COMUNE DI NOCERA TERINESE

(PROVINCIA DI CATANZARO)

LETTERA DI NOMINA

D. Lgs. 101/2018

Alle *Persone che, ai sensi dell'art. 2- quaterdecies, risultano autorizzate al trattamento dei dati e che operano sotto la responsabilità e nell'ambito del proprio assetto organizzativo del Responsabile del trattamento.*

Tommaso Bruno

Nocera Terinese, 08/04/2024

SPETT.LE
TOMMASO LUCIANO BRUNO
C/O SEDE COMUNE DI NOCERA TERINESE

OGGETTO: Lettera di nomina alla persona autorizzata al trattamento dei dati afferenti l'AreaFinanziaria.

La presente per comunicarle che nell'esecuzione della sua attività lavorativa esegue trattamenti di dati personali e prende visione di documenti che contengono i dati stessi.

La normativa sulla Privacy, già col D. Lgs. 30.6.2003 n. 196 ed il nuovo GDPR (UE 2016/679), ha disposto che il personale che presta l'attività a favore del Titolare dei dati o del Responsabile del trattamento può accedere ai dati personali, se autorizzato al trattamento per iscritto, a compiere le operazioni stesse del trattamento dal Responsabile del trattamento e sempre che operi sotto la diretta autorità, attenendosi alle istruzioni da questi impartite (ex art.30 D. Lgs. 30.6.2003 n. 196) e recepite nell'art. 2- quaterdecies del D. Lgs. 101/18

Lo scrivente, quindi, in qualità di Titolare dei dati personali, conformemente a quanto stabilito dal D. Lgs. 10.08.2018 n. 101 (art. 2-quaterdecies) conferma che nello svolgimento della sua attività potrà trattare:

a) i dati personali contenuti nei documenti che deve utilizzare nello svolgimento delle attività indicate all'oggetto, col mantenimento del riserbo di tutti i dati trattati presso la sede comunale;

b) i dati personali contenuti in archivi e in strumenti elettronici di cui alle areedi volta in volta individuate dal diretto responsabile;

Nell'effettuare il trattamento dei dati personali devono essere soddisfatti i principi della normativa vigente in materia di trattamento dei dati; infatti, *i dati personali devono essere trattati in modo lecito e secondo correttezza, raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi, devono essere esatti e, se necessario, aggiornati, pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati e la loro conservazione nella forma che consenta l'identificazione dell'interessato deve avvenire per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.*

Nello svolgimento delle sue mansioni voglia adottare idonee misure di custodia e di controllo ed in genere qualunque accorgimento che consenta di ridurre al minimo i rischi di distruzione o perdita, anche accidentale di dei dati stessi e che consenta di ridurre al minimo i rischi di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta e voglia osservare le procedure appositamente approntate per evitare quanto detto.

Precisiamo che dovrà eseguire le particolari regole di sicurezza specificamente previste dal D.Lgs. 196/03, dal GDPR (UE 2016/679) e dal D. Lgs. 101/18 secondo le istruzioni, organizzative e tecniche,indicate nel corso di Formazione sulla Privacy impartito. Si prega, altresì, di prendere nota del Mansionario Comportamentale allegato inerente il Trattamento dei Dati Personali.
Con la firma della presente, la persona autorizzata al trattamento dei dati è consapevole delle componenti di riservatezza, integrità, disponibilità e resilienza da adottare durante il trattamento dei dati e si obbliga, alla fine del rapporto lavorativo, di non divulgare, diffondere, comunicare o mantenere (sotto forma sia cartacea che elettronica) i dati e le informazioni dii cui è venuto a conoscenza nella Sede Comunale.

Il Responsabile del trattamento

(Saverio Russo)

La persona autorizzata del trattamento

(Tommaso Luciano Bruno)

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 ambitoUSA;
  - 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 obiettivola salvaguardiadelle 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 chele eventuali sanzioni del Garante saranno in capo a coloro i quali disattendono un atteggiamento responsabilesia durante la vita lavorativa chedopo.