



**GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI**

Provvedimento del 21 marzo 2024 [10002533]

VEDI ANCHE [Newsletter del 10 aprile 2024](#)

[doc. web n. 10002533]

Provvedimento del 21 marzo 2024

Registro dei provvedimenti
n. 195 del 21 marzo 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 "Codice in materia di protezione dei dati personali, recante 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 "Codice");

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 Garante 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, in www.gpdp.it, doc. web n. 1098801;

RELATORE l'avv. Guido Scorza;

PREMESSO

1. L'attività istruttoria.

A seguito di notizie stampa e delle notifiche di violazione dei dati personali trasmesse nei primi giorni di XX dalla Regione Lazio e dal Consiglio regionale del Lazio, ai sensi dell'art. 33 del

Regolamento, l'Autorità ha appreso che i sistemi informativi gestiti dalla società LAZIOcrea S.p.a. (di seguito "Società" o "LAZIOcrea"), in qualità di responsabile del trattamento per conto della Regione e di diversi enti del servizio sanitario regionale, tra cui quello della Azienda sanitaria locale Roma 3 (di seguito "Azienda"), erano stati oggetto di un attacco informatico, determinato da un malware di tipo ransomware.

In considerazione dell'elevato numero di interessati coinvolti e della natura dei dati personali oggetto di violazione, l'Ufficio ha richiesto informazioni alla predetta Società in merito alla citata violazione dei dati personali, nonché alle misure di sicurezza adottate, con particolare riferimento alle misure tecniche e organizzative adottate per garantire la disponibilità e la resilienza dei sistemi e dei servizi di trattamento e il ripristino tempestivo della disponibilità e dell'accesso dei dati personali in caso di incidente (note del XX e del XX cui la Società ha fornito riscontro con note del XX e XX, XX e XX).

Successivamente, è stata effettuata un'attività ispettiva nei confronti della Società nei mesi di XX e XX.

In seguito, nei mesi di XX, XX, XX, XX e XX, sono state svolte ulteriori attività istruttorie attraverso l'acquisizione di informazioni presso alcuni titolari del trattamento coinvolti nella predetta violazione, tra i quali la predetta Azienda che, sulla base della documentazione fornita da LAZIOcrea, risultavano coinvolti nella violazione dei dati personali.

Con la notifica del XX, la Regione Lazio ha dichiarato di aver "subito un attacco informatico che ha compromesso la funzionalità dei servizi offerti dal CED regionale; è in corso in queste ore una verifica tecnica di quanto accaduto, al momento non si è in grado di determinare se ci sia stata perdita dati, le categorie e il numero approssimativo di registrazioni dei dati personali in questione e le eventuali conseguenze della violazione dei dati personali".

Con nota del XX, la predetta Società, in riscontro alla citata richiesta di informazioni formulata dall'Ufficio, ha dichiarato che:

"a seguito dell'attacco informatico occorso nella notte del 31 luglio u.s. (determinato da Malware di tipo ransomware) sono stati disattivati alcuni sistemi informatici della Regione Lazio rendendo temporaneamente indisponibili i relativi servizi, i dati e le informazioni trattate";

era "impegnata a fornire supporto alle attività di indagine in corso di svolgimento da parte delle forze dell'ordine e delle altre Autorità competenti per la sicurezza nazionali";

erano "in corso le attività di analisi volte ad appurare l'ambito e la portata della violazione dei dati personali trattati [...] una volta appresa nel dettaglio la dinamica degli eventi anche sotto il profilo storico e tecnico";

si rendeva "necessario operare in parallelo per ripristinare i servizi ponendo in essere tutti i presidi e le cautele atte ad impedire che i sistemi stessi possano subire un ulteriore attacco". Successivamente, con nota del XX, la Società ha notificato, in via preliminare, la violazione dei dati personali, avvalendosi della facoltà di fornire ulteriori informazioni in fasi successive, fornite con le successive integrazioni del XX e il XX.

Nella predetta notifica è stato rappresentato, in particolare, che:

"l'attacco è iniziato nella tarda serata del 31 luglio ma se ne è avuta evidenza nelle prime ore della mattina del 1° agosto quando alcune macchine virtuali sono risultate inutilizzabili. Si tratta di un attacco informatico finalizzato alla propagazione di un malware appartenente alla famiglia nota come "RansomEXX", alias "Defray777" che è stato prontamente segnalato dal

nostro servizio di sicurezza informatica al CSIRT ed al CNAIPIC con informativa/esposto a mezzo mail del 1° agosto alle ore 10.22. L'attacco ha riguardato lo strato applicativo della virtualizzazione del data center costringendo la Società a mettere off line tutti i sistemi proprio per garantire che non venisse compromessa l'integrità e la riservatezza dei dati";

"i servizi essenziali relativi alle attività di emergenza del 112, del 118, dei centri trasfusionali, del Pronto Soccorso e della Protezione Civile non sono mai stati interrotti né compromessi anche nel corso delle attività investigative volte ad appurare la dimensione dell'incidente. In parte perché segregati rispetto alle altre applicazioni";

"tutti gli altri servizi ed applicativi residenti sul data center sono stati ripristinati o saranno ripristinati [...] dopo aver verificato l'avvenuta bonifica da ogni contaminazione residua e/o possibile ed aver riconfigurato i sistemi rispetto all'architettura di sicurezza preesistente. A puro titolo conoscitivo le attività di vaccinazione contro il Covid sono proseguite così come il servizio di prenotazione dei predetti vaccini è stato ripristinato in quattro giorni prima che si rendessero disponibili i nuovi slot di somministrazione. Slot che al momento dell'incidente erano per l'appunto già occupati sino al successivo 13 agosto. A partire dal 16 agosto p.v. i terzi fornitori di applicativi residenti nel data center avranno la possibilità di reinstallare i loro sistemi per riprendere la fornitura dei correlati servizi";

"l'origine dell'incidente sembra, allo stato, potersi ricondurre all'inoculazione, su uno o più computer client che operavano da remoto tramite VPN, di software malevoli che hanno creato un canale di comunicazione (backdoor) tra i computer client infettati e il gruppo di cyber criminali. I cyber criminali, sfruttando le stesse credenziali, sono così riusciti successivamente ad accedere alla rete aziendale e da là a muoversi "lateralmente" anche all'interno delle c.d. sotto reti effettuando una escalation su utenze amministrative che sono state probabilmente individuate intercettando a basso livello i pacchetti di dati che su quella rete avvenivano al momento del login degli utenti. Detti criminali sembrerebbe abbiano utilizzato le competenze di un altro gruppo di hacker cui sono state passate le password criptate. Quest'ulteriore gruppo di criminali, sfruttando una presumibile vulnerabilità del sistema operativo, è riuscito a decrittare una password che è poi stata abbinata ad uno dei quattro user id con privilegio di amministratore individuati in precedenza dagli hacker";

"da parte degli esperti sono state poi effettuate verifiche per valutare se l'attacco, che non ha compromesso l'integrità e la riservatezza dei dati, avesse consentito agli intrusi di appropriarsi degli stessi attraverso tecniche di esfiltrazione e/o trasferimento. Le analisi hanno confermato che ad oggi può essere esclusa l'esfiltrazione atteso che nel periodo dell'attacco non si riscontrano flussi dati verso l'esterno";

"i file ritrovati nelle directory temporanee sono infatti derivanti da automatismi dei tool utilizzati per l'attacco e volti principalmente a verificare l'architettura di sistema e l'inventario delle applicazioni presenti per poi predisporre meglio l'attacco a seconda delle configurazioni di sistema rilevate. Per di più le policy dei firewall attive nel corso dell'attacco non consentivano l'utilizzo dei protocolli FTP, SSH e SFTP dall'interno del perimetro del data center verso Internet. In ogni caso sono tutt'ora in corso attività di "Cyber Threat Intelligence" da parte dei consulenti ingaggiati per verificare che non vengano rese pubbliche informazioni appartenenti a Laziocrea anche se riferite a dati già noti prima dell'attacco. Al momento nonostante la scadenza dell'ultimatum nessuna nuova informazione è stata resa disponibile su web ed in particolare su quello illegale c.d. "darkweb";

"i dati e le informazioni presenti sui database sono pertanto risultate indisponibili per il tempo necessario al ripristino delle applicazioni ed alla messa in sicurezza del perimetro del data center riconfigurazione dello stesso. Per alcuni sistemi le informazioni rimarranno indisponibili sino alla riattivazione che avverrà in maniera completa nell'arco dei prossimi

giorni. Non si ravvedono perciò gravi limitazioni alle libertà ed ai diritti fondamentali degli interessati”.

Con la notifica integrativa del XX, la Società ha fornito l'elenco delle applicazioni e dei servizi coinvolti nella violazione – con l'indicazione di quelli ripristinati nell'immediato e in corso di ripristino – e l'elenco di quelli rimasti attivi in quanto segregati dall'infrastruttura oggetto di attacco, rappresentando, in particolare, che:

sulla base “delle indagini condotte dalla struttura di Sicurezza Informatica interna, dal CSIRT, dal CNAIPIC e dalla società Leonardo S.p.A. risulta che l'attacco, iniziato alle ore 15:05 del pomeriggio del 31 luglio 2021, è stato originato dalla compromissione di un account appartenente a un dipendente regionale le cui credenziali di accesso sono state sottratte per mezzo di artefatti malevoli (back door) installati sul computer personale dallo stesso utilizzato per i collegamenti da remoto alla rete aziendale necessari per il lavoro in smart working”;

“le attività di analisi forense hanno appurato che gli artefatti sono stati inoculati il 25 marzo 2021 e che gli stessi non erano rilevabili sul computer ospite dai software antivirus e malware. In sede di analisi forense della copia del computer in questione lo scan ha dato comunque esito negativo nonostante il c.d. “database delle firme” del software antivirus/malware fosse stato aggiornato dagli investigatori forensi alla più recente data del 10 agosto. I collegamenti remoti dell'utente con la rete aziendale erano comunque protetti da una VPN”;

“sono emersi anche tentativi di accessi anomali nei confronti di sei account di utenti sull'interfaccia OWA dei sistemi di posta a partire dal 12 aprile 2021 e sino al 26 luglio 2021. Tali tentativi non sembrano però collegati all'incidente e si sono per lo più risolti, con l'eccezione di una utenza, con il diniego di accesso al servizio di posta”;

“in conclusione, l'attacco è stato sferrato nel pomeriggio di sabato 31 luglio 2021 utilizzando il primo account compromesso ed è emerso in maniera percepibile quando nelle prime ore della mattina del 1° agosto si sono cominciati a verificare i primi malfunzionamenti di alcune macchine virtuali del Data Center”;

“l'attacco ha riguardato le macchine ubicate nella Sala “B” [del data center gestito dalla Società], dove presenti diverse tipologie di hardware sia per la parte computazionale che in termini di storage e apparati di rete (sostanzialmente Cisco, Dell, Fortigate, etc. etc.). Trattandosi di macchine modulari e comunque scalabili in termini di dotazioni e caratteristiche computazionali e di storage, le stesse sono gestite da firmware proprietari su cui sono stati installati gli ambienti operativi di virtualizzazione Microsoft Active Directory Hosts e VMWare & Microsoft Hyper-V environment. Su tale ambiente di virtualizzazione sono state configurate ed installate macchine virtuali con sistemi operativi Windows Server e Linux poste a servizio dei servizi e delle applicazioni necessarie ai trattamenti svolti da LAZIOcrea sia come Titolare che come Responsabile di altri Titolari, ed in particolare della Regione Lazio”.

Nel corso delle citate attività ispettive la Società ha inoltre dichiarato che:

“all'esito delle analisi forensi svolte, risulta che, nel mese di marzo 2021, un soggetto malintenzionato ha introdotto all'interno del PC portatile aziendale in uso [... a un] dipendente della Regione Lazio, una backdoor – non nota e non rilevata, né all'epoca né nel corso delle analisi, da più comuni software antivirus e antispyware – che è stata probabilmente utilizzata per acquisire le credenziali di autenticazione” attribuite al dipendente medesimo;

“il 31 luglio 2021 le predette credenziali di autenticazione sono state utilizzate per accedere da remoto alla rete della Società e per condurre le azioni prodromiche all’attacco informatico. In particolare, i soggetti malintenzionati hanno effettuato una serie di attività di scansione, finalizzate all’acquisizione di informazioni sulla rete e sui sistemi server ivi presenti. Nell’ambito di tali attività i medesimi hanno individuato il server con hostname “RLWSIRIFT01” su cui era installato software di base per cui non erano più disponibili aggiornamenti o patch di sicurezza del produttore. Tale circostanza era dovuta alla necessità di garantire il funzionamento di un’applicazione web legacy che richiedeva una particolare versione del sistema operativo e dell’application server. Sfruttando vulnerabilità note del software di base presente sul citato server i soggetti malintenzionati sono riusciti a venire in possesso di credenziali di autenticazione con privilegi amministrativi [...] utilizzate nelle successive fasi dell’attacco informatico”;

“la Società è venuta a conoscenza dell’attacco informatico mediante una segnalazione di un operatore sanitario che, non riuscendo ad accedere a taluni servizi erogati dalla Società, alle ore 05:00 circa del 1° agosto 2021, ha contattato telefonicamente il sistemista reperibile per i servizi dell’area sanitaria. A seguito della segnalazione e delle prime analisi svolte, il sistemista ha constatato la rilevanza dell’incidente di sicurezza e ha provveduto a contattare altri sistemisti, alcuni dei quali si sono recati immediatamente presso il data center. Alle ore 06:15 circa del XX la segnalazione è stata portata all’attenzione del direttore della Direzione Sistemi infrastrutturali della Società”;

“con riferimento alle iniziative assunte a seguito del rilevamento di “attività ostili” (2.189 allarmi) da parte della “console Microsoft Windows Defender ATP” nella serata del 31 luglio 2021, [...] nelle more dell’attivazione del servizio SOC di Leonardo S.p.a., tale strumento di monitoraggio non era presidiato H24” e, pertanto, “non si è potuto gestire tali allarmi con “maggiore” tempestività”.

Nella documentazione acquisita in fase istruttoria la Società ha altresì fornito l’elenco dei titolari per conto dei quali effettuava i trattamenti di dati personali coinvolti nella violazione, tra i quali è stata anche indicata l’Azienda Sanitaria Locale Roma 3 (cfr. notifica del XX, all. alla sezz. G, H e I, e nota del XX, all. A7)).

1.1 Le misure in essere al momento della violazione

Con riferimento alle misure in essere al momento della violazione la Società ha dichiarato che “il Data center e le procedure aziendali per la sicurezza e protezione dei dati sono certificate ISO 27001” (v. notifica del XX, p. 8 e all. 6).

In particolare, 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, la Società ha fornito copia delle procedure di backup, del piano di business continuity e disaster recovery, del processo di gestione degli incidenti e della procedura di gestione delle violazioni di dati personali in essere alla data del 31 luglio 2021 (cfr. nota del XX, all. C e D in risposta alla richiesta di infiorazioni dell’Ufficio del XX).

Nel corso delle attività ispettive la Società ha poi dichiarato che:

“utilizza come sistema di autenticazione informatica l’Active Directory di Microsoft. Tale sistema è utilizzato per l’autenticazione degli utenti della Società, della Regione e di altri enti esterni per l’accesso ai sistemi attestati al dominio (postazioni di lavoro e server) e ad alcune applicazioni web, nonché per l’accesso remoto, tramite VPN, alla rete della Società” precisando che “al momento in cui si è verificata la violazione dei dati personali, non era

prevista una procedura di autenticazione informatica a più fattori per l'accesso VPN”;

“ha definito password policy differenti per le diverse tipologie di account in uso al personale della Società, della Regione Lazio e di altri enti. In particolare, al momento in cui è avvenuta la violazione dei dati personali, le password degli account senza privilegi amministrativi dovevano essere composte da un numero minimo di 8 caratteri, contenere caratteri di almeno tre categorie (lettere maiuscole, lettere minuscole, numeri, caratteri speciali), non coincidere con le ultime quattro password, ed essere modificate al massimo ogni 90 giorni; le password degli account con privilegi amministrativi dovevano invece essere composte da un numero minimo di 20 caratteri, contenere caratteri di almeno tre categorie (lettere maiuscole, lettere minuscole, numeri, caratteri speciali), non coincidere con le ultime quattro password, ed essere modificate al massimo ogni 30 giorni”;

“ha posto in essere misure per segregare i sistemi che sono presenti all'interno del data center. In particolare, i server che ospitano le diverse banche dati sono attestati a reti segregate rispetto alle altre reti, motivo per cui l'attacco informatico di fine luglio non ha coinvolto i dati conservati all'interno di tali server. Analoghe misure di segregazione sono applicate ai server che erogano servizi particolarmente critici [...] o dedicati a specifici clienti [...]”;

con riferimento alle misure di sicurezza relative alla segregazione delle reti, in essere al momento della violazione dei dati personali, “sono presenti due livelli di firewalling: il primo è dedicato al filtraggio delle comunicazioni tra le reti su cui sono attestate le postazioni di lavoro dei dipendenti della Regione Lazio e della Società (attestate su reti LAN accessibili presso le sedi degli uffici regionali e della Società) e quelle su cui sono attestati i sistemi server; il secondo è invece utilizzato per il filtraggio del traffico di rete da e verso il data center e delle comunicazioni tra le reti su cui sono attestati i sistemi server. In particolare, le regole di firewalling sono configurate sulla base delle indicazioni fornite dai diversi responsabili di progetto. In alcuni casi, il filtraggio del traffico di rete è attuato anche tra i diversi layer architetturali di un sistema (front-end, back-end, database) o per i diversi ambienti (sviluppo, collaudo e produzione). Alcuni sistemi o servizi critici [...] sono invece attestati a reti dedicate e separate, anche fisicamente, rispetto agli altri sistemi presenti nel data center”;

“a fine luglio 2021, quando si è verificato l'incidente di sicurezza oggetto dell'accertamento ispettivo, le regole di filtering non impedivano, a livello di rete, la raggiungibilità dei sistemi server compromessi dalla rete utilizzata per l'accesso VPN dei dipendenti della Regione Lazio, tra i quali [...] l'account del dipendente]. Per tale ragione, i soggetti malintenzionati sono riusciti a effettuare una ricognizione dei sistemi server visibili dalla rete utilizzata per l'accesso VPN, nonché a individuarne uno con sistema operativo obsoleto (“RLWSIRIFT01”) affetto da alcune vulnerabilità note. [...] una di queste vulnerabilità è stata poi sfruttata per acquisire le credenziali di autenticazione con privilegi amministrativi [...] utilizzate nelle successive fasi dell'attacco informatico” ;

“fino al 30 giugno 2021, si avvaleva di un servizio di Security Information and Event Management (SIEM), basato su tecnologia IBM e fornito da Fastweb S.p.a. nell'ambito di una convenzione Consip. Dal XX la Società ha attivato un nuovo servizio SIEM, basato su tecnologia Microsoft (Sentinel). Al momento in cui si è verificato l'attacco informatico la Società non disponeva di personale (interno o esterno) dedicato all'analisi H24 degli alert generati dal SIEM di Microsoft, in attesa dell'attivazione di un servizio di security operations center (SOC) fornito da Leonardo S.p.a., poi avvenuta nei primi giorni di agosto 2021”;

“al momento dell'incidente di sicurezza, utilizzava come sistema di gestione dei backup il prodotto Data Domain di Dell. Non erano state definite specifiche procedure di gestione dei

backup, ma era previsto che ciascun referente di progetto comunicasse, al momento del rilascio in esercizio, mediante un apposito modello, fra le altre, anche informazioni sul tipo e sulla retention dei backup da effettuare. La periodicità dei backup era giornaliera (con avvio alle ore 20:00 circa);

ha eseguito attività di audit sul processo di gestione degli incidenti e ha fornito copia dei piani e dei rapporti di audit;

“con cadenza annuale, effettua attività di audit interno su ciascuno dei processi previsti dal SGSI [...] La Società ha pianificato, nell’ambito del programma di audit dell’anno 2022, l’esecuzione di una specifica attività di audit sull’incidente di sicurezza verificatosi a fine luglio 2021, anche al fine di chiudere l’osservazione formulata dall’organismo di certificazione (Apave Certification Italia S.r.l.) nel corso della visita di sorveglianza per il mantenimento della certificazione ISO 27001 avvenuta il XX e il XX”.

1.2 Le misure adottate a seguito della violazione

Con riferimento alle misure adottate a seguito della violazione, la Società, con la notifica integrativa del XX, ha rappresentato che:

“al momento dell’incidente unitamente alla messa off line dei sistemi si è provveduto a porre in essere azioni correttive tra cui: i) la costituzione di un team di crisi; ii) l’arruolamento di consulenti esterni esperti nelle attività specialistiche di incident response, cyber security e bonifica dei sistemi; iii) la riattivazione di ogni sistema applicativo previa compatibilità con le attività di indagine e la verifica della sicurezza degli applicativi medesimi anche ricorrendo ad installazioni ponte su ambienti Cloud forniti da provider CSP certificati Agid; iv) l’attivazione di tutte le attività ed i controlli necessari a garantire il perimetro di sicurezza fisica e logica del data center; v) l’individuazione di una serie di azioni di rimedio per aumentare la sicurezza dei sistemi e la conseguente protezione dei dati personali, ciò nonostante i livelli di sicurezza ante attacco rispondessero già agli standard di settore avendo la Società ottenuto la certificazione ISO 27001”;

“in tutti i casi è stata fatta una comunicazione sia sul sito istituzionale della Regione Lazio che su quello di Laziocrea per informare tutti gli utenti e gli interessati dell’effettiva portata del disservizio e dei rischi inerenti i dati personali”;

“sono state ripristinate tutte le applicazioni sia di Titolarità di Laziocrea che gestite da Laziocrea quale Responsabile della Regione Lazio o degli altri Titolari [...]. Il trattamento gestito per conto della Regione come Responsabile [...] (REG 09 – RES065 nell’ambito di trattamento DSINF 45 -Sviluppo, Manutenzione, Amministrazione, Assistenza all’utente del sistema di Gestione Avvisi e Bandi di Regione Lazio per la Cultura) è stato ripristinato dal back-up e per i Bandi Cine Produzione e Cine Promozione pur contenendo tutte le istanze presentate ha dato alcuni problemi con il ripristino della documentazione allegata alle predette istanze. Il problema riguarda le pratiche finanziate per gli anni 2017-2018-2019 e 2020 che sono circa 1.800, per alcune di queste non è stato possibile ripristinare dai back up tutti gli allegati delle istanze oramai archiviate [...]. Vi è comunque la possibilità che parte dei documenti non sia ripristinabile perché corrotto il file ripristinato”;

“al momento non c’è evidenza di esfiltrazione di dati strutturati pur non potendo escludere con assoluta certezza che non possano essere stati visionati o consultati nel corso dell’attacco file contenenti informazioni. Nell’arco temporale in cui è avvenuta la propagazione del ransomware non sono state osservate connessioni verso l’esterno che lascerebbero presupporre un possibile trasferimento non controllato di informazioni”.

Per effettuare le operazioni di ripristino dei dati e dei sistemi, la Società ha rappresentato che, in assenza di strumenti per la decifratura dei “file cifrati dal ransomware”, ha recuperato “porzioni di file di grandi dimensioni mediante l'utilizzo di strumenti di data carving” (cfr. par. 5 dell'Executive & Technical Report di Leonardo S.p.a., all. B alla nota del XX).

Inoltre, nel corso delle predette attività ispettive la stessa ha dichiarato che:

“a seguito dell'incidente è stata attivata la procedura con doppio fattore di autenticazione, basata sull'utilizzo di username/password e di una one time password (OTP)” (v. verbale del XX, p. 3);

“a seguito della violazione dei dati personali, le password policy degli account senza privilegi amministrativi sono state modificate, incrementando la lunghezza minima a 10 caratteri” (v. verbale del XX, p. 4);

“sulla base delle indicazioni fornite dalla Regione in termini di priorità nel ripristino dei servizi e compatibilmente con le esigenze investigative manifestate dall'autorità giudiziaria, la Società ha provveduto a reinstallare tutti i server del dominio, inclusi i domain controller, utilizzando le copie integre delle diverse applicazioni. Nell'ambito di tale attività di ripristino, la Società si è avvalsa anche della consulenza di Microsoft che ha certificato l'assenza di cc.dd. “utenze civetta” sull'Active directory che potevano essere state create dai soggetti malintenzionati durante l'attacco informatico” (v. verbale del XX, p. 5);

“adottato un nuovo sistema di gestione dei backup basato su tecnologia Commvault, che è ubicato on premises presso il data center della Società, ma che consente, ove necessario, di utilizzare anche il servizio cloud offerto dal fornitore. Il nuovo sistema consente una più semplice gestione e monitoraggio del backup dei dati e dei sistemi. Tuttora è previsto che ciascun referente di progetto comunichi, al momento del rilascio in esercizio, mediante un apposito modello, fra le altre, anche informazioni sul tipo e sulla retention dei backup da effettuare” (v. verbale del XX, p. 4);

“a seguito dell'incidente di sicurezza, alcuni servizi e sistemi sono stati ripristinati, e tuttora sono erogati, in ambiente cloud, in particolare: sul cloud AWS di Amazon (data center ubicato in Lombardia) il sistema di prenotazione delle prestazioni sanitarie (ivi inclusi i vaccini e i tamponi anti-SARS-CoV-2) e l'Anagrafe vaccinale regionale; sul cloud Azure di Microsoft (data center ubicato in Irlanda) il sistema di Identity and access management (IAM) e diversi portali web istituzionali (es. portale della Regione Lazio)”;

“a seguito dell'incidente di sicurezza verificatosi a fine luglio 2021 [...] ha avviato una serie di iniziative volte a rivedere e rafforzare le regole di filtering applicate alle comunicazioni tra e verso i sistemi server”;

“l'accesso remoto ai sistemi e servizi presenti nel data center avviene mediante VPN (basata su tecnologia Pulse Secure). In tale caso, un primo livello di policy di filtering è effettuato dai concentratori VPN che applicano privilegi e regole diverse in base ai gruppi di dominio di cui l'utente è membro”;

“ha individuato i (pochi) server che, per garantire il funzionamento di alcuni servizi legacy, utilizzano ancora sistemi operativi obsoleti e ha provveduto ad adottare opportune misure di segregazione, a livello di rete, nonché di monitoraggio degli eventi di sicurezza”.

1.3 Le informazioni sulla violazione fornite dal responsabile del trattamento

La Società ha fornito copia delle “note inviate alla Regione [...], nonché le note inviate agli altri Titolari del trattamento”, precisando che le “note inviate ai Titolari diversi dalla Regione hanno il

medesimo contenuto per cui si inviano a titolo esemplificativo i tre modelli [...] delle tre differenti note spedite” e allegando un “elenco dei Titolari [...] che hanno ricevuto dette note, con l’indicazione dei riferimenti dell’Ente, delle date di trasmissione e del protocollo di LAZIOcrea” (v. nota del XX, p. 1).

Con riferimento ai titolari del trattamento coinvolti, tra i quali figura la predetta Azienda, la Società ha rappresentato di aver inviato agli stessi tre comunicazioni:

con nota del XX, ha fornito “informazioni in relazione all’attacco cibernetico al Data Center dell’Amministrazione regionale perpetrato da ignoti cyber criminali in data XX/XX”, “comunicare affinché i riceventi abbiano gli elementi per procedere autonomamente ad una notifica preliminare del data breach al Garante per la protezione dei personali”; la Società ha evidenziato che “i servizi e gli applicativi residenti sul data center sono stati ripristinati o saranno ripristinati nei prossimi giorni dopo aver verificato l’avvenuta bonifica da ogni contaminazione residua e/o possibile ed aver riconfigurato i sistemi rispetto all’architettura di sicurezza preesistente. A partire dal 16 agosto p.v. i terzi fornitori di applicativi residenti nel data center avranno la possibilità di reinstallare i loro sistemi per riprendere la fornitura dei correlati servizi” e ha comunicato una serie di azioni correttive adottate a seguito dell’incidente; codesta Società ha inoltre rappresentato che “sono state poi effettuate verifiche per valutare se l’attacco, che non ha compromesso l’integrità e la riservatezza dei dati, avesse consentito agli intrusi di appropriarsi degli stessi attraverso tecniche di esfiltrazione e/o trasferimento”, che “hanno confermato che ad oggi può essere esclusa l’esfiltrazione atteso che nel periodo dell’attacco non si riscontrano flussi dati verso l’esterno”, evidenziando che “i dettagli tecnici dell’attacco e di ogni singola azione di rimedio posta in essere saranno più compiutamente esposti nelle relazioni finali sull’incidente che sono in corso di redazione sia da parte del team indipendente di esperti sia da parte delle strutture aziendali deputate alla sicurezza e alla tutela dei dati”;

con nota del XX, ha fornito “ulteriori informazioni in relazione all’attacco cibernetico al Data Center dell’Amministrazione regionale perpetrato da ignoti cyber criminali in data XX/XX”, evidenziando che “le indagini condotte hanno accertato la sola compromissione e perdita di riservatezza [di ...] due account aziendali con esclusione di qualsivoglia compromissione dei dati gestiti dagli applicativi e dai sistemi in esercizio in termini di integrità e riservatezza”;

con nota del XX, ha rappresentato che “sono stati ripristinati tutti i sistemi applicativi gestiti da LAZIOcrea sia come titolare che come responsabile del trattamento per conto della Regione Lazio e/o di altri soggetti” e che “alcuni Siti Web informativi sono ancora in corso di riprogettazione per migliorarne la sicurezza attesa l’obsolescenza delle piattaforme applicative su cui erano stati a suo tempo sviluppati”; la Società ha inoltre evidenziato che “le informazioni ricevute dalla Autorità investigative (CNAIPIC, DIS e CSIRT) portano ad escludere che il data breach abbia comportato l’esfiltrazione di dati legati ai trattamenti svolti da LAZIOcrea sia come Titolare che come Responsabile”, anche in ragione del fatto che “sul dark web non è stato pubblicato alcun dato neppure in vicinanza della scadenza dell’ultimatum degli Hacker”.

Nel corso dell’istruttoria, è inoltre emerso che diversi titolari del trattamento, dopo aver appreso dell’attacco informatico attraverso notizie di stampa, hanno provveduto a richiedere alla Società informazioni al riguardo.

1.4 le informazioni fornite dall’Azienda

L’Azienda, in riscontro alle predette richieste di informazioni, nella nota del XX, ha rappresentato, in particolare, che:

l'Azienda, con nota del XX, ha chiesto alla Società informazioni circa "quali e quanti dati personali afferenti agli interessati/pazienti/utenti della [...] Azienda sono stati, ed in quale modo, coinvolti nel data breach" (v. nota dell'Azienda del XX);

"a seguito dell'attacco informatico [...] l'Azienda ha avviato tutte le attività necessarie a garantire una minimizzazione dei rischi connessi al trattamento dei dati personali";

"si è provveduto a isolare la connettività verso il Data Center Regionale e si è proceduto all'analisi degli apparati interni per verificare la possibile propagazione del malware individuato da Lazio Crea";

"tutte le analisi effettuate hanno dato esito negativo e, pertanto, risulta che i sistemi aziendali non abbiano subito danni e l'erogazione dei relativi servizi sia avvenuta in via continuativa";

"alla luce della nota inviata da Regione Lazio in data XX, nella quale erano descritte le modalità dell'attacco informatico, sono state attivate procedure interne per consentire l'accesso degli utenti alle prestazioni riservate ai servizi e alla fruibilità dei dati degli interessati";

"per quanto riguarda le informazioni fornite ai soggetti interessati, sebbene, come già riferito, l'attacco informatico non abbia intaccato direttamente i sistemi aziendali e i servizi ospedalieri, sono state attivate forme di comunicazione necessarie ad avvisare l'utenza dell'accaduto sia per mezzo del sito internet istituzionale dell'Azienda sia per mezzo di piattaforme di social network"

"è stato attivato un call center aziendale per consentire le prenotazioni delle prestazioni specialistiche, evitando così di utilizzare i sistemi di Lazio Crea".

Successivamente, in riscontro all'ulteriore richiesta di informazioni volta ad acquisire copia della documentazione sulla violazione dei dati personali, tenuta dal titolare ai sensi dell'art. 33, par. 5, del Regolamento, l'Azienda ha fornito alcuni elementi (descrizione della violazione; descrizione dei sistemi, software, servizi e infrastrutture IT coinvolti nella violazione; misure tecniche e organizzative, in essere al momento della violazione, adottate per garantire la sicurezza dei dati personali coinvolti; misure tecniche organizzative adottate, o di cui si propone l'adozione, per porre rimedio alla violazione e attenuarne i possibili effetti negativi per gli interessati; misure tecniche organizzative adottate, o di cui si propone l'adozione, per prevenire simili violazioni future; comunicazioni agli interessati) evidenziando che "ogni determinazione [...] è esclusivamente basata su quanto riferito dalla Regione Lazio/LAZIOcrea S.p.a. tramite le note ufficiali dalle medesime diramate nelle more della gestione e dell'analisi del menzionato attacco informatico" (v. nota dell'Azienda del XX).

Sulla base di quanto sopra rappresentato, con nota del XX (prot. XX) l'Ufficio ha effettuato una notifica di violazione di cui all'art. 166, comma 5 del Codice all'Azienda, in quanto è stato rilevato che il trattamento di dati personali in esame è stato effettuato in violazione degli obblighi di cui all'art. 33, parr. 1 e 5, del Regolamento da parte della Azienda in relazione ai trattamenti effettuati in qualità di titolare;

Con nota del XX, l'Azienda ha inviato le proprie memorie difensive, nell'ambito delle quali ha ribadito quanto già dichiarato in atti, la propria collaborazione nei confronti dell'Autorità e ha evidenziando di aver anche richiesto all'epoca dei fatti oggetto di contestazione un parere ad uno studio legale (parere in atti) nel quale è stato evidenziato che "stando alle informazioni in mio possesso, tale evento non ha comportato alcun malfunzionamento o disservizio per la ASL Roma 3 e, soprattutto, non sono stati registrati tentativi di accesso abusivo ai sistemi informatici o di sottrazione, alterazione o distruzione di dati personali dell'Azienda stessa [...] In tale contesto, si è

dell'opinione che non sia necessario effettuare una notifica al Garante per la protezione dei dati personali salvo che, a seguito di ulteriori accertamenti o di eventuali comunicazioni della Regione Lazio e/o di LazioCrea S.p.A., dovesse evincersi che l'evento di data breach ha coinvolto anche dati personali, anche non necessariamente di natura sensibile, trattati dalla Vostra Azienda. [...] In ogni caso, ma esclusivamente in ottica di accountability si consiglia di annotare l'evento occorso in data 1° agosto u.s. nel registro dei data breach detenuto dalla ASL Roma 3”

2. Esito dell'attività istruttoria.

Con riferimento alla disciplina applicabile, si osserva che:

ai sensi del Regolamento 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). Il considerando n. 35 del Regolamento precisa poi che i dati relativi alla salute “comprendono informazioni sulla persona fisica raccolte nel corso della sua registrazione al fine di ricevere servizi di assistenza sanitaria”; “un numero, un simbolo o un elemento specifico attribuito a una persona fisica per identificarla in modo univoco a fini sanitari”;

il Regolamento prevede che i dati personali siano essere “trattati in maniera da garantire un’adeguata sicurezza [...] compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»)” (art. 5, par. 1, lett. f), del Regolamento);

l’art. 33 del Regolamento stabilisce che “in caso di violazione dei dati personali, il titolare del trattamento notifica all’autorità di controllo [...] senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche [...]” (par. 1) e che “qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo” (par. 4);

le “Linee guida 9/2022 sulla notifica delle violazioni dei dati personali ai sensi del RGPD” (di seguito “Linee guida sulla notifica”), adottate dal Comitato europeo per la protezione dei dati il 28 Marzo 2023, evidenziano che “a seconda della natura della violazione, il titolare del trattamento può avere la necessità di effettuare ulteriori accertamenti per stabilire tutti i fatti pertinenti relativi all’incidente [...]. Ciò significa che il Regolamento prende atto del fatto che il titolare del trattamento non sempre dispone di tutte le informazioni necessarie su una violazione entro 72 ore dal momento in cui ne è venuto a conoscenza, dato che non sempre sono disponibili entro tale termine dettagli completi ed esaustivi su un incidente. Pertanto, il Regolamento consente una notifica per fasi. È più probabile che ciò si verifichi in caso di violazioni più complesse, quali alcuni tipi di incidenti di sicurezza informatica nel contesto dei quali, ad esempio, può essere necessaria un’indagine forense approfondita per stabilire appieno la natura della violazione e la portata della compromissione dei dati personali. Di conseguenza, in molti casi il titolare del trattamento dovrà effettuare ulteriori indagini e dare seguito alla notifica fornendo informazioni supplementari in un secondo momento. Ciò è consentito a condizione che il titolare del trattamento indichi i motivi del ritardo, in conformità all’articolo 33, paragrafo 1” (sez. II.B.2). Ciò, anche al fine di consentire all’Autorità di controllo di valutare l’adeguatezza delle decisioni assunte dal titolare in merito alla comunicazione agli interessati e alle misure adottate per porre rimedio alla violazione;

il citato art. 33 del Regolamento prevede che “il titolare del trattamento documenta qualsiasi

violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio” (par. 5);

con riguardo alla documentazione della violazione, le Linee guida sulla notifica stabiliscono che “indipendentemente dal fatto che una violazione debba o meno essere notificata all’autorità di controllo, il titolare del trattamento deve conservare la documentazione di tutte le violazioni”, che “tale obbligo è collegato al principio di responsabilizzazione”, di cui all’art. 5, par. 2, del Regolamento e che “lo scopo della tenuta di registri delle violazioni non notificabili, oltre a quelle notificabili, è collegato anche agli obblighi del titolare del trattamento ai sensi dell’articolo 24, e l’autorità di controllo può richiedere di consultare tali registri. Di conseguenza il titolare del trattamento è incoraggiato a creare un registro interno delle violazioni, indipendentemente dal fatto che sia tenuto a effettuare la notifica o meno” (sez. V.A);

le medesime Linee guida sulla notifica specificano che “sebbene spetti al titolare del trattamento determinare quale metodo e struttura utilizzare per documentare una violazione, determinate informazioni chiave dovrebbero essere sempre incluse”, che il titolare del trattamento è tenuto a “registrare i dettagli relativi alla violazione, comprese le cause, i fatti e i dati personali interessati. Dovrebbe altresì indicare gli effetti e le conseguenze della violazione e i provvedimenti adottati per porvi rimedio” e raccomandano “di documentare anche il ragionamento alla base delle decisioni prese in risposta a una violazione. In particolare, se una violazione non viene notificata, è opportuno documentare una giustificazione di tale decisione. La giustificazione dovrebbe includere i motivi per cui il titolare del trattamento ritiene improbabile che la violazione possa presentare un rischio per i diritti e le libertà delle persone fisiche. In alternativa, se ritiene che una delle condizioni di cui all’articolo 34, paragrafo 3, sia soddisfatta, il titolare del trattamento dovrebbe essere in grado di fornire prove adeguate della circostanza che ricorre nel caso di specie. Se il titolare del trattamento notifica una violazione all’autorità di controllo, ma la notifica avviene in ritardo, il titolare del trattamento deve essere in grado di fornire i motivi del ritardo; la documentazione relativa a tale circostanza potrebbe contribuire a dimostrare che il ritardo nella segnalazione è giustificato e non eccessivo” (sez. V.A);

le “Linee-guida 01/2021 su esempi riguardanti la notifica di una violazione dei dati personali” (di seguito “Linee guida sui casi di violazione dei dati personali”), adottate dal Comitato europeo per la protezione dei dati il 14 dicembre 2021, richiamando le Linee guida sulla notifica, specificano che la documentazione interna di una violazione è un obbligo indipendente dai rischi connessi alla violazione stessa e deve essere predisposta in ogni singolo caso (punto 15);

gli incidenti determinati da malware di tipo ransomware rappresentano una causa frequente di notifica di violazione dei dati personali e possono di regola essere classificati come violazioni della disponibilità, ma potrebbero comportare anche violazioni della riservatezza (punto 16). In relazione agli esempi di violazioni dei dati personali determinate da ransomware (cfr. casi 1, 2, 3 e 4), le medesime Linee guida sottolineano la necessità che i titolari del trattamento documentino tale tipologia di violazione a prescindere dal relativo rischio per i diritti e le libertà degli interessati (cfr. punti 25, 35, 40 e 47).

Preso atto di quanto rappresentato dall’Azienda nella documentazione in atti e nelle memorie difensive, si osserva che:

con riferimento alla violazione degli obblighi di cui all’art. 33, par. 1, del Regolamento:

a fronte dell’indisponibilità, anche prolungata, dichiarata dalla stessa Azienda di alcuni sistemi gestiti dalla Società (es. Telemed, Advice, sistemi deputati al teleconsulto e alla tele

refertazione in emergenza) e dei dati sulla salute ivi trattati dall'Azienda in qualità di titolare, quest'ultima non ha provveduto a notificare la violazione dei dati personali all'Autorità, né ha fornito adeguata documentazione sulle decisioni assunte e sulle valutazioni svolte, in grado di comprovare che, con riferimento a tali trattamenti, fosse improbabile che la violazione presentasse un rischio per i diritti e le libertà degli interessati;

al riguardo, le citate Linee guida sulla notifica ricordano che “le violazioni possono essere classificate in base ai seguenti tre principi ben noti alla sicurezza delle informazioni” e che può verificarsi una “violazione della disponibilità, in caso di perdita, accesso o distruzione accidentali o non autorizzati di dati personali”. In particolare, le Linee guida evidenziano che “può verificarsi perdita di disponibilità anche in caso di interruzione significativa del servizio abituale di un'organizzazione” e che “un'infezione da ransomware (software dannoso che cifra i dati del titolare del trattamento finché non viene pagato un riscatto) potrebbe comportare una perdita temporanea di disponibilità se i dati possono essere ripristinati da un backup. Tuttavia, si è comunque verificata un'intrusione nella rete e potrebbe essere richiesta una notifica se l'incidente è qualificato come violazione della riservatezza (ad esempio se chi ha effettuato l'attacco ha avuto accesso a dati personali) e ciò presenta un rischio per i diritti e le libertà delle persone fisiche” (sez. I.B.2);

le Linee guida sui casi di violazione dei dati personali, in relazione ad alcuni esempi di violazioni dei dati personali determinate da ransomware (cfr. casi 2, 3 e 4), evidenziano che, in caso di rischio per i diritti e le libertà degli interessati, i titolari del trattamento sono tenuti a notificare la violazione all'autorità di controllo (cfr. punti 35, 40 e 47); a tal fine non rileva la circostanza che l'Azienda, dopo essere venuta a conoscenza dell'incidente, abbia inviato all'Autorità copia della nota con cui richiedeva informazioni alla Regione Lazio e alla Società circa il “data breach del 1° agosto 2021” (v. nota dell'Azienda del XX);

con riferimento alla violazione degli obblighi di cui all'art. 33, par. 5, del Regolamento:

dalla documentazione in atti si rileva inoltre che l'Azienda, anche contrariamente a quanto indicato nel predetto parere legale, non ha provveduto a documentare adeguatamente la violazione. In particolare, solo a seguito di specifiche richieste di informazioni dell'Ufficio, la stessa ha predisposto e fornito all'Autorità alcuni documenti che, nel loro complesso, risultano comunque privi delle informazioni chiave indicate nelle citate Linee guida sulla notifica quali, a esempio, gli effetti e le conseguenze della violazione per gli interessati, il ragionamento alla base delle decisioni prese (inclusa quella di non notificare la violazione al Garante), nonché la valutazione del rischio derivante dalla violazione.

3. Conclusioni.

Alla luce delle valutazioni sopra richiamate, tenuto conto delle dichiarazioni rese dall'Azienda 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 nelle memorie difensive non consentono di superare i rilievi notificati dall'Ufficio con l'atto di avvio del procedimento, non ricorrendo, peraltro, alcuno dei casi previsti dall'art. 11 del Regolamento del Garante n. 1/2019.

Per tali ragioni, si confermano le valutazioni preliminari dell'Ufficio e si rileva l'illiceità della condotta assunta dall'Azienda sanitaria locale Roma 3, nei termini di cui in motivazione, in violazione dell'art. 33, parr. 1 e 5, del Regolamento.

4. 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 dell'art. 33, parr. 1 e 5 del Regolamento, causata dalla condotta dell'Azienda, è soggetta all'applicazione della sanzione amministrativa pecuniaria ai sensi dell'art. 83, par.4 del Regolamento.

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

La predetta sanzione amministrativa pecuniaria inflitta, in funzione delle circostanze di ogni singolo caso, va determinata nell'ammontare tenuto conto dei principi di effettività, proporzionalità e dissuasività, indicati nell'art. 83, par. 1, del Regolamento, alla luce degli elementi previsti all'art. 85, par. 2, del Regolamento in relazione ai quali si osserva che:

la violazione concerne l'indisponibilità, anche prolungata, di alcuni sistemi informativi utilizzati dall'Azienda in qualità di titolare nell'ambito dei quali sono trattati dati sulla salute degli assistiti (es. Telemed, Advice) (art. 83, par. 2, lett. a) e g) del Regolamento);

l'Azienda non ha provveduto a notificare la violazione dei dati personali all'Autorità, né a fornire adeguata documentazione sulle decisioni assunte e sulle valutazioni svolte, in grado di comprovare che, con riferimento a tali trattamenti, fosse improbabile che la violazione presentasse un rischio per i diritti e le libertà degli interessati (art. 83, par. 2, lett. b) e h) del Regolamento);

l'Azienda ha prestato piena collaborazione all'Autorità nel corso dell'istruttoria (art. 83, par. 2, lett. f) del Regolamento);

i fatti sono accaduti durante il contesto emergenziale da Covid-19 (art. 83, par. 2, lett. k) del Regolamento);

l'Azienda è stata informata tardivamente e solo parzialmente dal responsabile del trattamento in merito alla violazione in esame, anche a seguito di specifiche richieste da parte della stessa (art. 83, par. 2, lett. k) del Regolamento);

non risultano precedenti violazioni pertinenti commesse dall'Azienda o precedenti provvedimenti di cui all'art. 58 del Regolamento in merito alle disposizioni sopra richiamate (art. 83, par. 2, lett. e) del Regolamento);

Alla luce di tali circostanze, si ritiene che, nel caso di specie, il livello di gravità delle violazioni commesse dal titolare del trattamento sia basso (Guidelines 04/2022 on the calculation of administrative fines under the GDPR, adottate dal Comitato il 23 maggio 2023, punto 60).

In ragione dei suddetti elementi, valutati nel loro complesso, si ritiene di determinare l'ammontare della sanzione pecuniaria prevista dall'art. 83, parr. 3 e 4, del Regolamento nella misura di euro 10.000,00 (diecimila) per la violazione dell'art. 33, parr. 1 e 5, del Regolamento, quale sanzione amministrativa pecuniaria ritenuta, ai sensi dell'art. 83, par. 1, del Regolamento, effettiva, proporzionata e dissuasiva.

Si rileva, infine, 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.

TUTTO CIÒ PREMESSO IL GARANTE

dichiara l'illiceità del trattamento di dati personali effettuato dall'Azienda sanitaria locale Roma 3 per la violazione dell'art. 33, parr. 1, 2 e 5, del Regolamento nei termini di cui in motivazione.

ORDINA

ai sensi degli artt. 58, par. 2, lett. i), e 83 del Regolamento, nonché dell'art. 166 del Codice, all'Azienda sanitaria locale Roma 3, codice fiscale 04733491007, in persona del legale rappresentante pro-tempore, di pagare la somma di euro 10.000,00 (diecimila) a titolo di sanzione amministrativa pecuniaria per le violazioni indicate nel presente provvedimento; si rappresenta che il contravventore, ai sensi dell'art. 166, comma 8, del Codice, ha facoltà di definire la controversia mediante pagamento, entro il termine di 30 giorni, di un importo pari alla metà della sanzione comminata.

INGIUNGE

alla predetta Azienda, in caso di mancata definizione della controversia ai sensi dell'art. 166, comma 8, del Codice, di pagare la somma di euro 10.000,00 (diecimila) secondo le modalità indicate in allegato, entro 30 giorni dalla notificazione del presente provvedimento, pena l'adozione dei conseguenti atti esecutivi a norma dall'art. 27 della legge n. 689/1981.

DISPONE

ai sensi dell'art. 166, comma 7, del Codice, dispone la pubblicazione per intero del presente provvedimento sul sito web del Garante e l'annotazione del presente provvedimento nel registro interno dell'Autorità, previsto dall'art. 57, par. 1, lett. u), del Regolamento, delle violazioni e delle misure adottate in conformità all'art. 58, par. 2, 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, 21 marzo 2024

IL PRESIDENTE
Stanzione

IL RELATORE
Scorza

IL SEGRETARIO GENERALE
Mattei