COMUNE DI NOCERA TERINESE

(PROVINCIA DI CATANZARO)

LETTERA DI NOMINA

Responsabile del trattamento art. 28 GDPR

Nocera Terinese, 08/04/2024

SPETT.LE
DOTT. SSA FRANCESCA GANCI
C/O SEDE COMUNALE
88047NOCERA TERINESE (CZ)

OGGETTO: Lettera di Nomina a Responsabile del Trattamento dei dati.
Unità Organizzativa:Segreteria Comunale.

Il Sindaco pro-tempore, 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

AllaDott.ssa Francesca Ganci, in qualità di Responsabile dell' Areain oggettopresso il Comune di Nocera Terinese, 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

(Francesca Ganci)

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** e che afferiscono alla propria Unità Organizzativa, 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 e **dovranno essere controllati e custoditi dalle persone 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 delle persone 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 persona autorizzata 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 ciascuna persona 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.**

Il Responsabile del Trattamento dei dati dovrà avviare una elevata collaborazione col DPO, che dovrà curare la tenuta di un Registro dei Trattamenti, gli adempimenti di Data Breach, in seno ai dati trattati e fungere da interfaccia con la Struttura Garante.

Il calcolo dei Rischi, effettuato dal DPO, sarà attuato in collaborazione con tutti i Responsabili del Trattamento (art. 32 del regolamento europeo).

Periodicamente **il DPO verificherà**, con audit interni, **il perfetto andamento delle Policy** impartite redigendo dei verbali, da sottoporre al Titolare dei dati, indicanti l'andamento delle direttive, che consentano una piena attuazione del GDPR.

Trimestralmente il DPO convocherà tutti i Responsabili del Trattamento al fine di rendere più performante le attività di trattamento. **Ogni *Incident* di sicurezza dovrà essere reso noto all'intera struttura,** per il tramite del DPO, per mezzo di comunicazioni ufficiali mirate alla minimizzazione del rischio.

Dovendo **il Responsabile del Trattamento dei dati coordinare la propria Unità Organizzativa,** avrà l'onere di consegnare la Lettera di nomina alle persone autorizzate del trattamento dei dati che operano sui dati della struttura organizzativa.

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.

MANSIONARIO COMPORTAMENTALE

A tutela e protezione dei dati personali

Il trattamento dei dati personali, e a maggior ragione quelli sensibili e giudiziari, deve essere ricondotto a: **riservatezza** (garanzia che il dato sia trattato solo da colui che ne è autorizzato), **integrità** (garanzia che il dato sia quello che è stato trattato originariamente), **disponibilità** (garanzia che il dato sia sempre reso disponibile all'utilizzatore concretamente autorizzato) e **resilienza** (garanzia che il dato sia trattato secondo le condizioni al contorno).

A questo punto è lecito introdurre il concetto di sicurezza dei dati, specificando che con il termine "sicurezza" s'intende l'insieme di misure, di carattere organizzativo e tecnologico, adeguate ad assicurare a ciascun utente autorizzato esclusivamente i servizi previsti per l'utente stesso, nei tempi e nelle modalità stabilite.

Più formalmente, secondo la nota definizione ISO, la sicurezza è "l'insieme delle misure atte a garantire la riservatezza, l'integrità e la disponibilità delle informazioni gestite" e dunque l'insieme di tutte le misure atte a difendere il sistema informativo dalle possibili minacce d'attacco riducendo il rischio.

Il rischio è dato dalla formula **R = P x D** ; dove il rischio R è funzione della probabilità (P) di accadimento di una minaccia e della magnitudo del danno (D).

La minaccia è il potenziale accadimento di un "evento (azione o "non Azione") non desiderato", che, sia deliberato o accidentale, può arrecare danno a chi lo subisce.

L'attacco è la modalità con cui una minaccia viene attuata, sfruttando le eventuali vulnerabilità.

Appare opportuno in questa fase, giacché per il trattamento dei dati vengono utilizzati strumenti elettronici, introdurre gli ambiti normativi relativi alla sicurezza che sono così classificati:

- Norme funzionali relative ai prodotti, aventi come scopo principale la ricerca dell'interoperabilità dei sistemi informatici;
- Criteri di valutazione della fiducia riposta nella sicurezza di specifici sistemi e prodotti informatici:
  - TCSEC (Trusted Computer System Evaluation Criteria), applicato in ambito USA;
  - ITSEC (Information Technology Security Evaluation Criteria), applicato in Europa;
  - ISO/IEC 15408;
  - Direttiva "Stanca" sulla sicurezza ICT
- Norme relative al sistema di gestione della sicurezza:
  - ISO/IEC TR 13335 (parti 1,2,3,4);
  - BS7799 (parti 1 e 2);
  - ISO/IEC 17799:2000 (che recepisce la parte 1 delle BS7799);
  - ISO/IEC 27001:2013
- Vigenti normative nazionali ed europee.

Il titolare dei dati e/o il responsabile del trattamento dei dati, in funzione di quanto appena detto, ha l'obbligo di effettuare un'attenta analisi dei rischi, valutando (Privacy by Design) opportunamente tutte le minacce e le relative vulnerabilità che possono concretizzarsi in uno o più attacchi alla propria banca dati. A valle di questa analisi occorrerà individuare (Privacy by Default) le opportune contromisure per contrastare/minimizzare gli attacchi in modo da ridurre il rischio, dandone evidenza nel PIA (Privacy

Impact Assessment) per come prescritto nel GDPR (UE 2016/679), ricordando che in caso di controllo da parte del Garante occorrerà dimostrare la propria perfetta buona fede.
Per prevenire gli attacchi è necessario che i Responsabili del trattamento e le persone autorizzate del trattamento, utilizzino idonee misure di sicurezza. La Policy della "Clear Desktop e Clear Screen" dovrà diventare un modello attuativo quotidiano, da parte degli incaricati del trattamento, per evitare che estranei, appropriandosi di informazioni, possano esporre, a sanzioni civili e penali, loro stessi nonché lo stesso Titolare dei dati.
Spesso, a tal proposito, viene sottovalutato l'art. 2050 del codice civile (indicato, nella sostanza, nel GDPR e di prossimo recepimento con la nuova Normativa Italiana che sostituirà/integrerà il D. Lgs. 196/03) che richiama a proposito di risarcimento, comprendente anche il danno non patrimoniale. Si ricorda, infatti, che l'attività di trattamento dei dati personali è qualificata dalla Magistratura ordinaria di merito come attività pericolosa, disciplinata dal Codice Civile. Il che significa che il titolare del trattamento, in caso di richiesta di risarcimento del danno da parte del soggetto che si ritiene leso dalle modalità del trattamento dei propri dati, è tenuto a provare di avere adottato le misure idonee ad evitare il danno (onere dell'inversione della prova).

Pertanto occorrerà adottare le seguenti misure di sicurezza per ridurre il rischio:

- utilizzare una password, di accesso sul proprio PC, di almeno otto caratteri alfanumerici, evitando di assemblare in essa elementi della propria vita privata e/o comunque a essa riconducibile;
- cambiare la password ogni tre mesi, trattando dati di cui all'Art. 9 del GDPR in cui vengono ripresi i dati sensibili e/o giudiziari;
- far attivare una password di screen saver, quando il proprio PC già in uso durante la sessione di lavoro non è presidiato, ricordando che l'avviamento della stessa è *sub judice* ad un lasso di tempo di attivazione che non tutela l'incaricato del trattamento, si consiglia, pertanto, di attivarla manualmente alla bisogna (tasto Windows + L);
- evitare di comunicare a chicchessia la propria password, trascriverla su di un foglio e consegnarla, in busta chiusa (sigillata e controfirmata sui lembi di chiusura), al Custode delle Password;
- il custode delle Password dovrà annotare sul registro delle Password le date in cui le stesse sono state cambiate al fine di darne evidenza oggettiva in caso di controlli da parte del Garante;
- evitare di lasciare informazioni cartacee, prima e dopo il trattamento, incustodite sulla propria scrivania e custodirle in armadi e/o cassettiere muniti di serratura;
- accertarsi che tali armadi/cassettiere siano rigorosamente sempre chiusi a chiave prima, durante e dopo l'operazione di trattamento (soprattutto se l'ambiente non è presidiato);
- ricordare che il dato elettronico e il dato cartaceo sono sempre sostanzialmente equiparati e, pertanto, qualsiasi dato stampato ed incustodito equivale ad un accesso al proprio PC, anche se spento;
- proteggere i dati (elettronici e cartacei) chiudendo a chiave la propria stanza;
- ricordare che le stanze di lavoro, spesso, vengono pulite da personale esterno all'azienda e, soprattutto, non in presenza degli incaricati del trattamento dei dati;

- utilizzare sempre un criterio di cifratura, quale per esempio la separazione del dato personale da qualsiasi fattore che violi la dignità dell'individuo, adottando, per esempio, le iniziali del nome/cognome eliminando altre componenti che possano far individuare la persona (età, via di residenza, provenienza, ecc.) per la cui violazione si arrecherà danno allo stesso (violazioni di carattere morale, psicologico e materiale, che dovranno, poi, essere annotati sul Registro di data Breach);
- si ricorda che la violazione del dato deve essere comunicata al Garante entro e non oltre le 72 ore (ed entro le 48 ore all'Interessato se si è in presenza di una violazione significativa);
- comunicare/consegnare informazioni personali (certificati, documenti in generale, referti, cartelle cliniche, ecc.) solo al diretto interessato o a persona espressamente e preventivamente delegata;
- mantenere uno stretto riserbo delle informazioni rinvenienti dalle attività lavorative;

Più in generale:

- provvedere ad aggiornare o far aggiornare, quotidianamente, l'antivirus, il firewall, l'antispamming, ecc.;
- evitare di installare software, anche free, se non espressamente autorizzato dal Titolare dei dati;
- evitare di aprire mail sospette (che spesso possono contenere malware) e dare comunicazione al Responsabile della Protezione dei Dati dell'evento sia che sia andato a buon fine che non, per consentire di poter comunicare all'intera Organizzazione la minaccia occorsa;
- evitare di avvalersi di amici e/o esperti di informatica, esterni alla propria struttura, facendoli intervenire sul proprio PC, per qualsivoglia motivo;
- avvalersi di personale, deputato alla manutenzione Hardware, che sia stato nominato con Lettera di Nomina a Responsabile del Trattamento dei Dati (in esterno - ex outsourcing), in caso difforme avvisare il Responsabile della Protezione dei Dati;
- qualora l'intervento manutentivo sull'hardware avvenisse in loco sarà cura dell'utilizzatore garantire che lo stesso avvenga in sua presenza o in presenza di personale di fiducia;
- evitare, ove possibile, di trasferire dati personali all'esterno del perimetro di sicurezza, dove esiste una protezione (organizzativa, fisica e logica) del proprio ambito lavorativo;
- ricordare che i supporti removibili (HD esterni, chiavi USB, CD-ROM, ecc.) non sono sufficientemente protetti e, pertanto, vanno custoditi diligentemente e se non più utilizzati devono essere distrutti;
- effettuare o far effettuare da personale deputato il salvataggio dei dati che risiedono sul proprio PC e che, vari motivi, non sono salvati sui Server, provvedendo ad una conservazione sicura dei supporti che li contengono ed in posti diversi da dove è ubicato ogni singolo PC (al fine di evitare attacchi di natura "*Acts of God*);
- ricordare che il trattamento dei dati personali deve avvenire nel massimo rispetto della dignità della persona al fine di preservarla da ogni violazione, per cui occorrerà fare in modo che i dati siano riservati, integri, disponibili e siano trattati con la dovuta resilienza;

- quindi occorrerà che, durante il trattamento, non si verifichino: accesso illegittimo ai dati, modifiche ai dati e perdita dei dati. Qualora si verificasse ciò bisogna subito avvertire il DPO/RPD per gli adempimenti conseguenti;

Atteggiamenti da tenere da parte dell'Organizzazione :

- avere in debita considerazione l'Accountability - la Responsabilizzazione da tenere durante il trattamento dei dati; nel senso che chiunque tratti dati in nome e per conto del Titolare avrà come obiettivo la salvaguardia delle informazioni e dei dati delle persone con cui entra in contatto;
- occorre mantenere la massima cooperazione e comunicazione degli eventi che possono provocare un attacco ai dati, comunicandolo al DPO;
- ricordare che un banale incidente dovuto ad attacchi (interni/esterni) può provocare la perdita, l'accesso indesiderato o la modifica dei dati. Ciò potrà avere conseguenze enormi sugli Interessati (a livello morale, fisico e materiale);
- mantenere sempre un profilo alto durante le operazioni di trattamento, sapendo che le eventuali sanzioni del Garante saranno in capo a coloro i quali disattendono un atteggiamento responsabile sia durante la vita lavorativa che dopo.