Provvedimento del 13 febbraio 2025 [10116834]

VEDI ANCHE Provvedimento dell'8 giugno 2023

[doc. web n. 10116834]

Provvedimento del 13 febbraio 2025

Registro dei provvedimento
n. 83 del 13 febbraio 2025

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 dott. Claudio Filippi vice 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 la prof.ssa Ginevra Cerrina Feroni;

PREMESSO

1. La violazione dei dati personali

In data XX la ASL 1 Avezzano Sulmona L'Aquila, di seguito “Azienda”, ha trasmesso all’Autorità, ai sensi dell’art. 33 del Regolamento, una notifica di violazione dei dati personali integrata, con note del XX, XX, XX e XX, riguardante un attacco informatico ai sistemi informativi dell’Azienda, determinato da un malware di tipo ransomware, da parte di un gruppo di hacker denominato “MONTI”.

In considerazione del numero di interessati coinvolti e della natura dei dati personali oggetto della violazione, l’Ufficio ha ritenuto necessario approfondire le circostanze nelle quali si è verificata la violazione, mediante una richiesta di informazioni (nota del XX) a cui l’Azienda ha fornito riscontro con nota del XX e, successivamente, è stata effettuata un’attività ispettiva nei confronti dell’Azienda (XX).

2. Il fatto

Dall’esame degli atti e all’esito della citata attività ispettiva, è risultato quanto segue.

2.1. La notifica della violazione al Garante

Preliminarmente, con la notifica del XX, l’Azienda ha dichiarato che si era verificata un’“applicazione illecita di crittografia ai server virtuali dell’azienda” (v. sez. XX, punto XX).

Successivamente, l’Azienda ha aggiornato le informazioni riguardanti la violazione dichiarando che “trattasi di attacco di un gruppo di hacker denominato “MONTI” che utilizza un sofisticato ransomware progettato per crittografare i dati e richiedere il pagamento in bitcoin per gli strumenti di decrittazione. Trattasi di attacco capace di bypassare le misure di sicurezza ordinarie (ad es. firewall, antimalware, edr) eseguendo codice malevolo con escalation di privilegi, movimenti laterali e applicazione di crittografia simmetrica e asimmetrica. Le evidenze confermano che tale ransomware utilizza artefatti non ancora conosciuti o riconoscibili dai moderni antivirus/antimalware, come dimostra la ricerca di alcuni IOC (indicatori di compromissione) svolta sul portale VirusTotal” (v. notifica del XX, sez. XX, punto XX).

Da ultimo, l’Azienda ha aggiunto che “nella notte del XX, all'indirizzo XX è stata inviata una e-mail di phishing contenente un link malevolo. (…) I log di sicurezza hanno evidenziato che i movimenti laterali sono proseguiti incessantemente (ma con frequenza minore) dalla notte del XX al mattino del XX, coinvolgendo diversi host. La bassa frequenza rilevata dalla piattaforma (…) nella sequenza delle azioni di spostamento da un host all'altro (attività di Lateral Movement) porta ad ipotizzare che l’esfiltrazione dei file sia avvenuta proprio in questa fascia temporale e il periodo trascorso tra ciascuna azione potrebbe essere imputata all’azione di copia dei file. Tale ipotesi è avvalorata anche dalla datazione dei file che sono stati temporaneamente pubblicati sulla pagina Monti nel dark web (in un range che va proprio dal XX al XX). Altro elemento che è stato oggetto di approfondimento e che suffraga l’ipotesi che in tale fascia temporale sia avvenuta l'esfiltrazione dei dati è l’analisi del traffico di rete. A seguito di approfondite analisi è stato rilevato un picco anomalo nella giornata del XX non riscontrabile in altri giorni, pur non potendo, ovviamente, entrare nel merito dei protocolli coinvolti. Inoltre, visto il costante beaconing (modalità di comunicazione tra i server dell'attaccante e gli host infettati) verso siti web malevoli, è ipotizzabile anche la volontà dell'attaccante di creare un meccanismo di persistenza su determinate PdL. In conclusione, il gruppo hacker, ha impostato un’immagine e il messaggio con cui si richiedeva il riscatto sui sistemi che sono stati cifrati dal ransomware Monti. A ridosso dell’attacco, sul Dark Web risultavano pubblicati 389 Gigabyte di dati riconducibili all’ASL 1. A far data dal XX u.s. questi dati non risultano più pubblicati online” (v. notifica dell’XX e XX, sez. XX, punto XX).

Per quanto attiene al numero di interessati i cui dati sulla salute sono stati coinvolti dall'attacco l'Azienda ha dichiarato che sono stati oggetto di violazione "per Dipendenti/Consulenti (n. 3814): dati anagrafici, dati di contatto, dati di accesso e di identificazione, dati di pagamento, dati relativi a documenti di identificazione/riconoscimento, dati che rivelano l'appartenenza sindacale. Per Beneficiari o assistiti/Per Minori/Per Pazienti/Per persone vulnerabili (es. vittime di violenza o abusi, rifugiati, richiedenti asilo) (n. 6817) dati anagrafici, dati di contatto, dati relativi a condanne penali e ai reati o a connesse misure di sicurezza, dati che rivelano l'origine razziale o etnici, dati relativi alla vita sessuale o all'orientamento sessuale, dati relativi alla salute (es. scheda paziente, diario clinico, terapie, diagnosi, lettera di dimissione), dati genetici" (v. notifica del XX, sez. XX, punto XX).

2.2. Attività ispettive

Nel corso delle attività ispettive l'Azienda ha dichiarato che "sono stati coinvolti tutti i trattamenti, eccetto la radiologia (sistemi RIS PACS) e il 60% del volume dei dati esfiltrati riguardavano dati personali" e ha inteso precisare che "la violazione dei dati personali in questione ha coinvolto tutti i trattamenti effettuati su supporto informatico a causa della cifratura - ad opera degli attaccanti - dei principali sistemi informatici dell'ASL, eccetto i trattamenti relativi a "esecuzione esami diagnostici" dei sistemi RIS-PACS di radiologia. Pertanto, i trattamenti coinvolti corrispondono a circa il 50% dei 551 trattamenti censiti nel Registro dei trattamenti. Di questi, poi, i trattamenti coinvolti nella esfiltrazione dei dati sono complessivamente 19. Inoltre, si rappresenta che al momento dell'attacco del XX il patrimonio informativo della ASL su supporto informatico ammontava a circa 358 TB, di cui 337 TB costituito da dati sanitari e 21 TB da dati amministrativi. Dunque, i dati esfiltrati - pari a 389 GB - rappresentano una minima parte del patrimonio informativo aziendale memorizzato su supporto informatico" (v. verbali del XX, pag. XX e nota del XX a scioglimento delle riserve). Inoltre, l'Azienda ha rappresentato che "dal XX la pagina dove erano pubblicati i dati oggetto di esfiltrazione non è più raggiungibile e che, a partire dall'attacco (…) svolge attività di threat intelligence per verificare su clear e dark web l'eventuale presenza dei dati riferibili o riconducibili alla ASL [ed] è intenzione dell'Azienda di dotarsi di strumenti per automatizzare tali verifiche" (v. verbale del XX, pag. XX).

Con riguardo alle modalità e tempistiche dell'attacco, durante le attività ispettive, l'Azienda ha "confermato quanto presente nel report incidente (documento "ANALISI INCIDENTE DATA BREACH ASL1 ABRUZZO" del XX redatto dalla società DeepCyber di seguito "report incidente")" e ha dichiarato che "il core dell'attacco si è verificato a partire dal XX in orario notturno, a seguito di precedenti eventi di user enumeration su account email e massiccia attività di brute forcing seguita da autenticazioni con successo di 4 utenze, sebbene non si abbia evidenza di sfruttamento delle medesime utenze nelle fasi successive dell'attacco. Il XX, sulla casella XX, acceduta da più operatori, è stata inviata una mail di phishing con un link malevolo, successivamente rimosso; pertanto non è stato possibile avere contezza delle possibili interazioni con l'utente (fornitura di credenziali o esecuzione di codice malevolo) che il link richiedeva" e che "la vulnerabilità, con ragionevole certezza, è riconducibile al server Exchange, tecnica di attacco OWASSRF che presuppone lo sfruttamento in sequenza di due CVE (XX e XX) e le credenziali di un utente senza privilegi, sebbene nei log non vi siano evidenze che siano state sfruttate entrambe" (v. verbale del XX, pagg. XX e XX).

Per quanto concerne la portata della violazione con riferimento agli applicativi aziendali di ordine sanitario e amministrativo contabile, l'Azienda ha dichiarato che "alle XX del XX si è deciso di disconnettere la ASL da internet quale misura cautelare in caso di presenza di backdoor o persistenza dell'attaccante all'interno della propria infrastruttura IT. Il blocco dei sistemi, di circa una settimana, era volto a consentire le necessarie attività di analisi, indagine, bonifica e ripristino" e che "il CUP e le altre procedure sono state tempestivamente sostituite con altre procedure informatiche o registrazione cartacea; tutte le prestazioni sono state erogate, con registrazione di piccoli ritardi alle casse per le prestazioni brevi e differibili; in particolare la chirurgia non ha subito

ritardi e la radiologia non ha avuto impatti dall'attacco. A partire dal XX sono stati, progressivamente, ripristinati i sistemi informatici di supporto al CUP, ADT e pronto soccorso. Per le prestazioni ambulatoriali, inoltre, sono stati aumentati gli appuntamenti rispetto a quanto previsto nel periodo prima dell'attacco; ciò al fine di offrire un maggior servizio e garantire la continuità dell'erogazione delle prestazioni" (v. verbale del XX, pagg. XX e XX). L'Azienda ha inoltre confermato che "sono stati esfiltrati dati personali e sulla salute di circa 6800 interessati" (v. verbale del XX, pag. XX).

A scioglimento della riserva assunta in corso di ispezione, l'Azienda, con nota del XX, ha precisato che "la violazione dei dati personali in questione ha coinvolto tutti i trattamenti effettuati su supporto informatico a causa della cifratura - ad opera degli attaccanti - dei principali sistemi informatici dell'ASL, eccetto i trattamenti relativi a "esecuzione esami diagnostici" dei sistemi RIS-PACS di radiologia. Pertanto, i trattamenti coinvolti corrispondono a circa il 50% dei 551 trattamenti censiti nel Registro dei trattamenti. Di questi, poi, i trattamenti coinvolti nella esfiltrazione dei dati sono complessivamente 19".

3. Le misure in essere al momento della violazione

3.1. Notifica della violazione al Garante

Con riferimento alle misure in essere al momento della violazione, l'Azienda ha dichiarato che adottava "a) Regolamento aziendale per la protezione dei dati personali (…); b) Procedura per la protezione dei dati in ambito Smart-Working/Lavoro Agile (…); c) Regolamento per la gestione degli archivi e delle procedure di scarto di documenti/atti d'archivio di natura cartacea […]; d) Disciplinare interno per l'utilizzo delle risorse strumentali informatiche e telematiche aziendali (…); e) Regolamento aziendale per la compilazione e la gestione della cartella clinica (…); f) Corsi di formazione a distanza (FAD) in materia di Privacy e Cybersicurezza del personale dipendente (…); g) Gestione della sicurezza della rete, Firewalling XX e Proxy Server (…); h) Gestione delle identità digitali e sicurezza applicativa tramite Accordo Quadro SPC 2 (Deliberazione n. XX del XX), comprendente: • Progetto di segmentazione della rete con VLAN • Vulnerability management tramite XX; i)Dynamic application security testing Implementazione antimalware/XX (acquisto con Deliberazione n. XX del XX e successivo rinnovo con ordinativo Mepa n. XX del XX) j) Accordo Consip SPC Connettività con Fastweb (deliberazioni del Direttore Generale n. XX del XX, n. XX, n. XX, n. XX e n. XX) (scadenza XX – rinnovato fino al XX) per i seguenti servizi: 1. Connettività geografica; 2. Connettività anche per disaster recovery; 3. Connettività di emergenza degli ospedali in caso di evento imprevedibile; 4. Backup; 5. Supporto ufficio privacy. 6. Servizi di sicurezza: Servizio di XX e XX che sono composti inoltre dai seguenti servizi: Firewall, VPN ISPEC XX e Intrusion Detection & Prevention System (IDS/IPS); k) Soluzione di VPN XX (acquisto con determinazione n. XX del XX e rinnovo assistenza e manutenzione con Deliberazione n. XX del XX); l) Sistema di autenticazione, autorizzazione e accounting tramite XX; m) Password policy per account ordinari e amministrativi; n) Sistema centralizzato di aggiornamento dei sistemi operativi lato client e server; o) Policy del least privilege e need to know; p) Filtri antispam e antiphishing; q) Procedure di backup multipli on-line e off-site; r) Canali di trasmissione dati cifrati SSL TLS v 1.2 o sup.; s) Misure di sicurezza fisica presso il CED (accesso selezionato, gruppi di continuità, antincendio, rilevatore fumi, climatizzazione ambienti); t) Programmazione di vulnerability assessment e penetration test periodici tramite società specializzate" (v. notifica del XX, sez. XX, punto XX).

3.2. Attività ispettive

Durante le attività ispettive l'Azienda ha dichiarato che, circa le misure di sicurezza adottate per il servizio XX "il servizio XX era dotato di sistema anti spam e anti phishing" e, circa i servizi di vulnerability assessment e i servizi professionali per la segmentazione delle reti citati nel report incidente ha dichiarato che "il primo documento riportante gli esiti di tali attività (riconducibili

all’accordo quadro SPC Cloud lotto2) risale ad XX; le attività sono state successivamente interrotte a causa della pandemia COVID-19 e delle conseguenti modifiche all’assetto infrastrutturale dell’Azienda per consentire lo smart working dei dipendenti. Le attività sono quindi riprese nel XX e da XX è stata elaborata una bozza di capitolato tecnico per il rafforzamento delle misure di sicurezza, considerata la notevole complessità e l’impatto nei confronti dell’operatività delle strutture della ASL” (v. verbale del XX, pag.XX).

In ordine alle misure tecniche e organizzative relative all’aggiornamento periodico (patch management) in essere al momento della violazione dei dati personali l’Azienda ha dichiarato che “si avvaleva di strumenti quali XX e XX che migliorano la postura di sicurezza dei sistemi e che l’aggiornamento periodico delle postazioni di lavoro e del server XX era in capo alla UO dei sistemi informativi, tenendo conto della continuità dei servizi e del tipo di intervento richiesto (minor o major release) e avendo cura di non dare disservizio agli applicativi erogati da terze parti” (v. verbale del XX, pag. XX).

In relazione alla segmentazione della rete l’Azienda ha dichiarato che “era stato avviato un progetto di evoluzione dell’infrastruttura sul cloud che prevedeva anche la segmentazione delle reti, alcune delle componenti di sicurezza dell’infrastruttura erano già migrate e isolate su cloud XX, una parte della rete era stata segmentata e sottoposta a NAC (network access control) mentre la parte interessata dall’attacco, ove erano attestati i sistemi server, era ancora flat e priva di segmentazione. Tale circostanza è dimostrata nel report incidente dagli elementi in esso citati (log)” (v. verbale del XX, pagg. XX e XX).

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 ai dati personali in caso di incidente, l’Azienda ha dichiarato che “il backup dei sistemi e dei dati era replicato su due siti (Avezzano e l’Aquila) XX; in aggiunta in un data center secondario era conservato un backup dei dati con diversa periodicità dei job. Dopo l’attacco, in linea con la nuova architettura PSN che prevede più data center in Italia, i sistemi di backup, divisi per tipologia (server, data base, etc..), sono stati migrati in tale architettura a cui si è affiancata una ulteriore tecnologia XX. Sulla console di gestione dei backup operava, e opera tuttora, personale sistemista della ASL. Sono stati previsti alert via mail XX. Il piano di disaster recovery della ASL vigente al momento dell’attacco è stato un utile punto di partenza per la gestione post incidente e le azioni messe in campo hanno consentito il ripristino tempestivo dei servizi e dei dati per garantire l’operatività delle prestazioni sanitarie e ospedaliere. Dopo l’attacco, pur mantenendo la classificazione della tipologia dei servizi, sono state modificate le modalità e i tempi di ripristino dei sistemi e dati che hanno tenuto conto anche del mutato quadro tecnologico (cloud regionale e PSN)” (v. verbale del XX pag. XX).

Quanto agli strumenti di monitoraggio degli eventi di sicurezza utilizzati per il rilevamento in tempo reale degli incidenti di sicurezza, con particolare riferimento ai software di monitoraggio, l’Azienda ha rappresentato che “era dotata di diversi strumenti quali XX, XX, XX, che consentivano la registrazione ma non la correlazione degli eventi. La ASL disponeva di un servizio SOC XX fino al XX, successivamente il SOC è stato sostituito con un servizio di security device management gestito in autonomia e con personale interno dalla UO sistemi informativi. In ogni caso la catena degli eventi relativi all’attacco è avvenuta principalmente di notte e durante periodi a ridosso di festività” (v. verbale del XX, pag. XX).

Dalla documentazione acquisita durante l’attività ispettiva (v. report redatto dalla società XX - Avezzano Sulmona L’Aquila”, di seguito “report XX”) si evince che “le prime attività sospette sui sistemi risulterebbero iniziare a partire dal giorno XX (…); l’analisi di uno dei Domain Controller non virtualizzato (…); ha evidenziato che l’attaccante abbia utilizzato proprio questo sistema come “pivot” per gestire le attività di attacco, accedendo con l’utenza specifica “XX” associata ad un consulente non più operante presso la ASL” e che “la configurazione adottata di XX sia in modalità

detect permettendo la detection di eventuali anomalie ma non effettua nessun tipo di blocco" (v. report XX, pagg. XX e XX).

Per quanto riguarda le modalità con le quali gli incidenti di sicurezza sono gestiti e portati a conoscenza dei soggetti a vario titolo coinvolti l'Azienda ha precisato che "per qualunque problematica afferente all'area informatica gli utenti interni si rivolgevano alla UO sistemi informativi, ed erano disponibili diversi canali di contatto: interno gestito da personale della ASL (ufficio privacy con coinvolgimento dei sistemi informativi per quanto di competenza), esterno mediante mail XX o modulistica disponibile nella sezione privacy del sito istituzionale, è stato previsto, altresì, un canale di comunicazione da parte dei responsabili del trattamento e/o dei contitolari. È stato definito un team, reperibile a recapiti telefonici fissi e mobili, fin dal XX per la gestione degli incidenti, composto da: responsabile della UOSD sistemi informativi, responsabile della transizione digitale, coordinatore dell'ufficio privacy, RPD e responsabile del dipartimento eventualmente coinvolto" e che "dispone di una procedura per la gestione dei data breach dal XX, diffusa ai dipendenti e inserita negli eventi formativi sulla privacy a partire dal XX. Tale procedura è stata aggiornata ed è in attesa di essere adottata con delibera" (v. verbale del XX, pag. XX).

Per quanto riguarda la formazione e sensibilizzazione dei dipendenti, anche in relazione al rischio di phishing, l'Azienda ha rappresentato che "dal XX la ASL aveva reso disponibile per tutto il personale amministrativo, tecnico e sanitario, dirigenti e non dirigenti, due corsi: "privacy nella sanità" personalizzato con le procedure, misure e modello organizzativo privacy della ASL e "cybersecurity nella sanità" livello base sempre personalizzato per la ASL. Tali corsi erano e sono tutt'ora fruibili mediante piattaforma FAD e sono utilizzati per i neo assunti. A XX erano 2095 su 3973 i dipendenti che avevano superato il corso "privacy nella sanità", a XX erano 2236 su 4277 i dipendenti che avevano superato il corso "cybersecurity nella sanità". Alla data della violazione oltre il 50% dei dipendenti avevano superato il corso "privacy nella sanità" e poco meno del 50% quelli che avevano superato il corso "cybersecurity nella sanità" livello base. Ad oggi la quasi totalità dei dipendenti ha superato il corso "privacy nella sanità" e il direttore generale ha sollecitato la conclusione del corso relativo alla cybersicurezza" (v. verbale del XX, pag.XX).

4. Le misure adottate a seguito della violazione

4.1. Notifica della violazione al Garante

Con riferimento alle misure adottate a seguito della violazione, l'Azienda ha rappresentato che "in data XX alle ore XX si è svolta una riunione di coordinamento con la presenza di personale della Polizia Postale e dell'Agenzia della Cybersicurezza Nazionale (ACN – CSIRT), pianificando le seguenti attività: investigazione su infrastruttura servente virtualizzata; compartimentazione/isolamento dei sistemi compromessi; coinvolgimento dei fornitori applicativi; eradication/bonifica dei server e degli endpoint; ripristino dei sistemi e delle reti con l'attivazione del piano di disaster recovery; attivazione di un servizio di Cyber Threat Intelligence per tracciare la eventuale presenza di informazioni della ASL1 in forums e black markets del clear web e del dark web; comunicazione sul sito internet istituzionale per trasparenza informativa; coinvolgimento del Responsabile della protezione dei dati. Al XX risultavano attivati i seguenti servizi: servizio cup; i ricoveri ospedalieri programmati e d'urgenza non hanno subito alcuna riduzione; le attività delle sale operatorie sono continuate secondo la normale programmazione e soprattutto in piena sicurezza, in quanto sono state immediatamente applicate le linee guida del Centro Nazionale Sangue per fronteggiare gli attacchi hacker al Sistema Trasfusionale. Il numero degli interventi chirurgici risulta invariato in alcuni casi in aumento rispetto al precedente periodo; le unità operative oncologiche hanno garantito la continuità delle terapie farmacologiche e delle prestazioni diagnostiche; sono riprese le prestazioni radioterapiche dal XX, con il contestuale recupero sia dei pazienti in lista sia dei nuovi pazienti da sottoporre a terapia; i laboratori di analisi, sia pure con comprensibili rallentamenti, stanno assicurando gli esami ematochimici e microbiologici sia con carattere di urgenza che programmati; pubblicazione di informative verso

l’utenza con l'invito a non scaricare, diffondere, condividere materiale proveniente dal dark web; pubblicazione della diffida verso le testate giornalistiche locali, regionali e nazionali con l'intimidazione a non diffondere materiale reso disponibile dal gruppo hacker “Monti” proveniente dal dark web. Per la riduzione degli effetti negativi per gli interessati l’Asl: ha istituito tre Centri di Ascolto Psicologico per offrire, a chiunque ne faccia richiesta, un adeguato percorso di assistenza e consulenza specialistica nonché per fornire specifico supporto sul modo in cui proteggersi dalle possibili conseguenze e prevenire o attenuare l’eventuale disagio psicologico; ha provveduto ad istituire un numero verde dedicato contattabile per ottenere ulteriori informazioni […] già dalla data del XX sono stati ripristinati tutti i sistemi operativi ed i relativi archivi consentendo di riportare a piena funzionalità ed efficienza i servizi di cui all’elenco che segue: Servizio CUP Gestione dei ricoveri, prestazioni ambulatoriali, flussi ministeriali Gestione sale operatorie Radiologia, radioterapia, Servizi amministrativi, Laboratorio analisi e ritiro online dei referti, Pronto soccorso, Servizio trasfusionale, Servizio Trapianti, Servizio farmaceutico, Servizi distrettuali, Servizi ambulatoriali, Servizi di salute mentale, Servizi veterinari, Servizio di igiene e sanità pubblica, Servizio di prevenzione e sicurezza sul lavoro, Servizio di medicina legale” e che si prevedevano le seguenti misure: “1. Implementazione della piattaforma XX […] 2. Migrazione dei servizi critici in Cloud sul Polo Strategico Nazionale. 3. Rafforzamento dell’organico dei Sistemi informativi aziendali con maggiori investimenti nello sviluppo di competenze specialistiche. 4. Piano di ripristino della rete interna: è stato applicato un piano in più fasi: isolamento della infrastruttura interna, bonifica e riattivazione. Sono stati isolati tutti i computer interni rispetto sia internet sia le altre WAN dell’ASL e la rete MPLS della Regione Abruzzo. Ambiente Cloud segregato: è stata bonificata ogni singola macchina mediante un agente software XX che ha consentito: - isolamento di ogni macchina mantenendo un unico canale di comunicazione con un server di gestione centralizzato; - scansione e blocco di tutti potenziali malware; - individuazione e analisi dei canali di comando e controllo. Il citato isolamento ha reso tutti gli host immuni da minacce, sterilizzato i malware e chiuso eventuali canali di comando e controllo. Al termine della bonifica è stata adottata una politica Zero-Trust relativamente ad accessi e canali di comunicazione. L’ambiente segregato è stato implementato nel cloud del Polo Strategico Nazionale. Sul PSN ciascun fornitore opera in zone dedicate e segregate. Sono stati ricostruiti ex novo due Domain Controller su XX. Sono state resettate tutte le password utenti e amministrative introducendo policy di controllo e limitazione degli accessi amministrativi. È stata attivata la dual factor authentication per l’accesso amministrativo al dominio e create utenze nominative singole per ciascun fornitore. A far data dal XX, è stata applicata la multi factor authentication su tutte le utenze XX. Nelle aree segregate del PSN sono state installate 55 macchine virtuali secondo le specifiche dei singoli fornitori applicativi. Il dialogo fra le isole applicative (è) regolat(o) tramite XX. Il disaccoppiamento tra cloud e infrastrutture dei client e fornitori è garantito da XX e load balancer. L’infrastruttura in cloud è stata collegata a quella delle LAN attraverso una VPN XX mentre ai fornitori sono state create VPN XX con permessi di accesso limitati esclusivamente alle loro macchine di pertinenza. Le nuove macchine virtuali sono state sottoposte a processi di hardening ed inserite nell’elenco delle scansioni realizzate dal sistema di continuous vulnerability assessment installato in apposita area di monitoraggio che contempla anche strumenti di analisi delle performance e un log collector degli eventi di sistema e applicativi. Il sistema di firewalling è stato migrato da XX a XX per unificare e centralizzare i controlli su piattaforma omogenea. Le basi dati XX sono sottoposte a backup. Apposita pianificazione garantisce una retention sufficiente. Lo storage è diversificato ed offre caratteristiche di immutabilità. Operativamente viene eseguito il costante monitoraggio degli eventi generati dagli hosts in rete. Verranno condotti Vulnerability Assessment semestrali con l’obiettivo di individuare eventuali criticità ed apporre le opportune remediation. L’XX ha il controllo di tutti i server oltre che della rete client. È stato rilasciato un server XX che consente di gestire centralmente e monitorare gli aggiornamenti ed il patching dei sistemi XX. È stato istituito un servizio di Help Desk interno, con tecnici dedicati, che tiene traccia e risponde alle problematiche IT segnalate dal Personale della ASL. È stata prorogata al XX la formazione in modalità FAD, destinata a tutto il personale, relativa alle tematiche di Cybersicurezza e protezione dei dati personali. Sono in corso di svolgimento sessioni formative dedicate al Personale IT e relative ai

seguenti ambiti: gestione XX, Multi Factor Authentication, Conditional Access, Self Service Password Reset, Incident Response basato su piattaforma XX. È istituito un servizio di Cyber Threat Intelligence che monitora costantemente Internet e il Dark Web in ottica di prevenzione delle minacce e verifica della postura di sicurezza esterna" (v. notifica del XX, sez. XX, punti XX e XX).

4.2. Attività ispettive

Nel corso delle attività ispettive, l'Azienda ha dichiarato, con riferimento allo stato di attuazione delle azioni di mitigazione, recupero, miglioramento e potenziamento delle misure di sicurezza indicate nella "Tab 4 – Sintesi attività in corso ed effettuate post incidente" del report incidente che "tutte le azioni definite "prioritarie" sono concluse, quali, a esempio, l'adozione di procedure di autenticazione a più fattori al momento dell'accesso ai sistemi XX, inizialmente prevista per gli utenti con privilegi amministrativi e, successivamente, estesa per tutti gli altri utenti aziendali, la cifratura dei dati XX, con particolare attenzione all'utilizzo di dispositivi mobili. È intenzione (…) potenziare le misure di sicurezza perimetrale con l'adozione di un sistema XX. Inoltre (…) oltre al monitoraggio reattivo già esistente basato sugli eventi prodotti dai diversi apparati e sistemi, (…) ha autonomamente attivato un monitoraggio proattivo degli eventi di sicurezza che comporta un arricchimento dei dati mediante uno specifico prodotto di threat intelligence che utilizza tecniche di intelligenza artificiale e governa le azioni dei diversi sistemi di monitoraggio degli eventi di sicurezza (XDR). (…) attualmente, è dotata di un SOC XX a cui si affianca il SOC XX del fornitore e che la scelta dei prodotti software tiene conto delle peculiarità del contesto sanitario" (v. verbale del XX, pagg. XX e XX).

Per quanto concerne le misure tecniche e organizzative l'Azienda ha, inoltre, evidenziato che "dopo l'attacco, la ASL ha modificato i rapporti con il fornitore, adottando un approccio di maggior presenza e accompagnamento durante le attività di installazione, patching, ed effettua un'analisi di ciò che viene installato fornendo evidenza di eventuali criticità anche a beneficio delle altre aziende sanitarie della regione. L'esperienza maturata dalla ASL a fronte dell'attacco costituisce, infatti, un importante punto di riferimento per tutte le realtà regionali" e che "oltre a rafforzare le procedure di autenticazione informatica, la ASL ha interposto XX che verificano, controllano e tracciano, rispettivamente, il traffico in uscita dalla ASL e quello in ingresso al PSN" (v. verbale del XX, pag. XX).

A scioglimento della riserva assunta in corso di ispezione, l'Azienda, alla citata nota del XX, ha inteso trasmettere "a supporto di quanto già descritto e prodotto in sede di ispezione relativamente alle azioni di mitigazione, recupero, miglioramento e potenziamento delle misure di sicurezza", una relazione dettagliata ("Relazione delle azioni di potenziamento delle misure di sicurezza adottate a seguito dell'incidente informatico del XX"), "al fine di rendere più agevole la comprensione delle informazioni già condivise in forma sintetica".

5. La comunicazione della violazione agli interessati

In relazione agli obblighi informativi nei confronti degli interessati coinvolti dalla violazione, l'Azienda ha preliminarmente rappresentato che erano "necessari ulteriori elementi per effettuare la valutazione del rischio per i diritti e le libertà delle persone fisiche" e che aveva effettuato la comunicazione mediante "pubblicazione di un comunicato sul sito internet istituzionale" (v. notifica del XX, sezz. XX, punto XX e XX, punto XX).

Con successiva notifica integrativa del XX, l'Azienda ha dichiarato di ritenere che "la violazione sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche (…) a causa della potenziale compromissione di dati personali di cui agli articoli 6, 9 e 10 del Regolamento 679/2016", rappresentando di aver proceduto a informare gli interessati ai sensi dell'art. 34 del Regolamento tramite "pubblicazione giornaliera di comunicati sul sito internet

istituzionale" (v. notifica del XX, sezz. XX, punto XX e XX, punto XX).

A seguito di approfondimento istruttorio dell'Ufficio e degli elementi acquisiti, il Garante, con il provvedimento n. 255 dell'8 giugno 2023 (doc. web n. 9896217), ha ingiunto all'Azienda di comunicare -individualmente a tutti gli interessati coinvolti- la violazione dei dati personali, descrivendone la natura e le possibili conseguenze, fornendo i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto appositamente istituito presso cui ottenere più informazioni, nonché fornendo informazioni sulle misure adottate per porre rimedio alla violazione e per attenuarne i possibili effetti negativi; ciò in quanto ha ritenuto che le iniziative intraprese dall'Azienda, fino a quel momento, per adempiere l'obbligo di comunicazione agli interessati –sebbene avessero rappresentato una misura opportuna per informarli circa le attività svolte nell'immediato e richiamare la loro attenzione su potenziali conseguenze della violazione, offrendo un recapito dedicato al quale rivolgersi– non consentivano, tuttavia, di informare efficacemente tutti gli interessati coinvolti, specialmente quelli appartenenti alle categorie per cui il rischio era stato valutato come critico, anche al fine di permettere loro di prendere le precauzioni necessarie in considerazione della diversa natura dei dati personali oggetto di violazione che li riguardavano.

Con nota del XX, l'Azienda ha fornito riscontro a quanto ingiunto dal Garante nel provvedimento dell'XX, comprovando con specifica documentazione, l'attività effettuata e l'impegno profuso.

6. 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 novembre 1981). In particolare, con atto n. XX del XX, l'Autorità ha ritenuto che l'Azienda fosse incorsa nella violazione dei principi di "liceità, correttezza e trasparenza" e di "integrità e riservatezza", di cui agli artt. 5, par. 1, lett. a) e f), e 12 del Regolamento nonché degli obblighi in materia di sicurezza del trattamento, di cui all'art. 32 del Regolamento e di comunicazione della violazione di dati personali agli interessati, di cui all'art. 34 del Regolamento.

La medesima Azienda ha fatto pervenire le proprie memorie difensive, ai sensi dell'art. 166, comma 6, del Codice. In particolare, con nota del XX, ha precisato quanto già dichiarato in atti e nel corso dell'attività ispettiva, dichiarando che:

- "giova, in via preliminare, ricordare che i fatti di cui al presente fascicolo istruttorio sono relativi ad un complesso attacco informatico, perpetrato da un gruppo di ignoti criminali informatici, di cui l'Azienda (…) è la prima vittima";

- "l'ASL (…) ha sempre profuso il massimo impegno per prevenire simili minacce e - in seguito all'attacco - ha sempre garantito la continuità delle attività di cura e assistenza, assicurando la massima trasparenza nei confronti degli assistiti e degli interessati, prestando completa collaborazione all'Autorità e lavorando a un continuo miglioramento della sicurezza dei propri sistemi e dei dati trattati";

- sulla mancata adozione di misure adeguate a rilevare tempestivamente la violazione dei dati personali, "la contestata mancata tempestività nell'individuazione dell'attacco non sia da ricondurre all'assenza di adeguate misure di sicurezza (e quindi a responsabilità dell'ASL), ma alle caratteristiche dello stesso dal momento che (…) l'attività degli attaccanti è stata

particolarmente complessa";

- "in particolare, quanto all'implementazione di misure adeguate a rilevare tempestivamente l'azione malevola, si evidenzia che, già in epoca precedente all'attacco, la ASL si era attivata per migliorare la propria sicurezza";

- "l'Azienda aveva acquisito un servizio SOC tramite Accordo Quadro SPC L2 Cloud Servizi di Sicurezza erogato fino al XX. Successivamente, nelle more della definizione di un nuovo Accordo Consip, si era altresì autonomamente dotata di un proprio Centro operativo con finestra di erogazione XX e supportato da strumenti di detection attivi XX tra i quali, in particolare, il sistema di alert e security di XX e quello di XX con capacità di monitoraggio e tempestiva risoluzione dei problemi che interessavano l'operatività delle Strutture Ospedaliere, delle altre strutture sanitarie e degli utenti presenti nel territorio di competenza";

- "anche dopo la scadenza della convenzione quadro Consip, l'Azienda si era adoperata per garantire il miglior avvicendamento contrattuale dei servizi di sicurezza informatica, prestando altresì la massima attenzione al monitoraggio del funzionamento della rete e alla tempestiva identificazione e risoluzione dei problemi, a garanzia della fruibilità dei servizi per gli utenti e per il comparto medico sanitario";

- "nella definizione e attuazione delle politiche di sicurezza, si è sempre tenuto conto dello stato dell'arte e, in particolar modo, 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";

- "a dimostrazione dell'impegno concreto in materia di sicurezza dei dati, si ritiene utile riepilogare i numerosi investimenti che l'ASL ha effettuato negli ultimi anni e prima dell'attacco informatico in ambito ICT e Cybersecurity, con primarie società nazionali ed internazionali";

- "sul punto, si riportano di seguito le principali delibere dell'ASL in materia, distinte a seconda delle diverse tecnologie per le quali il Titolare ha effettuato i relativi investimenti:

Antivirus ed EDR

a) Con delibera n. XX del XX, l'AV Symantec veniva sostituito con tecnologia Kaspersky, per una durata di 36 mesi.

b) Con delibera n. XX del XX, Kaspersky veniva sostituito con XX, in conseguenza del D.Lgs. 21 del 21 marzo 2022, il quale proibiva l'utilizzo della tecnologia russa e forniva un determinato tempo di adeguamento per le PA.

c) Poco prima della scadenza di XX - prevista il XX - e, quindi, nelle more dell'attacco informatico, l'ASL, tramite procedura MEPA, acquistava il rinnovo delle licenze di XX per ulteriori 12 mesi.

L'investimento in materia ammontava a circa 40-60.000 euro per ogni anno di licenza.

Firewall

Con delibera n. XX del XX veniva sostituita la tecnologia firewall già esistente ed in end of maintenance, contrattualizzando il tutto per 36 mesi (fino alla fine del XX).

L'investimento in questione ammontava a circa 167.000 euro per il totale dei 36 mesi.

Servizi di Cyber security

Nel XX, utilizzando la procedura Consip - denominata SPC Cloud lotto 2 - l'ASL ha effettuato importanti investimenti in materia di cyber security, acquistando XX una serie di servizi, di seguito elencati:

- firma digitale, marca temporale remota;

- test di sicurezza dinamici;

- vulnerability assessment;

- servizi professionali per definire un progetto di segmentazione della rete dell'ASL.

L'investimento ammontava a circa 882.000 euro.

Connettività di rete

Nel corso degli anni, con delibere del Direttore Generale n. XX del XX, n. XX del XX, n. XX del XX, n. XX del XX e n. XX del XX, ricorrendo al sopracitato accordo Consip SPC Connettività di rete a favore di Fastweb, l'ASL ha stipulato una serie di contratti (con scadenza in data del XX e prorogati al XX) per i seguenti servizi:

- connettività geografica;

- connettività anche per disaster recovery;

- connettività di emergenza degli ospedali in caso di evento imprevedibile;

- backup;

- supporto ufficio privacy.

Con riguardo specifico ai servizi di sicurezza, sono stati contrattualizzati il servizio di XX e XX, a loro volta costituiti altresì dai seguenti servizi: firewall; VPN ISPEC XX e Intrusion Detection & Prevention System (IDS/IPS).

L'investimento complessivo ammonta a circa 6 milioni di euro.

VPN

Con delibere n. XX del XX (e successive delibere n. XX del XX e n.XX del XX) sono state acquistate numerose applicazioni professionali per consentire l'accesso VPN ai dipendenti. Si evidenzia che vi è stato un incremento dei suddetti investimenti durante il Covid19, al fine di consentire agli stessi di effettuare agevolmente lo smart working.

L'investimento totale ammontava a circa 95.000 euro.

Tanto precisato in ordine agli sforzi compiuti dall'ASL, si sottolinea che, nel valutare la tempestività del Titolare nell'individuazione dell'attacco, non si può prescindere dal considerare le modalità e le tempistiche dello stesso, le quali, come ampiamente descritto, si sono rivelate particolarmente elaborate e, dunque, difficili da intercettare.

Infatti, tenuto conto che l'attacco si è sviluppato in una più ampia finestra temporale, il Centro Operativo, così come strutturato e supportato, sarebbe stato in grado di intercettarlo se non fosse stato per il singolare livello di sofisticatezza messo in campo

dall’attaccante (ad esempio, bassa frequenza dei movimenti laterali), che ha consentito di bypassare la presenza di differenti livelli di sicurezza (defense in depth)(…). (…), gli attaccanti (ovvero il Gruppo Monti) sono di fatto una costola del gruppo Conti, noto per aver bloccato nel XX - con un attacco mirato - tutta la sanità dell’Irlanda, tanto da richiedere un intervento di supporto degli Stati Uniti”;

- in relazione alla mancata adozione di misure adeguate a garantire la sicurezza delle reti e di misure organizzative per assicurare la consapevolezza e l’accesso degli incaricati ai sistemi, “con riguardo alla contestata mancata segregazione delle reti (…), sono diverse le iniziative intraprese da questa ASL prima dell’incidente in oggetto e finalizzate a migliorare l’infrastruttura in essere”, che “aveva in corso un progetto di evoluzione dell’infrastruttura sul cloud, la quale prevedeva la segmentazione delle reti, così come documentato anche in fase ispettiva. Le attività erano state avviate a far data da XX, quando veniva accettato e quindi autorizzato il pagamento delle attività di progettazione della segmentazione della rete e verifica dei log, per un totale di 173.000 euro. Nonostante le problematiche incontrate nella fase operativa, un piano di segmentazione della rete che tenesse conto della numerosità dei punti di erogazione (4 ospedali, 2 Presidi Territoriali di Assistenza, 2 Ospedali di Comunità, 1 Residenza per l'esecuzione di misure di sicurezza, 3 Case circondariali e ulteriori 70 presidi assistenziali e amministrativi) era già in fase di attuazione al momento del breach. A riprova di ciò: i) alcune delle componenti di sicurezza dell’infrastruttura erano già migrate e isolate sul cloud di XX; ii) una parte della rete era stata segmentata e sottoposta a NAC (network access control)”;

- “la parte di infrastruttura fino a quel momento segmentata è riuscita ad evitare che potenziali compromissioni potessero propagarsi a tutti i sistemi ed archivi di dati personali; l’attacco, infatti, non si è propagato, né avrebbe potuto farlo, a specifiche aree della rete ove erano presenti repliche dei sistemi di accounting, accesso e monitoraggio e anche i backup sono stati salvaguardati. A ciò si aggiunga che i log dettagliati sono stati raccolti durante l’incidente, documentando la catena degli eventi e le singole azioni degli attaccanti”;

- “questi log rappresentano una prova del fatto che le misure di sicurezza adottate erano adeguate, consentendo un monitoraggio accurato e tempestivo delle attività anomale”;

- “inoltre, nel XX, era stato elaborato anche un capitolato tecnico per il rafforzamento delle misure di sicurezza, considerata la notevole complessità e l’impatto nei confronti dell’operatività delle strutture della ASL”;

- “la violazione contestata non sia riconducibile a un’inerzia del Titolare o a una mancata sensibilità dello stesso verso il tema della sicurezza e della protezione dei dati personali. Anzi, da quanto sopra riportato, si evince l’impegno per potenziare le misure di sicurezza in essere ancor prima dell’attacco hacker e, dunque, a prescindere dagli obblighi di compliance rafforzata che ne sono conseguiti, anche per scongiurare l’avverarsi di eventi analoghi in futuro”;

- “in merito, poi, all’avvenuta propagazione della mail di phishing tramite l’account di un consulente non più operativo presso la ASL, si fa presente che tale account era in fase di dismissione; a ciò si aggiunga che, sotto il profilo dell’awareness dei dipendenti, l’ASL ha investito diffusamente nella formazione costante degli utenti e del personale IT tramite un sistema di Formazione A Distanza (FAD) che fornisce corsi specifici in materia di sicurezza informatica e protezione dei dati”;

- sulla comunicazione della violazione dei dati agli interessati, “si premette che l’ASL ha sempre riconosciuto l'importanza di assicurare una corretta e tempestiva informazione agli interessati e ha messo in atto una serie di azioni mirate, fin dall’individuazione della

violazione, per garantire la trasparenza su quanto accaduto e per minimizzare ulteriori rischi per i soggetti coinvolti";

- "si ritiene che la valutazione di codesta Autorità non possa prescindere dal contesto in cui sono state adottate le scelte circa le modalità e le tempistiche della prima comunicazione. Nell'ambito della situazione emergenziale, l'ASL ritiene di aver agito in modo diligente e proporzionato, adottando tutte le misure ragionevolmente possibili per informare gli interessati della violazione dei dati; le attività di comunicazione che oggi vengono contestate rappresentavano solo il primo passo di un percorso di trasparenza. Infatti, si fa presente che - parallelamente alle attività di recupero e ripristino - l'ASL ha avviato, con il supporto di soggetti specializzati nel frattempo coinvolti, l'analisi finalizzata a chiarire la dinamica dell'incidente e a individuare puntualmente le informazioni oggetto di esfiltrazione";

- "le difficoltà riscontrate nell'individuazione dei soggetti interessati effettivamente coinvolti dalla violazione hanno reso tale analisi particolarmente complessa, richiedendo, di conseguenza, il tempo necessario per i dovuti approfondimenti";

- "la natura del data breach oggetto dell'analisi, ma più in generale la natura dei breach di tale tipologia, è caratterizzata da un ingente mole di file di diverso formato, organizzati all'interno di cartelle. I dati oggetto di breach non consentivano una diretta connessione con indirizzi email, residenze e codici fiscali, in quanto spesso riportavano solo nome e cognome o poche altre informazioni protocollari. L'analisi di specie, quindi, ha comportato l'implementazione di una metodologia, volta a esaminare in dettaglio la vasta varietà di dati forniti. Ciò, al fine di garantire una categorizzazione efficiente dei diversi tipi di file presenti nel breach e quindi un lavoro a ritroso di connessione tra i dati oggetto di violazione, l'accettazione del paziente che richiedeva quella prestazione e l'anagrafica, per poter estrapolare un indirizzo valido per la comunicazione all'interessato. Tale approccio si è reso necessario per identificare compiutamente le persone, evitare rischi di omonimie o dati incompleti o dati non necessariamente connessi a persone fisiche; queste attività erano state organizzate prima del provvedimento di codesta Autorità dell'XX e avevano già l'obiettivo di indirizzare comunicazioni precise e individuali ai singoli interessati, parallelamente al completamento del processo di notifica";

- "in attesa che tale analisi venisse completata, l'ASL ha adottato comunque un primo approccio per informare gli interessati, tenendo conto della specificità della situazione e delle circostanze particolari che caratterizzano l'erogazione di servizi sanitari. Nello specifico, le misure inizialmente intraprese sono state: Pubblicazione giornaliera di comunicati sul sito internet istituzionale, con l'obiettivo di fornire una comunicazione tempestiva e trasparente sull'accaduto, accessibile a tutti gli interessati, in conformità all'art. 34 del GDPR. La ASL ha provveduto immediatamente dopo il fatto ad attivare un'apposita sezione informativa e di comunicazione nella Home Page rivolta agli utenti del portale aziendale attualmente denominata "INFORMATI INSIEME" al cui interno sono state pubblicate le comunicazioni di seguito elencate, di cui si allega copia sub "A":

1) XX: DIREZIONE SANITARIA

2) XX: UOSD DERMATOLOGIA GENERALE E ONCOLOGIA DU

3) XX: DIREZIONE AZIENDALE

4) XX: RIATTIVAZIONE CUP

5) XX: DIREZIONE SANITARIA

6) XX: RIATTIVAZIONE CUP OSPEDALIERI PER TUTTI I TIPI DI PRENOTAZIONE

7) XX: AGGIORNAMENTO PER I CITTADINI

8) XX: CASELLE EMAIL FUNZIONANTI

9) XX: AGGIORNAMENTO: LE ATTIVITÀ NEI DISTRETTI

10) XX: COMUNICAZIONE VIOLAZIONE DEI DATI PERSONALI ALL'INTERESSATO

11) XX: MANTENUTI I STESSI LIVELLI DI ATTIVITÀ CHIRURGICA

12) XX: ATTACCO HACKER ALLA ASL ABRUZZO, GARANTE: SCARICARE I DATI È UN REATO

13) XX: NESSUNA INTERRUZIONE NELLA FILIERA DELL'EMERGENZA

14) XX: AGGIORNAMENTI SUI CUP: TUTTI ATTIVI

15) XX: NESSUN DATO ANDATO PERDUTO

16) XX: BACKUP SALVI, RISPRISTINO PIÙ SEMPLICE

17) XX: INCREMENTARE LE ATTIVITÀ AMBULATORIALI
REGIONE ABRUZZO

18) XX: ASSISTENZA PSICOLOGICA: ATTIVI 3 CENTRI DI ASCOLTO (disposizione n.XX del XX)

19) XX: SISTEMA GESTIONALE DEI PRONTO SOCCORSO TOTALMENTE OPERATIVO

20) XX (TASK FORCE INFORMATICA): "VIA ALLE FASE 2, IL 70% DEI DATI GIA' IN CLOUD"; Comunicazione tramite il portale on-line del dipendente; Comunicazione tramite e-mail e pec a consulenti e collaboratori";

- "già in data anteriore al provvedimento di Codesta Autorità dell'XX, l'ASL aveva provveduto a diffondere la notizia del data breach tramite plurimi canali alla più ampia platea possibile di interessati. In aggiunta, si sottolinea che nel frattempo l'ASL ha garantito altresì il tempestivo riscontro alle istanze che pervenivano da parte degli interessati e dalla stampa; l'ASL ha ritenuto di inviare le comunicazioni individuali per posta ai singoli interessati solo all'esito della complessa analisi post breach, condotta dai consulenti esterni e, comunque, prima della trasmissione a codesta Autorità di tutte le ulteriori informazioni raccolte dalla ASL (v. notifica conclusiva del XX). Invero, solo terminata tale analisi successivamente alla notifica del provvedimento dell'XX, la ASL ha proceduto con le ulteriori comunicazioni ai sensi dell'art. 34 del GDPR nelle modalità individuate dall'Autorità, confidente del fatto di avere acquisito un quadro esaustivo circa la gravità dell'incidente, circa la reale portata dei conseguenti rischi per i diritti e le libertà degli interessati, nonché la certezza ed evidenza che i destinatari delle stesse fossero effettivamente soltanto i soggetti coinvolti. Ciò al precipuo fine di evitare allarmismi a causa di comunicazioni incomplete o rivolte a destinatari errati";

- "a fronte della complessità delle operazioni svolte dagli attaccanti, il breach ha riguardato solo una minima parte dei dati oggetto di trattamento dall'ASL a causa delle sue funzioni istituzionali (prestazione di servizi sanitari e socio-sanitari)";

- "questa Amministrazione ha da sempre prestato la massima collaborazione con il Garante sia mediante i riscontri alle note ricevute e le informazioni fornite in sede di notifica, sia

nell’ambito della visita ispettiva”;

- “l’ASL - con nota del XX - ha documentato il pieno rispetto di quanto disposto dall’Autorità Garante con il provvedimento dell’XX”;

- “ad oggi, risultano implementate una serie di misure di sicurezza avanzate che consentono di ridurre drasticamente la replicabilità dell’attacco subito, con esternalizzazione degli archivi di dati personali sul Polo Strategico Nazionale (PSN)”;

- “per le stesse ragioni, nella denegata ipotesi in cui venisse comunque comminata una sanzione, si chiede di tenere conto di tutti gli elementi forniti e, comunque, di non applicare la sanzione accessoria della pubblicazione sul sito web dell’Autorità”.

Durante l’audizione del XX, è stato, altresì dichiarato che:

- “l’Azienda è stata vittima dell’attacco hacker di grande portata e, pertanto, è stata la prima ad essere danneggiata. La ASL opera con finanza derivata e ha investito molte risorse per garantire i servizi ai cittadini. L’attacco avrebbe potuto avere un danno rilevante in termini di perdita di fiducia da parte dei cittadini ma l’impegno sempre profuso dall’Azienda ha evitato questo rischio. L’attacco ha altresì determinato costi imprevisti anche dovuti alle attività successive al breach, ivi compresa la comunicazione agli interessati”;

- “l’attacco è stato effettuato in modo estremamente sofisticato e innovativo da parte di hacker internazionali abilissimi del gruppo Monti, costola del gruppo Conti, che aveva già danneggiato la sanità irlandese, in relazione al quale è molto difficile predisporre barriere difensive. Tale aspetto è stato anche rilevato dalla società XX nel report predisposto, in atti”;

- “la reazione della ASL all’attacco è stata tempestiva, estesa e solida: non si è verificata nessuna interruzione dei servizi sanitari, ma solo marginali disfunzioni; gli assistiti hanno potuto usufruire dei servizi sanitari e alcune attività sono state potenziate a dimostrazione che il sistema organizzativo e funzionale della ASL era robusto e resiliente, tanto che non vi è stata perdita di fidelizzazione degli assistiti”;

- “non si è verificata nessuna perdita di dati grazie alle politiche di backup adottate dall’Azienda”;

- “l’esfiltrazione dei dati ha riguardato una quantità marginale, pari allo 0,1% dei dati, in rapporto al patrimonio informativo della ASL. Pertanto, il 99,9 % dei dati è stato protetto dalle misure dell’Azienda”;

- “la ASL ha collaborato con ACN e la polizia postale e ha ottemperato agli obblighi previsti dal Regolamento europeo”;

- “la ASL ha investito molto in sicurezza informatica nonostante le criticità di bilancio intervenute dal XX con la pandemia COVID e a seguito della guerra in Ucraina; ciò ha determinato la chiusura del bilancio con un disavanzo di XX milioni di euro nel XX, di XX milioni di euro nel XX e di XX milioni di euro nel XX; la portata dei predetti investimenti è stata anche dimostrata dalla continuità del servizio assicurata a fronte dell’attacco”;

- “con riguardo alla comunicazione agli interessati il Direttore Generale ha coordinato, partecipando in prima persona, il gruppo di lavoro che si è occupato dell’esame dei dati esfiltrati, nell’ottica di effettuare, sin da subito, comunicazioni individuali. Tali informazioni erano contenute in documenti in formati diversi (scansioni, word, excel); ciò comportava la difficile e laboriosa individuazione di quali documenti fossero riferiti a persone fisiche e la successiva identificazione delle persone attraverso le anagrafiche aziendali e regionali; la

ASL ha, pertanto, richiesto l'intervento di consulenti specializzati. Le predette attività hanno avuto inizio non appena si è avuta la consapevolezza dell'esfiltrazione e ciò ha consentito di ottemperare al provvedimento prescrittivo dell'Autorità nei termini previsti (fatto altrimenti non tecnicamente possibile) e a inviare così una comunicazione individuale a 6817 assistiti";

- "la ASL continua a investire in cybersicurezza anche con l'istituzione di una UO Cybersicurezza, un continuo aggiornamento tecnologico, la migrazione sul Polo Strategico Nazionale (PSN) (prima Azienda sanitaria in Italia), l'attivazione di servizi di Cyber Threat Intelligence e SOC esteso. Il Dipartimento Transizione Digitale ha individuato la ASL come esempio di buona pratica per il progetto di cloud sicuro che, tra gli altri, prevede interventi volti a prevenire potenziali incidenti. La roadmap delle azioni pianificate a valle dell'incidente sta procedendo secondo i tempi programmati, con particolare riferimento alle campagne di sensibilizzazione sul phishing; ciò, senza interferire con la continuità operativa dei servizi sanitari".

7. Esito dell'attività istruttoria

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

si considerano "dati relativi alla salute", "i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute" (art. 4, par. 1, n. 15, del Regolamento);

l'art. 5, par. 1, lett. a), del Regolamento stabilisce che i dati personali devono essere "trattati in modo lecito, corretto e trasparente nei confronti dell'interessato" (principio di "liceità, correttezza e trasparenza");

in applicazione del predetto principio, l'art. 12, par. 1, del Regolamento prevede che "il titolare del trattamento adotta misure appropriate per fornire all'interessato […] le comunicazioni di cui […] all'articolo 34 relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori. Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici";

l'art. 34 del Regolamento stabilisce che "quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo" (par. 1), che "la comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d)" (par. 2) e che "non è richiesta la comunicazione all'interessato […] se è soddisfatta una delle seguenti condizioni: […] c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia" (par. 3).

le "Linee guida n. 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) evidenziano che "in linea di principio, la violazione dovrebbe essere comunicata direttamente agli interessati coinvolti, a meno che ciò richieda uno sforzo sproporzionato. In tal caso, si procede a una comunicazione pubblica o a una misura simile che permetta di informare gli interessati con analoga efficacia (articolo 34, paragrafo 3, lettera c)" (sez. III.C);

i dati personali devono essere “trattati in maniera da garantite 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” (principio di «integrità e riservatezza», art. 5, par. 1, lett. f), del Regolamento);

l’art. 32 del Regolamento, concernente la sicurezza del trattamento, stabilisce che “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, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio” (par. 1) e che “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” (par. 2);

le citate “Linee guida 9/2022 sulla notifica delle violazioni dei dati personali ai sensi del RGPD” chiariscono, inoltre, 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;

il Considerando n. 87 precisa che “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”.

8. Valutazioni del Garante e conclusioni.

In primo luogo si rileva che i trattamenti effettuati nel contesto in esame, che hanno ad oggetto anche dati appartenenti anche a categorie particolari e riguardano un numero molto rilevante di interessati, 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), del Regolamento, tutte quelle che si rendono necessarie al fine di attenuare i rischi che i medesimi trattamenti presentano e di non compromettere la riservatezza, l’integrità e la disponibilità dei dati personali.

Alla luce di quanto sopra rappresentato, 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) e 32 del Regolamento, in relazione ai seguenti profili:

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

Nel corso dell'istruttoria è emerso che i soggetti malintenzionati hanno effettuato una serie di operazioni propedeutiche all'attacco informatico e che "le prime attività sospette sui sistemi risulterebbero iniziare a partire dal giorno XX (…) (v. report XX, pag. XX). L'Azienda "era dotata di diversi strumenti (…) che consentivano la registrazione ma non la correlazione degli eventi (…) disponeva di un servizio SOC XX fino al XX, successivamente il SOC è stato sostituito con un servizio di security device management gestito in autonomia e con personale interno dalla UO sistemi informativi. In ogni caso la catena degli eventi relativi all'attacco è avvenuta principalmente di notte e durante periodi a ridosso di festività" (v. verbale del XX, pag. XX) e "la configurazione adottata di XX sia in modalità detect permette (…) la detention di eventuali anomalie ma non effettua nessun tipo di blocco" (v. report XX, pag. XX). Dopo l'attacco l'Azienda "oltre al monitoraggio reattivo già esistente basato sugli eventi prodotti dai diversi apparati e sistemi (…) ha autonomamente attivato un monitoraggio proattivo degli eventi di sicurezza che comporta un arricchimento dei dati mediante uno specifico prodotto di threat intelligence che utilizza tecniche di intelligenza artificiale e governa le azioni dei diversi sistemi di monitoraggio degli eventi di sicurezza (XDR); (…) attualmente, è dotata di un SOC XX a cui si affianca il SOC XX del fornitore e che la scelta dei prodotti software tiene conto delle peculiarità del contesto sanitario" (v. verbali del XX, pag. XX e del XX, pagg. XX e XX).

Tali circostanze non hanno consentito all'Azienda di venire tempestivamente a conoscenza della violazione dei dati personali occorsa.

La mancata adozione, al momento in cui si è verificato l'attacco hacker, di misure adeguate a rilevare tempestivamente le violazioni dei dati personali (es., assenza di blocchi e di correlazione di specifici eventi di sicurezza e di comportamenti anomali, quali orario e tipologia degli accessi, SOC non operativo in modalità "estesa"), non risulta 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, tenuto conto di quanto previsto dalle citate Linee guida, richiede che il titolare e il responsabile del trattamento debbano mettere in atto misure per "individuare […] tempestivamente una violazione".

8.2. Mancata adozione di misure adeguate a garantire la sicurezza delle reti e di misure organizzative per assicurare la consapevolezza e l'accesso degli incaricati ai sistemi

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. Infatti, al momento della violazione dei dati personali "la parte interessata dall'attacco, ove erano attestati i sistemi server, era ancora flat e priva di segmentazione" (v. verbale del XX, pag. XX) e "una parte della rete era stata segmentata e sottoposta a NAC (network access control)(v. memoria del XX).

Nel corso dell'istruttoria è emerso, altresì, che il ransomware si è propagato mediante una "e-mail di phishing contenente un link malevolo" e che "l'attaccante abbia utilizzato [una] utenza (…) associata ad un consulente non più operante presso la ASL".

Tali circostanze non risultano pienamente conformi alle disposizioni di cui all'art. 5, par. 1, lett. f), e all'art. 32, par. 1, del Regolamento che 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)).

8.3. Inidonea comunicazione della violazione dei dati personali agli interessati

In considerazione del fatto che, nel caso di specie, la violazione dei dati personali in esame presentava un rischio elevato per i diritti e le libertà delle persone fisiche, come già rilevato nel citato provvedimento del Garante dell'8 giugno 2023 n. 255, ricorrevano i presupposti per la comunicazione agli interessati, ai sensi dell'art. 34, par. 1, del Regolamento. Ciò, tenuto conto

della natura della violazione dei dati personali, delle categorie dei dati personali oggetto di violazione, delle categorie di interessati coinvolti (che si trovano anche in condizioni di vulnerabilità o fragilità), della gravità e persistenza delle possibili conseguenze per le persone fisiche che potrebbero derivare dalla violazione (quali, a esempio, discriminazione, disagio psicologico, umiliazione, danni alla reputazione o altri danni materiali o immateriali), nonché del ruolo rivestito dall'Azienda nel sistema sanitario locale, che richiede un elevato grado di responsabilizzazione al fine di garantire la fiducia nei suoi confronti da parte degli assistiti, soddisfacendo, in particolare, le legittime aspettative di trasparenza e sicurezza del trattamento.

Nel corso dell'istruttoria è emerso che l'Azienda ha proceduto a informare gli interessati ai sensi dell'art. 34 del Regolamento tramite "pubblicazione giornaliera di comunicati sul sito internet istituzionale" e che prevedeva la consegna della comunicazione agli interessati da parte degli "operatori sanitari, brevi manu, al primo contatto utile con l'assistito o familiare/tutore/amministratore a seconda dei contesti, presso le Strutture sanitarie sia Ospedaliere che Territoriali", mediante "un format di lettera diversificato in base alle categorie di interessati e relativo profilo di rischio associato" (v. anche nota di riscontro del XX alla richiesta di informazioni).

Tuttavia, tale prima comunicazione inviata dall'Azienda è apparsa solo in parte idonea all'assolvimento degli obblighi di cui all'art. 34 del Regolamento. L'inidoneità della richiamata modalità informativa è confermata dal fatto che il Garante ha ritenuto necessario ingiungere all'Azienda, con il sopra riportato provvedimento (non oggetto di specifica impugnativa), di provvedere all'assolvimento dell'obbligo di cui all'art. 34, par. 1, del Regolamento. Infatti, il Garante ha ritenuto che le prime iniziative intraprese dall'Azienda per adempiere l'obbligo di comunicazione agli interessati – sebbene avessero rappresentato una misura opportuna per metterli a conoscenza delle attività svolte nell'immediato e richiamare la loro attenzione sulle potenziali conseguenze della violazione, offrendo un recapito dedicato al quale rivolgersi – non consentivano di informare tempestivamente ed efficacemente tutti gli interessati coinvolti, specialmente quelli appartenenti alle categorie per cui il rischio era stato valutato come critico, che non si trovavano nelle condizioni di avere un contatto con l'Azienda, essendo rimessa all'iniziativa dei singoli che via via le si rivolgevano; ciò, anche al fine di permettere loro di prendere le precauzioni necessarie in considerazione della diversa natura dei dati personali oggetto di violazione che li riguardavano.

Al riguardo, inoltre, l'Azienda, pur avendo espressamente evidenziato di aver posto in essere la complessa analisi dei dati, immediatamente dopo la violazione, non ha comprovato in alcun modo, la sussistenza della condizione di cui all'art. 34, par. 3, del Regolamento in relazione allo sforzo sproporzionato che la predetta comunicazione agli interessati coinvolti richiederebbe né che l'iniziativa dalla stessa adottata avesse avuto analoga efficacia informativa come richiesto dall'art. 34, par. 3, lett. c) del Regolamento né che fossero soddisfatte le previsioni di cui all'art. 2-duodecies, comma 2 del Codice circa la possibilità di ritardare, limitare o escludere l'adempimento della comunicazione "nella misura e per il tempo in cui ciò costituisca una misura necessaria e proporzionata […] per salvaguardare l'indipendenza della magistratura e dei procedimenti giudiziari".

In tale quadro, confermando i rilievi formulati dall'Ufficio, con il citato atto del XX, si ritiene che l'Azienda non abbia completamente ottemperato agli obblighi di comunicazione della violazione di dati personali agli interessati; ciò, in violazione degli artt. 5, par. 1, lett. a) 12 e 34 del Regolamento.

Ciò premesso, tenuto conto che:

- la violazione è stata determinata da un comportamento doloso da parte di un soggetto terzo, denunciato formalmente alle autorità competenti;

- il Garante ha preso conoscenza dell'evento a seguito della notifica di violazione effettuata dall'Azienda, ai sensi dell'art. 33 del Regolamento e da alcune istanze pervenute al Garante sull'accaduto;

- il titolare, al fine di evitare la ripetizione dell'evento occorso, si è impegnato nella realizzazione di misure, delle quali alcune pianificate in un tempo antecedente il verificarsi della violazione dei dati personali, volte a incrementare il livello di sicurezza dei trattamenti svolti e, quindi, a ridurre la replicabilità dell'evento occorso e ad attenuare il danno subito dagli interessati;

- il titolare ha cooperato con l'Autorità ben oltre l'obbligo previsto dall'art. 31 del Regolamento in ogni fase dell'istruttoria, ivi compresa quella ispettiva, al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi;

- l'Azienda non è stata destinataria di un precedente provvedimento sanzionatorio in relazione a violazioni pertinenti;

- la gestione dell'emergenza pandemica ha comportato modifiche all'assetto infrastrutturale dell'Azienda per consentire lo smart working dei dipendenti e l'interruzione delle attività inerenti i servizi di vulnerability assessment e volti alla segmentazione delle reti ma non ha, comunque, impedito i forti investimenti in sicurezza informatica nonostante le criticità di bilancio intervenute dal XX a seguito della predetta emergenza pandemica;

le circostanze del caso concreto inducono a qualificare lo stesso come "violazione minore", ai sensi del Considerando n. 148 del Regolamento e delle "Linee guida riguardanti l'applicazione e la previsione delle sanzioni amministrative pecuniarie ai fini del regolamento (UE) n. 2016/679", adottate dal "Gruppo di Lavoro Art. 29" il 3 ottobre 2017, WP 253 e fatte proprie dal Comitato europeo per la protezione dei dati con l'"Endorsement 1/2018" del 25 maggio 2018. 2018. Si ritiene, pertanto, relativamente al caso in esame, che sia sufficiente ammonire il titolare del trattamento ai sensi degli art. 58, par. 2, lett. b), del Regolamento.

Si rileva, altresì, che ricorrono 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.

Si informa, infine, che copia del presente provvedimento verrà pubblicata sul sito web della scrivente Autorità, ai sensi dell'art. 154-bis, comma 3, del Codice e dell'art. 37 del Regolamento del Garante n. 1/2019.

TUTTO CIÒ PREMESSO IL GARANTE

a) dichiara, ai sensi dell'art. 57, par. 1, lett. a), del Regolamento, l'illiceità del trattamento effettuato dal titolare del trattamento, ASL 1 Avezzano Sulmona L'Aquila, con sede in Loc. Campo di Pile (L'Aquila), Via G. Saragat – c.a.p. 67100 - Partita Iva/Codice Fiscale n. 01792410662;

b) ai sensi dell'art. 58, par. 2, lett. b), del Regolamento, ammonisce tale titolare del trattamento per aver violato le disposizioni di cui agli 5, par. 1, lett. a) e f), 12, 32 e 34 del Regolamento, nei termini di cui in motivazione;

c) in conformità all'art. 17 del Regolamento del Garante n. 1/2019, dispone l'annotazione della violazione nel registro interno dell'Autorità di cui all'art. 57, par. 1, lett. u), del Regolamento.

Ai sensi dell'art. 78 del Regolamento, degli artt. 152 del Codice e 10 del d.lgs. n. 150/2011,

avverso il presente provvedimento può essere proposta opposizione all’Autorità giudiziaria ordinaria, con ricorso depositato al tribunale ordinario del luogo individuato nel medesimo art. 10, entro il termine di trenta giorni dalla data di comunicazione del provvedimento stesso, ovvero di sessanta giorni se il ricorrente risiede all'estero.

Roma, 13 febbraio 2025

IL PRESIDENTE
Stanzione

IL RELATORE
Cerrina Feroni

IL VICE SEGRETARIO GENERALE
Filippi