



Al Direttore U.O.C.
Sistemi Informatici ITC
Ing. Bruno Cavalcanti

Al Direttore U.O.C.
Relazioni con il Pubblico
Dott.ssa Angela Improta

Al Responsabile Protezione dei Dati
Avv. Camilla Dolce

Oggetto: Nomina Responsabile della sicurezza dei sistemi informatici

In allegato si trasmette la nomina di cui all'oggetto, di cui alla nota prot. n. 146390 del 12.10.2018, per il seguito di rispettiva competenza.

Il Direttore Amministrativo
Dott. Domenico Concilio



aslnapoli3sud

Direzione Generale Asl Na 3 Sud
Via Marconi n.66 (ex presidio Bottazzi)-Torre del Greco (Na)

Oggetto: nomina responsabile della sicurezza dei sistemi informatici, in applicazione del Regolamento Generale sulla Protezione dei Dati 2016/679 art. 28.

Egr. Ing. Bruno Cavalcanti

In relazione al ruolo funzionale svolto in Azienda in qualità Direttore U.O.C. dei Sistemi Informatici, considerato che, nell'ambito di tale incarico, la S.V. sovrintende, con autonomia operativa, alle procedure del trattamento dei dati e che, per preparazione ed esperienza e competenza tecnica, può fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati personali, ivi compreso il profilo relativo alla sicurezza, con la presente La nomino **responsabile della sicurezza dei sistemi informatici**, nel rispetto delle prescrizioni della Normativa Vigente in materia di Privacy.

Con il presente atto di nomina, Le si affidano l'organizzazione, la gestione e la supervisione di tutte le operazioni di trattamento dei dati personali effettuate attraverso i sistemi informatici.

In particolare alla S.V. sono affidati i seguenti compiti:

- 1) **organizzazione, progettazione e sviluppo dei sistemi informativi per l'immagazzinamento, la gestione e la trasmissione di dati e informazioni digitali delle operazioni di trattamento dei dati, compiute attraverso i sistemi informatici**, nel rispetto delle disposizioni di legge previste dalla normativa vigente.
- 2) **identificazione, nell'area di Sua responsabilità, e nomina per iscritto sia degli Amministratori di sistema sia degli incaricati del trattamento dei dati personali e/o sensibili**, attraverso un atto di nomina individuale, corredato da strumenti idonei a impartire istruzioni e indicazioni pertinenti ed efficaci per garantire la conoscenza di quanto disposto dalla normativa in materia;
- 3) **controllo e vigilanza sul rispetto dell'incarico attribuito e sulle istruzioni specifiche impartite agli Amministratori di Sistema ed agli incaricati del trattamento dei dati personali e garanzia che tutte le misure di sicurezza riguardanti i dati personali siano applicate da tutti i soggetti dalla S.V. incaricati del trattamento;**
- 4) **identificazione e nomina per iscritto, qualora la S.V. lo ritenga necessario, di un incaricato della gestione e della manutenzione degli strumenti elettronici, di un Incaricato della custodia delle copie delle credenziali e di un Incaricato delle copie di sicurezza delle banche dati;**
- 5) **aggiornamento, ad ogni variazione: a) dell'elenco delle banche dati oggetto di trattamento; b) dell'elenco dei sistemi di elaborazione; c) dell'elenco delle sedi e degli uffici di Sua competenza;**
- 6) **verifica periodica delle modalità di accesso e di protezione ai locali nonché cura di impartire istruzioni particolari per la custodia e la conservazione dei supporti utilizzati per le copie dei dati;**
- 7) **organizzazione del trattamento in modo tale, che agli interessati possa venir data pronta soddisfazione nell'esercizio dei loro diritti, di cui all'articolo 15 (Diritto di accesso) del GDPR (General Data Protection Regulation 679/2016);**
- 8) **comunicazione immediata al Titolare del trattamento di ogni richiesta, ordine o attività di controllo da parte del Garante o di Autorità Giudiziaria;**
- 9) **trasmissione periodica al titolare del trattamento, entro il mese di gennaio di ogni anno, di una relazione attestante l'osservanza degli obblighi previsti dalla normativa privacy con riferimento all'anno precedente;**
- 10) **adozione di tutte le misure necessarie per garantire che il trattamento dei dati informatizzati in Azienda sia conforme ai principi di protezione dei dati (in altre parole, è necessario applicare, caso per caso, il principio di**

ba

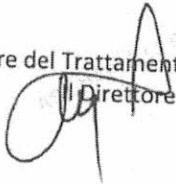
adeguatezza alle finalità perseguite una specie di dovere di minimizzazione dei dati da parte del responsabile del trattamento).

In funzione dell'incarico conferito, la S.V. è tenuta a :

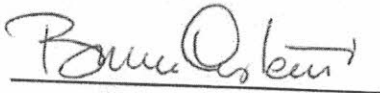
- 11) **Verificare in anticipo se la sicurezza informatica è conforme alle disposizioni generali e specifiche applicabili al settore;**
- 12) **Provvedere a diffondere, fra gli Amministratori di sistema e gli incaricati del trattamento, le istruzioni necessarie per la sicurezza e contribuire, sulla base della sua applicazione, alla revisione periodica di tutti i documenti in materia;**
- 13) **Controllare che :**
 - il trattamento dei dati da parte del personale posto alle Sue dirette dipendenze avvenga in modo lecito e secondo correttezza;
 - la raccolta e la registrazione avvengano: a) per scopi determinati, compatibili, legittimi e nell'ambito del trattamento necessari a quanto prefissato in azienda (protezione della proprietà e degli individui ed altri interessi legittimi); b) in modo esatto e, se necessario, con gli opportuni aggiornamenti; c) rispettando il criterio che essi risultino pertinenti, completi e non eccedenti rispetto alle finalità di raccolta; d) in maniera che la loro conservazione sia funzionale al periodo di tempo necessario allo scopo per il quale sono stati raccolti e successivamente trattati.

La presente dovrà essere restituita firmata per accettazione in ogni sua pagina.

Il Titolare del Trattamento dati ASL Napoli 3 Sud
Il Direttore Generale



Il Responsabile della Sicurezza informatica
Firma per accettazione



PRESCRIZIONI GENERALI PER IL RESPONSABILE AZIENDALE DELLA SICUREZZA INFORMATICA

- Il responsabile Aziendale per la sicurezza informatica è garante della gestione e dell'esercizio dei Sistemi Informatici dell'Azienda. Ha la responsabilità complessiva dei progetti, della manutenzione e dell'esercizio dei sistemi esistenti. Di conseguenza, sovrintende e guida gli amministratori di sistema e gli incaricati rispettivamente delle reti, dei centri dati, dei progetti informatici, e dell'elaborazione per utenti finali. Collabora e guida i consulenti aziendali eventualmente nominati sui requisiti, lo sviluppo e l'esercizio dei sistemi informatici. Avendo chiara competenza e comprensione delle implicazioni delle Tecnologie informatiche sulla strategia aziendale, è garante delle pratiche di pianificazione e di controllo della loro gestione. Ha il compito di identificare gli impatti di tipo legale, di privacy, di sicurezza e di altri regolamenti sui sistemi informatici e, con il supporto di specifici consulenti, cura di intraprendere iniziative appropriate per attenersi a tali regolamenti. Intraprende azioni di gestione del cambiamento per assicurare l'efficacia dei progetti di sistemi informatici.
- Operando su sistemi informativi complessi - *sistemi di tecnologie informatiche e di automazione e quindi tutta l'infrastruttura ICT dell'Azienda* - o con consulenti su progetti più ampi o complicati, definisce l'architettura dei sistemi, identifica e seleziona piattaforme adeguate per il software applicativo, assicura adeguati requisiti utente, pianifica e assicura il collaudo e l'esercizio dei sistemi documentando tutto il lavoro mediante standard, metodi e strumenti richiesti. Gioca un ruolo fondamentale nella pianificazione dell'installazione dei sistemi informatici (software, hardware, rete) interagendo con tutte le parti interessate per assicurare che siano soddisfatte le priorità d'installazione e che si minimizzino i disturbi all'azienda.
- Laddove i sistemi informatici siano stati dati in outsourcing, supporta la negoziazione dei contratti per ottenere il livello di servizio richiesto, stabilendo le procedure di risoluzione dei problemi e definendo le conseguenze per le non conformità. S'interfaccia con i progettisti e i pianificatori di fornitori esterni e opera all'interno dei gruppi che si occupano dell'approvvigionamento di apparati, software, servizi di consulenza e altri servizi per i sistemi informativi.
- Si assume la responsabilità di curare la pianificazione dell'installazione e dell'aggiornamento delle piattaforme e del software applicativo e hardware correlati operando insieme ai dipendenti responsabili centro dati, responsabili delle reti, responsabili di progetto di sistemi informativi - se designati - e così via).
- Diagnostica e cura della risoluzione dei problemi (ad esempio scarse prestazioni) e guasti (ad esempio guasti di sistema) che possono verificarsi nell'esercizio, verificando che si tenga conto dei livelli di servizio concordati e delle necessità di qualità, sicurezza informatica, disponibilità e tutela della salute.
- Risponde a richieste da parte di utenti, specialisti o altri e affronta in modo efficace un ampio insieme di problemi di complessità moderata, assicurandosi che la documentazione dei sistemi e dei software supportati sia disponibile e in formato adeguato. Mantiene registrazioni per assicurare che i problemi siano gestiti in conformità con gli standard e le procedure concordati.
- Valuta, come richiesto, i miglioramenti di progetto, i cambiamenti di capacità, le disposizioni di emergenza e ripristino ed è consapevole dei requisiti operativi, soprattutto in termini di livelli di servizio, disponibilità di rete, tempi di risposta, sicurezza e tempi di ripristino. Controlla l'allineamento dei sistemi informatici alle pratiche e alle tecnologie migliori.
- S'informa delle implicazioni della legislazione pertinente o di altri regolamenti esterni che influenzano la sicurezza in ogni ambito dei servizi e delle attività di rete.

Il Responsabile della Sicurezza Informatica
per accettazione

Bruno Ortemi