Provvedimento del 28 settembre 2023 [9941232]

VEDI ANCHE Newsletter del 23 ottobre 2023

[doc. web n. 9941232]

Provvedimento del 28 settembre 2023

Registro dei provvedimenti
n. 426 del 28 settembre 2023

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, alla quale hanno preso parte il prof. Pasquale Stazione, presidente, la prof.ssa Ginevra Cerrina Feroni, vicepresidente, il dott. Agostino Ghiglia e l'avv. Guido Scorza, componenti, e il cons. Fabio Mattei, segretario generale;

VISTO il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE, "Regolamento generale sulla protezione dei dati" (di seguito "Regolamento");

VISTO il d.lgs. 30 giugno 2003, n. 196 recante il "Codice in materia di protezione dei dati personali", contenente disposizioni per l'adeguamento dell'ordinamento nazionale al Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE (di seguito il "Codice");

VISTO il d.lgs. 10 agosto 2018, n. 101 recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE";

VISTO il Regolamento n. 1/2019 concernente le procedure interne aventi rilevanza esterna, finalizzate allo svolgimento dei compiti e all'esercizio dei poteri demandati al Garante per la protezione dei dati personali, approvato con deliberazione del n. 98 del 4/4/2019, pubblicato in G.U. n. 106 dell'8/5/2019 e in www.gpdp.it, doc. web n. 9107633 (di seguito "Regolamento del Garante n. 1/2019");

VISTA la documentazione in atti;

VISTE le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del Regolamento del Garante n. 1/2000 sull'organizzazione e il funzionamento dell'ufficio del Garante per la protezione dei dati personali, doc. web n. 1098801;

Relatore il dott. Agostino Ghiglia;

PREMESSO

1. La violazione dei dati personali e le istanze degli interessati

In data XX la Asl Napoli 3 Sud (di seguito "Azienda") ha notificato all'Autorità, ai sensi dell'art. 33 del Regolamento, una violazione dei dati personali -successivamente integrata con note del XX e XX, XX e XX- riguardante un attacco informatico, determinato da un malware di tipo ransomware, ai sistemi informativi della stessa.

In considerazione dell'elevato numero di interessati coinvolti e della natura dei dati personali oggetto di violazione, l'Ufficio ha richiesto informazioni all'Azienda in merito alla citata violazione di dati personali, al fine di acquisire, in particolare, elementi sia sulle misure tecniche e organizzative adottate in merito alle procedure di autenticazione informatica per l'accesso in VPN e alle postazioni di lavoro, che erano in essere al momento della violazione, sia sullo stato di avanzamento degli interventi di adozione di misure idonee a prevenire simili violazioni future (nota del XX).

A tale richiesta, l'Azienda ha fornito riscontro, con nota del XX, dichiarando che:

- "da un'analisi della documentazione in possesso della ASL Napoli 3 Sud, relativa al sinistro privacy occorso e notificato in data XX, (…) non risultano correlazioni rispetto alle credenziali e utenze compromesse in tale evento e le credenziali oggetto di data leak nel data breach di XX";

- "in relazione alle risultanze connesse al sinistro privacy di XX e relativo alle "credenziali rubate e pubblicate sul dark web per guadagnare un accesso fraudolento in VPN", si fornisce (…) un prospetto riepilogativo delle correlazioni tra l'Incident Report "Executive & Technical Report — Sabbath Ransomware Security Incident" del XX, (…) e le indagini condotte dallo IOC nel black market riportate nel report "XX"";

- "l'unità ICT Aziendale ha adottato il "Regolamento per l'utilizzo del sistema informatico e telematico aziendale" contenente agli artt. 13 e 31, rispettivamente, l'indicazione delle caratteristiche delle password e l'indicazione per l'accesso al Virtual Private Network (VPN). Nello specifico, al momento della violazione le procedure di autenticazione informatica utilizzate nell'ambito dell'accesso in VPN e alle postazioni di lavoro non prevedevano l'uso del doppio fattore di autenticazione, mentre la password policy non comprendeva una differenziazione tra utenze con privilegi amministrativi e utenza senza privilegi amministrativi. In particolare, le password erano create dal servizio informatico definite con modalità di active directory secondo caratteristiche che prevedevano: la creazione di password con almeno 8 caratteri, la scadenza automatica a XX dal rilascio e la presenza nella chiave di caratteri maiuscoli, minuscole e numeri. Giova evidenziare come, allo stato attuale, a seguito di adesione a gara su portale MePA n. 2006825, a far data dalla notificazione conclusiva del sinistro privacy occorso, l'ente ha efficacemente adottato l'autenticazione multi-fattore per le connessioni VPN "instaurata con il Firewall perimetrale XX con doppio fattore di autenticazione (XX)".

Nella stessa occasione, l'Azienda ha descritto lo stato di avanzamento degli interventi di adozione nelle misure tecniche e organizzative per prevenire simili violazioni future, individuate nel documento "Progressi delle attività di ripristino e relative misure di sicurezza adottate" prodotto dalla società Leonardo S.p.A.

In ordine alla medesima vicenda, sono pervenute, tra XX e XX, alcune istanze da parte di cittadini nei confronti dell'Azienda che, informati dell'evento occorso, si sono rivolti all'Autorità.

Successivamente, è stata effettuata un'attività ispettiva nei confronti dell'Azienda nel mese di XX,

al fine di acquisire elementi utili alla compiuta valutazione del fatto.

2. La violazione dei dati personali

2.1. Il fatto

La violazione dei dati personali è stata descritta sia nell'ambito della notifica effettuata ai sensi dell'art. 33 all'Autorità, successivamente e più volte integrata, sia nel corso della citata attività ispettiva. In particolare, è risultato quanto segue.

2.1.1. La notifica della violazione al Garante

Con la notifica del XX, l'Azienda ha dichiarato che:

> - "nella mattinata del XX si sono verificati malfunzionamenti dei sistemi sanitari sottesi all'erogazione dei servizi ospedalieri e di Laboratorio. Le prime verifiche effettuate non hanno consentito un accesso alle infrastrutture necessario per il ripristino delle funzionalità: tutti i server su cui veniva tentato l'accesso presentavano anomalie e il mancato riconoscimento delle utenze con profilo di amministratore. La rete locale interna non consentiva il normale accesso e la navigazione sul web anche verso piattaforme esterne al perimetro aziendale se non tramite linee di accesso secondarie";
>
> - "si è potuto appurare che: 1. l'intera infrastruttura del Datacenter (Server, Domain Controller, Proxy, VPN) è stato oggetto di attacco hacker di tipo cryptoLocker con attività di encryption dei dati aziendali e dei volumi virtuali che consentono il funzionamento di tutti gli applicativi aziendali; 2. sono stati compromessi gli elenchi degli utenti di dominio con profilo di amministratore rendendo impossibili gli accessi ai sistemisti aziendali; 3. è stata riscontrata su tutte le diverse postazioni la presenza di un file denominato DECRYPTION.txt con il quale viene comunicata la natura dell'attacco, il gruppo criminale "54BB47H" (Sabbath) che ha effettuato il medesimo attacco e le modalità con le quali entrare in contatto al fine di riscattare i codici per il Decrypting dei file compromessi";
>
> - "sono stati coinvolti tutti i software e dati relativi alle piattaforme applicative installate sui server virtuali del Data Center Principale di Castellammare di Stabia (Na) e Data Center Disaster Recovery di Brusciano (Na). Inoltre, sono coinvolti i Data Center delocalizzati installati presso i Presidi Ospedalieri di Nola, Sorrento, Boscotrecase, Castellammare di Stabia presso i quali sono installati i software applicativi del Pronto Soccorso, ADT e diagnostica per immagini. Il blocco dei Data Center Aziendali causa il fermo di tutti gli applicativi aziendali di ordine sanitario e amministrativo contabile; restano funzionanti le applicazioni su piattaforme esterne (Regionale, SORESA, Ministeriale) quali CUPR, Vaccinazioni, Anagrafe Assistibili, 118, Vaccinazioni e Tamponi Covid-19" (v. notifica del XX).

Successivamente, avvalendosi della facoltà di fornire ulteriori informazioni in fasi successive, l'Azienda ha integrato la predetta notifica in data XX e XX, XX e XX, rappresentando:

> - di aver "ricevuto a mezzo mail due differenti comunicazioni rispettivamente in data XX e XX: la prima da parte di XX con la quale la "terza parte" si offre di decrittare gratuitamente le informazioni ostaggio del gruppo cyber criminale Sabbath; la seconda da parte di più indirizzi mail, direttamente riconducibili al gruppo Sabbath, con la quale si descriveva la sola e unica modalità di decrittazione dei file colpiti dal cryptolocker, ossia mediante diretta collaborazione col suddetto gruppo di cybercriminali. Si rappresenta, altresì, che tali nuove circostanze sono state oggetto di pronta informativa e costituiranno oggetto di formale integrazione di denuncia alla Polizia Postale" (v. notifica del XX);

- che “all’interno del portale associato al ransomware Sabbath (http://...), è stata individuata la pubblicazione afferente la ASL Napoli 3 Sud, accessibile al seguente link: http://...” (v. notifica del XX);

- che “le analisi condotte, per mezzo delle prove acquisite dal CCMT Leonardo, rilevavano una potenziale compromissione dalla rete VPN utilizzata dagli operatori e dai fruitori dei servizi medicali della ASL NAPOLI 3 SUD. Analisi OSINT hanno successivamente confermato la compromissione di numerosi account non privilegiati e la loro pubblicazione su diversi black market. Le credenziali pubblicate sul Web hanno permesso a molteplici attori di accedere alla rete interna della ASL NAPOLI 3 SUD senza destare alcun sospetto potenzialmente notificabile dagli apparati di sicurezza in uso presso l’Azienda. L’attaccante (…), accedeva ai server dell’Azienda per mezzo del canale VPN il giorno XX alle ore XX effettuando in breve arco temporale l’innalzamento dei privilegi ad amministratore di sistema. Nei giorni successivi, dal XX al XX, l’attaccante procedeva con le azioni di persistenza garantendosi molteplici vie di accesso, tra cui la diffusione di tool di comando e controllo remoto noto come Cobalt Strike. Contemporaneamente, lo stesso, effettuava azioni di harvesting accumulando documenti e reperti residenti su asset di dipendenti, successivamente esfiltrati. Il giorno XX alle ore XX l’attaccante guadagnava nuovamente l’accesso tramite canale VPN preparando la rete interna ad un attacco distruttivo. La mattina del XX veniva avviato il ransomware Arcane.exe (Sabbath) cifrando molteplici files e documenti. A valle dell’attività di cifratura, gli operatori IT dell’Azienda notavano il cambio dell’estensione dei file residenti sul disco dei propri asset ed una lettera di riscatto (…)” (v. notifica del XX);

- che “i servizi che hanno subito solo parzialmente un’interruzione sono stati individuati rispetto i seguenti item: (i) stipendi del personale dipendente; (ii) acquisizione e liquidazione fatture fornitori e rimborsi. Si specifica che l’erogazione dei servizi verso l’utenza e la somministrazione della prestazione sanitaria è stata svolta in maniera continuativa senza soffrire interruzioni di qualsivoglia sorta” (v. notifica del XX).

2.1.2. Le attività ispettive

Nel corso delle attività ispettive, l’Azienda, riguardo alle modalità e alle tempistiche dell’attacco, ha inoltre “confermato la […] timeline [presente nel report XX] e riferito che le analisi forensi hanno ricostruito la violazione a partire dai primi accessi abusivi, a XX, da IP estero, tramite VPN, con le credenziali di personale non tecnico della ASL, disponibili nel dark web. Tali credenziali sono state, poi, utilizzate per ottenere privilegi di administrator. A seguire, dopo una fase silente, l’attaccante ha proceduto a installare e distribuire il malware e, nel mese di XX, sono state compromesse le credenziali di amministratori di dominio e lanciata la cifratura sul Hypervisor dei VMDK (file fisici delle macchine virtuali). L’incidente è stato, quindi, rilevato il XX mattina da un operatore sanitario che, riscontrato un malfunzionamento dell’applicazione (IL), ha contattato la persona reperibile dei sistemi informatici che, a seguito di specifiche verifiche, constatando la modifica delle credenziali di amministratore di dominio, ha dato l’allarme”. Nella medesima occasione l’Azienda ha dichiarato che “il XX mattina [è stato] trovato, accedendo a un server bloccato, il messaggio di richiesta di riscatto degli attaccanti”, che “l’esfiltrazione dei dati, presumibilmente, è avvenuta fra XX e XX” e “che la violazione non ha coinvolto gli applicativi di ingegneria clinica nei singoli presidi (es. TAC, RMN, monitor) né strumentazione RIS-PACS dei presidi, mentre sono stati bloccati tutti gli applicativi aziendali serviti dal data center compresi i sistemi di ADT che hanno avuto priorità nel ripristino” (v. verbale del XX, pagg. 3 e 4).

2.2. Le misure in essere al momento della violazione

2.2.1. Notifica della violazione al Garante

Con riferimento alle misure in essere al momento della violazione, nell'ambito della notifica e delle conseguenti integrazioni, l'Azienda ha dichiarato che "il sistema informatico aziendale si basa su un dominio XX applicativo On-premise per tutti i software applicativi sanitari e amministrativo contabili e un dominio XX per la gestione XX della posta elettronica aziendale, Office Automation, sito web e PEC XX. La rete LAN aziendale è estesa all'intero territorio di competenza ASL tramite contratto SPC in convenzione Consip con fornitore Fastweb. Sono stati previsti i seguenti strumenti di sicurezza:

a. Accesso dall'esterno tramite VPN Firewall XX

b. Firewall perimetrali XX per il controllo del traffico I/O gestiti da Fastweb tramite contratto CONSIP

c. Proxy XX per il collegamento dei client come unico accesso verso internet con restrizioni all'accesso a siti normativamente/aziendalmente non autorizzati, limitazione sui flussi pubblicitari e popup

d. Sistemi Firewall XX per il monitoraggio del traffico di rete per I/O con SSL Ispection per i pacchetti di Posta Elettronica (XX)

e. Antivirus/Antimalware XX su Server e client supportati da ulteriore software di monitoraggio XX (XX) per gestione comportamentale

f. Sistema di monitoraggio XX per la gestione, virtual patching e messa in sicurezza delle strumentazioni elettromedicali presenti in azienda (attualmente in prova gratuita)

g. Policy privacy data breach con relativi allegati" (v. notifiche del XX e XX).

Ulteriori elementi sul punto sono stati forniti dall'Azienda con la sopra citata nota del XX, trasmessa in riscontro a una specifica richiesta di informazioni dall'Ufficio (nota del XX) circa le procedure di autenticazione informatica utilizzate nell'ambito dell'accesso in VPN e alle postazioni di lavoro in essere al momento della violazione e le password policy previste per le diverse tipologie di utenze (cfr. par. 1 del presente provvedimento).

2.2.2. Attività ispettive

Nel corso delle attività ispettive l'Azienda ha, altresì, chiarito che "gli utenti che si avvalevano della VPN erano circa 1200, che non era prevista una procedura di autenticazione a più fattori e che l'autenticazione veniva effettuata mediante le credenziali di dominio […]", che "le credenziali riconducibili ai medici di medicina generale (MMG) erano censite in Active Directory in uno specifico gruppo per cui era impedito interactive logon consentendo solo l'utilizzo di uno specifico applicativo dedicato ai medesimi MMG esposto in VPN", che "all'epoca dell'incidente di XX, era prevista una diversa password policy per le utenze dei sistemisti administrator dei server (XX)", che "all'epoca dell'incidente di XX, non era attivo il meccanismo di password history per impedire il riutilizzo delle password" (v. verbale del XX, pag. 3).

Con riguardo alle misure tecniche e organizzative adottate per garantire la disponibilità e la resilienza dei sistemi e dei servizi di trattamento, nonché il ripristino tempestivo della disponibilità e dell'accesso dei dati personali in caso di incidente, l'Azienda, nel corso delle medesime attività ispettive ha dichiarato che "non c'è una procedura formalizzata e che il backup dei dati e dei sistemi aziendali è effettuato "full" una volta a settimana e "incrementale" gli altri giorni" e che "l'Azienda al momento della violazione non disponeva di un piano di rispristino dei diversi servizi con particolare riguardo a quelli definiti "critici" e che, a seguito dell'incidente, ha predisposto una proposta di piano di ripristino che la direzione aziendale ha approvato" (v. verbale del XX, pag. 5).

2. 3. Le misure adottate a seguito della violazione

2.3.1. Notifica della violazione al Garante

Con riferimento alle misure adottate a seguito della violazione, l'Azienda, nell'ambito della notifica della violazione, effettuata ai sensi dell'art. 33 del Regolamento, ha rappresentato che:

- "si è proceduto a isolare le connessioni e le comunicazioni dall'esterno al fine di interrompere la possibile propagazione del malware. È stata avviata un'attività di indagine tesa all'analisi del sinistro e delle sue cause al fine di pervenire alla bonifica dei sistemi. Si intende procedere nell'immediato alla creazione di un'infrastruttura parallela per il ripristino, altresì, delle attività essenziali" (nota del XX);

- "gli effetti osservati hanno evidenziato uno scenario in cui risultavano sospesi diversi sistemi e servizi ICT critici. Il reparto IT della ASL, compreso l'evento ha avviato le più immediate azioni di contenimento, tra le quali: isolamento dell'infrastruttura e dei servizi ICT, rendendoli temporaneamente indisponibili; interruzione di tutti i servizi informatici indipendentemente dal loro posizionamento, per evitare la propagazione dell'infezione. L'attacco ha creato un disservizio limitato sull'erogazione dei servizi critici nei confronti degli utenti finali in quanto il sito web, la posta ed ulteriori servizi risultavano ospitati da terze parti; coinvolgimento di partner e stakeholder e attivazione di un'unità di crisi al fine di identificare le azioni di contenimento e di rimozione definitiva della minaccia. Tra le diverse azioni immediate, si segnalano:

  • avvio delle attività di analisi in ambito cyber threat hunting;

  • avvio di opportune analisi in ambito Cyber Threat Intelligence a supporto delle attività di Response;

  • avvio delle attività di ripristino dell'infrastruttura compromessa mediante la creazione di una nuova zona denominata green zone;

  • creazione di una taskforce [multidisciplinare] dedicata alla valutazione della sensibilità dei dati oggetto di pubblicazione sul portale dell'attaccante" (nota del XX).

Con la predetta nota del XX, l'Azienda ha ulteriormente rappresentato che, "con espressa istanza rivolta al fornitore Fastweb S.p.A., si è inteso richiedere specifica attività di analisi del malfunzionamento teso all'identificazione delle cause e degli effetti del data breach. È stato affidato specifico incarico alla Leonardo S.p.A. per l'analisi dell'incidente in Second Opinion e redazione di report finalizzati alle specifiche attività di remediation, oltreché per la rimodulazione e aggiornamento del piano di disaster recovery che consenta di garantire la business continuity, nonché la predisposizione di tutte le misure tecniche e organizzative adeguate volte al monitoraggio, controllo e prevenzione del perimetro tecnologico e di sicurezza aziendale. Si è proceduto, altresì, all'attivazione di nuove connessioni VPN dedicate con doppia autenticazione per poter accedere in modo sicuro all'interno della struttura informatica aziendale al fine di porre in essere le attività di accertamento e analisi sui sistemi, che sono tutt'ora in corso di esecuzione. L'ASL Napoli 3 Sud, conclusa la prima fase critica di contenimento dell'incidente informatico, attraverso attività di progettazione di Green Zone, di crisis management e di intelligence security assessment, intende, mediante il supporto del fornitore Leonardo S.p.A., procedere all'implementazione dei seguenti strumenti, policy e servizi al fine di prevenire simili future violazione ed elidere ogni restante profilo di vulnerabilità nel sistema di sicurezza:

Ripristino dei servizi con attività di Application Security Testing, VA, PT;

Servizi tuning XDR, RTSM+IH, TIS, Basket Crisis Management & Incident Response;

Progettazione di un Sistema per le applicazioni;

Attività di Threat Intelligence System (Early Warning, Data Loss Prevention, Brand Abuse, Anti-Phishing con takedown);

Supporto specialistico on premise con risorse TAM, CERT con skill cyber;

Policy Enforcement, Awareness, Phishing Campaign, Data Rescue.

A seguito dell'implementazione di tali servizi, da considerarsi a Priorità Alta, seguirà l'adozione degli ulteriori servizi di seguito elencati: Unified End-Point Management UEM/MDM; DNS Secure; Verifica analisi sistema di backup, Anti DDoS, NACSistema di mail secure; Assessment FNCS; Attack simulation e resilience testing – Cyber Exercise. Alle attività e servizi tecnici sopracitati si aggiungono l'implementazione di un Sistema di Gestione per la Sicurezza delle Informazioni (SGSI), nonché un servizio di formazione con messa a disposizione di una piattaforma FAD asincrona in materia di Sicurezza delle Informazioni in favore di tutto il personale dipendente dell'ASL Napoli 3 Sud".

2.3.2. Attività ispettive

Nel corso delle attività ispettive, con riferimento alle operazioni di ripristino dei dati e dei sistemi, l'Azienda ha dichiarato che "è stato definito un piano di ripristino dei sistemi grazie alla presenza dei backup" (verbale del XX, pag. 4) e che "le azioni di bonifica, recupero e ripristino attivate immediatamente dopo l'effettuazione delle copie forensi, hanno portato la disponibilità dei primi sistemi (CACOMM e AREAS) al XX e, a seguire, gli altri fino a inizio XX, anche sulla base della citata proposta. Parallelamente si è proceduto alla bonifica, recupero e ripristino delle postazioni di lavoro" (verbale del XX, pag. 2).

2.4. La comunicazione della violazione agli interessati

In relazione alla comunicazione della violazione agli interessati, l'Azienda ha preliminarmente rappresentato che "gli interessati sono stati informati mediante comunicazione pubblicata sul sito web istituzionale" (v. notifica del XX) e, successivamente, che tale comunicazione sarebbe stata effettuata "entro il XX" allegando anche il "sample della comunicazione ex art. 34 GDPR da trasmettere ai circa 67000 interessati coinvolti nella violazione" (v. notifica del XX).

Da ultimo, l'Azienda ha dichiarato che "deve ritenersi il rischio per gli interessati alto e, dunque, necessario procedere con le comunicazioni agli interessati ex art. 34 GDPR. Atteso che per numero 70.891 interessati è già stata predisposta comunicazione ad personam per il tramite della società Mavasoft a r.l.s., appositamente nominata ex art. 28 GDPR, ovvero per comunicazione e-mail nel caso dei dipendenti; per il restante elevato numero di interessati deve considerarsi quanto già affermato alla Sez. F, p. 7 (Descrizione della Violazione) in termini di costi e sforzo sproporzionato ai sensi dell'art. 34, par. 3, lett. c) GDPR, come anche già descritto e paventato per il tramite di comunicazione PEC inviata a codesta Autorità in data XX. Per tali ordini di ragioni, (…) la scrivente Azienda ha inteso procedere con comunicazioni informative verso l'utenza a carattere generale" e che "ha necessariamente dovuto gestire e adottare due distinte modalità di comunicazione agli interessati, intrinsecamente legate alle caratteristiche dei due data set ed al loro diverso momento di analisi e valutazione […] per una visione completa della gestione delle comunicazioni di seguito si riporta la suddivisione schematica della gestione delle comunicazioni agli interessati ex art. 34 GDPR in relazione alle peculiarità dei due dataset gestiti da parte di codesta azienda: 70.738 interessati pazienti/utenti raggiunti da comunicazione ad personam tramite raccomandata a/r, con servizio affidato al responsabile del trattamento ex art. 28 GDPR MAVASOFT srls; 153 interessati dipendenti raggiunti da comunicazione ad personam tramite servizio di mail aziendale, mail personale ovvero raccomandata XX interessati pazienti/utenti,

tramite comunicazione generale (…)" (v. notifica del XX).

3. Valutazioni del Dipartimento sul trattamento effettuato e notifica della violazione di cui all'art. 166, comma 5 del Codice

In ordine alla fattispecie descritta l'Ufficio, sulla base di quanto rappresentato dal titolare del trattamento nell'atto di notifica di violazione e di quanto emerso nel corso dell'attività ispettiva, nonché delle successive valutazioni, ha notificato all'Azienda, ai sensi dell'art. 166, comma 5, del Codice, l'avvio di un procedimento per l'adozione dei provvedimenti di cui all'art. 58, par. 2, del Regolamento, invitando il predetto titolare a produrre al Garante scritti difensivi o documenti ovvero a chiedere di essere sentito dall'Autorità (art. 166, commi 6 e 7, del Codice; nonché art. 18, comma 1, dalla legge n. 689 del 24/11/1981). In particolare, con atto n. XX del XX, che qui deve intendersi integralmente riprodotto, l'Autorità ha ritenuto che l'Azienda ha effettuato il trattamento di dati personali in questione in violazione dei principi di "integrità e riservatezza", di cui all'art. 5, par. 1, lett. f), della "protezione dei dati fin dalla progettazione" di cui all'art. 25, par. 1, del Regolamento, nonché degli obblighi in materia di sicurezza, di cui all'art. 32 del Regolamento.

L'Azienda ha fatto pervenire le proprie memorie difensive, ai sensi dell'art. 166, comma 6, del Codice, senza chiedere di essere ascoltata dall'Autorità. In particolare, con nota del XX, ha dichiarato che:

> "la violazione ha comportato una perdita di riservatezza e di disponibilità dei dati. La duplice natura della violazione si articola verosimilmente in due distinte fasi: (i) la perdita di riservatezza si può constatare nel momento in cui gli attaccanti hanno effettivamente avuto accesso ai sistemi informatici dell'ASL, nonché nel momento in cui hanno proceduto all'esfiltrazione del dataset individuato; (ii) la perdita di disponibilità, al contrario, è avvenuta al momento dell'exploit dell'attacco attraverso il "lancio" del programma CobaltStrike per il criptaggio dei sistemi informativi della ASL";
>
> "in relazione alla gravità della violazione non è stato possibile non considerarla come elevata. Infatti, in ragione del numero e della tipologia di interessati coinvolti, nonché in merito al volume e tipologie di dati personali impattati, non poteva potenzialmente ab initio non considerarsi come avente un'alta probabilità di avere cagionato conseguenze lesive per i diritti e le libertà degli interessati. Conseguenze che (…), non sembrerebbero, tuttavia, essersi concretizzate in effettivi e riscontrabili nocumenti per gli interessati";
>
> "per quanto attiene alla durata della violazione, bisogna opportunamente distinguere il momento dell'exploit dell'attacco, da quanto emerso dalle attività di cyber threat intelligence poste in essere dalla Leonardo S.p.A. nell'ambito dell'incarico affidato circa il sinistro privacy. Infatti, (…), il primo momento in cui sono state rilevate tracce di accesso ai sistemi informativi dell'ASL risalirebbe al XX, momento in cui sarebbe partita l'attività di scouting silente che avrebbe portato al lancio del software malevolo nella giornata del XX. In un'ottica di coerenza intellettuale, la violazione, benché veda effettivamente il suo momento consumativo proprio il XX, non può definirsi conclusa se non nel momento in cui l'Azienda, con il supporto dei fornitori nominati, ha effettivamente raggiunto la bonifica dei sistemi interessati, con ripresa dei servizi annessi; bonifica intervenuta nel mese di XX";
>
> "la violazione in questione ha impattato su trattamenti di tipo informatizzato aventi ad oggetto, nello specifico, i software e dati relativi alle piattaforme applicative installate sui server virtuali del Data Center Principale di Castellammare di Stabia (Na) e Data Center Disaster Recovery di Brusciano (Na). Inoltre, sono stati coinvolti i Data Center delocalizzati installati presso i Presidi Ospedalieri di Nola, Sorrento, Boscotrecase e di Castellammare di Stabia presso i quali sono installati i software applicativi del Pronto Soccorso, ADT e diagnostica per immagini. Si rappresenta ulteriormente che i servizi che hanno subito solo

parzialmente un'interruzione sono stati individuati rispetto ai seguenti item: (i) stipendi del personale dipendente; (ii) acquisizione e liquidazione fatture fornitori e rimborsi. Si specifica che l'erogazione dei servizi verso l'utenza e la somministrazione delle prestazioni sanitarie è stata svolta in maniera continuativa senza soffrire interruzioni di qualsivoglia sorta, compresi i servizi essenziali connessi alla procedura emergenziale da Covid-19";

"le finalità dei trattamenti di cui trattasi si rinvengono prevalentemente nella cura, diagnosi, assistenza sanitaria e nelle finalità amministrative correlate alla cura dei pazienti e degli utenti della ASL e nelle finalità di gestione del personale per quanto attiene ai lavoratori dipendenti della medesima";

"in merito al numero di interessati coinvolti nella violazione, questi sono stati individuati in n. 842.118 dalla mastodontica attività posta in essere da parte della Task Force multidisciplinare, appositamente istituita dall'ASL Napoli 3 Sud. Nella relazione conclusiva, (…), è stato possibile suddividere il numero di interessati, rispetto alla tipologia, nel modo che segue: - 841.965 pazienti/utenti; - 153 dipendenti";

"la violazione contestata (…) (è) causa diretta di un'azione intenzionale esterna, realizzata da cybercriminali professionisti che, attraverso l'utilizzo di innovativi e sofisticati strumenti e conoscenze tecnico-informatiche, si sono dolosamente e abusivamente introdotti nel sistema informatico aziendale, al fine di accedere indebitamente e illegittimamente ai dati e alle informazioni in possesso del Titolare del trattamento. Tant'è vero che, nell'immediatezza dell'azione illecita subita, si è provveduto senza ritardo a formalizzare denuncia-querela presso l'Autorità Giudiziaria, al fine di cristallizzare anche in sede penale il fatto-reato che vede l'ASL quale persona offesa";

"è indubbio che l'elemento soggettivo eventualmente contestabile all'Azienda debba ricondursi, tuttalpiù, nell'alveo della responsabilità colposa da fatto illecito altrui, dovendosi categoricamente escludere qualsivoglia profilo di addebito a titolo di dolo. Infatti, la natura squisitamente colposa della violazione si palesa laddove, rispetto a una valutazione ex post delle circostanze in cui è avvenuto il predetto sinistro, emergerebbe - alla luce del paventato grado di sviluppo tecnologico di allora – la non perfetta aderenza del perimetro di sicurezza implementato rispetto ai più alti standard disponibili all'epoca, ciò anche tenuto doverosamente conto delle effettive possibilità di investimento sul tema a disposizione della Pubblica Amministrazione";

"senz'ombra di dubbio, l'Azienda si era comunque prodigata nella costruzione di un'infrastruttura di sicurezza, finalizzata alla protezione degli asset informativi della medesima. Ne è prova l'adesione a numerose convenzioni e/o lotti incentrati sull'erogazione di servizi di connettività e sicurezza, rappresentative di uno standard adeguato, all'epoca, per le Autorità e Agenzie di settore. Rilevano, in tal senso e a titolo esemplificativo, le adesioni ai lotti: XX";

"sin dai primi momenti in cui si è verificata la violazione, il Titolare poneva in essere una serie di azioni volte a mitigare gli effetti nascenti dal data breach. Innanzitutto, risultando sospesi diversi sistemi e servizi ICT, l'omonimo reparto ha avviato le più immediate azioni di contenimento, tra le quali l'isolamento dell'infrastruttura e dei servizi ICT, rendendoli temporaneamente indisponibili, e l'interruzione di tutti i servizi informatici, indipendentemente dal loro posizionamento, per evitare la propagazione dell'infezione; ciò ha comportato, nell'immediato, esclusivamente un disservizio limitato delle prestazioni nei confronti degli utenti finali, mentre gli altri servizi strategici non sono risultati impattati in quanto ospitati da terze parti";

"per ridurre al minimo la perdita di disponibilità conseguente alla violazione privacy, l'Azienda

Sanitaria, per il tramite anche del fornitore Leonardo S.p.A., ha intrapreso un'attività di bonifica, ripristino, aggiornamento e rafforzamento dei sistemi impattati dall'incidente di sicurezza. Tale attività si è concretizzata nell'esecuzione di analisi in ambito cyber threat hunting e intelligence, a supporto delle attività di response, con creazione di conseguente ambiente protetto, per l'avvio delle attività di ripristino dell'infrastruttura compromessa (Green zone)";

"dapprima, grazie alle azioni intraprese dall'Unità ICT aziendale e, successivamente, dai fornitori incaricati, è stato possibile interrompere in maniera netta l'aggravarsi delle probabili conseguenze lesive scaturenti dall'attacco";

"l'interruzione ha scongiurato l'ulteriore propagarsi del malware e la possibilità, da parte dell'attaccante, di esfiltrare ulteriori data set individuabili, limitando di fatto la perdita di riservatezza, mentre l'attività di bonifica e di creazione della c.d. Green zone, di concerto con il recupero, tramite i sistemi di backup aziendali in uso, dei dati preesistenti all'attacco, hanno consentito di continuare ad erogare, anche in via alternativa, i servizi in favore dei pazienti/utenti e dei dipendenti dell'Azienda, limitando la perdita di disponibilità";

"tali elementi di fatto non possono non essere presi in considerazione, nella concitazione dei momenti successivi all'attacco, per valutare un'attività che abbia ridotto i possibili effetti negativi nei confronti degli interessati. Ad ulteriore riprova di ciò, anche al fine di poter procedere compiutamente agli obblighi informativi verso gli interessati, l'Azienda costituiva la Task Force multidisciplinare ASL Napoli 3 Sud Data Breach con Nota prot. em. n. XX del XX, poi formalizzata con apposita Delibera n. XX del XX. L'opera considerevole della Task Force si è incentrata sull'analisi del data set oggetto di esfiltrazione (circa 3 GB suddivisi in circa 4000 files) al fine di individuare scrupolosamente il numero e tipologie di interessati, nonché il volume e le categorie di dati personali. La suddetta attività rivestiva carattere di necessità ed urgenza in quanto intrinsecamente connessa all'individuazione di tutti gli elementi utili per fornire informazioni sempre più aggiornate ed esatte all'Autorità Garante e Giudiziaria e per garantire le comunicazioni agli interessati ex art. 34 GDPR. Proprio su tale ultimo punto, non può misconoscersi l'attività effettuata dall'Azienda che, sin dal primo momento, ha avuto tra i suoi principali obiettivi quello di garantire e non ledere il diritto di informazione degli interessati attraverso le fondamentali operazioni della Task Force che hanno con successo portato all'individuazione di tutti i soggetti impattati dalla violazione cercando, susseguentemente, le migliori e più efficienti modalità per raggiungere questi ultimi, non senza un impegno di rilevante portata per l'Amministrazione" considerato che "per l'inoltro delle comunicazioni verso gli interessati, sono stati sostenuti costi per circa 300.000,00 euro, al fine di raggiungere circa 66.627 interessati, per il tramite dell'affidamento alla Società Mavasoft s.r.l.s.";

si è provveduto all'"acquisto di ulteriori servizi volti a sanare le problematiche emerse ed efficientare la postura di sicurezza (si fa riferimento agli incarichi a Leonardo S.p.A., Mavasoft S.r.l.s., Covisian S.p.A., ecc.)" e "appare evidente l'impegno economico affrontato da parte dell'Azienda per mitigare gli effetti della violazione, soprattutto nell'interesse primario dell'utenza";

"a seguito dell'incidente occorso e ormai da più di un anno, l'ASL ha intrapreso un percorso virtuoso volto ad efficientare l'infrastruttura di sicurezza Aziendale oltre che ad aumentare le risorse umane e tecnologiche a disposizione della UOC ICT; infatti, sono stati assunti, in totale n. 6 unità di personale, di cui n. 4 di livello dirigenziale, n. 1 funzionario e n. 1 assistente tecnico-informatico";

"anche grazie al supporto dei fornitori esterni, l'Azienda ha completato le seguenti implementazioni tecnologiche:

• attività di incident response e crisis management, incluse indagini ed analisi approfondite, mirate all'identificazione delle dinamiche associate all'incidente e alla definizione di opportune azioni di contenimento e risposta della minaccia;

• attività di Vulnerability Assessment volta alla verifica dinamica della sicurezza dei dispositivi di rete, allo scopo di identificare eventuali vulnerabilità, configurazioni di sicurezza errate e carenze sui livelli di protezione attivi tali da esporre l'Azienda ad attacchi interni ed esterni;

• design e progettazione dell'infrastruttura Green zone ove sono migrate tutte le applicazioni sensibili di pertinenza dell'Azienda, nell'ambito del programma di consolidamento delle misure di sicurezza intrapreso dall'Amministrazione;

• attività di monitoraggio continuativo degli eventi di sicurezza, per il tramite del fornitore Leonardo S.p.A., anche alla luce delle crescenti minacce informatiche per le organizzazioni. Infatti, è divenuto fondamentale rivedere l'approccio alla gestione del rischio e individuare strategie per ridurre la vulnerabilità delle infrastrutture informatiche. In tale ottica, la presente attività di monitoraggio continuativo è stata svolta per mezzo di un SOC h/24, 365 giorni l'anno, composto da un team di specialisti (analisti, system engineer, security tester e malware specialist);

• viene utilizzata la piattaforma di Security Information and Event Management (SIEM) presente presso le infrastrutture Leonardo, con attività aggiuntive di Incident Handling da remoto. A supporto di tale attività sono presenti in sede n. 2 presidi fissi di Leonardo e n. 1 coordinatore da remoto per la gestione delle anomalie/minacce informatiche, segnalate attraverso il servizio di monitoraggio in real time, con interazione diretta con il SOC Leonardo, responsabile della definizione delle attività di gestione delle anomalie. Tale attività delle risorse in presidio è stata svolta in collaborazione con il personale della scrivente Azienda, in modo da favorire l'interazione del personale interno sui processi di gestione degli incidenti di sicurezza e sulle tecnologie in uso;

• supporto specialistico del fornitore per tuning del servizio di monitoraggio continuativo, finalizzato a supportare l'Azienda nell'eseguire tale attività sulle piattaforme di erogazione del servizio stesso;

• attività di device management, volto a gestire e monitorare continuativamente le piattaforme di protezione perimetrale e la piattaforma centralizzata di management EDR;

• implementazione del servizio migliorativo di Managed Detection & Response (MDR) volto a (i) ridurre al minimo le possibili finestre d'esposizione a eventuali attacchi informatici per gli endpoint in perimetro; (ii) effettuare attività di remediation automatica per gli incidenti riconosciuti come "veri positivi" ed a criticità massima; (iii) proteggere gli endpoint anche in assenza momentanea di connessione ad Internet; (iv) consentire la possibilità di isolare dalla rete un endpoint compromesso conservandone il controllo dalla piattaforma in cloud e, infine, (v) proteggere in tempo reale dagli attacchi conosciuti e non che utilizzano metodologie e/o indicatori noti;

• attività di Policy Review, ossia svolgimento di analisi dei flussi perimetrali (inbound e outbound) per una valutazione rapida ed efficace dello stato di conformità della struttura complessa di firewall;

• Cyber Threat Intelligence, Early Warning Data Breach, brand abuse e anti-phishing con takedown;

• progettazione di un sistema per la sicurezza delle applicazioni (Web Application Firewall) e di sistemi di protezione perimetrale dei siti periferici (Next Generation Firewall);

• Cyber Security Awareness per workforce operativa; la presente attività è volta a proporre contenuti formativi che, tramite tecniche di storytelling, puntano a conferire a tutto il personale dell'Azienda una conoscenza dei concetti e delle best practices afferenti alla sicurezza informatica, con il fine ultimo di mitigare l'esposizione della struttura alle minacce che fanno leva sul fattore umano;

• campagne di Phishing simulato per tutto il personale dell'Azienda mediante l'utilizzo di strumenti specifici predisposti dal fornitore. L'azione si pone l'obiettivo di valutare il livello di esposizione dell'Amministrazione a minacce veicolate tramite e-mail e aumentare la consapevolezza del personale e, quindi, la robustezza dell'intera Azienda";

"appare opportuno evidenziare il costante ed elevato grado di cooperazione che l'Azienda ha mantenuto con l'Autorità Garante per la Protezione dei Dati Personali sin dal primo momento in cui la stessa ha avuto contezza circa il verificarsi del sinistro in questione" evidenziando "la frequenza con cui la scrivente Azienda ha inteso garantire un adeguato flusso informativo in merito a tutte le evidenze ottenute in relazione all'attività delittuosa subita. Infatti, ai sensi dell'art. 33 GDPR, l'Azienda ha proceduto già in data XX alla notificazione preliminare, nei termini stabiliti dalla legge, a cui hanno fatto seguito le successive integrative delXX e XX, XX e, infine, la conclusiva del XX"; "l'attività informativa non si è esaurita in meri adempimenti scadenzati, bensì in un'attività dinamica, costante, collaborativa e propositiva al fine di intraprendere correttamente tutti gli step necessari alla risoluzione del sinistro e al supporto degli interessati coinvolti indirettamente dall'attacco hacker";

"la scrivente Azienda, in sede di comunicazione agli interessati, ha inteso curare ogni singolo aspetto al fine di raggiungere efficacemente tutti gli interessati, anche potenzialmente, coinvolti nella violazione";

"l'Azienda ha (…) provveduto al riscontro nei termini di legge della richiesta di informazioni aggiuntive ex art. 157 d.lgs. n. 196/2003, pervenuta in data XX. Infine, il più cristallino elemento in senso collaborativo con l'Autorità è senz'altro rappresentato dal supporto fornito alla stessa in sede di attività ispettiva, effettuata ai sensi dell'art. 58, par. 1, lett. a), e) ed f), GDPR e degli artt. 157 e 158 d.lgs. n. 196/2003, nonché ai sensi degli artt. 21 e 22 del Regolamento n. 1/2019 del Garante per la protezione dei dati personali, svolta presso la sede di Castellammare di Stabia (NA) - C.so Alcide De Gaspari n. 167, nelle giornate del XX, XX e XX";

"la suddetta attività ha coinvolto sia le componenti aziendali (nello specifico UOC ICT e Ufficio Privacy, supportato dal Responsabile per la Protezione dei Dati Personali) sia le componenti esterne che a vario titolo hanno partecipato alla gestione del sinistro privacy in parola. Ebbene, in tutte le tre giornate l'Autorità ha avuto modo di "toccare con mano" l'impegno e i progressi concreti che l'Azienda ha messo in campo sia per mitigare gli effetti nefasti dell'incidente che per prevenire e ridurre al minimo il rischio che situazioni simili possano nuovamente configurarsi. Nello specifico, si è provveduto a rispondere puntualmente alle richieste avanzate dai Funzionari in sede di auditing, anche attraverso il supporto di presentazioni e produzioni documentali allegate ai verbali redatti in loco";

"con il supporto della cospicua documentazione già in possesso di codesta ill.ma Autorità, appare evidente come l'Azienda abbia fornito il massimo supporto e collaborazione nell'acquisizione di quanti più elementi istruttori utili alla puntuale delimitazione del fatto e

alla corretta determinazione delle conseguenze e dei riflessi sui dati personali e sui diritti e le libertà degli interessati";

"(…), le categorie di dati personali impattati dalla violazione, circa gli utenti e i pazienti sono (i) dati personali identificativi (cognome e nome, codice fiscale, numero di telefono, indirizzo mail) e (ii) dati relativi alla salute ex art. 9 GDPR (prenotazione visite mediche con indicazioni di sospetto diagnostico, esito tampone Covid, dati di vaccinazione). Per quanto attiene ai dipendenti, invece, le categorie di dettaglio dei dati personali impattati sono (i) attività del personale (turni dipendenti, schede di performance, rendiconto di presenze in servizio); (ii) documentazione contabile del personale (dati bancari e fatture elettroniche); (iii) documenti identificativi personali e (iv) referti/certificazioni";

"l'Azienda non ha aderito, né aderisce, allo stato, ad alcun codice di condotta ai sensi dell'art. 40 GDPR. Tuttavia, si rappresenta l'intrapresa attività aziendale volta all'implementazione di un Sistema di Gestione della Sicurezza delle Informazioni (S.G.S.I.). Tale circostanza è ben evidenziata anche dalla cospicua attività già svolta da parte della scrivente Azienda a seguito della violazione sul tema di sicurezza delle informazioni che ha portato al compimento di n. 5 giornate formative erogate in favore dei nominati Referenti aziendali per la Sicurezza delle Informazioni e dalla messa a disposizione, in favore di tutto il personale aziendale, di una piattaforma FAD sulla materia in questione con rilevamento del grado di consapevolezza raggiunto dai discenti. Inoltre, di concerto con i partner contrattualizzati, si è provveduto ad adottare specifiche policy sul tema della sicurezza. Infine, l'Azienda ha adottato un documento espressivo del contesto interno ed esterno della medesima, oltre al documento di valutazione del rischio specificatamente predisposto per la sicurezza delle informazioni";

"è doveroso evidenziare (…), come l'Azienda a seguito dell'evidente exploit del XX abbia comunque reagito prontamente, garantendo in maniera continuativa tutti i servizi sanitari e amministrativo-sanitari nei confronti dei pazienti/utenti e adoperandosi, altresì, con successo alla predisposizione di canali alternativi rispetto a quelli ufficiali per garantire i servizi verso i dipendenti che di fatto sono continuati in maniera regolare";

"a ciò si aggiunga il rilevante dato per cui la contestata violazione non sembrerebbe aver avuto riverberi significativi in termini di effetti della stessa in quanto, nonostante l'ampio raggio di pubblicità e messa a disposizione di canali di informazione appositamente predisposti per l'utenza (nello specifico, la casella e-mail XX e relativo numero verde) non sono pervenuti da parte di quest'ultima significativi contatti, lamentele, ricorsi e/o reclami e messe in mora. (…) non può non prendersi in considerazione anche la circostanza in cui l'attività criminosa è avvenuta, ossia durante uno dei momenti storici più critici per la sanità mondiale, dovuto alla propagazione dell'infezione del virus SARS-CoV-2. Infatti, deve riconoscersi l'enorme impatto che la pandemia ha avuto sulla vita della popolazione e sull'operato delle Pubbliche Amministrazioni in campo sanitario, messe a dura prova da un'emergenza sanitaria di tale portata che per la prima volta sono state costrette a fronteggiare numerose difficoltà tanto a livello operativo e gestionale, quanto a livello di spesa. La rapidissima propagazione della pandemia ha costretto, altresì, le Aziende sanitarie di tutto il mondo ad un repentino cambio di organizzazione dell'attività lavorativa di ogni giorno, immettendo in via generalizzata nuovi strumenti (ad es. VPN) per consentire, da una parte, la possibilità di smart and remote working, e, dall'altra parte, permettendo senza soluzione di continuità l'espletamento delle mansioni in favore dell'altissimo numero di soggetti impattati dal virus. In ultima istanza, giova in questa sede evidenziare che nel contesto della pandemia, benché fosse volontà di codesta Azienda, anche nelle more dell'incidente, proseguire con i percorsi pianificati di implementazione lato sicurezza (a titolo esemplificativo la MFA con profili di segregazione e segmentazione delle reti) tale intento risultava scarsamente praticabile nel breve termine. Ciò in ragione del fatto che le suddette

operazioni avrebbero comportato, a causa della necessaria sostituzione e lavorazione di tutti gli account di dominio aziendali, l'interruzione di servizi fondamentali nell'ambito della continuità assistenziale", con ciò ponendo "l'attenzione sull'evidente difficoltà scaturente da una situazione emergenziale del tutto eccezionale, imprevedibile e senza precedenti cui si è cercato di porre rimedio con spirito pronto e resiliente…".

4. Esito dell'attività istruttoria

Preso atto di quanto rappresentato dall'Azienda nel corso del procedimento, si osserva che:

per "dato personale" si intende "qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato")" e per "dati relativi alla salute" "i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute" (art. 4, par. 1, nn. 1 e 15 del Regolamento). Il Considerando n. 35 del Regolamento precisa poi che i dati relativi alla salute "comprendono informazioni sulla persona fisica raccolte nel corso della sua registrazione al fine di ricevere servizi di assistenza sanitaria"; "un numero, un simbolo o un elemento specifico attribuito a una persona fisica per identificarla in modo univoco a fini sanitari". Questi ultimi dati meritano una maggiore protezione dal momento che il contesto del loro trattamento potrebbe creare rischi significativi per i diritti e le libertà fondamentali (Cons. n. 51 del Regolamento);

il titolare del trattamento è, in ogni caso, tenuto a rispettare i principi in materia di protezione dei dati, fra i quali quello di «integrità e riservatezza», secondo il quale i dati personali devono essere "trattati in maniera da garantire un'adeguata sicurezza (…), compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali" (art. 5, par. 1, lett. f) del Regolamento);

in materia di sicurezza del trattamento, il titolare del trattamento e il responsabile del trattamento, "tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche (…) mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio […]"; "nel valutare l'adeguato livello di sicurezza si tiene 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" (art. 32, parr. 1 e 2 del Regolamento);

anche qualora il titolare del trattamento si avvalga di un responsabile per lo svolgimento di alcune attività di trattamento, al quale deve impartire specifiche istruzioni, anche sotto il profilo della sicurezza (Cons. n. 81 e art. 32, parr. 1, lett. d) e 4, del Regolamento), spetta in ogni caso, al medesimo titolare "mettere in atto misure adeguate ed efficaci [e a …] dimostrare la conformità delle attività di trattamento con il […] Regolamento, compresa l'efficacia delle misure" adottate (Cons. n. 74 del Regolamento). Infatti, il titolare rimane responsabile dell'attuazione delle misure tecniche e organizzative adeguate per garantire e essere in grado di dimostrare che il trattamento è effettuato in conformità al Regolamento (artt. 5, par. 2, e 24 del Regolamento; cfr. le "Linee guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del del GDPR", adottate dal Comitato europeo per la protezione dei dati il 7 luglio 2021, spec. punto n. 41);

l'art. 25, par. 1, del Regolamento, nell'enucleare il principio della protezione dei dati fin dalla progettazione, prevede che "tenendo conto dello stato dell'arte e dei costi di attuazione,

nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento [debba mettere] in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati" (cfr. anche Cons. n. 75 del Regolamento);

secondo il Considerando n. 78 del Regolamento il titolare dovrebbe adottare politiche interne e attuare misure che soddisfino il citato principio. Secondo le "Linee guida 4/2019 sull'articolo 25 - Protezione dei dati fin dalla progettazione e per impostazione predefinita" adottate dal Comitato europeo per la protezione dei dati il XX, il citato Considerando "suggerisce una responsabilità dei titolari, ossia quella di valutare costantemente se stiano utilizzando, in qualunque momento, i mezzi appropriati di trattamento e se le misure scelte contrastino effettivamente le vulnerabilità esistenti. Inoltre, i titolari dovrebbero effettuare revisioni periodiche delle misure di sicurezza poste a presidio e tutela dei dati personali, nonché della procedura per la gestione delle violazioni dei dati". "L'obbligo di mantenere, verificare e aggiornare, ove necessario, il trattamento si applica anche ai sistemi preesistenti. Ciò implica che i sistemi progettati prima dell'entrata in vigore del Regolamento devono essere sottoposti a verifiche e manutenzione per garantire l'applicazione di misure e garanzie che mettano in atto i principi e i diritti degli interessati in modo efficace" (cfr. spec. punti nn. 7, 38, 39 e 84);

con particolare riferimento agli elementi principali della progettazione e dell'impostazione predefinita, relativi all'integrità e alla riservatezza, il titolare deve:

valutare i rischi per la sicurezza dei dati personali, considerando l'impatto sui diritti e le libertà degli interessati, e contrastare efficacemente quelli identificati;

tenere conto non appena possibile dei requisiti di sicurezza nella progettazione e nello sviluppo del sistema, integrando e svolgendo costantemente test pertinenti;

definire il trattamento dei dati in modo tale che un numero minimo di persone abbia bisogno di accedere ai dati personali per svolgere le proprie funzioni, e limitare l'accesso di conseguenza;

proteggere i dati personali da modifiche e accessi non autorizzati e accidentali, sia durante il loro trasferimento che durante la loro conservazione;

registrare gli eventi rilevanti ai fini della sicurezza delle informazioni e monitorandoli per rilevare in modo tempestivo eventuali incidenti di sicurezza (cfr. le citate "Linee guida 4/2019 sull'articolo 25", spec. punto n. 85).

le "Linee guida 9/2022 sulla notifica delle violazioni dei dati personali ai sensi del RGPD" adottate dal Comitato europeo per la protezione dei dati il 28 Marzo 2023 (https://edpb.europa.eu/system/files/2023-04/edpb_guidelines_202209_personal_data_breach_notification_v2.0_en.pdf) chiariscono che "la capacità di individuare, trattare e segnalare tempestivamente una violazione deve essere considerata un aspetto essenziale" delle misure tecniche e organizzative che il titolare e il responsabile del trattamento devono mettere in atto, ai sensi dell'art. 32 del Regolamento, per garantire un livello adeguato di sicurezza dei dati personali (punto n. 41). Al riguardo, inoltre, il Considerando n. 85 precisa che "una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o

immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata". Analogamente, secondo il Considerando n. 87, "è opportuno verificare se siano state messe in atto tutte le misure tecnologiche e organizzative adeguate di protezione per stabilire immediatamente se c'è stata violazione dei dati personali e informare tempestivamente l'autorità di controllo e l'interessato. È opportuno stabilire il fatto che la notifica sia stata trasmessa senza ingiustificato ritardo, tenendo conto in particolare della natura e della gravità della violazione dei dati personali e delle sue conseguenze e effetti negativi per l'interessato".

5. Valutazioni del Garante e conclusioni.

A fronte di quanto sopra rappresentato, si rileva che i trattamenti effettuati nel contesto in esame richiedono l'adozione dei più elevati standard di sicurezza al fine di non compromettere la riservatezza, l'integrità e la disponibilità dei dati personali di milioni di interessati. Ciò, tenendo altresì conto delle finalità dei trattamenti e della natura dei dati personali trattati, appartenenti anche a categorie particolari. Su tale base, gli obblighi di sicurezza imposti dal Regolamento richiedono l'adozione di rigorose misure tecniche e organizzative, includendo, oltre a quelle espressamente individuate dall'art. 32, par. 1, lett. da a) a d), tutte quelle necessarie ad attenuare i rischi che i trattamenti presentano.

Alla luce delle valutazioni sopra richiamate, tenuto conto delle dichiarazioni rese dal titolare del trattamento nel corso dell'istruttoria e considerato che, salvo che il fatto non costituisca più grave reato, chiunque, in un procedimento dinanzi al Garante, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi ne risponde ai sensi dell'art. 168 del Codice "Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante" gli elementi forniti dal titolare del trattamento nella memoria difensiva sopra richiamata, seppure meritevoli di considerazione, non consentono di superare i rilievi notificati dall'Ufficio con il richiamato atto di avvio del procedimento, non ricorrendo, peraltro, alcuno dei casi previsti dall'art. 11 del regolamento del Garante n. 1/2019.

Dall'esame delle informazioni e degli elementi acquisiti nonché della documentazione fornita dall'Azienda è emerso che il trattamento è stato effettuato in violazione degli artt. 5, par. 1, lett. f), 25 e 32 del Regolamento, in relazione ai seguenti profili:

5.1. Mancata adozione di misure adeguate a rilevare tempestivamente la violazione dei dati personali

Nel corso dell'istruttoria è emerso che "la ricostruzione degli eventi colloca il potenziale primo accesso dell'attaccante alla VPN di ASL Napoli 3 SUD approssimativamente alle ore XX del XX, in concomitanza con l'inizio di un'attività di scansione interna del servizio Remote Desktop ed eventi di accesso RDP anomali ad asset strategici" e che i soggetti malintenzionati hanno effettuato una serie di operazioni propedeutiche all'attacco informatico, a seguito delle quali, sono stati prodotti "alert generati dall'apparto di sicurezza XX" da cui sono emersi "evidenti segnali anomali che vedono un notevole incremento delle scansioni e dei comportamenti sospetti nei giorni che precedono l'accesso in VPN dell'attore malevolo", in particolare dal XX, "ulteriori autenticazioni amministrative anomale venivano registrate durante le ore serali del XX, da un sistema avente indirizzo IP XX" nonché il XX "molteplici allarmi relativi a comandi e ad attività di enumerazione sospetti, eseguiti sfruttando il protocollo SMB, in concomitanza con l'accesso in VPN da parte dell'attaccante, utilizzando l'account XX" (v. pagg. 12 e 13, 16 - 18 del report XX).

L’Azienda ha dichiarato che “l’esfiltrazione dei dati, presumibilmente, è avvenuta fra XX e XX e che i sistemi di logging non rilevavano l’intero traffico uscente dalle postazioni di lavoro dell’Azienda ma solo gli eventi principali”, che “l’incidente è stato […] rilevato il XX mattina da un operatore sanitario che, riscontrato un malfunzionamento dell’applicazione (IL), ha contattato la persona reperibile dei sistemi informatici che, a seguito di specifiche verifiche, constatando la modifica delle credenziali di amministratore di dominio, ha dato l’allarme”. In particolare, l’Azienda ha dichiarato che al momento in cui si è verificato l’attacco informatico “disponeva di un firewall XX per la difesa perimetrale su cui non c’era presidio h24, un firewall XX per difesa interna nonché agent XX (XX) che, al momento dell’incidente di XX, era in fase di roll-out, ovvero non installato su tutte le macchine, per il monitoraggio interno per deep defence. Non vi era, pertanto, un’organizzazione strutturata per la lettura e analisi quotidiana dei log” e “disponeva di limitatissime risorse tecnologiche e umane” (v. verbali del XXp. 4, XX p. 4, e del XX, p. 2).

Da quanto sopra rappresentato, è emersa una gestione inadeguata dei predetti allarmi, che non ha consentito all’Azienda di venire tempestivamente a conoscenza della violazione dei dati personali occorsa. Pertanto, la mancata adozione di misure adeguate a rilevare tempestivamente la violazione dei dati personali non è risultata conforme alle disposizioni di cui all’art. 5, par. 1, lett. f), e all’art. 32, par. 1, del Regolamento che, tenuto conto di quanto previsto dalle citate “Linee guida 9/2022 sulla notifica delle violazioni dei dati personali ai sensi del RGPD”, richiede che il titolare e il responsabile del trattamento debbano mettere in atto misure per “individuare […] tempestivamente una violazione” (punto n. 41).

5.2. Mancata adozione di misure adeguate a garantire la sicurezza delle reti

Nel corso dell’istruttoria è emerso che l’Azienda non aveva adottato adeguate misure per segmentare e segregare le reti su cui erano attestate le postazioni di lavoro dei propri dipendenti, nonché i sistemi (server) utilizzati per i trattamenti. In particolare “la mancata segmentazione tra i servizi critici, gli applicativi e le postazioni di lavoro [hanno comportato] l’estensione della singola compromissione all’intera infrastruttura” (v. notifica del XX). Infatti, come emerso nel corso delle attività ispettive “al momento della violazione dei dati personali, non erano previste misure di sicurezza relative alla segmentazione delle reti, con particolare riferimento a quelle adottate per limitare le comunicazioni tra le reti a cui sono attestati i sistemi server, nonché le comunicazioni tra le predette reti e quelle a cui sono attestate le postazioni di lavoro degli operatori” (v. verbale del XX, pp. 3 e 4).

Al riguardo, nell’ambito delle attività di analisi e ripristino condotte da Leonardo S.p.a. in relazione alla violazione dei dati personali in esame, è stato definito un documento denominato “Progressi delle attività di rispristino e relative misure di sicurezza adottate” (di seguito “Piano ripristino”) che prevede l’adozione, tra le altre, di specifiche azioni volte alla segregazione e messa in sicurezza dei diversi sistemi gestiti dall’Azienda. In particolare, tali azioni prevedono una “soluzione architetturale […] utile al ripristino dei servizi critici precedentemente impattati nell’attacco informatico verificatosi nel mese di XX. La progettazione e l’implementazione di tale zona infrastrutturale denominata “Green Zone” è caratterizzata da alcune peculiarità, quali: segmentazione e segregazione” e “la creazione di diverse VLAN quali: la VLAN di Management, una di Demilitarized Zone, ossia una DMZ, un’ulteriore dedicata ai servizi infrastrutturali ed infine una dedicata alla componente Server Farm. Questa zona segmentata sarà segregata e quindi controllata per mezzo di policy Firewall specifiche e puntuali tramite l’apparato XX” (v. notifica del XX).

Peraltro, al momento in cui si è verificata la violazione dei dati personali, l’accesso remoto, tramite VPN, alla rete dell’Azienda, avveniva mediante una procedura di autenticazione informatica basata solo sull’utilizzo di username e password. In relazione a tale aspetto, l’Azienda, solo a seguito dell’incidente, ha ritenuto necessario attivare una procedura con doppio fattore di autenticazione (v. verbale del XX, p. 3).

La mancata adozione di misure adeguate a garantire la sicurezza delle reti, sia in relazione alla segmentazione e segregazione delle stesse, sia con riferimento all'accesso remoto tramite VPN, non è risultata conforme alle disposizioni di cui all'art. 5, par. 1, lett. f), e all'art. 32, par. 1, del Regolamento che, nel caso in esame, richiede che il titolare e il responsabile del trattamento debbano mettere in atto misure per "assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento" (lett. b)).

5.3. La protezione dei dati fin dalla progettazione

Come rappresentato nei paragrafi precedenti, risulta che il titolare non aveva adottato misure e garanzie adeguate ad attuare efficacemente il principio di "integrità e riservatezza" e a proteggere da trattamenti non autorizzati o illeciti. Alla luce di quanto sopra esposto, si ravvisano gli estremi, altresì, di una violazione del descritto principio della "protezione dei dati fin dalla progettazione", di cui all'art. 25, par. 1, del Regolamento, da parte dell'Azienda, considerati i rischi per i diritti e le libertà degli interessati derivanti dai trattamenti in esame, in relazione alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento.

Per tali ragioni si confermano le valutazioni preliminari dell'Ufficio e si rileva l'illiceità del trattamento di dati personali effettuato dall'Asl Napoli 3 Sud, in violazione del principio di "integrità e riservatezza", di cui all'art. 5, par. 1, lett. f), del Regolamento; del principio della "protezione dei dati fin dalla progettazione" di cui all'art. 25, par. 1, del Regolamento e degli obblighi in materia di sicurezza di cui all'art. 32 del Regolamento.

La violazione delle predette disposizioni rende applicabile, ai sensi dell'art. 58, par. 2, lett. i), la sanzione amministrativa prevista dall'art. 83, parr. 4 e 5 del Regolamento.

In tale quadro, considerato, in ogni caso, che la condotta ha esaurito i suoi effetti e considerato che l'Azienda ha rappresentato, nei termini sopra illustrati, di aver adottato ulteriori specifiche misure ritenute necessarie per scongiurare futuri analoghi accadimenti, non ricorrono i presupposti per l'adozione di provvedimenti di tipo prescrittivo o inibitorio, di cui all'art. 58, par. 2, del Regolamento.

6. Adozione dell'ordinanza ingiunzione per l'applicazione della sanzione amministrativa pecuniaria e delle sanzioni accessorie (artt. 58, par. 2, lett. i e 83 del Regolamento; art. 166, comma 7, del Codice).

La violazione degli artt. 5, par. 1, lett. f), 25, par. 1 e 32 del Regolamento, causata dalla condotta posta in essere dall'Azienda, è soggetta all'applicazione della sanzione amministrativa pecuniaria ai sensi dell'art. 83, parr. 4 e 5 del Regolamento.

Si consideri che il Garante, ai sensi degli artt. 58, par. 2, lett. i) e 83 del Regolamento, nonché dell'art. 166 del Codice, ha il potere di "infliggere una sanzione amministrativa pecuniaria ai sensi dell'articolo 83, in aggiunta alle [altre] misure [correttive] di cui al presente paragrafo, o in luogo di tali misure, in funzione delle circostanze di ogni singolo caso" e, in tale quadro, "il Collegio [del Garante] adotta l'ordinanza ingiunzione, con la quale dispone altresì in ordine all'applicazione della sanzione amministrativa accessoria della sua pubblicazione, per intero o per estratto, sul sito web del Garante ai sensi dell'articolo 166, comma 7, del Codice" (art. 16, comma 1, del Regolamento del Garante n. 1/2019).

La predetta sanzione amministrativa pecuniaria inflitta, in funzione delle circostanze di ogni singolo caso, va determinata nell'ammontare tenuto conto dei principi di effettività, proporzionalità e dissuasività, indicati nell'art. 83, par. 1, del Regolamento, alla luce degli elementi previsti all'art. 83, par. 2, del Regolamento in relazione ai quali, per i casi in esame, si osserva che:

l'Autorità ha preso conoscenza dell'evento a seguito della notifica di violazione dei dati

personali effettuata dal titolare e da alcune istanze pervenute al Garante sull'accaduto (art. 83, par. 2, lett. h) del Regolamento);

il trattamento dei dati effettuato dall'Azienda ha riguardato dati idonei a rilevare informazioni sulla salute di un numero molto rilevante di interessati (art. 83, par. 2, lett. a) e g) del Regolamento);

il titolare del trattamento non ha manifestato alcun atteggiamento intenzionale, in quanto l'episodio risulta essere stato determinato da un comportamento doloso da parte di un soggetto terzo, denunciato formalmente alla polizia postale (art. 83, par. 2, lett. a) e b) del Regolamento);

l'Azienda ha preso in carico la problematica introducendo, dopo l'evento occorso, una serie diversificata di misure volte non solo ad attenuare il danno subito dagli interessati ma anche a ridurre la replicabilità dell'evento stesso (art. 83, par. 2, lett. c) del Regolamento);

il titolare, sin da subito, ha dimostrato un altissimo grado di cooperazione con l'Autorità in ogni fase dell'istruttoria, ivi compresa quella ispettiva (art. 83, par. 2, lett. f) del Regolamento).

In ragione dei suddetti elementi, valutati nel loro complesso, si ritiene di determinare l'ammontare della sanzione pecuniaria prevista dall'art. 83, parr. 4 e 5 del Regolamento, nella misura di euro 30.000,00 (trentamila) per la violazione degli artt. 5, par. 1, lett. f), 25 e 32 del Regolamento, quale sanzione amministrativa pecuniaria ritenuta, ai sensi dell'art. 83, par. 1, del Regolamento, effettiva, proporzionata e dissuasiva.

Si ritiene, altresì, che debba applicarsi la sanzione accessoria della pubblicazione sul sito del Garante del presente provvedimento, prevista dall'art. 166, comma 7, del Codice e art. 16 del Regolamento del Garante n. 1/2019, in considerazione dell'elevato numero di soggetti coinvolti e della tipologia di dati personali oggetto di illecito trattamento.

Si rileva, infine, che ricorrono i presupposti di cui all'art. 17 del regolamento del Garante n. 1/2019 concernente le procedure interne aventi rilevanza esterna, finalizzate allo svolgimento dei compiti e all'esercizio dei poteri demandati all'Autorità.

TUTTO CIÒ PREMESSO IL GARANTE

dichiara l'illiceità del trattamento di dati personali effettuato dall'Asl Napoli 3 Sud, per la violazione degli artt. 5, par. 1, lett. f), 25 e 32 del Regolamento, nei termini di cui in motivazione.

ORDINA

ai sensi degli artt. 58, par. 2, lett. i) e 83 del Regolamento, nonché dell'art. 166 del Codice, all'Asl Napoli 3 Sud, con sede legale a Torre del Greco, in Via Marconi, 66, C.F. e P. Iva 06322711216, in persona del legale rappresentante pro-tempore, di pagare la somma di euro 30.000,00 (trentamila) a titolo di sanzione amministrativa pecuniaria per la violazione indicata nel presente provvedimento; si rappresenta che il contravventore, ai sensi dell'art. 166, comma 8, del Codice, ha facoltà di definire la controversia mediante pagamento, entro il termine di 30 giorni, di un importo pari alla metà della sanzione comminata.

INGIUNGE

alla predetta Asl Napoli 3 Sud, in caso di mancata definizione della controversia ai sensi dell'art. 166, comma 8, del Codice, di pagare la somma di euro 30.000,00 (trentamila)

secondo le modalità indicate in allegato, entro 30 giorni dalla notificazione del presente provvedimento, pena l'adozione dei conseguenti atti esecutivi a norma dall'art. 27 della legge n. 689/1981.

DISPONE

ai sensi dell'art. 166, comma 7, del Codice, la pubblicazione per intero del presente provvedimento sul sito web del Garante e ritiene che ricorrano i presupposti di cui all'art. 17 del Regolamento n. 1/2019 concernente le procedure interne aventi rilevanza esterna, finalizzate allo svolgimento dei compiti e all'esercizio dei poteri demandati al Garante.

Ai sensi dell'art. 78 del Regolamento, degli artt. 152 del Codice e 10 del d.lgs. n. 150/2011, avverso il presente provvedimento è possibile proporre ricorso giurisdizionale dinnanzi all'autorità giudiziaria ordinaria, a pena di inammissibilità, entro trenta giorni dalla data di comunicazione del provvedimento stesso ovvero entro sessanta giorni se il ricorrente risiede all'estero.

Roma, 28 settembre 2023

IL PRESIDENTE
Stanzione

IL RELATORE
Ghiglia

IL SEGRETARIO GENERALE
Mattei