COMUNICAZIONE AGLI INTERESSATI EX ART. 34, PAR. 3, LETT. C) DEL REGOLAMENTO EUROPEO (UE) 2016/679

Agli Utenti della Azienda Sanitaria Napoli 3 Sud,

l'ASL Napoli 3 Sud è stata vittima di un attacco hacker perpetrato in data 7.1.2022 da parte di un noto gruppo di cyber criminali, i quali sono riusciti ad accedere illegalmente ai sistemi informatici dell'Azienda, sottraendo *file* aziendali contenenti dati personali.

Non essendo stato possibile individuare ogni interessato al fine di procedere alle comunicazioni individuali, e considerando sproporzionato lo sforzo per raggiungere tali soggetti, l'ASL Napoli 3 Sud rende note le seguenti informazioni e canali di contatto agli interessati non raggiunti già da comunicazione personale.

L'Azienda ha da subito coinvolto le Forze dell'Ordine competenti e prontamente informato, e costantemente continua ad aggiornare, le principali Autorità di settore (***Garante Privacy***, ***Agenzia per l'Italia Digitale*** e ***CSIRT dell'Agenzia Nazionale Cyber Security***).

Inoltre, per porre rimedio alla violazione, l'ASL Napoli 3 Sud ha subito isolato i sistemi e le macchine colpite dal virus malevolo e ha proceduto alla bonifica dell'intero sistema informatico, innalzando, altresì, i livelli di sicurezza degli stessi.

Infatti, mediante l'affidamento di specifico incarico a rilevanti società in ambito *cyber security* e *compliance* aziendale, si è acquisita la strumentazione informatica di ultima generazione per monitorare h 24, 7 giorni su 7, il perimetro aziendale e rilevare tempestivamente l'esistenza di ulteriori minacce potenziali o latenti, anche per prevenire simili violazioni in futuro.

È stata anche istituita un'apposita Task Force il cui compito è stato principalmente quello di analizzare le informazioni carpite al fine di individuare le tipologie di dati personali e di interessati coinvolti nella violazione, per procedere efficientemente agli obblighi previsti dalla legge.

Da tale analisi, è stato possibile individuare tracce di attività di lettura/copiatura delle seguenti tipologie di dati, per cui si ha il forte sospetto di una potenziale esfiltrazione.

Di seguito, si riporta analiticamente l'elenco:

Tipologia di Interessati	Tipologia di dati personali
PAZIENTI	Dati personali identificativi
	Dati relativi alla salute
	Esito tampone Covid
	Dati vaccinazione
MINORI DI ETÀ	Dati personali identificativi
	Dati relativi alla salute
	Esito tampone Covid
	Dati vaccinazione
DIPENDENTI	Attività del personale
	Documentazione giuridica e contabile del personale
	Documenti personali
	Referti/certificazioni

Eventuali ulteriori evidenze che dovessero emergere nel corso dell'analisi, tuttora in atto, saranno prontamente comunicate attraverso il presente canale, nonché attraverso il sito web istituzionale della ASL Napoli 3 Sud.

Scusandoci per il disagio, che va comunque ricondotto ad un crimine vile e imperdonabile, ci teniamo a specificare che la scrivente Azienda fin dai primi momenti ad ora, ha fatto tutto quanto in suo potere e facoltà per porre rimedio agli effetti dell'attacco subito e alle possibili conseguenze per gli interessati, nonché per prevenire simili attacchi in futuro tramite l'implementazione di ulteriori misure di sicurezza organizzative e tecniche ai sensi dell'art. 32 GDPR.

Per ulteriori chiarimenti e/o informazioni di dettaglio, può contattare il Responsabile della Protezione Dati dell'Azienda - Dr. Maurizio Pastore– **assistenza.databreach@aslnapoli3sud.it** o chiamare il **numero verde dedicato per l'emergenza 081-18408323**

Cordiali saluti,
Il Direttore Generale, Ing. Gennaro Sosto