Provvedimento del 17 ottobre 2024

[doc. web n. 10086523]

Provvedimento del 17 ottobre 2024

Registro dei provvedimenti
n. 621 del 17 ottobre 2024

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

Il XX l'Azienda Ospedaliero-Universitaria SS. Antonio e Biagio e Cesare Arrigo, di Alessandria, 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 e XX - riguardante un attacco informatico ai sistemi informativi dell'Azienda determinato da un malware di tipo ransomware "Ragnar Locker".

Tenuto conto dell'elevato numero di interessati coinvolti e della natura dei dati personali oggetto di violazione, è stato necessario approfondire le circostanze nelle quali si è verificata la predetta violazione dei dati personali, nonché le misure di sicurezza adottate, mediante un'attività ispettiva nei confronti dell'Azienda nel mese di gennaio 2024.

2. Il fatto

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

2.1. La notifica della violazione al Garante

Preliminarmente, con la notifica del XX, l'Azienda ha dichiarato che "l'infrastruttura dell'Azienda è stata oggetto di attacco informatico da parte di un gruppo che ha rilasciato un ransomware denominato "Ragnar Locker"" (v. notifica del XX, sez. XX, punto XX).
Successivamente, l'Azienda ha aggiornato le informazioni riguardanti la violazione dichiarando che "nella notte tra il XX indicativamente a partire dalle ore XX e le XX del giorno successivo, l'infrastruttura informatica dell'Azienda ospedaliera (…) ha visto molti dei pc della sua rete invasi da un messaggio che notificava un attacco hacker da parte di un gruppo denominato "Ragnar Locker". Nel messaggio si legge che il contenuto esfiltrato dalle cartelle condivise sarebbe stato oggetto di vendita presso terze parti se entro tre gg. non ci fosse stato un contatto su canale TOR per istruzioni. Si precisa che l'attacco è stato limitato alla sola parte della infrastruttura dell'Ospedale che contiene dati condivisi dagli utenti, ovvero i file condivisi tramite file server. Non sono stati attaccati gli applicativi sanitari installati presso il data center centrale aziendale. Non sono stati violati software o servizi all'utenza. Pertanto l'ospedale non ha subito disservizi o limitazioni nell'esercizio della sua funzione istituzionale" (v. notifica del XX e XX, sez. X, punto X).
Per quanto attiene al numero di interessati i cui dati sulla salute sono stati coinvolti dall'attacco, l'Azienda ha dichiarato che "il contenuto delle cartelle violate è in corso di valutazione in quanto sono state pubblicate sul canale TOR informazioni in data XX da parte del gruppo "Ragnar Locker"" e che gli interessati sono riconducibili alle macrocategorie dipendenti, consulenti e pazienti (v. notifica del XX, sez. XX, punto XX).

2.2. Attività ispettive

Nel corso delle attività ispettive l'Azienda, con riguardo alle modalità e tempistiche dell'attacco, ha dichiarato che "sono state oggetto dell'attacco le postazioni di lavoro (PdL) e il sistema di file sharing (utilizzato di fatto come unico gestore documentale) a cui le PdL erano collegate" e, confermando quanto già dichiarato nella notifica di violazione dei dati personali "ha chiarito che, dalla ricostruzione, posta in essere grazie anche all'intervento dello CSIRT e alla disponibilità dei log del firewall, i primi tentativi di accesso risalgono a XX, periodo nel quale sono state rilevate attività di discovering e, quindi, di lateral movement per poi sferrare l'attacco, verosimilmente, ai primi di XX. Dalla predetta ricostruzione, il punto di origine, sebbene non si abbiano evidenze certe in quanto l'Azienda non disponeva di un sistema di log management, sembra essere stato lo sfruttamento di una vulnerabilità del firewall aziendale XX tramite cui i soggetti malintenzionati hanno recuperato alcune credenziali di dominio e condotto movimenti laterali che, mediante una

connessione VPN any to any, hanno consentito l'accesso a un PC aziendale con VPN aperta, la priviledge escalation ad amministratore, lo scarico delle credenziali memorizzate nel servizio LSASS, infine quello massivo dei contenuti del file server su storage sito in Olanda e installazione di una backdoor SSH. (…) Tutte le cartelle del file server erano accessibili da qualsiasi PdL dell'ospedale. (…) I soggetti malintenzionati hanno disattivato l'antivirus e inoculato il codice eseguibile che ha scaricato la ransom note sulle PdL, sebbene non abbiano proceduto alla cifratura dei dati", (…) "dalla ricostruzione effettuata, per l'attacco era stata utilizzata un'utenza, per accedere alla VPN, appartenente al personale del fornitore, recuperata dal file di configurazione del firewall XX" (v. verbali del XX, pagg. XX e XX e del XX, pag. X).

Per quanto concerne la portata della violazione con riferimento agli applicativi aziendali di ordine sanitario e amministrativo contabile, l'Azienda ha dichiarato che "gli applicativi aziendali non hanno avuto alcun impatto e non si sono verificati disservizi né interruzioni dell'erogazione delle prestazioni sanitarie a favore degli assistiti. Per gli utenti interni si è verificata una limitazione degli accessi a seguito della revisione delle policy di gestione delle utenze e dell'assegnazione dei privilegi agli amministratori che, al momento della violazione, non era differenziata. Ciò, sia per consuetudine che per semplificazione operativa, anche con riferimento ai fornitori degli applicativi e delle apparecchiature elettromedicali che effettuano la manutenzione delle stesse. La violazione ha, pertanto, riguardato solo il profilo della riservatezza" e ha inteso precisare che "il gruppo hacker Ragnar Locker, autore dell'attacco, è stato smantellato, come da notizie di cronaca" (v. verbale del XX, pag. XX).

Sempre nel corso delle attività ispettive, l'Azienda ha dichiarato che "non è stato possibile stimare il numero approssimativo degli interessati coinvolti dalla violazione, in quanto ogni struttura aveva una cartella condivisa sul citato file server utilizzato sia per l'attività di gestione dei reparti ma anche per la conservazione di documenti sanitari. Per comprendere la natura e il contenuto di tali documenti (anche in relazione alla tipologia di dati trattati e di interessati coinvolti), che non erano indicizzati, sarebbe stata necessaria un'attività di analisi dei file puntuale e non automatizzabile. Inizialmente, infatti, era stato dato mandato alle singole strutture di operare in tal senso ma, a seguito della ingente mole di documentazione da esaminare e delle priorità individuate dalla Regione nel periodo post COVID di recupero delle liste di attesa, tale attività è stata interrotta. La parte ha precisato che è verosimile che tra gli interessati ci siano anche minori" (v. verbale del XX, pagg. XX e XX).

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 "tramite lo strumento della formazione in particolare dal XX è stato attivato un corso di cyber awareness per aumentare l'uso consapevole degli strumenti tra cui la condivisione di documenti e dati sensibili XX o file sharing. Nel XX la direzione generale ha inviato una nota con l'obbligo di rispettare le regole di corretto storage e condivisione di file su file server dopo aver riscontrato comportamenti gravemente anomali nell'uso dell'ambiente di file sharing" (v. notifica del XX, sez. XX, punto XX).

3.2. Attività ispettive

Durante le attività ispettive, l'Azienda ha dichiarato che "è dotata di un Regolamento di utilizzo dell'infrastruttura ICT adottato nel 2021 e aggiornato nel 2022 nel quale, fra le altre, erano individuate istruzioni e indicazioni con riguardo alle password policy e al corretto utilizzo del file server. In data 3 aprile 2023 è stata, inoltre, trasmesso XX il "Decalogo Cybersecurity" pubblicato sulla intranet aziendale; (inoltre era stata inviata una) nota (…) XX a tutto il personale nel

settembre 2022, che richiamava parte di quelle indicazioni con particolare riferimento al corretto utilizzo del file server"; che "ha un sistema di gestione della qualità certificato ISO 9001, tramite il quale vengono rilevate anche le eventuali criticità in ambito privacy grazie al processo di customer satisfaction e audit interni. Al riguardo sono stati appositamente formati auditor interni e il modello di audit del sistema di gestione della qualità viene tenuto in conto dal team DPO" e che "la configurazione delle postazioni di lavoro (PdL) al momento dell'incidente prevedeva per il 70% il sistema operativo XX e per il restante 30% il sistema operativo XX. Successivamente alla violazione, tramite il piano di acquisto di nuove PdL in convenzione CONSIP, sono state progressivamente sostituite tutte le postazioni. Il software antivirus utilizzato per le PdL e i server (XX) non aveva configurazioni differenziate per i diversi sistemi operativi e consentiva una profilazione dei livelli di protezione (più o meno elevati). Il livello di protezione previsto era più basso sulle macchine XX e, in particolari casi, su alcune macchine XX, in considerazione del potenziale impatto negativo sull'operatività della macchina e delle relative prestazioni anche dovuto alle risorse hardware presenti (…) i servizi di sicurezza perimetrale connessi alla gestione del medesimo Firewall erano garantiti nell'ambito dell'accordo quadro CONSIP SPC 2 ; non erano adottate misure di sicurezza per proteggere e limitare l'accesso all'area di memoria utilizzata dal processo lsass.exe (Local Security Authority Subsystem Service - LSASS) quali attività di hardening sul sistema operativo (es. corretta configurazione della relativa chiave di registro. (…) erano utilizzati server Hitachi, acquisiti mediante affidamento diretto con gestione e manutenzione da parte di risorse esterne. Successivamente è stato attivato un progetto di aggiornamento tecnologico del data center e dei backup, collaudato a marzo 2023 (…)"; che "al momento della violazione dei dati personali, era in corso l'aggiudicazione della gara per la realizzazione del predetto progetto" (v. verbali del XX pag. XX e del XX pagg. XX e 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, l'Azienda, nel corso delle attività ispettive, ha dichiarato che:

- "non era prevista una procedura di autenticazione informatica a più fattori (MFA) per l'accesso remoto in VPN, utilizzato prima della pandemia esclusivamente dai fornitori e, successivamente, anche dai dipendenti per la "remotizzazione" delle PdL, previa acquisizione dell'elenco del personale da autorizzare. Le utenze di "manutenzione" erano spesso generiche, non individuali, con massimi privilegi amministrativi. A valle dell'incidente si è proceduto: ad attivare la MFA, a certificare la VPN e a individuare utenze nominali (mediante modulistica apposita), nel rispetto del principio del "minimo privilegio"";

- "nonostante fossero state fornite indicazioni al personale circa la scelta della password, ispirate alle buone pratiche di settore, non era prevista alcuna configurazione dei sistemi che recepisse tali indicazioni. Gli utenti che svolgevano le funzioni di amministratore utilizzavano utenze differenziate, a seconda che si trattasse di utenza personale di dominio o utenza con privilegi amministrativi. In tale ultimo caso le credenziali, che non avevano una specifica password policy, erano tendenzialmente condivise fra i diversi amministratori" (v. verbale del XX, pag. XX).

Nel corso delle attività ispettive, in riferimento alle misure di sicurezza, in essere al momento della violazione dei dati personali, relative alla segmentazione delle reti, l'Azienda ha dichiarato che "la rete era sostanzialmente flat, non vi era una segmentazione logica o fisica e l'infrastruttura di rete era gestita da personale esterno nell'ambito dei servizi acquisiti tramite il citato accordo quadro; da dicembre 2022, l'Azienda ha acquisito una risorsa interna come sistemista senior proprio per governare le attività di progettazione e revisione della rete. Al momento è prevista la segmentazione per le nuove installazioni ed è in corso l'adeguamento dell'infrastruttura esistente e degli oltre 6000 dispositivi collegati. A livello organizzativo si è proceduto, altresì, a partire da luglio 2023, all'accorpamento dell'unità di ingegneria clinica nella nuova unità organizzativa complessa "ICT e Innovazione Tecnologica" per una gestione integrata e più efficiente degli

applicativi e dispositivi elettromedicali" (v. verbale del XX, pag. 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 dei dati personali in caso di incidente, l'Azienda ha dichiarato che "l'infrastruttura dedicata al backup effettuava uno screenshot periodico (tipicamente settimanale) delle macchine virtuali senza una politica di retention" (v. verbale del XX, pag. XX).

Circa gli 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 "a valle di un assessment effettuato nei primi mesi del 2022 […] si è rilevata la necessità di dotarsi di: un sistema di asset management; un SIEM, unitamente a un servizio SOC h24 con componente SOAR (orchestrazione di alert e correlazione eventi); certificati SSL per i domini registrati a nome dell'Azienda e nuovi firewall" (v. verbale del XX, pag. XX).

Dalla documentazione acquisita durante l'attività si evince che al momento dell'attacco erano presenti numerose vulnerabilità a livello di rete ("non esiste una segmentazione a livello tre del traffico di rete. (…) Non (sono differenziate a livello di rete) postazion(i) di lavoro (e) server. (…) Molti (utenti) avevano i massimi diritti di amministrazione. Il database (…) è un XX che presenta molte falle di sicurezza. (…) Possono essere attuate tecniche di escalation. Sono attivi ancora vari protocolli di comunicazione obsoleti. (…) Le utenze delle VPN erano collegate al dominio e quelle delle ditte erano anche amministratori di dominio") (v. allegato 1 al verbale del XX, pagg. XX e XX).

Per quanto riguarda le modalità con le quali gli incidenti di sicurezza sono portati a conoscenza dei soggetti a vario titolo coinvolti e il processo di gestione degli incidenti di sicurezza nel caso in cui questi comportino una violazione dei dati personali, l'Azienda ha precisato che "al momento della violazione dei dati personali, esisteva una istruzione operativa allegata al Regolamento di utilizzo strumenti IT, (…) avente a oggetto l'incident management con focus principalmente sugli eventi segnalati dai sistemi di sicurezza perimetrale e rivolta principalmente al personale IT"; che "l'Azienda ha costituito mediante delibera (…) un gruppo privacy del quale fanno parte componenti di diverse strutture dell'Azienda, operativo al momento della violazione dei dati personali"; che "si è dotata di uno strumento software denominato "XX" per la gestione della protezione dei dati personali trattati dall'Azienda" e che "ha predisposto una procedura di data breach, inserita nel sistema qualità e resa nota a tutti i dipendenti XX e disponibile anche sulla intranet" (v. verbale del XX, pagg. XX e XX).

In ogni caso, è stato evidenziato che "da un anno e mezzo prima del XX, aldilà dell'evento emergenziale, il tema della sicurezza informatica era stato oggetto di una pianificazione che vedeva l'Azienda impegnata in una complessa opera di potenziamento dell'infrastruttura di sicurezza e di miglioramento della consapevolezza sui rischi legati agli attacchi cyber verso l'utenza. (…) Nel novembre 2021, tra i primi in Piemonte, l'Azienda aveva condotto anche una survey, basata su 110 domande attinenti a 9 domini e 35 aree di controllo, per quantificare il livello di esposizione al rischio delle principali aree di settore e di confrontarle con dei benchmark di settore. L'analisi ha poi anche suggerito, in base anche all'esperienza in materia di cybersecurity, le aziende con livelli di rischio simili e le linee di indirizzo per la pianificazione degli investimenti". "Da gennaio 2022, partendo dall'analisi del livello di adeguatezza allo standard dei livelli minimi delle linee guida AgID n.2/2017, abbiamo identificato già nel primo trimestre 2022 l'elenco delle remediation per arrivare al livello di pieno rispetto almeno del set minimo e del 95% del set standard entro il 2023. Tale pianificazione era poi confluita nel documento "P 02_Piano di adeguamento misure minime AgID" di giugno 2022, procedura di settore dell'Area ICT facente parte del corpus documentale del Sistema di Gestione della Qualità" (v. allegato 1 al verbale del XX, pagg. XX e 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 "a livello preventivo (sono state) ulteriormente ristrett(e) (…) le regole di accesso alla rete internet tramite il firewall", si è limitato "l'accesso in qualità di amministratore ad utenze esterne alla rete aziendale (tipicamente i manutentori dei fornitori di applicativi)", è stata "avviata analisi congiunta con il fornitore dell'antivirus e con il partner gestore della rete e relativi apparati attivi per verificare potenziali vulnerabilità di loro competenza o azioni contenitive" e, successivamente, che "le contromisure operative realizzate dopo l'attacco sono state le seguenti: sistema di autenticazione a due fattori su ogni servizio accessibile dall'esterno con particolare riferimento a VPN, Posta elettronica, cloud server antivirus e cloud clients antivirus. Gestione dominio tramite XX (in particolare sono stati rivisti e quindi ridotti considerevolmente gli utenti amministratori calibrando l'accesso in funzione delle attività che gli utenti devono svolgere) Gestione firewall Comunicazioni e segnalazioni agli enti preposti (Polizia postale, ACN, immediata comunicazione alla direzione generale e agli operatori interessati con un decalogo operativo delle azioni da porre in essere)" (v. notifiche del XX e XX, sez. XX, punto XX).

4.2. Attività ispettive

Nel corso delle attività ispettive, l'Azienda ha dichiarato che "a seguito della segnalazione della presenza della ransom note da parte del servizio IT, è stato contattato il RPD e la direzione generale mediante una mail contenente informazioni circa il tipo violazione subita, il contenuto della ransom note (richiesta di riscatto dei dati pubblicati). In seguito è stata fatta la segnalazione tramite il servizio dedicato dello CSIRT (ACN) ed è stata sporta denuncia alla polizia postale. Sono state anche inviate diverse comunicazioni sia fra i direttori delle strutture coinvolte sia a tutto il personale. (…) A seguire è stata effettuata un'ulteriore fase di approfondimento (…); è stato verificato che l'attaccante non persisteva nella rete rimanendo collegato passivamente, la backdoor, infatti, è stata smantellata e non sono state rilevate ulteriori evidenze di persistenza"; che i "livelli di protezione (delle postazioni di lavoro) sono stati progressivamente innalzati" e che "è stato consolidato il backup dei dati e dei sistemi (caselle di posta, file server, gestionali, etc..) con strategia di tipo [OMISSIS]" (v. verbale del XX, pag. XX).

Per quanto concerne il file server coinvolto nella violazione dei dati personali l'Azienda ha dichiarato che "è in fase avanzata di dismissione ed è attualmente accessibile in sola lettura. Tale server è stato sostituito da una nuova infrastruttura di file sharing, con permessi e autorizzazioni correlati a ciascuna struttura di riferimento che dispone di cartella denominata con il codice del relativo centro responsabilità. Su tale cartella il direttore della struttura ha tutti i permessi (es. lettura, scrittura, condivisione, etc..) e gestisce le autorizzazioni dei propri collaboratori. In aggiunta a tale ambiente è disponibile lo strumento di file sharing in XX, XX" (v. verbale del XX, pagg. XX e XX).

Per quanto concerne le misure tecniche e organizzative l'Azienda ha, inoltre, rappresentato che "il piano di potenziamento strutturale dei servizi informatici ha avuto origine a seguito dell'assessment effettuato all'inizio del 2022 (…) in cui erano indicate le principali misure da adottare, al fine di mitigare le criticità rilevate, indicando le ipotesi di termine delle attività (fine 2022) utili anche al fine di ripartire gli investimenti economici necessari. A valle dell'attacco sono state riviste le priorità del piano, con particolare riferimento a: revisione delle autorizzazioni delle utenze, riorganizzazione dell'XX aziendale (creati nuovi domain controller, riduzione del numero di utenti appartenenti al gruppo admin ristretto solo ai sistemisti, revisione delle policy), piano di segmentazione della rete sia logica (VLAN) che fisica delle diverse strutture, acquisto di un

bilanciatore XX per la gestione del traffico in entrata e uscita, gestione dei carichi e per realizzare la VPN con MFA. Nel 2023, grazie ai fondi del PNRR: sono stati attivati il servizio SIEM e SOC, è stato acquisito un WAF, si è proceduto all'aggiornamento tecnologico degli apparati e dell'infrastruttura del centralino VOIP XX, è stata aggiornata la piattaforma antivirus (modulo XDR per endpoint e server), è stato avviato un progetto di supporto metodologico alla struttura di ingegneria clinica per l'analisi della postura di sicurezza dei dispositivi elettromedicali connessi e la gestione del ciclo di vita dei dispositivi, al fine del rispetto dei requisiti di sicurezza nelle varie fasi (es. acquisto, installazione, manutenzione); è stato, inoltre, acquisito un sistema di asset management XX". E' stato, inoltre, dichiarato che è stato "attivato un percorso di formazione in e-learning sui temi della cyber awareness per tutti gli operatori, in più moduli con test finale di apprendimento, che ha visto, al momento, la partecipazione attiva di circa il 45% del personale. Per rendere pienamente efficace tale misura la predetta attività di formazione è stata inserita negli obiettivi aziendali 2024. Inoltre, l'Azienda ha aderito alla piattaforma di formazione "Syllabus", messa a disposizione dal Dipartimento Funzione Pubblica della Presidenza del Consiglio dei Ministri", "che sono state fornite istruzioni operative interne per il corretto reset delle password e, a breve, sarà disponibile un portale per effettuare in automatico il reset delle password nel rispetto delle regole stabilite nella password policy" fornendo il documento "Misure per la Cybersecurity AOU AL – Milestone dei principali interventi circa le azioni di mitigazione dei rischi connessi alle vulnerabilità sulla sicurezza informatica dell'Azienda" (v. verbale del XX, pagg. XX e XX).

Infine, con riguardo al piano strategico, l'Azienda "ha chiarito che l'attuale direzione ha cominciato a operare a fine 2021, in piena pandemia. Tale piano strategico (..) è il risultato dell'integrazione del precedente piano con due nuove direttrici: "ritorno alla normalità" e "digitalizzazione, cybersicurezza e privacy". Da aprile 2022 l'ing. (…) ha assunto la responsabilità della struttura IT, sono state acquisite figure professionali apicali esperte ed è stato potenziato e riorganizzato il servizio privacy. È stato, altresì, creato un gruppo trasversale (IT, DPO, responsabile qualità) coordinato dalla direzione amministrativa" (v. verbale del XX, pag. XX).

5. 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. 0059959 del 17 maggio 2024, l'Autorità ha ritenuto che l'Azienda fosse incorsa nella violazione del principio di "integrità e riservatezza", di cui all'art. 5, par. 1, lett. f), del Regolamento nonché degli obblighi in materia di sicurezza del trattamento (art. 32 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, corredata da corposa documentazione, ha precisato quanto espresso nelle notifiche di violazioni e nel corso l'attività ispettiva, dichiarando che:

- in relazione alla mancata adozione di misure adeguate a rilevare tempestivamente la violazione dei dati personali, "pur non disponendo ancora all'epoca degli eventi di un SIEM (security information and event management) integrato e di un servizio di SOC (Security Operations Center) per il monitoraggio h24 degli allarmi, l'Azienda era dotata di un servizio di monitoraggio dei log dei firewall aziendali, nell'ambito dell'adesione all'Accordo Quadro CONSIP SPC Cloud lotto 2, ad oggetto: "Servizi di Cloud Computing, di sicurezza, di realizzazione di portali e servizi

on-line e di cooperazione applicativa per le pubbliche amministrazioni – ID SIGEF 1403", aggiudicato al R.T.I composto da XX (mandataria) e IBM SpA - SISTEMI INFORMATIVI S.r.l. - XX Spa (mandanti), approvata con Delibera nr. 857 del 13/09/2017, poi rinnovata con Determinazione dirigenziale n. 2032 del 29/12/2021 fino a tutto il 2023" (…). In particolare, il servizio in oggetto prevedeva, tramite l'utilizzo della soluzione "XX" e di servizi di XX" (erogati da XX in subappalto nell'ambito della fornitura in oggetto nella quale aggiudicataria era XX), garantiva le caratteristiche necessarie per identificare le minacce portate al network aziendale e le attività di analisi della rete di pari passo con i cambiamenti del network o dell'Azienda in generale. Inoltre, dai primi giorni di XX, circa tre settimane prima della notifica di attacco, era stata installata la soluzione XX, una piattaforma centralizzata per l'aggregazione e l'analisi dei dati telemetrici in tempo reale per il rilevamento e la conformità delle minacce. XX ha raccolto dati sugli eventi dai firewall e da alcune delle macchine del Data Center aziendale coadiuvando la ricognizione eseguita grazie al supporto del team di ACN a valle della segnalazione dell'attacco per ricostruire i movimenti laterali degli attaccanti. A valle dell'attacco è stato poi implementato l'investimento per l'installazione del SIEM (Security information and event management), un sistema di gestione delle informazioni e degli eventi sulla sicurezza che, analizzando i log relativi ai dispositivi connessi all'infrastruttura di rete, consente la gestione e l'elaborazione di contromisure operative a potenziali minacce e vulnerabilità. L'investimento è stato già a suo tempo pianificato in sede di programmazione aziendale nell'ambito degli interventi finanziabili con la misura 1.1.1 Digitalizzazione DEA, Missione 6 del PNRR";

- in relazione alla mancata adozione di misure adeguate a garantire la sicurezza delle reti, "al momento dell'attacco la rete aziendale (era) strutturata su un'unica VLAN nativa, utilizzata anche per il traffico dati client e/o server. Consapevole della criticità che tale configurazione rappresentasse, l'Azienda Ospedaliera, nell'ambito dello sviluppo del piano strategico 21 – 24 – area strategica cybersicurezza (…), ha avviato una procedura di mobilità nel marzo 2022 (…) con specifiche competenze sistemistiche di cybersecurity, per coordinare i servizi di assistenza e manutenzione della rete aziendale e delle sue componenti di sicurezza perimetrale. Tale ruolo in Azienda risultava non più coperto dal 17/06/2020," (…) e la definitiva assunzione del candidato risultato più idoneo per esperienza e competenza sia stata possibile solo a far data dal XX, praticamente meno di un mese prima della notifica dell'attacco subito. Occorre sottolineare che, immediatamente dopo l'attacco, e proprio grazie anche alla competenza progettuale della figura di sistemista senior finalmente integrata nella pianta organica della Area ICT, è stato predisposto un piano di remediation basato sui seguenti tre pilastri concettuali:

• segmentazione a livello capillare, con una rete logica per ogni armadio di piano, una VLAN per i dispostivi elettromedicali differenziata per specialità d'uso (una per i biomedicali di radiologia, una per i medicali di laboratorio, una per le workstation di radiologia, una per i medicali generici) e VLAN dedicate per servizi che in qualche modo potessero mettere a rischio la sicurezza aziendale attraverso uscite dirette su internet, tipicamente per servizi di assistenza da remoto o per implementare monitoraggi su piattaforme in cloud.

• Messa in sicurezza della comunicazione tra una VLAN e l'altra, attraverso adeguati filtri ACL (Access Control List) per limitare il traffico. L'infrastruttura aziendale permette di usare un'ACL uguale ad ogni VLAN in modo da aumentare le performance. Importantissimo è stato vietare il traffico RDP (Remote Desktop Protocol) verso i server centrali, ad esclusione di quelli autorizzati (ad esempio i terminal server).

• Implementazione di un sistema di gestione automatica delle VLAN, attraverso l'implementazione, [OMISSIS], in modo da autorizzare all'accesso alla rete aziendale solo macchine autorizzate. Con questo meccanismo è possibile isolare quelle non autorizzate e attivare politiche di blocco verso quelle porte di rete risultate compromesse da un MAC address non autorizzato";

- “tale pianificazione (…) è in fase di implementazione”;

- in relazione alla procedura di autenticazione informatica, “la proliferazione del numero di VPN abilitate nel biennio di gestione della pandemia da COVID-19 (attivazione postazioni in smart working), ha sicuramente peggiorato la postura di sicurezza dell’infrastruttura di rete. Ciò detto, è indubbio che, al momento dell’attacco, le VPN attive non avessero l’autenticazione a due fattori. In ogni caso, preme evidenziare l’immediata responsività dell’infrastruttura subito dopo la notifica di attacco, implementando già entro la prima metà di gennaio il sistema MFA (Multi Factor Authentication), [OMISSIS]. Inoltre, è stata predisposta una pianificazione di riprogettazione delle VPN nella logica di:

• creare un vero e proprio LDAP server separato ed implementando ACL per ogni utente/ditta, in modo che l’accesso sia governato dal principio Role Based Access.

• Implementare una serie di accessi tramite terminal server ai principali servizi applicativi web dell’ospedale, gestiti dal sistema bilanciatore;

• Avviare attività formative e informative all’utenza, in modo da rendere sensibili gli utenti sulla rilevanza che non tutti i servizi erogati in rete locale possano essere raggiungibili al di fuori della rete aziendale”;

- in relazione all’obsolescenza dei software di base installati su alcuni sistemi di trattamento, “sebbene l’aggiornamento della patch relativo alla CVE indicata nella relazione allegata a seguito della notifica di data breach sia poi avvenuto a seguito dell’attacco stesso, ad oggi non ci sono evidenze che la vulnerabilità riscontrata sul firewall sia stata la causa diretta di infiltrazione nella rete aziendale. Anzi, è molto più probabile che non ci sia un’unica causa diretta, ma che sia stato il combinato disposto delle concause già esplicitate nella succitata relazione a determinare la vulnerabilità. Nonostante questo, consapevole dell’importanza di acquisire un sistema di inventory & asset management che consentisse la gestione degli aggiornamenti e delle vulnerabilità del parco installato, l’Azienda, con ordine sulla piattaforma MEPA (Mercato Elettronico per la Pubblica Amministrazione) di settembre 2022 (quindi pochi mesi prima dell’attacco), aveva avviato l’iter di acquisizione e successiva installazione di una piattaforma per la discovery di tutti dispositivi collegati alla rete, la valutazione dell’indice CVSS rischio della vulnerabilità e la gestione delle CVE collegate a ciascuno degli asset stessi, OMISSIS”;

- “l’attuale direzione strategica, insediatasi in AO AL nel giugno 2021 in un contesto peraltro ancora caratterizzato dall’eccezionalità legata all’emergenza pandemica, ha fortemente voluto un deciso cambio di passo sul fronte digitalizzazione e cyber sicurezza. Ciò emerge innanzitutto dalla revisione del Piano Strategico (delibera n° 196 del 29/04/2022 – approvazione PIAO), con la quale si è voluto dare da un lato un segnale di sostanziale continuità rispetto al precedente piano, dall’altro un segnale di forte discontinuità su due aspetti ritenuti fondamentali: 1. Digitalizzazione e competenze, ed un forte impulso alla cybersicurezza ed alla privacy (Area strategia 1 - “C - Competenze e digitalizzazione”); 2. azioni propedeutiche all’uscita dalla pandemia e ad un ritorno alla “normalità” (Area strategica 2 - “O - Ordine dopo la tempesta”). All’interno delle due aree strategiche implementate è la digitalizzazione quella su cui l’azienda ha deciso di impostare una strategia prioritaria, e delle principali direttrici la “Cybersicurezza, trasparenza e privacy” assume rilevanza pregnante”;

- in relazione alle principali azioni intraprese e all’organizzazione e dotazione in Area ICT, “nel corso del 2022 e con maggiore compiutezza nel corso proprio del 2023, l’AO-AL ha consolidato sia le componenti tecnologiche delle proprie infrastrutture di rete (sia dati che fonia), che le competenze del personale afferente. Una delle prime azioni avviate ad inizio 2022 ha riguardato la profonda riorganizzazione dell’area ICT. Partendo dal cambio al vertice della struttura (…) la

struttura è stata rafforzata, con l'assunzione di un'ulteriore dirigente analista e con l'assunzione di un Collaboratore Tecnico cat. D esperto di reti e cybersicurezza. Con il nuovo atto, la S.C. "Area ICT" ha acquisito anche la responsabilità della SS Ingegneria clinica, modificando il nome in S.C. "ICT e Innovazione tecnologica" e creando così i presupposti per una completa integrazione tra due mondi ormai interconnessi ed integrati sul digitale. È stato inoltre individuato l'incarico professionale di "Gestione infrastruttura ICT e cybersicurezza" ed affidato, da gennaio 2023, a dirigente della struttura ICT l'incarico di "Gestione e ottimizzazione delle installazione software aziendali";

- in relazione alle principali azioni intraprese e all'organizzazione e dotazione in Area Privacy, "con delibera n° 420 del 27/07/2021 è stato istituito il "Gruppo di lavoro aziendale privacy" con specifici compiti espressamente indicati e "con la revisione dell'atto aziendale è stato creato il nuovo Servizio Privacy, in staff alla Direzione strategica" che si occupa di specifici determinati aspetti;

- "è stata avviata una collaborazione con CSI Piemonte (società in house della Regione Piemonte di cui l'AOU è socia) per "attività di supporto in ambito GDPR" (….) nell'applicazione del principio di "Accountability" previsto dal REGOLAMENTO (UE) 2016/679", rispetto a specifiche esigenze espresse;

- in relazione alla natura, gravità e durata della violazione "il sistema violato è quello delle cartelle condivise in ambiente XX della rete di PdL (Postazioni di lavoro) dell'Azienda Ospedaliera. Le cartelle condivise costituiscono un sistema aziendale in cui è possibile memorizzare, da parte dei dipendenti, documenti, fogli di calcolo, presentazioni, e più in generale qualsiasi file utile all'organizzazione del lavoro. Teoricamente all'interno di detto sistema dovrebbero esserci solo documenti per finalità di produttività individuale (quindi file per l'organizzazione dei reparti, documentazione di lavoro, ma non attinente alle attività sui pazienti), mentre i dati sanitari relativi ai percorsi clinici dei pazienti dovrebbero essere gestiti solo attraverso gli applicativi aziendali che generano le cartelle cliniche elettroniche. In pratica però, in esso erano presenti anche dati sanitari (es copie referti, di esami, ecc.), sebbene occorra precisare che si trattasse di file non indicizzati, considerabili più delle "copie di lavoro" che degli elementi di gestione dei trattamenti";

- "la questione si ricollega pertanto ad un utilizzo più consapevole da parte dell'utenza dei dipendenti ospedalieri dell'ambiente di File Sharing e delle infrastrutture IT in generale e dei rischi connessi in tema di mancato rispetto dei principi di protezione del trattamento dei dati sanitari e di sicurezza informatica. Si veda a tal riguardo la sezione relativa alle comunicazioni inviate con frequenza almeno mensile da parte della Direzione a tutto il personale medico circa il richiamo a utilizzare il file server per gli scopi suoi propri nel capitolo dedicato alle misure organizzative messe in atto a seguito della notifica di attacco. In ogni caso, i giorni trascorsi a seguito dell'attacco (a partire dal 2 gennaio 2023) sono stati spesi analizzando, con il supporto dell'Agenzia per la Cybersicurezza Nazionale (ACN), e il supporto di un SOC (Security Operations Center), immediatamente ingaggiato dal servizio I.C.T. dell'Azienda per un supporto sulle attività di analisi dei log e remediation, i movimenti degli attaccanti nei sistemi dell'infrastruttura di rete dell'Azienda, allo scopo di identificare la modalità di primo accesso";

- "quello all'AO AL si inserisce all'interno di un contesto nazionale ben descritto dall'autorevole rapporto CLUSIT 2024, in cui il settore sanitario nel 2023 è stato il quarto settore più colpito dagli attacchi informatici di successo e di pubblico dominio, dopo Manufacturing, Professional/Scientific/Technical e ICT, con una percentuale sul totale degli incidenti censiti del 9%. Tale percentuale è quadruplicata rispetto al periodo di analisi dello stesso rapporto dell'anno precedente, in cui il settore sanità costituiva il 2,2% degli attacchi subiti dalle infrastrutture informatiche di riferimento";

- "l'AOU (…) ha messo a disposizione tutti i propri canali casella di mail e numero verde per

gestire ogni possibile contatto con gli interessati dalla violazione di riservatezza. Ad oggi, non è pervenuta alcuna segnalazione, ricorso, reclamo o messa in mora. Da un punto di vista infrastrutturale, già a partire dal giorno XX, data in cui un team DFIR (Digital Forensic & Incident Response) dell'Agenzia per la Cybersicurezza Nazionale veniva distaccato presso l'Azienda Sanitaria Ospedaliera di Alessandria per fornire supporto tecnico nelle attività di analisi e ripristino dei servizi, e per i circa 30 giorni successivi, sono state introdotte, come immediate contromisure operative per attenuare gli effetti della violazione, le seguenti operazioni: • Blocco del traffico dati al di fuori dell'Italia; • autenticazione a due fattori su ogni servizio accessibile dall'esterno (tecnologia MFA – Multi Factor Authentication), con particolare riferimento agli accessi agli account di posta aziendale e di accesso alla rete aziendale dall'esterno tramite VPN (Virtual Private Network); • Attivazione dell'autenticazione a due fattori della console del sistema antivirus, sia lato endpoint che server, non attiva al momento dell'attacco; • Consolidamento del sistema XX aziendale, diminuendo drasticamente, innanzitutto, il numero di utenti nel gruppo domain admin, […] escludendo quindi anche gli utenti di servizio. Inoltre, è stata ripristinata la copia delle cartelle, è stato eliminato il preesistente domain controller e creati due nuovi domain controller su ambiente con sistema operativo aggiornato a XX di lettura e scrittura più due domain controller di sola lettura, inserendo i primi in nuova VLAN con i servizi DNS dedicati. È stata resettata due volte la password XX. Con l'applicativo XX sono state monitorate giornalmente le principali vulnerabilità e apportate le relative modifiche di sicurezza. Questa attività è stata eseguita in collaborazione con il supporto tecnico della squadra tecnica di ACN";

- in relazione alle misure tecniche e organizzative messe in atto ai sensi degli articoli 25 e 32 del Regolamento: prima dell'attacco, "aldilà dell'evento emergenziale, il tema della sicurezza informatica era stato oggetto di una pianificazione che vedeva l'Azienda impegnata in una complessa opera di potenziamento dell'infrastruttura di sicurezza e di miglioramento della consapevolezza sui rischi legati agli attacchi cyber verso l'utenza già nel periodo tra la fine del 2019 e l'inizio del 2022. Si riportano di seguito le principali attività da cui l'attenzione e gli sforzi di pianificazione risultano evidenti:

• Dicembre 2019: acquisizione, in una logica di refresh tecnologico della soluzione previgente, di una piattaforma di sicurezza per la protezione di Endpoint, Server e dispositivi mobili con funzionalità di Antimalware, Firewall, Intrusion Prevention System, Encryption ed Application Control. La soluzione identificata, i prodotti "XX è inserita da Gartner all'interno del celebre report denominato "Magic quadrant for endpoint protection platforms" nel riquadro riservato alle tecnologie "Leader", il quadrante in alto a destra (si veda a tale riguardo la Determinazione dirigenziale n. 518 del 30/03/2020 …);

• Luglio 2020: attivazione corso di formazione FAD "Corso GDPR - Regolamento UE 2016/679 – e sicurezza informatica", inserito nel Piano di formazione aziendale negli anni dal 2020 al 2024 con 4 crediti ECM. Il corso si configurava quale corso di base per tutti i dipendenti ed esterni disponibile in piattaforma ECM Piemonte;

• Luglio 2021 in conformità ed ai sensi dell'art. 36 del GDPR ha effettuato con XX una attività di "valutazione d'impatto sulla protezione dei dati" (…). La DPIA aveva il fine di supportare il titolare del trattamento nel definire strategie per la protezione dei dati analizzati (in particolare DSE, Trattamenti di dati relativi alla salute dei pazienti ed utenti dei servizi internistico ed Emergenza urgenza, Controllo di gestione). L'analisi ha evidenziato anche le misure di sicurezza e tecniche necessarie a mitigare il rischio che sono state inserite in un Piano di trattamento del rischio ed un action plan di breve periodo per assicurare la protezione dei dati personali relativamente ai trattamenti sottoposti a valutazione di impatto;

• Novembre 2021: partecipazione, nell'ambito di un'iniziativa regionale di analisi dei livelli di rischio informatico ai fini di profilazione assicurativa quale Azienda capofila, ad una valutazione promossa

dalla XX. L'attività di assessment è stata basata sulla compilazione del questionario [OMISSIS]. La valutazione del rischio cyber, pur nella sua parziale aleatorietà, essendosi basato unicamente sulla risposta ai quesiti del questionario e data la natura complessa della tematica, ha permesso in ogni caso di quantificare il livello di esposizione al rischio delle principali aree di settore e di confrontarle con dei benchmark di settore. Inoltre (…) l'Azienda ha ricevuto nella comunicazione di invio del report in questione, conferma che il percorso intrapreso risultasse essere un notevole cambio di marcia ed evidenziando che "molte delle attività consigliate all'interno del report XX sono in linea proprio con il percorso di mitigazione iniziato, denotando l'ottima consapevolezza e volontà di intervenire per migliorare la situazione";

• Dicembre 2021 - Gennaio 2022: attivazione di un percorso formativo, giunto ormai alla sua terza edizione nel 2024, di cyber awareness, ovvero utilizzo consapevole delle infrastrutture e strumenti IT per sviluppare nei dipendenti una chiara consapevolezza dei rischi cyber attraverso l'utilizzo avanzato dei sistemi multimediali e il reale coinvolgimento di tutti gli utenti;

• Gennaio 2022: avvio di una valutazione, conclusasi ad Agosto 2022, del livello di vulnerabilità ("Vulnerability Assessment"), in modo da poter pianificare poi le principali azioni correttive e di consolidamento. In particolare, lo studio ha permesso di identificare le vulnerabilità presenti sui sistemi target e di definire un piano di rientro, basato sulle criticità dei problemi di sicurezza identificati e quindi dando la corretta priorità alle attività di patching. Si veda a tale riguardo il documento "Vulnerability Assessment 2022" (…). Tale piano di rientro è stato poi integrato, nel giugno 2022, nella Procedura di settore dei servizi ICT, elaborando un documento, integrato poi nel Sistema di Gestione della Qualità del servizio stesso che allineava tali contromisure con l'adeguamento alle misure standard di sicurezza contenute nelle Linee Guida AgID come da Circolare del 18 aprile 2017, n. 2/2017. Il documento conteneva anche una pianificazione di massima delle attività di consolidamento e delle azioni correttive per il rientro delle anomalie rilevate entro il terzo trimestre 2024. Si veda a tale riguardo la procedura "P 02_Piano di adeguamento misure sicurezza AgID";

• Marzo 2022: (..) pianificazione degli investimenti PNRR Missione 6 componente 2, investimento 1.1.1, dove sono stati previsti (…), investimenti per acquisire know-how e tecnologie necessarie per potenziare la sicurezza infrastrutturale e applicativa dei sistemi ospedalieri" e "revisione della Procedura di Settore della SC Area ICT e contestuale diffusione alla popolazione di utenti aziendale. La comunicazione contiene anche un riepilogo sintetico, ma esaustivo delle best practice da adottare per una maggiore consapevolezza da parte degli utenti dipendenti dell'Azienda nell'uso delle credenziali e degli strumenti informatici in generale (…);

• Agosto – Ottobre 2022: integrazione nel corpus documentale del Sistema di Gestione della Qualità dell'Area ICT delle istruzioni operative, elaborate contestualmente al Vulnerability Assessment del Gennaio 2022, relative a: Change Management - IO_2 (…); Gestione delle Immagini Server e PdL – IO_3 (….); Security Incident Management - IO_4 (…); Vulnerability Management – IO_5 (…); Gestione delle comunicazioni da e verso il settore Area ICT – IO_6;

• Settembre 2022: invio di comunicazione da parte della Direzione Generale alla tenuta di norme comportamentali adeguate nell'utilizzo dell'ambiente di File Sharing aziendale, a seguito della notifica dalla SC Area ICT di attività illecite. Nella comunicazione si ricordava contestualmente il recente episodio di violazione occorso alla ASL Città di Torino, ribadendo l'importanza di comportamenti ortodossi per la salvaguarda della cybersecurity ospedaliera. Si veda la nota con numero di protocollo 19678 del 5-09-2022 (…), in cui si ribadisce che il sistema file server, oggetto dell'attacco, è "destinato a contenere solo files di lavoro, e non altri documenti quali documenti personali di pazienti (esami, referti in word, ecc.)";

• Settembre 2022: gap analysis per aderenza alla norma ISO/IEC 27001:2013. L'analisi è stata

finalizzata alla valutazione dello stato dei processi attualmente implementati presso l'Azienda Ospedaliera, (regolamentati dal Sistema di Gestione della Qualità a norma ISO 9001:2015) e delle prassi consolidate in uso tra il personale e valutazione del gap attualmente presente rispetto alla conformità degli stessi alla norma ISO/IEC 27001:2013, di possibile, futura implementazione. La conclusione del report evidenziava come, a seguito delle interviste effettuate, si potesse evincere che lo stato di implementazione dei processi risultasse abbastanza avanzato, soprattutto in riferimento alle attività quotidiane dell'Area ICT, che con buona probabilità "costituirà il cuore della futura certificazione a norma ISO/IEC 27001" (…);

- in relazione alle misure tecniche messe in atto a seguito della notifica di attacco, "a valle dell'analisi compiuta di concerto con il gruppo DFIR di ACN, (…), si riportano di seguito le principali azioni correttive implementate: 1. Sistema di autenticazione a due fattori su ogni servizio accessibile dall'esterno, con particolare riferimento a: VPN: 1. Le VPN aziendali sono basate su tecnologia XX. Non avevano l'autenticazione a due fattori. Essa è stata implementata sfruttando la tecnica dell'OTP (One Time Password) XX. Come mail è stata utilizzata quella personale dell'utente, o comunque non del dominio interessato e cioè XX. È stata avviata contestualmente, ed è tuttora in corso, la completa riprogettazione delle VPN, creando un vero e proprio LDAP server separato, implementando inoltre una ACL per ogni utente/ditta, in modo da realizzare pienamente un accesso di tipo Role Based Acces Control; posta elettronica: 1. La posta elettronica è basata su tecnologia XX. Tutta la parte di filtri ed antispam è gestita da XX. All'interno dell'ospedale vi è solo un server che fa il sync con XX. Viene replicato il dominio XX (come posta elettronica). Il connettore, obsoleto e mal funzionante, è stato rifatto su nuovo server e ultima release di XX; cloud server antivirus: poiché una delle vulnerabilità più rilevanti che hanno permesso il lancio dell'eseguibile per diffondere la ransom note sui pc aziendali è stata eliminata la possibilità di accedere alla console dell'antivirus aziendale, tramite utenza di amministratore, è stata richiesta al fornitore la MFA ora inserita. Anche in questo caso, gli account sono basati su mail XX in modo da evitare il single point of failure; cloud client antivirus; 2. Gestione dominio tramite XX: Utilizzo di tool specifici con il supporto di ACN per l'analisi dell'XX (XX, XX) e per il monitoraggio degli indicatori di rischio di dominio (XX; sono stati ridotti considerevolmente gli utenti amministratori, come da best practice per l'uso di XX, calibrando quindi l'accesso in funzione delle attività che gli utenti devono svolgere (secondo l'approccio ROLE BASED ACCESS CONTROL); divisione dei ruoli di amministrazione, postazioni di lavoro, dominio, server centralizzati, server ditte esterne; 3. Gestione firewall: chiusi tutti gli accessi diretti ad internet ritenuti non indispensabili; aggiornamento delle vulnerabilità; filtro sul traffico al di fuori dell'Italia; potenziamento dell'attività di raccolta e analisi dei log; 4. gestione utenze: sviluppato internamente un portale, per la gestione in autonomia da parte dei dipendenti del reset della password di dominio (per accedere ai PC e alla posta), disponibile ad un link internet https. Il collegamento a questa pagina è reso anche disponibile sulla Intranet, e offre agli utenti la possibilità di modificare o reimpostare la password, senza coinvolgimento dell'amministratore o dell'help desk, impostando inoltre domanda e risposta segreta e-mail secondaria di recupero password in caso di smarrimento. È inoltre funzionale a mantenere aggiornata le anagrafiche dipendenti riducendo quindi il rischio legato ad accessi con utenze non più in uso";

- in relazione alla vulnerabilità riscontrata a valle dell'attacco, avente ad oggetto la "mancanza di una segmentazione a livello tre del traffico di rete, compresa anche la differenziazione tra una postazione di lavoro ed un server", l'azione risolutiva è stata: "da subito dopo l'attacco sono state implementate nuove VLAN con annesse ACL per la sicurezza. La bonifica delle vecchie VLAN è in corso di completamento XX";

- in relazione alla vulnerabilità riscontrata a valle dell'attacco, avente ad oggetto la "gestione dei livelli di accesso delle utenze non in linea con il principio del privilegio minimo (principle of least privilege), dato che circa 130 utenti avevano i massimi diritti di amministrazione", l'azione risolutiva è stata: "gli amministratori di dominio si sono ridotti a quattro, che corrispondono ai sistemisti

dell’infrastruttura”;

- in relazione alla vulnerabilità riscontrata a valle dell’attacco, avente ad oggetto la “mancanza di sistema di Asset e Inventory management per la gestione e identificazione delle macchine, anche off-line”, l’azione risolutiva è stata “durante l’attacco sono stati adoperati XX. Attualmente, l’Azienda adopera la soluzione XX”;

- in relazione alla vulnerabilità riscontrata a valle dell’attacco, avente ad oggetto la “mancanza di procedure organizzative per l’inserimento delle macchine in rete o di una modulistica per la gestione delle richieste di VPN sottostanti e regole di identificazione”, l’azione risolutiva è stata: “rivisto regolamento Postazioni di lavoro e creata modulistica ed iter per la conservazione della modulistica e delle richieste”;

- in relazione alla vulnerabilità riscontrata a valle dell’attacco, avente ad oggetto la “mancanza di un collegamento procedurale tra il database dell’applicativo che gestisce l’anagrafica dei dipendenti e l’assegnazione degli strumenti di lavoro aziendali in maniera proporzionale agli inquadramenti contrattuali, e quindi ai livelli di responsabilità previsti per ogni profilo”, è stato “creato portale che collega l'anagrafica del personale agli account di rete. Fornisce privilegi e licenze in base alla mansione”;

- in relazione alla vulnerabilità riscontrata a valle dell’attacco, avente ad oggetto la “mancanza di un sistema centralizzato per la gestione delle utenze e di conseguenza per la gestione delle password”, è stato “creato portale che collega l'anagrafica del personale agli account di rete. Fornisce privilegi e licenze in base alla mansione”;

- in relazione alla vulnerabilità riscontrata a valle dell’attacco, avente ad oggetto l’“organizzazione del sistema di gestione delle identità XX non ottimale, con l’inserimento di molti degli utenti delle anagrafiche dipendenti all’interno di più gruppi con vari privilegi di accesso, con la possibilità dio attuazione di tecniche di escalation”, è stato “rivisto il sistema dei gruppi e delle annesse autorizzazioni con il supporto dell'applicativo XX”;

- in relazione alla vulnerabilità riscontrata a valle dell’attacco, consistente nel fatto che erano “ancora attivi protocolli di comunicazione obsoleti, tra cui l’smbv1 e NTLMv1”, è stato “eliminato il 90% dei server con protocolli smbv1 ed avviati iter ai fornitori per la bonifica del resto”;

- in relazione alla vulnerabilità riscontrata a valle dell’attacco, consistente nel fatto che “per la gestione delle attività di assistenza e manutenzione di molti applicativi, erano configurati utenti di servizio con privilegi di amministratore, determinando l’impossibilità di ridurre il livello di privilegi degli stessi, pena l’interruzione di disponibilità dei servizi correlati” e che “molte utenze per l’accesso alle VPN concesse alle aziende erogatrici di servizi di assistenza degli applicativi erano collegate al dominio e/o anche amministratori di dominio” è stata “creata doppia autenticazione vpn ed XX” e “bonificati amministratori di dominio”;

- “in merito agli investimenti strutturali, aldilà delle contromisure operative per contenere le esposizioni riscontrate a valle dell’attacco, l’AOU di Alessandria ha avviato investimenti finalizzati all’attivazione di servizi di controllo e all’acquisizione di sistemi di sicurezza perimetrale” (…) che hanno interessato numerosissimi profili;

- in relazione alle misure organizzative messe in atto a seguito della notifica di attacco, “innanzitutto, è stata avviata una serie di comunicazioni sia interne che segnalazioni agli enti preposti come di seguito specificato: • immediata segnalazione alla Polizia Postale e alla ACN; • segnalazione preliminare del data breach all’Autorità Garante entro le 72 ore come da Regolamento; • immediata comunicazione alla Direzione Generale e da questa agli operatori

sanitari interessati con un decalogo operativo delle azioni da porre immediatamente in atto per contrastare il rischio. A questo riguardo si segnalano le comunicazioni inviate XX aziendale riguardanti: 1. l'invito a tutti i dipendenti a riavviare i PC aziendali e seguire le indicazioni per la generazione di una nuova password di accesso secondo le buone prassi ribadite anche nel regolamento aziendale. Si veda a tale proposito la mail del XX del Direttore di Struttura Area I.C.T. (…); 2. contatto con il referente tecnico della ditta dalla cui utenza generica per le attività di assistenza sull'applicativo di ematologia installato presso i server della AOU di Alessandria è risultato il movimento di accesso degli attaccanti, come evidenziato dalla relazione prodotta dal team di ACN. Si veda a tale proposito la mail del XX del Direttore di Struttura Area I.C.T. (…); 3. Comunicazione a tutto il personale dipendente della Direzione Generale contenente disposizioni in materia di sicurezza informatica (…); 4. comunicazione a tutti i dipendenti di aggiornamento delle attività di ripristino e consolidamento in corso a valle dell'attacco (…); 5. revisione del regolamento aziendale, formalmente approvato con Deliberazione del Direttore Generale n. 150 del XX sull'utilizzo corretto dell'infrastruttura I.C.T. della AOU di Alessandria e relativa informativa a tutti i dipendenti (…); 6. creazione della nuova infrastruttura di File sharing aziendale e nuove disposizioni sul suo utilizzo con informativa a tutti i dipendenti (…); 7. ulteriore condivisione del nuovo regolamento aziendale e sollecito all'attivazione delle utenze per il nuovo sistema di File Sharing aziendale all'utenza dell'ospedale (…); 8. Comunicazione a tutto il personale dipendente della Direzione Generale contenente disposizioni in materia di sicurezza informatica (…); 9. ulteriore sollecito all'attivazione delle utenze per il nuovo sistema di File Sharing aziendale all'utenza dell'ospedale (…); 10. Comunicazione a tutto il personale dipendente della Direzione Generale contenente solleciti ad adempiere alle disposizioni in materia di sicurezza informatica (…); 11. Attivata funzionalità "blocca" di XX e inviata informativa all'utenza dell'ospedale (…); 12. Segnalazione altri attacchi di phishing (…); 13. Attivata massiccia campagna comunicativa rivolata al personale dipendente in materia "cyber sicurezza";

- "in merito alle misure organizzative e procedurali: è stato adeguato il regolamento aziendale recante disposizioni per un utilizzo sicuro dell'infrastruttura ICT dell'Azienda, (…) "Approvazione regolamento aziendale 2023 utilizzo servizi ICT". Tale revisione introduce i nuovi criteri per la profilazione delle utenze aziendali secondo il principio del minor privilegio possibile, aggiorna la modulistica di richiesta di utenze, definisce le nuove regole di accesso al nuovo sistema di File Sharing e di posta aziendale, esemplifica le modalità di accesso alla VPN con tecnologia di autenticazione MFA (Multi Factor Authentication). Ribadisce inoltre un utilizzo consapevole delle password di accesso e la loro costante revisione secondo le buone prassi di generazione per evitare che siano banali e facilmente identificabili";

- "sono state predisposte adeguate istruzioni operative e linee guida per la Gestione integrata degli aggiornamenti dei dispositivi elettromedicali e per il controllo periodico delle vulnerabilità dalla piattaforma di MDSP di recente acquisizione";

- "sono stati predisposti allegati contrattuali per le attuali e future iniziative di approvvigionamento di applicativi e dispositivi elettromedicali da connettere alla rete in modo tale da gestire, già in fase di redazione del capitolato di gara o di definizione dell'Ordine di Acquisto, elementi informativi quali i requisiti del processo di sicurezza, la determinazione iniziale del rischio del dispositivo, lo schema comunicativo";

- "durante l'attività ispettiva (…), si è provveduto ad argomentare e reperire una serie corposa di supporti documentali per una ricostruzione precisa e puntuale dell'evento del XX, seguendo minutamente le richieste collaborative dei funzionari e recependo le loro indicazioni per confermare o implementare tutti gli step necessari alla complessiva e completa valutazione ponderata delle attività messe in campo per risolvere le problematiche sottese all'attacco hacker e agevolare la corretta determinazione della conseguenze e dei riflessi sui dati personali e sui diritti e libertà degli interessati potenzialmente coinvolti. L'Azienda ha mantenuto altresì un costante

rapporto di collaborazione con ACN (...);

- “le categorie di dati impattati dalla violazione sono dati anagrafici (nome, cognome, sesso data di nascita luogo di nascita, codice fiscale) dati di contatto (indirizzo postale o di posta elettronica, numero di telefono fisso o mobile) dati di accesso e di identificazione (username, password) dati relativi alla salute per utenti fornitori e pazienti nonché dipendenti. Per quanto concerne i dipendenti i dati impattati sono costituiti da documentazione relativa alle attività normo economiche inerenti agli stessi ed eventuali contenuti ulteriori personali depositati nelle cartelle di file server”;

- “l’Azienda (…), ha agito negli ultimi anni in un contesto di particolare criticità congiunturale: • Il SSR della regione Piemonte solo nel 2017 è uscito dal Piano di rientro condotto in collaborazione e sotto la vigilanza del MEF, cd “Tavolo Massicci”, che ha determinato una forte contrazione del flusso di spesa in parte corrente ed in conto investimenti, con pesanti tagli al personale con blocco totale delle assunzioni per 7 anni nei ruoli tecnico amministrativo che hanno fortemente depauperato le HR informatiche in un campo a forte sviluppo tecnologico; i tagli sono stati effettuati anche nel settore acquisti di beni e servizi ICT e di adeguamento degli stessi alle nuove realizzazioni informatiche sui quali si sono innestati i vari interventi di spending review. • Il contagio da Covid-19, che si è abbattuto sul territorio alessandrino con particolare velocità e gravità già dal gennaio 2020, data la stretta vicinanza geografica con il territorio di prima diffusione dello stesso, ha portato ulteriori difficoltà nell’ambito della gestione del settore informatico chiamato in prima linea ad affrontare l’emergenza pandemica, rallentando i processi di adeguamento dei sistemi informatici a più alti livelli di sicurezza auspicati dalla direzione strategica aziendale per la migliore protezione dei dati personali. L’emergenza da pandemia Covid è cessata, come da provvedimenti dell’OMS, in data 5/5/2023”;

- “pur in tale contesto di gestione “straordinaria”, l’azienda è riuscita tra l’altro ad avviare un ambizioso piano di riprogettazione della propria infrastruttura informatica – informativa, a partire già dal 2021, con importanti investimenti in hardware, software e risorse umane, con un piano strategico che vede nella digitalizzazione e nella particolare attenzione alla cybersicurezza uno degli elementi fondanti. L'attacco doloso hacker è arrivato nel momento in cui tale piano era stato avviato ed in corso di attuazione con le risorse che finalmente erano a disposizione (anche grazie al PNRR), determinando la successiva accelerazione del piano di mitigazione dei rischi necessari alla luce dello sviluppo delle tecnologie e dei sistemi di trattamento dati”;

- “la notifica di infiltrazione nella rete ospedaliera e la conseguente analisi delle vulnerabilità che hanno permesso questo evento hanno accelerato bruscamente una serie di cambiamenti della cui necessità e improrogabilità, soprattutto rispetto alla situazione di configurazione dell’infrastruttura previgente, la Direzione era assolutamente convinta, e per i quali era in corso un percorso di profonda ristrutturazione e reingegnerizzazione, con importanti investimenti avviati. Tali attività hanno cercato (…), di non limitarsi alla pura e semplice acquisizione di tecnologia, ma, al contrario di partire dalla dimensione organizzativa della sicurezza informatica, di gran lunga più rilevante di quella tecnica. Sulla base di tale consapevolezza sono stati costruiti chiaramente i ruoli e i profili di accesso alla rete degli operatori, non solo tecnico amministrativi, ma soprattutto sanitari, sono state definite le regole di gestione in base alle quali certi dati possono essere veicolati sono attraverso certi canali (applicativi certificati e non le cartelle condivise sul File Server, ad esempio), è stato attivato un meccanismo di commitment forte dalla Direzione nel suo complesso (tramite l’assegnazione di specifici obiettivi nel Piano della Performance a tutta l’organizzazione), e non solo dal responsabile dei sistemi informativi, in modo che il piano di risposta alle vulnerabilità non sia orientato all’emergenza, ma la gestione degli aspetti di sicurezza dei dati personali e di tutela della privacy siano parte integrante della condotta lavorativa di ogni dipendente”.

6. 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);

- 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 "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 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;

- 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".

7. Conclusioni: dichiarazione di illiceità del trattamento.

Alla luce 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 un numero molto rilevante di interessati. Ciò, tenendo altresì conto delle finalità dei trattamenti e della natura dei dati personali trattati, appartenenti anche a categorie particolari e, in particolare, a dati sulla salute. A tal riguardo, gli obblighi di sicurezza previsti dal Regolamento impongono 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.

Sulla base 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 il trattamento effettuato dall'Azienda risulta illecito, in quanto posto in essere in violazione degli artt. 5, par. 1, lett. f) e 32 del Regolamento, in relazione ai profili di seguito riportati.

7.1. 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 "l'Azienda non disponeva di un sistema di log management" (v. verbali del XX, pagg. XX e XX e del XX, pag. XX). Dalla documentazione in atti si evince che "la gestione dell'emergenza dopo l'attacco ha richiesto di accelerare alcune delle misure oggetto di […] pianificazione" con particolare rifermento al SIEM (Security Information and Event Management) da collegare a "SOC esterni utilizzati come servizi ad integrazione degli orari di ufficio in vigore presso il servizio, in modo da garantire una copertura 24/7 dell'attività di controllo, analisi e supporto alla remediation" (v. allegato XX al verbale del XX, pag. X). La carenza evidenziata non ha consentito all'Azienda di rilevare e venire tempestivamente a conoscenza della violazione dei dati personali occorsa.

La mancata adozione di misure adeguate a rilevare tempestivamente le violazioni dei dati personali 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".

7.2. Mancata adozione di misure adeguate a garantire la sicurezza delle reti e obsolescenza dei software di base installati su alcuni sistemi di trattamento

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, come evidenziato anche dall'Azienda nel corso delle attività ispettive "la rete era sostanzialmente flat, non vi era una segmentazione logica o fisica" e non erano differenziate a livello di rete le postazioni di lavoro e i server (v. verbale del XX, pag. XX e allegato XX al verbale del XX, pagg. XX e 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 ha specificato che "non era prevista una procedura di autenticazione informatica a più fattori (MFA) per l'accesso remoto in VPN. (…) Le utenze di "manutenzione" erano spesso generiche, non individuali, con massimi privilegi amministrativi" e che "nonostante fossero state fornite indicazioni al personale circa la scelta della password, ispirate alle buone pratiche di settore, non era prevista alcuna configurazione dei sistemi che recepisse tali indicazioni. Gli utenti che svolgevano le funzioni di amministratore utilizzavano utenze differenziate, a seconda che si trattasse di utenza personale di dominio o utenza con privilegi amministrativi. In tale ultimo caso le credenziali, che non avevano una specifica password policy, erano tendenzialmente condivise fra i diversi amministratori" (v. verbale del XX, pag. XX). Con riferimento a tale profilo, l'Azienda, a seguito dell'incidente, ha ritenuto necessario "attivare la MFA, a certificare la VPN e a individuare utenze nominali (mediante modulistica apposita), nel rispetto del principio del "minimo privilegio"".

Nel corso dell'istruttoria è emerso che "si presume che l'attaccante possa aver sfruttato una vulnerabilità relativa al firewall perimetrale XX [e] che la versione del sistema operativo del firewall XX era vulnerabile" e che erano "attivi ancora vari protocolli di comunicazione obsoleti". In

relazione a tale aspetto, l'Azienda, a seguito dell'incidente, ha proceduto all'aggiornamento tecnologico degli apparati e dell'infrastruttura.

La mancata realizzazione, al momento della violazione, di misure adeguate a garantire la sicurezza delle reti e l'utilizzo di software di base obsoleti, per i quali non sono più disponibili aggiornamenti di sicurezza, non risulta pienamente 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)).

8. 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) e 32 del Regolamento, causata dalla condotta posta in essere dall'Azienda, comporta l'applicazione della sanzione amministrativa pecuniaria ai sensi dell'art. 83, par. 4 e 5 del Regolamento.

Il Garante, ai sensi dell'art. 58, par. 2, lett. i) del Regolamento e 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", mediante l'adozione di una ordinanza ingiunzione (art. 18 legge 24 novembre 1981, n. 689), in relazione al trattamento dei dati personali effettuato dall'Azienda, di cui è stata accertata l'illiceità, nei termini sopra esposti.

Ritenuto di dover applicare il par. 3 dell'art. 83 del Regolamento laddove prevede che "se, in relazione allo stesso trattamento o a trattamenti collegati, un titolare del trattamento […] viola, con dolo o colpa, varie disposizioni del presente Regolamento, l'importo totale della sanzione amministrativa pecuniaria non supera l'importo specificato per la violazione più grave", l'importo totale della sanzione è calcolato in modo da non superare il massimo edittale previsto dal medesimo art. 83, par. 5.

Alla luce di quanto sopra illustrato e, in particolare, della categoria di dati personali interessata dalla violazione, che, per loro natura, sono particolarmente sensibili sotto il profilo dei diritti e delle libertà fondamentali, si ritiene che il livello di gravità della violazione commessa dalla Azienda sia alto (cfr. Comitato europeo per la protezione dei dati, "Guidelines 04/2022 on the calculation of administrative fines under the GDPR" del 23 maggio 2023, punto 60), nonostante il carattere non intenzionale della violazione (l'episodio risulta essere stato determinato da un comportamento doloso da parte di un soggetto terzo, denunciato formalmente alla polizia postale).

Ciò premesso, sono valutati nel loro complesso taluni elementi e, in particolare, che:

- il Garante ha preso conoscenza dell'evento a seguito della notifica di violazione effettuata dall'Azienda, ai sensi dell'art. 33 del Regolamento e non sono pervenuti reclami o segnalazioni in ordine alla violazione oggetto del presente provvedimento (art. 83, par. 2, lett. h) e k) del Regolamento);

- il titolare, al fine di evitare la ripetizione dell'evento occorso, si è impegnato nell'introduzione di misure volte a ridurre la replicabilità dell'evento occorso e ha cooperato con l'Autorità in ogni fase dell'istruttoria, ivi compresa quella ispettiva, al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi (art. 83, par. 2, lett. c) e f) del Regolamento);

- la gestione dell'emergenza pandemica ha reso necessario il forte coinvolgimento del settore informatico, con il conseguente significativo rallentamento dei processi di adeguamento dei sistemi (art. 83, par. 2, lett. k) del Regolamento).

Alla luce degli elementi sopra indicati e delle valutazioni effettuate, si ritiene, nel caso di specie, di determinare l'ammontare della sanzione pecuniaria nella misura di euro 25.000,00 (venticinquemila/00) per la violazione degli artt. 5 e 32 del medesimo Regolamento, in ragione dei principi di effettività, proporzionalità e dissuasività ai quali l'Autorità deve attenersi, ai sensi dell'art. 83, par. 1, del Regolamento.

In tale quadro si ritiene, altresì, che, ai sensi dell'art. 166, comma 7, del Codice e dell'art. 16, comma 1, del Regolamento del Garante n. 1/2019, si debba procedere alla pubblicazione del presente capo contenente l'ordinanza ingiunzione sul sito Internet del Garante. Ciò, in considerazione della tipologia di dati personali oggetto di illecito trattamento e del numero di interessati coinvolti.

TUTTO CIÒ PREMESSO IL GARANTE

ai sensi degli artt. 57, par. 1, lett. f) e 83 del Regolamento, rileva l'illiceità del trattamento effettuato dalla all'Azienda Ospedaliero-Universitaria SS. Antonio e Biagio e Cesare Arrigo, con sede legale in Alessandria, via Venezia, 16 – 15121 - C.F. – P.I. n. 01640560064, nei termini di cui in motivazione, per la violazione degli artt. 5 e 32 del Regolamento;

ORDINA

ai sensi dell'art. 58, par. 2, lett. i) del Regolamento, alla medesima Azienda, in persona del legale rappresentante pro-tempore, di pagare la somma di euro 25.000,00 (venticinquemila/00) a titolo di sanzione amministrativa pecuniaria per la violazione indicata nel presente provvedimento.

INGIUNGE

alla predetta Azienda di pagare la somma di euro 25.000,00 (venticinquemila/00) 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. Si rappresenta che ai sensi dell'art. 166, comma 8 del Codice, resta salva la facoltà per il trasgressore di definire la controversia mediante il pagamento -sempre secondo le modalità indicate in allegato- di un importo pari alla metà della sanzione irrogata entro il termine di cui all'art. 10, comma 3, del d. lgs. 1° settembre 2011, n. 150 previsto per la proposizione del ricorso come sotto indicato.

DISPONE

a) ai sensi dell'art. 166, comma 7, del Codice e dell'art. 16, comma 1, del Regolamento del Garante n. 1/2019, la pubblicazione dell'ordinanza ingiunzione sul sito internet del Garante;

b) ai sensi dell'art. 154-bis, comma 3 del Codice e dell'art. 37 del Regolamento del Garante n. 1/2019, la pubblicazione del presente provvedimento sul sito internet dell'Autorità;

c) ai sensi dell'art. 17 del Regolamento del Garante n. 1/2019, l'annotazione delle violazioni e delle misure adottate in conformità all'art. 58, par. 2 del Regolamento, nel registro interno dell'Autorità previsto dall'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 è possibile proporre ricorso 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, 17 ottobre 2024

IL PRESIDENTE
Stanzione

IL RELATORE
Ghiglia

IL SEGRETARIO GENERALE
Mattei