al trattamento e dei relativi profili di autorizzazione.

I dati personali dovranno essere protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare ogni qualvolta vengano resi disponibili gli aggiornamenti.

Dovranno essere effettuati aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti.

Dovranno essere impartite istruzioni organizzative e tecniche per il salvataggio dei dati, con ragionevole frequenza, soprattutto sui singoli PC che non siano collegati ad un Server, o che, comunque, lavorino in modalità stand alone..

In modo da assicurare la dovuta padronanza di tutti i dipendenti delle Policy del Disaster Recovery e della Business Continuity**da regolamentare con il Direttore Tecnico - Amministratore di Sistema e di Rete, di concerto col DPO interno che interagirà col DPO del Comune.**

Il Responsabile del Trattamento dei dati dovrà avviare una elevata collaborazione col DPO del Comune, e dovrà curare la tenuta di un proprio Registro dei Trattamenti, gli adempimenti di Data Breach, in seno ai dati trattati e fungere da interfaccia con la Struttura Garante.In caso di Data Breach sui dati del Comune di Nocera Terinese dovrà immediatamente avvisare il DPO del Comune, entro e non oltre le 24 ore dall'avvenuta conoscenza dell'evento, per consentire al DPO del Comune gli adempimenti conseguenti (avvisare entro le 48 ore gli Interessati – se ne ricorre il caso; ed il garante entro le 72 ore).

Periodicamente **il DPO del Comune di Nocera Terinesepotrà verificareil perfetto andamento delle Policy** impartite dal responsabile del trattamento in esterno,in attuazione del GDPR.

Ogni *Incident* **di sicurezza dovrà essere reso noto al DPO dell'Ente.**

Dovendo **il Responsabile del Trattamento dei dati coordinare le persone autorizzate al trattamento,** avrà l'onere di consegnare la Lettera di nominaalle persone autorizzate del trattamento dei datiche operano sui dati del Comune di Nocera Terinese.

Responsabilità del Trattamento dei dati

Il Responsabile del trattamento ai sensi dell'art.28 del GDPR (UE 2016/679) dovrà garantire le misure di sicurezza tecniche ed organizzative adeguate non inferiori a quelle richieste dall'art.32 del UE 2016/679 e sotto riportate:

1) la pseudonimizzazione dei dati personali
2) la cifratura dei dati personali;
3) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
4) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
5) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
6) una procedura di valutazione dell'adeguato livello di sicurezza, che tenga conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.
7) una procedura che definisca che chiunque operi sotto la sua autorità abbia accesso a dati personali, non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.
8) l'adesione a un codice di condotta o a un meccanismo di certificazione approvati ai sensi della normativa pro tempore applicabile.