Provvedimento del 21 marzo 2024 [10002324]

VEDI ANCHE Newsletter del 10 aprile 2024

[doc. web n. 10002324]

Provvedimento del 21 marzo 2024

Registro dei provvedimenti
n. 194 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 il prof. Pasquale Stazione;

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, del Consiglio Regionale del Lazio e di diversi enti del servizio sanitario regionale, erano stati oggetto di un attacco informatico, determinato da un malware di tipo ransomware.

In particolare, con la notifica del , la Regione Lazio ha dichiarato di aver "subìto 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".

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.

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 XX 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, il 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 "il ritardo nella notifica è dipeso (i) dalla necessità di acquisire gli elementi minimi necessari per dare una informazione quanto più compiuta possibile (ii) dalla esigenza di ripristinare primariamente i servizi essenziali al cittadino della Regione Lazio e (iii) di appurare con la collaborazione di società di cyber security e con le Autorità di polizia giudiziaria l'effettiva portata dell'incidente sia in termini applicativi che con riferimento alla tutela dei dati personali ed alle libertà e ai diritti degli interessati che allo stato, salva la volontaria indisponibilità del dato, non sembrano essere state compromesse".

È stato inoltre rappresentato 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 rispristinato 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 XX, 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;

"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 1° agosto 2021 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 il seguente elenco dei titolari per conto dei quali effettuava i trattamenti di dati personali coinvolti nella violazione: Regione Lazio; Consiglio Regionale del Lazio; Azienda Sanitaria Locale Roma 1; Azienda Sanitaria Locale Roma 2; Azienda Sanitaria Locale Roma 3; Azienda Sanitaria Locale Roma 4; Azienda Sanitaria Locale Roma 5; Azienda Sanitaria Locale Roma 6; Azienda Unità Sanitaria Locale Frosinone; Azienda Sanitaria Locale Latina; Azienda Unità Sanitaria Locale Rieti; Azienda Sanitaria Locale Viterbo; Fondazione PTV Policlinico Tor Vergata; Azienda Ospedaliera San Camillo Forlanini; Azienda Ospedaliera Complesso Ospedaliero San Giovanni Addolorata; Azienda Ospedaliero-Universitaria Sant'Andrea; Istituto Nazionale Malattie Infettive Lazzaro Spallanzani IRCCS; Casa generalizia dell'Ordine Ospedaliero di San Giovanni di Dio – Fatebenefratelli (a cui è subentrata, dal XX, la società Gemelli Isola Società Benefit S.p.a.); Provincia religiosa di San Pietro dell'Ordine Ospedaliero di San Giovanni di Dio – Fatebenefratelli; Azienda Ospedaliero-Universitaria Policlinico Umberto I; Azienda Regionale Emergenza Sanitaria ARES 118; Istituto Figlie di San Camillo; Ospedale Pediatrico Bambino Gesù; European Hospital S.p.a.; Eurosanità S.p.a.; Fondazione Policlinico Universitario Agostino Gemelli IRCCS; Associazione dei Cavalieri Italiani del Sovrano Militare Ordine di Malta; Ospedale San Carlo di Nancy GVM Care & Research S.r.l.; Università Campus Bio-Medico di Roma; Ospedale Israelitico; Virginia Bracelli S.p.a.; Istituto nazionale per la promozione della salute delle popolazioni migranti e per il contrasto delle malattie della povertà; Casa di Cura Sant'Anna - Policlinico Città di Pomezia S.p.a.

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”.

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.

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 1° luglio 2021 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 26 e il 29 novembre 2021".

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”.

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)”;

“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”;

“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”;

“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”;

“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 La documentazione relativa alla violazione

Con riferimento alla documentazione sulle violazioni dei dati personali occorse, tenuta ai sensi dell'art. 33, par. 5, del Regolamento, la Società ha rappresentato che "mantiene un registro degli incidenti di sicurezza occorsi ai fini della certificazione ISO 27001, che è utilizzato anche per registrare le violazioni dei dati personali" e ha fornito un estratto del predetto registro relativo all'incidente di sicurezza verificatosi a fine luglio 2021 e alcuni documenti attestanti le azioni intraprese a seguito della violazione dei dati personali occorsa.

Inoltre, la Società ha evidenziato che "come previsto sia dalle procedure ISO 27001 che dal sistema privacy, è stato attivato un tavolo tecnico i cui risultati, unitamente ai report prodotti dalle varie strutture coinvolte (non ultime quelle del consulente Leonardo e la struttura interna di Sicurezza Informatica ed architetture infrastrutturali, già fornite a Codesta Autorità), sono state portate all'attenzione degli organi aziendali (CdA e OdV) da parte del Presidente. Tali comunicazioni sono state effettuate nel corso di tutta l'istruttoria interna prima verbalmente e per mail nel corso dell'immediatezza e poi per iscritto con note firmate digitalmente dal Presidente della Società in data XX e XX. A detti rapporti sono stati allegati gli esiti di tutte le attività, la documentazione delle violazioni riscontrate e le valutazioni svolte ivi comprese i correttivi e le azioni di rimedio da porre in essere. In particolare, nell'ultima relazione dell'XX sono state riportate le valutazioni finali della Società in ordine alla violazione riscontrata con riferimento ai rischi per la tutela dei diritti degli interessati".

1.4 Le informazioni sulla violazione fornite ai titolari 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".

Con riferimento alla Regione Lazio, la Società ha rappresentato di aver inviato alla stessa tre comunicazioni:

con nota del XX, inviata in riscontro a una richiesta della Regione del XX, ha fornito alcuni "chiarimenti ed informazioni utili riguardanti l'incidente informatico occorso al Data Center della Regione Lazio nella notte tra il 31 Luglio ed il 1 Agosto", evidenziando che "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" e che "tutti gli altri servizi ed 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"; la 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"; LAZIOcrea ha infine evidenziato 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 la nota del XX, inviata in riscontro a una richiesta della Regione del XX, ha fornito "informazioni in ordine all'elenco delle applicazioni, dei trattamenti, delle categorie degli interessati, delle tipologie di dati e delle date di prevista riattivazione", confermando che "non è occorsa alcuna compromissione dei dati gestiti dagli applicativi e dai sistemi in esercizio in termini di integrità e riservatezza";

con la nota del XX, ha informato la Regione 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".

Con riferimento agli altri titolari del trattamento coinvolti, 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 31 luglio 2021/1 agosto 2021", "comunicate 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 correttivi 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 31 luglio 2021/1 agosto 2021", 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 le note del XX e del XX (quest'ultima inviata solo alla Casa di Cura Sant'Anna - Policlinico Città di Pomezia S.p.a.), 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 chiedere alla Società informazioni al riguardo. In particolare:

l'Azienda Sanitaria Locale Roma 2, con nota del XX, ha chiesto alla Società di "ricevere […], nel più breve tempo possibile, apposita relazione che descriva almeno la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione; le probabili cause e conseguenze della violazione dei dati personali; le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi; nonché […] i dati di contatto del Vostro responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni" (v. notifica dell'azienda del XX) e, con successiva nota del XX, ha sollecitato la trasmissione di un "report conclusivo completo della violazione";

l'Azienda Sanitaria Locale Roma 3, 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";

l'Azienda Sanitaria Locale Roma 4, con nota dell'XX, ha chiesto alla Società "quali e quanti dati personali afferenti agli interessati/pazienti/utenti della scrivente Azienda sono stati, ed in quale modo, coinvolti nel data breach. La scrivente Azienda ha già inoltrato una comunicazione preventiva e cautelare al Garante per la Protezione dei Dati Personali in relazione al sinistro privacy occorso; tuttavia, la richiamata comunicazione necessiterebbe di puntuali indicazioni — come previste dal GDPR e dal Codice Privacy — che ci si è riservati di specificare a seguito del Vostro riscontro alla presente. Infatti, la notizia del data breach in oggetto ha reso quest'ultimo "fatto noto" ma non è dato, ancora, sapere le reali dinamiche in relazione all'attacco cyber e gli effetti subiti. Pertanto, laddove gli accertamenti fossero ancora in corso, eppur comprendendo il momento di emergenza, Vi chiediamo comunque di notiziarci per quanto già accertato e di aggiornarci per quanto ancora verrà accertato in seguito";

l'Azienda Sanitaria Locale Roma 5, con nota dell'XX, ha chiesto alla Società "quali e quanti dati personali afferenti agli interessati/pazienti/utenti della scrivente Azienda sono stati, ed in quale modo, coinvolti nel data breach. La scrivente Azienda ha già inoltrato una comunicazione preventiva e cautelare al Garante per la Protezione dei Dati Personali in relazione al sinistro privacy occorso; tuttavia, la richiamata comunicazione necessiterebbe di puntuali indicazioni — come previste dal GDPR e dal Codice Privacy — che ci si è riservati di specificare a seguito del Vostro riscontro alla presente legalmail. Infatti, la notizia del data breach in oggetto ha reso quest'ultimo "fatto noto" ma non è dato, ancora, sapere le reali

dinamiche in relazione all'attacco cyber e gli effetti subiti. Pertanto, laddove gli accertamenti fossero ancora in corso, eppur comprendendo il momento di emergenza, Vi chiediamo comunque di notiziarci per quanto già accertato e di aggiornarci per quanto ancora verrà accertato in seguito";

l'Azienda Sanitaria Locale Roma 6, con nota del XX, ha chiesto alla Società di "fornire, nel più breve tempo possibile, apposita relazione che descrivesse con il maggior livello di dettaglio possibile, almeno la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati coinvolti nonché le categorie e il numero approssimativo di registrazioni dei dati personali; le probabili cause e conseguenze della violazione dei dati personali; le misure adottate o di cui si proponeva l'adozione per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi", nonché "i dati di opportuno punto di contatto presso cui ottenere più informazioni";

l'Azienda Sanitaria Locale Rieti, con nota del XX, ha chiesto alla Società di "ricevere […], nel più breve tempo possibile, apposita relazione che descriva almeno la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione; le probabili cause e conseguenze della violazione dei dati personali; le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi; nonché […] i dati di contatto del Vostro responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni" (v. notifica dell'azienda del XX) e, con successiva nota del XX, ha sollecitato la trasmissione di un "report conclusivo completo della violazione";

l'Azienda Ospedaliero-Universitaria Sant'Andrea, con nota del XX, ha chiesto alla Società di "fornire, nel più breve tempo possibile, apposita relazione che descrivesse con il maggior livello di dettaglio possibile, almeno la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati coinvolti nonché le categorie e il numero approssimativo di registrazioni dei dati personali; le probabili cause e conseguenze della violazione dei dati personali; le misure adottate o di cui si proponeva l'adozione per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi", nonché "i dati di opportuno punto di contatto presso cui ottenere più informazioni";

l'Azienda Ospedaliera San Camillo Forlanini, con nota del XX, ha chiesto alla Società una "relazione sulla violazione in oggetto";

la Fondazione PTV Policlinico Tor Vergata, con nota del XX, ha chiesto alla Società di "fornire, nel più breve tempo possibile, apposita relazione che descrivesse con il maggior livello di dettaglio possibile, almeno la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati coinvolti nonché le categorie e il numero approssimativo di registrazioni dei dati personali; le probabili cause e conseguenze della violazione dei dati personali; le misure adottate o di cui si proponeva l'adozione per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi", nonché "i dati di opportuno punto di contatto presso cui ottenere più informazioni";

l'European Hospital S.p.a., con PEC del XX, ha chiesto alla Società "ogni informazione necessaria per poter correttamente inquadrare la tipologia e la titolarità dei dati coinvolti nell'incidente, onde poter valutare se procedere o meno a notificare l'accaduto al Garante per la protezione dei dati personali e/o agli interessati", evidenziando come "allo stato delle informazioni da Voi fornite, la Struttura non sia nelle condizioni di poter valutare se

nell'incidente risultino coinvolti dati della quale la stessa sarebbe Titolare, potendoli scindere dunque dai dati che ricadrebbero nella titolarità di altri soggetti quali, ad esempio, Regione o ASL che, come a Voi noto, raccolgono spesso dati riferiti a prestazioni erogate dalle Strutture sanitarie senza però che ciò possa far attribuire tali dati alla titolarità delle Strutture stesse. Da tale sostanziale presupposto e dall'assoluta indisponibilità di ogni informazione circa la tipologia concreta di dati coinvolti, discende, peraltro, anche che la Struttura non possa nemmeno procedere ad alcuna valutazione circa l'effettivo rischio che avrebbe inciso su tali ipotetici dati. Da tutto quanto sopra esposto consegue che la Struttura non sia al momento nella condizione di poter valutare l'eventuale effettiva esigenza di procedere o meno a notificare l'accaduto al Garante per la protezione dei dati personali e/o agli interessati";

la Provincia religiosa di San Pietro dell'Ordine Ospedaliero di San Giovanni di Dio, con nota del XX, ha chiesto alla Società di "fornire tutte le notizie utili relative all'attacco informatico subito nel luglio del 2021, nonché di adottare tutte le procedure previste dall'art. 33 GDPR".

Oltre alla citata attività ispettiva effettuata nei confronti della Società, 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 che, sulla base della documentazione fornita dalla Società, risultavano coinvolti nella violazione dei dati personali.

Dalla documentazione in atti si evince che, a seguito dell'attacco informatico in esame, le predette strutture sanitarie hanno rappresentato di aver subito la temporanea indisponibilità di numerosi sistemi informativi attraverso i quali sono trattati dati sulla salute dei loro assistiti (es. sistemi deputati alle prenotazioni sanitarie, alla vaccinazione Covid-19, al teleconsulto, alla gestione delle attività trasfusionali, alla trasmissione referti radiologici). La mancata disponibilità di accesso ai dati conservati sui predetti sistemi, che configura una violazione dei dati personali, è stata, da un lato, una conseguenza diretta dell'attacco informatico (che, cifrando il contenuto di alcuni sistemi server, li ha resi indisponibili) e, dall'altro, una sua conseguenza indiretta derivante dalla scelta di LAZIOcrea di spegnere tutti i sistemi server nell'impossibilità di determinare quali fossero compromessi e, stante l'assenza di una loro segregazione, di evitare un'ulteriore propagazione del malware.

1.5 Il procedimento avviato da parte dell'Autorità

Sulla base di quanto sopra rappresentato, con nota del XX (prot. n. XX) l'Ufficio ha effettuato una notifica di violazione di cui all'art. 166, comma 5, del Codice a LAZIOcrea S.p.a. 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, par. 1, del Regolamento da parte della Società in relazione ai trattamenti effettuati in qualità di titolare;

in violazione degli obblighi di cui all'art. 33, par. 5, del Regolamento da parte della Società in relazione ai trattamenti effettuati in qualità di titolare;

in violazione degli obblighi di cui all'art. 33, par. 2, del Regolamento da parte della Società in relazione ai trattamenti effettuati in qualità di responsabile per conto dei titolari del trattamento;

in maniera non conforme al principio di "integrità e riservatezza", in violazione dell'art. 5, par. 1, lett. f), del Regolamento, da parte della Società in relazione ai trattamenti effettuati in qualità di titolare e di responsabile per conto di altri titolari;

in violazione degli obblighi in materia di sicurezza del trattamento, in violazione dell'art. 32 del Regolamento da parte della Società in relazione ai trattamenti effettuati in qualità di

titolare e di responsabile per conto di altri titolari;

in maniera non conforme al principio della “protezione dei dati fin dalla progettazione” di cui all’art. 25, par. 1, del Regolamento da parte della Società in relazione ai trattamenti effettuati in qualità di titolare.

Con nota del XX, la Società ha chiesto la proroga del termine per presentare le memorie difensive, che è stata concessa dall’Ufficio in ragione della dichiarata “complessità dei sistemi e dei servizi gestiti da LAZIOcrea per conto della Regione Lazio e degli altri titolari”.

Con nota del XX, la Società ha inviato le proprie memorie difensive, nell’ambito delle quali ha contestato – in via preliminare –il tardivo avvio del procedimento da parte dell’Autorità in quanto “dai documenti ricevuti in sede di accesso agli atti si evince che le ultime informazioni sono state acquisite dal Garante il XX. Anche tenuto conto della sospensione feriale, dunque, la Comunicazione andava effettuata entro il XX”.

Con la medesima nota, rispetto a quanto già indicato in atti, è stato ulteriormente evidenziato che:

“gli hacker hanno dovuto effettuare una complessa decodifica dei dump di memoria di un server per appropriarsi di un account con privilegi amministrativi a sua volta protetto da una password di ben 20 caratteri secondo le regole stabilite da LAZIOcrea in conformità agli standard di sicurezza considerati di livello alto anche dalle disposizioni AgID”;

“la prova che i dati dei cittadini non sono mai stati compromessi si rinviene non solo nella mancata esfiltrazione degli stessi, ma anche nel pronto ripristino delle applicazioni più importanti ed in particolare, degli strumenti di supporto alla vaccinazione e alla prenotazione delle prestazioni sanitarie”;

“LAZIOcrea S.p.A. risulta, perciò, iscritta nell’elenco delle amministrazioni pubbliche inserite nel conto economico consolidato5 individuate ai sensi dell’articolo 1, comma 3 della legge 31 dicembre 2009, n. 196 e ss.mm. (Legge di contabilità e di finanza pubblica). LAZIOcrea, quindi, pur essendo costituita nella forma della società per azioni è uno strumento di sussidiarietà della Regione per il perseguimento di finalità pubbliche finanziata, senza perseguire finalità di lucro, con i fondi del bilancio regionale secondo il criterio del mero rimborso dei costi sofferti”;

la contestazione circa la violazione degli obblighi di cui all’art. 33, par. 1, del Regolamento è infondata in quanto:

“LAZIOcrea è venuta a conoscenza dell’Incidente in seguito al malfunzionamento di alcuni sistemi applicativi regionali, ospitati sulle macchine virtuali contaminate. Detto malfunzionamento riguardava applicativi informatici utilizzati nell’ambito dei trattamenti delegati dalla Regione Lazio e, dunque, svolti dalla Scrivente in qualità di responsabile del trattamento […] LAZIOcrea era perfettamente al corrente che la Regione Lazio, in qualità di titolare del trattamento, stava tempestivamente effettuando la notifica all’Autorità di controllo […] con riferimento ai trattamenti di titolarità di LAZIOcrea, erano assenti sintomi di malfunzionamento […] Le indagini tecniche, al fine di verificare se vi fosse stata una violazione dei dati (di titolarità LAZIOcrea), potevano essere avviate solo dopo il completamento delle azioni propedeutiche al ripristino dei servizi regionali resi indisponibili in seguito al precauzionale isolamento del data center”;

“solo nel XX – dopo i fatti di cui si discute – è stata raccomandata dall’EDPB la notifica in caso di ransomware anche in casi di indisponibilità momentanea, pur senza esfiltrazione dei dati e in presenza di back-up (ma anche questa ipotesi – a stare all’esempio contenuto nelle nuove Linee Guida - se vi è comunque stata cifratura dei

dati personali da parte dell'attaccante, cifratura che nel nostro caso non c'è stata)";

"escluso che la notifica costituisca un formalismo fine a sé stesso (essendo piuttosto un adempimento funzionale all'eventuale intervento dell'Autorità nell'ambito dei suoi compiti e poteri come chiarisce il Considerando 87 del GDPR), l'Autorità era insomma perfettamente al corrente dell'evoluzione della situazione ben prima del 12 agosto, tanto da esercitare i propri poteri di richiesta di informazioni";

la contestazione circa la violazione degli obblighi di cui all'art. 33, par. 5, del Regolamento è infondata in quanto:

"la norma, pertanto, individua come finalità quella di documentare l'Incidente, lasciando in capo al titolare piena discrezionalità in merito alla forma e ai mezzi di tale adempimento";

"ha dimostrato di aver correttamente assolto a tale obbligo, indicando tutte le informazioni richieste dall'art. 33, par. 5 del GDPR all'interno delle molteplici e altamente descrittive relazioni tecniche (già acquisite dall'Autorità), redatte dalle funzioni interne e/o dai consulenti esterni che si sono occupati delle analisi forensi";

"si ritiene, pertanto, del tutto ininfluente rispetto alle finalità della disposizione (che pretende la documentazione e non una modalità formale di documentazione) che non tutte tali informazioni siano state incluse anche nel registro degli incidenti di sicurezza tenuto dalla società secondo la propria procedura interna di gestione delle violazioni. Né assume rilievo la circostanza che l'inserimento di dette informazioni all'interno del registro degli incidenti tenuto dalla società fosse richiesto dalla procedura interna per la gestione delle violazioni";

la contestazione circa la violazione degli obblighi di cui all'art. 33, par. 2, del Regolamento è infondata in quanto:

"non si vede quale utilità possa esservi in ulteriori comunicazioni formali da parte di LAZIOcrea, una volta perfettamente nota al responsabile l'esistenza della notifica da parte della Regione";

con riferimento agli altri enti del servizio sanitario regionale, "si tratta di processi operativi che, pur vedendo coinvolti anche attori diversi dalla Regione, hanno nella Regione il soggetto di raccordo e il centro decisionale. Si tratta perciò di strumenti informatici predisposti dalla Regione per il tramite di LAZIOcrea e per cui la stessa Regione mantiene un ruolo di vertice e di predisposizione delle risorse tecniche ed economiche";

"il malfunzionamento riguardava gli stessi sistemi utilizzati dalla Regione e non può ritenersi che gli enti del SSR non fossero informati dell'Incidente sin dal momento in cui è occorso. Ipotizzare che tali enti siano stati all'oscuro dell'Incidente sino al 12 agosto è francamente irrealistico. Del resto le stesse contestazioni della Comunicazione di Avvio riportano lettere di ASL o di ospedali che prima del 12 agosto (ASL Rieti il 5 agosto, ASL Roma 2, Sant'Andrea, Forlanini il 6 agosto, ad esempio) chiedevano informazioni sulle indagini effettuate in merito all'Incidente. Lettere siffatte non potrebbero spiegarsi se non alla luce di una già maturata conoscenza dell'Incidente. Vi è poi che tutti gli utilizzatori dei sistemi regionali hanno appreso immediatamente della indisponibilità dei sistemi, così come gli interessati, dalle schermate predisposte da LAZIOcrea in accordo con la Regione nel momento in cui un utente cercava di raggiungere sulla rete la specifica risorsa informatica (sia esso un sito web o un portale

intranet di accesso ad una applicazione)";

con riferimento, più in generale, alla contestazione circa la violazione del principio di cui all'art. 5, par. 1, lett. f), e degli obblighi di cui all'art. 32 del Regolamento:

"le misure di sicurezza adottate ed implementate da LAZIOcrea per garantire la protezione delle operazioni di trattamento fossero adeguate e perfettamente in linea con le misure di mitigazione definite a seguito dell'analisi del rischio al momento in cui le stesse erano state implementate nell'ambito di un corretto rapporto costi/benefici rispetto alle risorse economiche a disposizione e, dunque, nel rispetto dell'art. 32 che - non a caso - reca come incipit: "Tenendo conto dello stato dell'arte e dei costi di attuazione"";

"l'inaugurazione del nuovo Data Center regionale, resa possibile dagli investimenti comunitari e nazionali, è avvenuta ufficialmente in data 9 novembre 2019, proprio pochi mesi prima dello scoppio della pandemia. Il tema della sicurezza cibernetica è stato posto sin dall'inizio alla base del progetto di realizzazione del nuovo Data Center ed è stato fatto oggetto di un percorso di certificazione ISO 27001 al fine di verificare il rispetto degli standard di sicurezza per la tutela delle informazioni […] il percorso di certificazione del Sistema di Gestione della Sicurezza delle Informazioni (SGSI), riferito specificamente anche alla gestione dell'infrastruttura del Data Center ed all'erogazione dei servizi, si è concluso con la visita ispettiva dei giorni XX e con l'ottenimento della certificazione in data XX";

"l'Incidente di cui ci stiamo occupando è, se non esclusivamente, in gran parte addebitabile alla momentanea indisponibilità di una parte, ed in seguito alla messa in esecuzione delle procedure di sicurezza, di tutto il Data Center. Misura che si è resa necessaria per reagire all'attacco presidiato che gli hacker stavano conducendo sullo strato applicativo. L'indisponibilità temporanea di alcune applicazioni è stata impostata dagli operatori di LAZIOcrea per seguire corrette procedure di ripristino utilizzando le copie off-line dei back-up. Copie che sono state ripristinate temporaneamente su macchine virtuali attestate su CSP certificati AgID";

con riferimento, in particolare, alla contestazione circa la mancata adozione di misure adeguate a rilevare tempestivamente la violazione di dati personali:

"LAZIOcrea, già prima del GDPR aveva effettuato una valutazione sui rischi connessi ai trattamenti e si era dotata di un sistema di gestione degli eventi di sicurezza generati dagli apparati hardware, dai sistemi operativi e dalle applicazioni (Security Information and Event Management - SIEM) presenti nel Data Center. Il sistema SIEM utilizzato al momento della prima certificazione del 2020 si basava sul prodotto Q-Radar. L'analisi dei log prodotti dal SIEM era affidata ad un Security Operation Center interno composto dal personale della Società attivo in presenza durante l'orario lavorativo dal lunedì al venerdì dalle 8 alle 20 e con un presidio di reperibilità per il restante orario mancante a coprire le 24 ore";

"dalla lettura dell'Allegato B al POA per l'anno 2021 si evince come il servizio di implementazione del nuovo SOC H/24, seppur non ancora finanziato, fosse inserito come attività da finalizzare previa copertura entro la fine del secondo semestre 2021";

"pur non costituendo il SOC h24 una misura obbligatoria per le pubbliche amministrazioni, LAZIOcrea e la Regione hanno cooperato per accelerare la messa in operatività di un siffatto controllo a maggiore frequenza rispetto a quello esistente (e giudicato adeguato dal certificatore) prendendo anticipatamente contatto già nei primi

mesi del 2021 con il fornitore Leonardo S.p.A. per l'effettuazione delle analisi preliminari, la redazione del piano dei fabbisogni e la configurazione dell'ordinativo di fornitura a valere sulle Convenzioni Consip con l'impegno di formalizzare il tutto al momento dello stanziamento dei fondi da parte della Regione. Anticipando così ai primi mesi del secondo semestre del 2021 l'avvio operativo del nuovo SOC";

"benché l'Incidente sia avvenuto prima della 'messa a terra' del nuovo SOC, non si può tacciare di tardività il comportamento con cui Responsabile e Titolare hanno operato per aumentare la sicurezza dei sistemi col progredire delle tecnologie e degli strumenti a disposizione degli hacker. I tempi, comunque nel rispetto delle regole pubbliche di spesa, sono stati addirittura anticipati rispetto al percorso amministrativo ed operativo che l'agire della Pubblica Amministrazione normalmente richiede";

con riferimento, in particolare, alla contestazione circa la mancata adozione di misure adeguate a garantire la sicurezza delle reti:

"LAZIOcrea aveva posto in essere misure per segregare i sistemi presenti all'interno del Data Center, attestando i server che ospitano le diverse banche dati a reti segregate rispetto alle altre reti. È proprio grazie all'efficienza di tale segregazione che l'Attacco non ha coinvolto le basi dati conservate all'interno del data center. Analoghe misure di segregazione erano applicate ai server che erogano servizi particolarmente critici o dedicati a specifici clienti, quali i servizi essenziali relativi alle attività di emergenza del 112, del 118, dei centri trasfusionali, del Pronto Soccorso e della Protezione Civile, che non sono stati compromessi dall'attacco, in quanto segregati anche fisicamente rispetto alle altre applicazioni";

"il responsabile dei sistemi di rete che, quale diretto responsabile della funzione, dichiara e certifica l'esistenza già all'epoca dell'Attacco di configurazioni accorte delle regole di accesso e di segregazione delle reti tramite: (i) l'approntamento di diverse sottoreti logiche; (ii) un primo livello di regole di filtering per dividere le reti su cui sono attestate le postazioni di lavoro e quelle dove sono attestati i sistemi server; (iii) un secondo livello di regole di filtering per dividere il traffico delle comunicazioni da e verso il data center da quello delle comunicazioni tra le reti su cui sono attestati i sistemi server; (iv) regole di firewalling e filtering per dividere il traffico sulla base del contesto applicativo (front end, back-end, database); (v) reti dedicate e separate anche fisicamente rispetto agli altri sistemi. Sulla segregazione delle basi dati abbiamo già detto. A ciò devono aggiungersi le regole dei concentratori VPN che applicavano privilegi e regole di accesso diverse in base ai gruppi di dominio ai quali l'utente apparteneva";

"non si può quindi sostenere che non esistessero delle "adeguate" regole di accesso e filtraggio delle comunicazioni e delle reti. Peraltro, qualora le reti non fossero state correttamente configurate e architetturalmente strutturate, le conseguenze dell'Attacco sarebbero state molto più rilevanti con un impatto di livello più che elevato sui diritti e le libertà degli interessati. Infatti, gli hacker avrebbero facilmente avuto accesso ai database contenti i dati personali, come purtroppo è avvenuto in tanti altri attacchi che sono stati sferrati in periodi successivi a quello dell'Incidente che ci occupa";

con riferimento, in particolare, alla contestazione circa l'obsolescenza dei software di base istallati su alcuni sistemi di trattamento:

"il sistema operativo obsoleto che ha facilitato l'attacco è Windows Server 2008 R2 Standard, per cui non erano più disponibili aggiornamenti di sicurezza da parte del produttore. Tale sistema non era immediatamente visibile dalla rete internet (non era

un servizio esposto ma richiamato da altre applicazioni) perché utilizzato solo come servizio interno al dominio dei sistemi accessibili. L' accesso era possibile solo dopo aver superato la barriera attuata dalla VPN. Tale sistema era installato ed utilizzato per la gestione dei progetti di edilizia scolastica della Regione Lazio. Si trattava di un sistema sviluppato su un linguaggio di programmazione ed una piattaforma oramai obsoleta e non disponibile per i sistemi operativi server più recenti. L'applicazione, che per lo più riguardava comunque l'utilizzo di dati comuni (non certamente dati personali dei cittadini), avrebbe dovuto essere completamente riscritta e progettata utilizzando nuove piattaforme";

"le tempistiche relative all'adozione e implementazione di nuove tecnologie da parte delle pubbliche amministrazioni, che agiscono all'interno di uno specifico quadro normativo di riferimento, non sempre risultano compatibili con le esigenze di continuità dei servizi. Attività per cui al momento non c'era disponibilità di alcun finanziamento regionale";

con riferimento, in particolare, alla contestazione circa la mancata adozione di misure adeguate ad assicurare la disponibilità e la resilienza dei sistemi e dei servizi di trattamento:

"in realtà, se LAZIOcrea successivamente all'Incidente ha effettuato interventi migliorativi, dotandosi di nuove procedure di back up, ciò non significa che la gestione dei back up implementata al momento dell'Incidente fosse inadeguata, e men che meno che non esistessero back up. I back up, come vedremo, risultavano perfettamente funzionanti, altrimenti, non sarebbe nemmeno stato possibile reinstallare ex novo, in tempi brevi, gli applicativi coinvolti nell'Incidente";

"LAZIOcrea ha valutato che il sistema di backup fosse adeguato a garantire la disponibilità e la resilienza dei sistemi assolvendo efficientemente al compito di conservazione e recupero dei dati. L'ente certificatore anche su questo punto non ha individuato criticità con riferimento al sistema di backup, che perciò era da ritenersi adeguato, pur nella consapevolezza di attuare le osservazioni di miglioramento indicate, come già detto, dall'ente certificatore nel suo rapporto di Audit del 24-26 novembre 2020";

con riferimento, in particolare, alla contestazione della violazione del principio di cui all'art. 25, par. 1, del Regolamento:

"si tratta di contestazione evidentemente irrituale in quanto l'Autorità non ha descritto i fatti, intesi come le azioni od omissioni ascrivibili alla Società, dai quali sarebbe derivata l'asserita violazione del citato precetto normativo";

"vale a riguardo osservare che l'art. 25, par. 1 GDPR contiene una fattispecie distinta da quella di cui all'art. 32. Si riferisce alla progettazione del trattamento che deve essere impostata dal titolare in maniera da minimizzare i rischi per i diritti e le libertà dell'interessato. Una cosa è la mancata adozione di misure di sicurezza adeguate, altra cosa è la progettazione di un trattamento in maniera irrispettosa dei diritti e delle libertà delle persone fisiche. Non a caso sinora l'applicazione dell'art. 25 ha riguardato situazioni ben diverse da un data breach (noti sono i casi dei trattamenti di geolocalizzazione forniti dai datori di lavoro su vetture aziendali non progettati in maniera da essere disattivati non appena finito l'orario di lavoro) in cui non erano stati selezionati i soli dati pertinenti, adeguati e limitati a quanto necessario per il raggiungimento della finalità del trattamento";

"i comportamenti che in ipotesi violerebbero l'art. 25 devono avere una loro precipua

indicazione che l'Autorità contestante deve ritualmente illustrare in un procedimento sanzionatorio. La preventiva contestazione dell'addebito appartiene al nucleo irriducibile delle garanzie del contraddittorio endo-procedimentale, il cui mancato rispetto, da parte dell'Amministrazione procedente, provoca ex se, l'illegittimità del provvedimento sanzionatorio eventualmente emesso e ne impone l'annullamento nel giudizio di opposizione dinanzi all'autorità giurisdizionale competente (cfr. Cass. civ, Sez. 2 -Sentenza n. 4521 del 11/02/2022)";

in merito agli elementi per le valutazioni di cui all'art. 83, par. 2, del Regolamento:

"l'Incidente, non ha comportato violazioni alla integrità e alla riservatezza di dati personali meno che mai di quelli appartenenti ai cittadini della regione Lazio. […] l'Incidente, infatti: • non ha comportato alcuna esfiltrazione di dati personali • non ha comportato alcuna perdita di dati personali • non ha comportato alcuna cifratura di dati personali • non ha comportato alcuna lesione alla riservatezza e all'integrità di dati personali • è stato risolto con tempestività grazie all'esistenza di adeguati back up […] l'unico effetto concreto che l'Incidente ha avuto nei confronti degli interessati ha riguardato la temporanea indisponibilità di alcuni servizi regionali a seguito della disattivazione dei relativi applicativi, effetto che a ben vedere è estraneo agli interessi pubblici alla protezione dei dati personali cui codesta Autorità sovraintende";

"nessun elemento di colpevolezza è a sé ascrivibile considerato quanto sopra illustrato in merito alla certificazione delle misure di sicurezza e alla massima tempestività con cui sono stati adottati i suggerimenti del certificatore, nonché in merito alla perfetta conoscenza da parte di LAZIOcrea dell'esistenza della notificazione della Regione";

"per attenuare il danno subito LAZIOcrea, dal momento dell'Attacco, ha reagito, - come illustrato sopra – disattivando immediatamente i sistemi e riavviando il Data Center in piena sicurezza. […] Il Data Center risulta oggi anche accreditato presso l'ACN ai più alti livelli di sicurezza informatica. Tutte le certificazioni sono riscontrabili sul sito dell'ente di accreditamento al seguente link https://services.accredia.it/. Infine, LAZIOcrea ha potenziato la struttura privacy interna con un maggior presidio sulla tematica e la nomina di un nuovo DPO";

la "società non è stata, in passato, oggetto di contestazioni o destinataria di provvedimenti correttivi di codesta Autorità";

la "società ritiene di aver tenuto nel corso di tutte le attività istruttorie fin qui svolte dalla stessa, un atteggiamento pienamente collaborativo e trasparente sin dal momento dell'Incidente avvenuto il 1° agosto, coinvolgendo un numero consistente di risorse (responsabili di funzione, tecnici, consulenti esterni) e mettendo a disposizione in maniera assolutamente trasparente ogni informazione necessaria nel contesto dell'istruttoria";

"LAZIOcrea non opera per finalità di lucro e che le somme ricevute dalla Regione sono esclusivamente a valere sulla contabilità pubblica quale rimborso dei costi sofferti. È addirittura discutibile che possa considerarsi impresa commerciale ai fini dei criteri di misurazione dei vantaggi economici di cui alla disposizione della lett. k). In questa prospettiva LAZIOcrea non ha goduto di alcun beneficio economico in ragione dell'eventuale "risparmio"".

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);

in virtù del richiamato principio di “integrità e riservatezza” (art. 5, par. 1, lett. f), del Regolamento), il titolare deve (cfr. le “Linee guida 4/2019 sull’articolo 25 - Protezione dei dati fin dalla progettazione e per impostazione predefinita”, adottate dal Comitato europeo per la protezione dei dati – di seguito “Comitato” – il 20 ottobre 2020, spec. punto 85):

> valutare i rischi per la sicurezza dei dati personali, considerando l’impatto sui diritti e le libertà degli interessati, e contrastare efficacemente quelli identificati;
>
> tenere conto non appena possibile dei requisiti di sicurezza nella progettazione e nello sviluppo del sistema, integrando e svolgendo costantemente test pertinenti;
>
> definire il trattamento dei dati in modo tale che un numero minimo di persone abbia bisogno di accedere ai dati personali per svolgere le proprie funzioni, e limitare l’accesso di conseguenza;
>
> proteggere i dati personali da modifiche e accessi non autorizzati e accidentali, sia durante il loro trasferimento che durante la loro conservazione;
>
> registrare gli eventi rilevanti ai fini della sicurezza delle informazioni e monitorandoli per rilevare in modo tempestivo eventuali incidenti di sicurezza;
>
> garantire il ripristino dei sistemi informatici in caso di disastro e la continuità operativa, assicurando la disponibilità dei dati personali a seguito di incidenti di sicurezza rilevanti;
>
> disporre di adeguate procedure per gestire le violazioni dei dati personali, comprese procedure per la loro documentazione;

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 il 28 marzo 2023, evidenziano che “un incidente di sicurezza che determina l’indisponibilità dei dati personali per un certo periodo di tempo costituisce una violazione, in quanto la mancanza di accesso ai dati può

avere un impatto significativo sui diritti e sulle libertà delle persone fisiche" (sez. I.B.2);

le medesime Linee guida ricordano 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 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);

l'art. 33, par. 2, del Regolamento stabilisce che "il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione". Al riguardo, le Linee guida sulla notifica chiariscono che "se il titolare del trattamento ricorre a un responsabile del trattamento e quest'ultimo viene a conoscenza di una violazione dei dati personali che sta trattando per conto del titolare del trattamento, il responsabile del trattamento deve notificarla al titolare del trattamento "senza ingiustificato ritardo" [… senza] valutare la probabilità di rischio derivante dalla violazione prima di notificarla al titolare del trattamento". Pertanto, "il responsabile del trattamento deve soltanto stabilire se si è verificata una violazione e quindi notificarla al titolare del trattamento" per consentire a quest'ultimo "di far fronte alla violazione e di stabilire se deve notificarla all'autorità di controllo ai sensi dell'articolo 33, paragrafo 1, e alle persone fisiche interessate ai sensi dell'articolo 34, paragrafo 1". Anche se "il regolamento non fissa un termine esplicito entro il quale il responsabile del trattamento deve avvertire il titolare del trattamento, salvo specificare che deve farlo "senza ingiustificato ritardo"" le predette Linee guida raccomandano al responsabile del trattamento di "effettuare la notifica al titolare del trattamento tempestivamente, fornendo successivamente le eventuali ulteriori informazioni sulla violazione di cui venga a conoscenza. Ciò è importante al fine di aiutare il titolare del trattamento a soddisfare l'obbligo di notifica all'autorità di controllo entro 72 ore" e specificano che "qualora fornisca servizi a più titolari del trattamento tutti interessati dal medesimo incidente, il responsabile del trattamento dovrà segnalare i dettagli dell'incidente a ciascun titolare del trattamento" (sez. II.B.1);

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);

art. 25, par. 1, del Regolamento prevede che "tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento [debba mettere] in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati" (cfr. anche cons. 75 e 78 del Regolamento);

sulla base del richiamato principio della "protezione dei dati fin dalla progettazione", i titolari dovrebbero effettuare revisioni periodiche delle misure di sicurezza poste a presidio e tutela dei dati personali, nonché della procedura per la gestione delle violazioni dei dati. L'obbligo di mantenere, verificare e aggiornare, ove necessario, il trattamento si applica anche ai sistemi preesistenti. Ciò implica che i sistemi progettati prima dell'entrata in vigore del Regolamento devono essere sottoposti a verifiche e manutenzione per garantire l'applicazione di misure e garanzie che mettano in atto i principi e i diritti degli interessati in

modo efficace. Tale obbligo si estende anche ai trattamenti svolti per mezzo di un responsabile del trattamento. Infatti, le operazioni di trattamento effettuate da un responsabile dovrebbero essere regolarmente esaminate e valutate dal titolare per garantire che continuino a rispettare i principi e permettano al titolare di adempiere gli obblighi previsti dal Regolamento (cfr. le citate "Linee guida 4/2019 sull'articolo 25 - Protezione dei dati fin dalla progettazione e per impostazione predefinita", spec. punti 7, 38, 39 e 84).

Preso atto di quanto rappresentato dalla Società nella documentazione in atti e nelle memorie difensive, si osserva che:

con riferimento alla contestata tardività dell'avvio del procedimento da parte dell'Autorità si evidenzia che, contrariamente a quanto asserito dalla Società, l'Ufficio ha notificato lo stesso nei termini di legge (XX) atteso che l'acquisizione di alcune informazioni rilevanti ai fini di una compiuta valutazione della conformità del complesso dei trattamenti in esame è stata completata soltanto nel mese di XX; ciò, anche in considerazione del fatto che l'istruttoria in esame presenta profili di particolare complessità, anche di natura tecnologica, con riferimento ai quali è stata fornita copiosa documentazione, e ha riguardato circa 35 soggetti coinvolti a vario titolo nel trattamento;

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

la Società è venuta a conoscenza della violazione il 1° agosto 2021 e ha notificato la medesima solo in data XX, evidenziando che il ritardo era dipeso "(i) dalla necessità di acquisire gli elementi minimi necessari per dare una informazione quanto più compiuta possibile (ii) dalla esigenza di ripristinare primariamente i servizi essenziali al cittadino della Regione Lazio e (iii) di appurare con la collaborazione di società di cyber security e con le Autorità di polizia giudiziaria l'effettiva portata dell'incidente";

le motivazioni addotte non consentono di giustificare il ritardo nella notifica della violazione dei dati personali poiché, pur non disponendo di tutte le informazioni di cui all'art. 33, par. 3, del Regolamento, la Società, con riferimento ai trattamenti di cui è titolare, avrebbe dovuto notificare la violazione entro 72 ore dal momento in cui ne era venuta a conoscenza, fornendo le informazioni di cui era in possesso e avvalendosi della facoltà di procedere con una "notifica per fasi";

considerato quanto precisato nelle memorie difensive prodotte dalla Società, nel condividere che la notifica non costituisce "un formalismo fine a sé stesso", la stessa rappresenta il principale mezzo attraverso il quale l'Autorità viene prontamente messa a conoscenza di una violazione dei dati personali e, quindi, nella condizione di esercitare i compiti previsti dal Regolamento; nel caso di specie, invece, il Garante ha agito d'ufficio a seguito di notizie stampa in merito ai fatti in esame e della ricezione delle notifiche presentate da altri titolari del trattamento coinvolti;

considerato quanto asserito dalla Società nelle memorie difensive circa il fatto che "solo nel dicembre 2021 – dopo i fatti di cui si discute – è stata raccomandata dall'EDPB la notifica in caso di ransomware anche in casi di indisponibilità momentanea, pur senza esfiltrazione dei dati e in presenza di back-up", già nel 2017, le "Linee guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679" del Gruppo di Lavoro Articolo 29 per la Protezione dei Dati del 3 ottobre 2017 – di recente sostituite dalle Linee guida sulla notifica del Comitato – chiarivano che "un incidente di sicurezza che determina l'indisponibilità dei dati personali per un certo periodo di tempo costituisce una violazione, in quanto la mancanza di accesso ai dati può avere un impatto significativo sui diritti e sulle libertà delle persone fisiche", richiedendo in tal caso la notifica all'autorità di controllo;

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

la Società non ha provveduto a documentare adeguatamente la violazione. In particolare, nel registro degli incidenti di sicurezza tenuto dalla Società, in relazione all'incidente del 31 luglio 2021, non sono inserite tutte le informazioni ivi previste (es. data e ora di chiusura dell'incidente, data e ora di risoluzione dell'incidente, soggetto che ha rilevato l'incidente, altre Organizzazioni contattate), e alcune di quelle presenti risultano inesatte (es. data di inizio dell'incidente) o poco dettagliate (es. descrizione dell'incidente, azioni di risposta effettuate);

anche tenendo conto di quanto affermato nelle memorie difensive, la documentazione in atti risulta priva delle informazioni chiave indicate nelle Linee guida sulla notifica quali, a esempio, gli effetti e le conseguenze della violazione per gli interessati, il ragionamento alla base delle decisioni prese, la valutazione del rischio derivante dalla violazione, nonché i motivi a giustificazione del ritardo nella notifica al Garante. Peraltro, tale comportamento non risulta pienamente in linea anche con quanto indicato nella procedura "Gestione delle violazioni - Data Breach" adottata dalla Società, che prevede la tenuta di un registro degli eventi in cui annotare le informazioni relative alle segnalazioni delle presunte violazioni (es. data della comunicazione, descrizione dell'evento, tipologia di dati personali coinvolti, estremi notifica al Garante, misure di contenimento, classificazione, stato) e la compilazione di un rapporto di analisi, da allegare al predetto registro, contenente anche il parere degli specialisti e la valutazione del rischio;

con riferimento alla violazione degli obblighi di cui all'art. 33, par. 2, del Regolamento:

la Società, venuta a conoscenza della violazione il 1° agosto 2021, nella sua qualità di responsabile del trattamento, ha informato tardivamente:

- la Regione Lazio con le comunicazioni del XX e del XX a seguito di specifiche richieste da parte della medesima Regione (rispettivamente del XX e del XX) e del XX, a conclusione delle attività di rispristino;

- gli altri titolari del trattamento coinvolti con le comunicazioni del XX, del XX, del XX e del X;

la Società ha informato la Regione e gli altri titolari del trattamento coinvolti – anche a seguito di specifiche richieste di informazioni inviate da questi, peraltro riscontrate in modo non tempestivo – a distanza di circa 2 settimane dal momento in cui si è verificato l'incidente. Al riguardo, si ritiene che la Società, pur non disponendo di informazioni dettagliate durante le prime fasi di gestione dell'incidente, avrebbe dovuto comunque informare tempestivamente i titolari fornendo loro gli elementi di cui era a conoscenza, al fine di consentire ai medesimi titolari di valutare i rischi per i diritti e le libertà delle persone fisiche derivanti dalla violazione e di adempiere gli obblighi di cui agli artt. 33 e 34 del Regolamento;

come chiaramente rilevabile dalla documentazione in atti, anche le successive comunicazioni della Società ai titolari sono state inviate a distanza di tempo e quelle indirizzate ai titolari del trattamento diversi dalla Regione, oltre a informazioni di carattere generale sulla violazione dei dati personali (natura, misure adottate o in corso di adozione con relative tempistiche), non contenevano neanche specifici riferimenti ai sistemi e servizi di trattamento coinvolti, utili a ciascun titolare per circoscrivere il perimetro della violazione e valutarne i rischi; la Società non ha fornito adeguate giustificazioni in ordine ai motivi dei predetti ritardi;

non può ritenersi ammissibile quanto sostenuto dalla Società nelle memorie difensive in ordine alla inutilità di “ulteriori comunicazioni formali da parte di LAZIOcrea” ai titolari del trattamento in quanto già informati sui fatti, poiché, in casi come quello in esame, spetta proprio al responsabile fornire loro i dettagli dell’incidente; tanto è vero che la maggior parte dei titolari, in assenza di comunicazioni da parte della Società, ha sentito la necessità di chiedere a quest’ultima specifiche informazioni sulla violazione;

con riferimento alla violazione del principio di cui all’art. 5, par. 1, lett. f), e degli obblighi di cui all’art. 32 del Regolamento:

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, anche sulla salute, di milioni di interessati assistiti. Ciò, tenendo altresì conto delle finalità dei trattamenti e della natura dei dati personali trattati, appartenenti anche a categorie particolari. Su tale base, gli obblighi di sicurezza imposti dal Regolamento richiedono l’adozione di rigorose misure tecniche e organizzative, includendo, oltre a quelle espressamente individuate dall’art. 32, par. 1, lett. da a) a d), tutte quelle necessarie ad attenuare i rischi che i trattamenti presentano;

in generale, con riferimento alle ricorrenti argomentazioni fondate sul possesso, da parte della Società, della certificazione del sistema di gestione per la sicurezza delle informazioni (SGSI) in conformità alla norma UNI CEI EN ISO/IEC 27001:2017, con estensione ai controlli della ISO 27017 e ISO 27018, si evidenzia che tale certificazione non rientra, al momento, tra quelle previste dall’art. 42 del Regolamento. In ogni caso, la certificazione ai sensi dell’art. 42 del Regolamento, seppur possa essere utilizzata, da titolari o responsabili, come elemento per dimostrare il rispetto degli obblighi del Regolamento, non ne implica automaticamente il rispetto. Inoltre, occorre considerare che la certificazione di un SGSI può essere limitata a specifici ambiti (servizi e/o sedi) dell’organizzazione (riportati sinteticamente nel certificato rilasciato dall’organismo di certificazione) e che il processo di certificazione di un SGSI, basato principalmente sui risultati degli audit (verifiche documentali e sul campo), contiene elementi di incertezza sia perché legato al concetto di rischio sia perché svolto su un campione dei processi che l’organizzazione, ferma restando la sua buona fede, sottopone a certificazione. La certificazione di un SGSI basato sulla ISO/IEC 27001, quindi, non garantisce, di per sé, livelli di sicurezza, controlli o misure di sicurezza stabiliti o fissati a priori, ma assicura l’adozione dei controlli che l'organizzazione ha identificato e ritenuto adeguati sulla base di una propria valutazione del rischio;

sulla mancata adozione di misure adeguate a rilevare tempestivamente la violazione di dati personali:

- il 31 luglio 2021, dalle ore 16:49 i soggetti malintenzionati hanno effettuato una serie di operazioni propedeutiche all’attacco informatico, a seguito delle quali, alle ore 21:12, “le piattaforme di sicurezza Microsoft generavano un incidente di sicurezza di severity High denominato Multi-stage incident involving Execution & Command and control on multiple endpoints reported by multiple sources, composto da un totale di 2189 allarmi. L’incidente segnalava la rilevazione, su molteplici sistemi, di attività malevole”. Dalle ore 00:00 del 1° agosto 2021 è stata “avviata la routine di cifratura dei sistemi”;

- la Società ha avuto “evidenza nelle prime ore della mattina del 1° agosto quando alcune macchine virtuali sono risultate inutilizzabili”; al riguardo, la stessa ha dichiarato che “a seguito del rilevamento di “attività ostili” (2.189 allarmi) da parte della “console

Microsoft Windows Defender ATP" nella serata del 31 luglio 2021, […] tale strumento di monitoraggio non era presidiato H24" e, pertanto, "non si è potuto gestire tali allarmi con "maggiore" tempestività"". Ciò anche in quanto 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" (v. verbali del XX, pp. 5 e 6, e del XX, p. 2);

- risulta, pertanto, accertato che l'inadeguata gestione dei predetti allarmi non ha consentito alla Società di venire tempestivamente a conoscenza della violazione dei dati personali occorsa; al riguardo, non rileva, infatti, quanto sostenuto dalla Società nelle memorie difensive in ordine alla circostanza che "il SOC h24 [non costituisse] una misura obbligatoria per le pubbliche amministrazioni", in quanto, sotto il profilo della protezione dei dati, il Regolamento, in ossequio al principio di responsabilizzazione, demanda al titolare e al responsabile il compito di individuare e adottare misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato ai rischi presentati dai trattamenti, che nel caso di specie risultavano elevati in ragione della natura dei dati trattati, della larga scala degli interessati, anche vulnerabili, coinvolti, nonché, in caso di violazione, delle possibili conseguenze negative nei confronti degli interessati con particolare riferimento all'esercizio del diritto all'accesso alle cure sanitarie;

con riguardo alla mancata adozione di misure adeguate a garantire la sicurezza delle reti:

- la Società non aveva adottato adeguate misure per segmentare e segregare le reti su cui erano attestate le postazioni di lavoro dei propri dipendenti, quelle dei dipendenti della Regione Lazio, nonché i sistemi (server) utilizzati per i trattamenti effettuati in qualità di responsabile (per conto dei diversi titolari) o di titolare. In particolare, le regole di filtering configurate sui sistemi firewall presenti nel data center gestito dalla Società, limitate solo a specifici sistemi o servizi critici, non hanno impedito la propagazione del malware su circa 180 sistemi;

- nell'ambito delle attività di analisi condotte da Leonardo S.p.a. in relazione alla violazione dei dati personali in esame, è stato definito un "Mitigation, Eradication & Improvement Plan" (di seguito "Piano") che prevede l'adozione, tra le altre, di specifiche azioni volte alla segregazione e messa in sicurezza dei diversi sistemi gestiti dalla Società. In particolare, tali azioni prevedono la "segmentazione delle reti evitando subnet eccessivamente ampie e limitando, di fatto, la possibilità per un potenziale attaccante di eseguire movimenti laterali", la "reinstallazione completa di tutti i sistemi server e contestuale posizionamento in segmenti di rete suddivisi per layer di sicurezza (Tier), ad accesso limitato e amministrabili solo da un numero limitato di workstation, a loro volta isolate dalle altre reti (PAW, Privileged Access Workstation)", nonché la "riprogettazione della network […] favorendo il principio del privilegio minimo";

- peraltro, al momento in cui si è verificata la violazione dei dati personali, l'accesso remoto, tramite VPN, alla rete della Società, avveniva mediante una procedura di autenticazione informatica basata solo sull'utilizzo di username e password. In relazione a tale aspetto, la stessa Società, a seguito dell'incidente ha ritenuto necessario attivare una procedura con doppio fattore di autenticazione (cfr. verbale del XX, p. 3), come previsto anche dal predetto Piano;

- quanto sostenuto dalla Società nelle memorie difensive non consente di superare le criticità rilevate nell'atto di avvio del procedimento in quanto, come dichiarato dalla

stessa Società nel corso dell'accertamento ispettivo, al momento della violazione, era possibile raggiungere i sistemi server, che sono poi stati compromessi, a partire dalla rete utilizzata per l'accesso VPN dei dipendenti della Regione Lazio;

con riguardo all'obsolescenza dei software di base istallati su alcuni sistemi di trattamento:

- dalla documentazione in atti è emerso che il server con hostname "RLWSIRIFT01" è stato "uno dei principali punti di snodo utilizzati dall'attaccante nella fase finale dell'attacco" informatico alla base della violazione dei dati personali in esame. La stessa Società ha evidenziato che sul "server con hostname "RLWSIRIFT01" […] 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". In particolare, è emerso che sul sistema di trattamento in questione era installato un sistema operativo obsoleto (Windows Server 2008 R2 Standard) per il quale il produttore (Microsoft) aveva cessato la distribuzione degli aggiornamenti di sicurezza. Ciò rendeva particolarmente difficile il patching di tale sistema, richiedendo l'adozione, realisticamente non tempestiva, di eventuali accorgimenti ad hoc in grado di fronteggiare nuove vulnerabilità;

- solo a seguito della violazione dei dati personali, la Società "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";

- quanto affermato dalla Società nelle memorie difensive non consente di superare i rilievi dell'Ufficio in ordine all'utilizzo di software di base obsoleti, per i quali non sono più disponibili aggiornamenti di sicurezza, anche in considerazione del fatto che i sistemi server su cui tali software erano installati non erano adeguatamente isolati da altri sistemi server mediante i quali erano effettuati trattamenti di dati anche relativi alla salute degli assistiti del Servizio sanitario regionale;

con riguardo alla mancata adozione di misure adeguate ad assicurare la disponibilità e la resilienza dei sistemi e dei servizi di trattamento:

- la Società, al momento dell'incidente di sicurezza, utilizzava un sistema di gestione dei backup e che "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";

- la gestione dei backup veniva effettuata mediante una "tabella contenente l'elenco di progetti per cui era effettuato il backup con l'indicazione dei referenti, del nome dello schema, degli host e delle relative policy di retention" (cfr. verbale del XX, p. 3);

- solo a seguito della violazione dei dati personali, la Società ha adottato un nuovo sistema di gestione dei backup che consente una più semplice gestione e monitoraggio del backup dei dati e dei sistemi sulla base di quanto indicato da ciascun referente di progetto, al momento del rilascio in esercizio;

- quanto affermato dalla Società nelle memorie difensive non consente di superare i rilievi dell'Ufficio in ordine alle modalità adottate per assicurare la disponibilità e la resilienza dei sistemi e dei servizi di trattamento, inclusa la gestione del backup, in quanto le stesse risultavano non in linea con le migliori pratiche di settore e non adeguate al contesto dei trattamenti svolti per conto della Regione Lazio e di numerosi enti del servizio sanitario regionale;

- la violazione ha determinato per le strutture sanitarie laziali "l'indisponibilità di gran parte dei sistemi informativi deputati al trattamento dei dati personali", ovvero l'impossibilità di utilizzare molti sistemi informativi che trattano dati sulla salute e attraverso i quali le predette strutture erogano servizi sanitari ai loro assistiti. In particolare, si fa presente l'indisponibilità dei seguenti sistemi informativi e dei dati sulla salute ivi trattati: Creazione anagrafica assistiti; nuovo RECUP: Gestione prenotazioni, accettazioni, disdette; ritiro referti tramite ESCAPE; pagamenti prestazioni afferenti attività specialistica ambulatoriale compreso pagamenti on line tramite PAGO PA; Sistema regionale invio flussi per debito informativo afferente prestazioni specialistiche in carico al SSN, prestazioni intramoenia, domiciliari e prestazioni effettuate presso i consultori, ricoveri ospedalieri, accessi di Pronto Soccorso; Sistema Regionale registrazione vaccinazioni; Sistema registrazione ricetta dematerializzata per prescrizione farmaci e prestazioni ambulatoriali; Rilascio codice STP-ENI per stranieri temporaneamente presenti sul territorio, o per europei non iscritti al Servizio Sanitario, per garantire accesso alle prestazioni sanitarie; attività di screening: sistema gestione e presa in carico di utenti appartenenti a determinate fasce d'età nei percorsi di screening mammografico – citologico e del colon retto; Visualizzazione e stampa scheda riepilogativa di tutte le vaccinazioni effettuate dall'utente; Sistema TS: Gestione tessera sanitaria, invio dei flussi Sogei, rilascio dei certificati Covid-19, inserimento test rapidi e molecolari, attivazione tessera sanitaria dell'utente; Piattaforma regionale di sorveglianza Covid-19; Sistema di gestione dei piani terapeutici dei pazienti con distribuzione dei farmaci; Sistema Regionale trasmissione online referti di Laboratorio Analisi; TELEMED: tele refertazione in emergenza; ADVICE: Sistema di teleconsulto per consulenze verso i DEA di secondo livello (impossibilità di inoltrare o ricevere richieste di consulenza); EMONET: Sistema di gestione dei Centri Trasfusionali e dei Dipartimenti di Medicina Immunotrasfusionali della Regione Lazio (impossibilità di utilizzo del sistema Emonet); S.I.A.T.: Sistema di gestione dell'Assistenza Domiciliare Territoriale; richiesta posti letto Covid-19; Sistema AVR – Anagrafe Vaccinale Regionale (impossibilità di registrazione e prenotazione delle vaccinazioni); sistema di integrazione ricetta dematerializzata (impossibilità di presa in carico ed emissione ricette dematerializzate), con impatto su tutte le accettazioni ambulatoriali, incluso drivein e centro prelievi; Raccolta dati in tempo reale dei Pronto Soccorso (mancato allineamento in tempo reale dei dati con la regione); Raccolta dati in tempo reale da sistemi ADT (mancato allineamento in tempo reale delle ammissioni, dimissioni e trasferimenti con la regione); RIS-REFERTI (Sistema trasmissione referti radiologici verso portale Regionale), S.I.R.D. (Sistema Regionale di gestione delle dipendenze (cfr. notifiche di violazione dei dati personali dell'Azienda ospedaliera S. Andrea, dell'Università Campus Biomedico, dell'ASL Roma 2, dell'ASL Rieti, della Fondazione Policlinico Tor Vergata, dell'Azienda ospedaliera universitaria S. Andrea, dell'ASL Roma 6);

- i predetti sistemi informativi, attraverso i quali sono trattati dati sulla salute degli assistiti del servizio sanitario regionale, sono stati indisponibili per le strutture sanitarie regionali per un arco temporale che va da poche ore (48) ad alcuni mesi; la Società Lazio crea ha infatti provveduto a ripristinare gli stessi, in ambiente cloud, in via graduale dando priorità a quelli maggiormente critici (es. vaccinazione Covid-19) per

completare il completo ripristino alla fine del mese di ottobre 2021 (cfr. notifiche della società LAZIOcrea del XX e XX, riserve del verbale degli accertamenti ispettivi del XX);

- la mancata disponibilità di accesso ai dati conservati sui predetti sistemi è stata determinata:

i) direttamente dall'attacco informatico che, compromettendo lo strato applicativo del sistema di virtualizzazione, ha quindi reso indisponibili circa 180 sistemi server virtuali e inaccessibili i dati ivi trattati;

ii) indirettamente dalla scelta di LAZIOcrea di spegnere tutti i sistemi server in quanto, al momento dell'attacco informatico, non era in grado né di determinare quali fossero compromessi, né di evitare un'ulteriore propagazione del malware stante l'assenza di una segregazione delle reti su cui gli stessi erano attestati;

- pertanto, qualora LAZIOcrea avesse provveduto a segregare adeguatamente le reti su cui erano attestati i sistemi server e le postazioni di lavoro dei propri dipendenti e della Regione Lazio, la stessa Società non avrebbe dovuto procedere allo spegnimento dei citati sistemi server, e quindi le strutture sanitarie non avrebbero subito l'indisponibilità di accesso a numerosi sistemi informativi e ai relativi dati;

- la segregazione delle reti è peraltro una delle più comuni misure adottate nell'ambito di data center che ospitano sistemi informatici deputati al trattamento di diverse categorie di dati personali, anche relativi allo stato di salute, che LAZIOcrea - in qualità di società che opera nel settore ICT secondo il modello in house providing - avrebbe senz'altro dovuto assicurare tenuto conto del contesto e delle caratteristiche dei trattamenti in relazione ai quali è stata designata responsabile dalla Regione e dalle strutture sanitarie;

con riferimento alla violazione del principio di cui all'art. 25, par. 1, del Regolamento:

l'art. 25 del Regolamento non richiede l'attuazione di specifiche misure tecniche e organizzative, bensì che le misure e le garanzie individuate e adottate dal titolare siano specificamente connesse all'attuazione dei principi di protezione dei dati nell'ambito dei trattamenti in concreto svolti; le misure e le garanzie devono essere concepite per essere robuste e il titolare del trattamento deve essere in grado di attuarne ulteriori al fine di far fronte a un eventuale aumento dei rischi. L'efficacia o meno delle misure dipende dal contesto del trattamento e degli altri elementi che il titolare deve tenere in considerazione all'atto della determinazione dei mezzi del trattamento;

alla luce di quanto rappresentato dalla Società nelle memorie difensive, risultano superati i rilievi in ordine alla violazione del principio di protezione dei dati fin dalla progettazione, in quanto sono state delineate con maggiore precisione le valutazioni svolte dalla Società in ordine all'adeguatezza e all'efficacia delle misure adottate in relazione al contesto e all'ambito dei trattamenti svolti in qualità di titolare;

benché non sia direttamente destinatario delle disposizioni di cui all'art. 25 del Regolamento, anche il responsabile del trattamento rappresenta una figura essenziale ai fini della protezione dei dati fin dalla progettazione e per impostazione predefinita e dovrebbe essere consapevole del fatto che il titolare è tenuto a trattare i dati personali solo utilizzando sistemi e tecnologie che integrano i principi di protezione dei dati. Il responsabile, infatti, nel trattare i dati per conto dei titolari, dovrebbe utilizzare le proprie competenze per instaurare un clima di fiducia e orientare questi ultimi verso soluzioni di progettazione che integrano la protezione dei dati nel trattamento (cfr. le

citate “Linee guida 4/2019 sull’articolo 25 - Protezione dei dati fin dalla progettazione e per impostazione predefinita”, punti 94 e 95).

3. Conclusioni.

Alla luce delle valutazioni sopra richiamate, tenuto conto delle dichiarazioni rese dalla società LAZIOcrea 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 tutti 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 rileva l’illiceità del trattamento di dati personali effettuato dalla società LAZIOcrea, nei termini di cui in motivazione, in violazione di:

a) gli obblighi di cui all’art. 33, parr. 1 e 5, del Regolamento in relazione ai trattamenti effettuati in qualità di titolare;

b) il principio di “integrità e riservatezza” di cui all’art. 5, par. 1, lett. f), del Regolamento, e gli obblighi in materia di sicurezza del trattamento, in violazione dell’art. 32 del Regolamento, in relazione ai trattamenti effettuati in qualità di titolare;

c) gli obblighi di cui all’art. 33, par. 2, del Regolamento in relazione ai trattamenti effettuati in qualità di responsabile per conto dei titolari del trattamento;

d) il principio di “integrità e riservatezza” di cui all’art. 5, par. 1, lett. f), del Regolamento, e gli obblighi in materia di sicurezza del trattamento, in violazione dell’art. 32 del Regolamento, in relazione ai trattamenti effettuati in qualità di responsabile per conto di altri titolari.

In tale quadro, considerato che sono state adottate misure volte a superare le criticità sopra descritte non ricorrono i presupposti per l’adozione delle misure correttive di cui all’art. 58, par. 2, 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).

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).
Nel caso di specie, la Società ha posto in essere quattro condotte distinte, le quali devono, pertanto, essere considerate separatamente ai fini della quantificazione delle sanzioni amministrative da applicarsi.

Le predette sanzioni amministrative pecuniarie inflitte, in funzione delle circostanze di ogni singolo caso, vanno determinate nell’ammontare tenendo in debito conto gli elementi previsti dall’art. 83, par. 2, del Regolamento.

4.1. Al riguardo, tenuto conto dell'art. 83, par. 3, del Regolamento, la violazione delle disposizioni citate nel par. 3, lett. a), del presente provvedimento (art. 33, parr. 1 e 5, del Regolamento) è soggetta all'applicazione della sanzione amministrativa pecuniaria prevista dall'art. 83, par. 4, del Regolamento.

Con specifico riguardo alla natura e alla gravità delle violazioni, nonché al grado di responsabilità del titolare (art. 83, par. 2, lett. a) e g) del Regolamento), occorre considerare che i dati personali oggetto di violazione, non appartenenti a categorie particolari, si riferivano a una platea ristretta di interessati (es. dipendenti della Società).

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).

A ciò si aggiunga, ai sensi dell'art. 83, par. 2, lett. e), del Regolamento, la Società non è stata destinataria di precedenti provvedimenti correttivi e sanzionatori.

Inoltre, ai sensi dell'art. 83, par. 2, lett. h), del Regolamento, l'Autorità ha inizialmente preso conoscenza dell'evento da alcune notizie stampa e da notifiche trasmesse da altri titolari coinvolti e, solo successivamente, dalla notifica trasmessa dalla Società.

In senso favorevole al titolare occorre comunque considerare, ai sensi dell'art. 83, par. 2, lett. f), del Regolamento, che la Società ha cooperato con l'Autorità.

In ragione dei suddetti elementi, valutati nel loro complesso, e del bilancio ordinario di esercizio della Società, si ritiene di determinare l'ammontare della sanzione pecuniaria prevista dall'art. 83, parr. 3 e 4, del Regolamento nella misura di euro 16.000,00 (sedicimila) 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.

4.2. Al riguardo, tenuto conto dell'art. 83, par. 3, del Regolamento, la violazione delle disposizioni citate nel par. 3, lett. b), del presente provvedimento (artt. 5, par. 1, lett. f), e 32, del Regolamento) è soggetta all'applicazione della sanzione amministrativa pecuniaria prevista dall'art. 83, par. 5, del Regolamento.

Con specifico riguardo alla natura e alla gravità delle violazioni, nonché al grado di responsabilità del titolare (art. 83, par. 2, lett. a), d) e g) del Regolamento), occorre considerare che, pur essendo i dati personali oggetto di violazione non appartenenti a categorie particolari e riferiti a una platea ristretta di interessati (es. dipendenti della Società), le misure in essere al momento dei fatti in esame non erano adeguate a garantire la sicurezza dei trattamenti. A tal riguardo, si consideri altresì che la Società, tra le principali attività, si occupa di progettazione, realizzazione e gestione di sistemi informatici.

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).

A ciò si aggiunga che, ai sensi dell'art. 83, par. 2, lett. e) e f), del Regolamento, la Società non è stata destinataria di precedenti provvedimenti correttivi e sanzionatori e ha cooperato con l'Autorità.

Inoltre, ai sensi dell'art. 83, par. 2, lett. c), del Regolamento, la Società, al momento in cui si è verificata la violazione dei dati personali, aveva già pianificato la realizzazione di alcuni interventi per incrementare il livello di sicurezza dei trattamenti svolti.

In ragione dei suddetti elementi, valutati nel loro complesso, e del bilancio ordinario di esercizio della Società, si ritiene di determinare l'ammontare della sanzione pecuniaria prevista dall'art. 83, parr. 3 e 5, del Regolamento nella misura di euro 25.000,00 (venticinquemila) per la violazione degli artt. 5, par. 1, lett. f), e 32, del Regolamento, quale sanzione amministrativa pecuniaria ritenuta, ai sensi dell'art. 83, par. 1, del Regolamento, effettiva, proporzionata e dissuasiva.

4.3. Al riguardo, tenuto conto dell'art. 83, par. 3, del Regolamento, la violazione delle disposizioni citate nel par. 3, lett. c), del presente provvedimento (art. 33, par. 2, del Regolamento) è soggetta, all'applicazione della sanzione amministrativa pecuniaria prevista dall'art. 83, par. 4, del Regolamento.

Con specifico riguardo alla natura e alla gravità delle violazioni, nonché al grado di responsabilità del responsabile del trattamento (art. 83, par. 2, lett. a), d) e g) del Regolamento), occorre considerare che tra i dati personali oggetto di violazione vi erano dati appartenenti alle categorie particolari che si riferivano ai soggetti assistiti dal servizio sanitario regionale. Occorre inoltre evidenziare che la Società, oltre a informare i titolari con due settimane di ritardo, ha trasmesso comunicazioni parziali non indicando gli specifici sistemi e servizi di trattamento coinvolti, utili a ciascun titolare per circoscrivere il perimetro della violazione e valutarne i rischi.

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

A ciò si aggiunga, ai sensi dell'art. 83, par. 2, lett. e), del Regolamento, la Società non è stata destinataria di precedenti provvedimenti correttivi e sanzionatori.

In ragione dei suddetti elementi, valutati nel loro complesso, e del bilancio ordinario di esercizio della Società, si ritiene di determinare l'ammontare della sanzione pecuniaria prevista dall'art. 83, parr. 3 e 4, del Regolamento nella misura di euro 90.000,00 (novantamila) per la violazione dell'art. 33, parr. 2, del Regolamento da parte della Società in qualità di responsabile del trattamento, quale sanzione amministrativa pecuniaria ritenuta, ai sensi dell'art. 83, par. 1, del Regolamento, effettiva, proporzionata e dissuasiva.

4.4. Al riguardo, tenuto conto dell'art. 83, par. 3, del Regolamento, la violazione delle disposizioni citate nel par. 3, lett. d), del presente provvedimento (artt. 5, par. 1, lett. f), e 32 del Regolamento) è soggetta all'applicazione della sanzione amministrativa pecuniaria prevista dall'art. 83, par. 5, del Regolamento.

Con specifico riguardo alla natura e alla gravità delle violazioni, nonché al grado di responsabilità del responsabile del trattamento (art. 83, par. 2, lett. a), d) e g) del Regolamento), occorre considerare che tra i dati personali oggetto di violazione vi erano dati appartenenti alle categorie particolari che si riferivano ai soggetti assistiti dal servizio sanitario regionale. Al riguardo, si rileva inoltre che la Società, operando come responsabile del trattamento di numerosi enti del servizio sanitario regionale, ha un ruolo fondamentale e strategico nell'individuazione e nell'adozione delle misure di sicurezza idonee ad attenuare i rischi presentati dai trattamenti dei dati personali di milioni di interessati.

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

Si rileva inoltre che, ai sensi dell'art. 83, par. 2, lett. c), f) e k) del Regolamento, la Società ha cooperato con l'Autorità introducendo – nella concomitanza del contesto emergenziale da Covid-19 – misure idonee a superare le criticità sopra evidenziate.

A ciò si aggiunga che, ai sensi dell'art. 83, par. 2, lett. e) del Regolamento, la Società non è stata destinataria di precedenti provvedimenti correttivi e sanzionatori.

In ragione dei suddetti elementi, valutati nel loro complesso, e del bilancio ordinario di esercizio della Società, si ritiene di determinare l'ammontare della sanzione pecuniaria prevista dall'art. 83, parr. 3 e 5, del Regolamento nella misura di euro 140.000,00 (centoquarantamila) per la violazione degli artt. 5, par. 1, lett. f), e 32 del Regolamento, da parte della Società in qualità di responsabile del trattamento, quale sanzione amministrativa pecuniaria ritenuta, ai sensi dell'art. 83, par. 1, del Regolamento, effettiva, proporzionata e dissuasiva.

4.5. Sulla base di quanto valutato nei precedenti parr. 4.1, 4.2, 4.3 e 4.4 del presente provvedimento, si ritiene di dover determinare l'ammontare totale della sanzione pecuniaria comminata alla Società nella misura di euro 271.000,00 (duecentosettantunomila) in relazione al complesso delle violazioni precedentemente descritte.

Tenuto conto che le violazioni poste in essere sono di significativa gravità, anche in considerazione del numero di interessati coinvolti (compresi gli assistiti del Servizio sanitario), della tipologia di dati personali oggetto di violazione e dell'ampiezza e dell'impatto sulla disponibilità dei servizi colpiti, si ritiene, altresì, che debba applicarsi la sanzione accessoria della pubblicazione sul sito del Garante del presente provvedimento, prevista dall'art. 166, comma 7, del Codice e dall'art. 16 del reg. del Garante n. 1/2019.

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 dalla società LAZIOcrea S.p.a. per la violazione degli artt. 5, par. 1, lett. f), 32 e 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, alla società LAZIOcrea S.p.a., codice fiscale 13662331001, in persona del legale rappresentante pro-tempore, di pagare la somma di euro 271.000,00 (duecentosettantunomila) 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 Società, in caso di mancata definizione della controversia ai sensi dell'art. 166, comma 8, del Codice, di pagare la somma di euro 271.000,00 (duecentosettantunomila) secondo le modalità indicate in allegato, entro 30 giorni dalla notificazione del presente provvedimento, pena l'adozione dei conseguenti atti esecutivi a norma dall'art. 27 della legge n. 689/1981.

DISPONE

ai sensi dell'art. 166, comma 7, del Codice, la pubblicazione per intero del presente provvedimento sul sito web del Garante e 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
Stanzione

IL SEGRETARIO GENERALE
Mattei

Provvedimento del 21 marzo 2024 [10002287]

VEDI ANCHE Newsletter del 10 aprile 2024

[doc. web n. 10002287]

Provvedimento del 21 marzo 2024

Registro dei provvedimenti
n. 196 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 la prof.ssa Ginevra Cerrina Feroni;

PREMESSO

1. L'attività istruttoria

Il XX la Regione Lazio (di seguito "Regione") ha trasmesso all'Autorità, ai sensi dell'art. 33 del Regolamento, una notifica di violazione dei dati personali, riguardante un attacco informatico,

determinato da un malware di tipo ransomware, ai sistemi informativi gestiti da 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 (notifica successivamente integrata in data XX e XX) .

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 XX, a cui LAZIOcrea ha fornito riscontro con note del XX e XX, XX e XX).

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

Con la notifica del XX, la Regione ha dichiarato di aver "subìto 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, LAZIOcrea, 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, LAZIOcrea ha rappresentato 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 rispristinato 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”.

Da ultimo, con la notifica del XX, LAZIOcrea 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 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 richiamate attività ispettive LAZIOcrea ha inoltre dichiarato, come indicato nel verbale delle operazioni compiute, 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;

"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"".

Nel corso dell'istruttoria LAZIOcrea ha altresì fornito l'elenco dei titolari, ivi inclusa la Regione Lazio, per conto dei quali effettuava i trattamenti di dati personali coinvolti nella violazione.

1.1 Le misure in essere al momento della violazione

Con riferimento alle misure in essere al momento della violazione la Regione, con la notifica integrativa del XX, ha dichiarato che "fermo restando che il Data center e le procedure di LazioCrea S.p.A. per la sicurezza e protezione dei dati sono certificate ISO 27001, si rappresenta che con determinazione dirigenziale n. XX del XX Regione Lazio ha disciplinato l'assegnazione e l'utilizzo delle dotazioni ICT per il personale in servizio […]. Inoltre, nell'ambito del Regolamento di organizzazione degli uffici e dei servizi della Giunta regionale n. 1/2002 e s.m.i. è disciplinato il modello organizzativo in tema di protezione dei dati personali ai sensi degli articoli 473, 474 e successivi. Infine, all'interno della intranet regionale sono disponibili delle frequently asked questions (FAQ) concernenti l'utilizzo dei dispositivi informatici durante lo smart working straordinario".

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.

Nel corso delle attività ispettive LAZIOcrea ha 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 1° luglio 2021 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 Regione, con la suddetta notifica del XX, ha inteso rimandare "alla documentazione allegata da LazioCrea alla notifica finale del XX". La Società, con la richiamata notifica 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, LAZIOcrea, 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".

Nel corso delle attività ispettive la predetta Società 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)";
>
> "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";
>
> "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";
>
> "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";
>
> "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".

Dalla documentazione in atti si evince che, a seguito dell'attacco informatico in esame, la Regione ha subito la temporanea indisponibilità di numerosi sistemi informativi, attraverso alcuni dei quali sono trattati dati sulla salute degli assistiti del Servizio sanitario regionale (es. sistemi deputati alle prenotazioni sanitarie, alla vaccinazione Covid-19, al teleconsulto, al deposito dei referti relativi ad esami di laboratorio – compresi quelli relativi ai tamponi da Covid-19 – alla ricetta digitale, nonché il sistema dell'anagrafe regionale vaccinale, il portale Salute Lazio). La mancata disponibilità di accesso ai dati conservati sui predetti sistemi, che configura una violazione dei dati personali, è stata, da un lato, una conseguenza diretta dell'attacco informatico (che, cifrando il contenuto di alcuni sistemi server, li ha resi indisponibili) e, dall'altro, una sua conseguenza indiretta derivante

dalla scelta di LAZIOcrea di spegnere tutti i sistemi server nell'impossibilità di determinare quali fossero compromessi e, stante l'assenza di una loro segregazione, di evitare un'ulteriore propagazione del malware.

1.3 Il procedimento avviato da parte dell'Autorità

Sulla base di quanto sopra rappresentato, con nota del XX (prot. n. XX) l'Ufficio ha effettuato una notifica di violazione di cui all'art. 166, comma 5, del Codice alla Regione Lazio in quanto è stato rilevato che il trattamento di dati personali in esame è stato effettuato:

> in maniera non conforme al principio di "integrità e riservatezza", in violazione dell'art. 5, par. 1, lett. f), del Regolamento;
>
> omettendo di mettere in atto misure tecniche e organizzative per individuare tempestivamente una violazione dei dati personali, nonché per assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento, in violazione dell'art. 32 del Regolamento;
>
> in maniera non conforme al principio della "protezione dei dati fin dalla progettazione" di cui all'art. 25, par. 1, del Regolamento.

Con nota del XX, la Regione ha chiesto la proroga del termine per presentare le memorie difensive, che è stata concessa dall'Ufficio in ragione della dichiarata "complessità dei sistemi e dei servizi gestiti da LAZIOcrea per conto dell'Ente Regionale Lazio e degli altri titolari" e tenuto conto che "con D.M. del 9 dicembre 2022 è stata fissata la data delle elezioni regionali per il Lazio al 12 e 13 febbraio 2023".

Con nota del XX, la Regione ha inviato le proprie memorie difensive, nell'ambito delle quali – in via preliminare – dopo aver precisato che "l'incidente accaduto nella notte tra sabato 31 luglio e domenica 1 agosto 2021 ha avuto una enfasi mediatica di gran lunga superiore alle effettive conseguenze dell'attacco informatico sui diritti e le libertà degli interessati", ha illustrato ruoli e rapporti "della Giunta Regionale (Titolare del trattamento) e di LAZIOcrea spa (Responsabile del Trattamento)", specificando, al riguardo, che:

> "LAZIOcrea S.p.A. è una società per azioni, interamente partecipata dalla Regione Lazio e costituita ai sensi dell'art. 5 della L.R. n. 12 del 24 novembre 2014 secondo il modello organizzativo dell'in-house providing", la quale presta servizi e attività "alle strutture della Giunta Regionale", con riferimento, in particolare, ad ambiti di intervento quali: "supporto tecnico-amministrativo, organizzativo e gestionale, connessi all'esercizio delle funzioni amministrative regionali […]; progettazione, realizzazione e gestione della strategia regionale di Agenda digitale, incluso il Sistema Informativo Regionale";
>
> "l'amministrazione regionale esercita nei confronti della stessa funzioni di programmazione, indirizzo strategico-operativo e controllo. La Regione Lazio esercita nei confronti di LAZIOcrea il c.d. "controllo analogo" e definisce gli obiettivi strategici e operativi. […] La Giunta Regionale, inoltre, approva con propria deliberazione le direttive in ordine alle attività di indirizzo e controllo anche ai fini dell'esercizio del controllo analogo sulla società in house";
>
> in base anche a quanto definito nello statuto, "la gestione del Sistema Informativo Regionale e del Data Center è, pertanto, totalmente demandata alla Società LAZIOcrea S.p.A", per cui quest'ultima, "nell'ambito delle proprie competenze, rende disponibili l'infrastruttura e il sistema informativo agli enti aderenti al Sistema Informativo Regionale, allo scopo di dotarli dei servizi informatici necessari al raccordo dei loro sistemi informatici con il predetto Sistema Informativo Regionale";

“in virtù del fatto che LAZIOcrea, effettuando per conto della Giunta Regionale, trattamenti strumentali all’erogazione di servizi essenziali, opera quale Responsabile del trattamento dei dati personali per la gestione del Data Center per conto del Titolare, è stata formalmente designata in tale ruolo con DGR 797/2017 e DGR 840/2018”, e tale designazione “è stata effettuata avendo evidenza che lo stesso fornisse garanzie ampiamente sufficienti per l’implementazione delle misure di sicurezza tecniche e organizzative adeguate, in termini di conoscenze specialistiche (competenze tecniche in materia di misure di sicurezza e violazioni dei dati), affidabilità e risorse disponibili”.

Con la medesima nota è stato evidenziato che:

“in merito alla individuazione, trattazione e tempestiva segnalazione della violazione, si ritiene che la condotta del Titolare del trattamento sia stata corretta ed adeguata. L’analisi delle tempistiche evidenzia infatti che, a fronte della violazione avvenuta tra il 31 luglio ed il 1° agosto 2021 (vale la pena di ricordare che il 31 luglio era sabato), il Titolare del trattamento, già nella serata del 1° agosto ha provveduto a mezzo PEC, per il tramite del proprio DPO pro tempore, ad informare codesta Autorità sull’incidente, ed in data XX, ha effettuato la notifica preliminare della violazione dei dati personali attraverso la procedura on line disponibile sul sito istituzionale del Garante: tutto ciò pertanto, senza ingiustificato ritardo e nel termine delle 72 ore prescritte dall’art. 33 del Regolamento. Sul punto si specifica inoltre che il Titolare del Trattamento, nell’ambito della sua funzione di controllo, all’epoca dell’accadimento, aveva evidenza del fatto che il Responsabile designato avesse già adottato i più elevati standard di sicurezza al fine di non compromettere la riservatezza, l’integrità e la disponibilità dei dati personali trattati per conto del Titolare”, avendo “conseguito in data 11 dicembre 2020 (data ben antecedente alla violazione in oggetto) la certificazione degli standard di sicurezza per la tutela delle informazioni UNI CEI EN ISO/IEC 27001:2017 per il tramite dell’Ente certificatore, APAVE Certification Italia S.R.L.”;

“in considerazione del fatto che lo stesso Regolamento incoraggia l’utilizzo delle certificazioni da conseguire attraverso appositi organismi di certificazione (artt. 42 e 43 del RGPD), si ritiene che la Giunta Regionale abbia operato conformemente al Regolamento sia nella fase di verifica della sussistenza in capo al Responsabile delle garanzie sufficienti per mettere in atto misure tecniche e organizzative volte ad assicurare trattamenti che presentino adeguata tutela dei diritti dell'interessato (acquisizione della certificazione), sia nella fase di implementazione delle misure e di miglioramento del sistema di sicurezza e di protezione dati, traducendo nel POA 2021 le osservazioni del certificatore in azioni di miglioramento finanziate con appositi stanziamenti di bilancio. Nell’ottica sopra evidenziata il Titolare si è assicurato che gli standard di qualità certificati sul sistema Informativo Regionale e sul Data Center fossero mantenuti anche nella gestione post incidente; al riguardo si evidenzia infatti che, grazie all’adeguamento dei sistemi di sicurezza ed all’adozione delle azioni di miglioramento finanziate nel POA 2021, LAZIOcrea ha conservato la certificazione ISO 27001 anche a seguito delle visite di mantenimento rispettivamente avvenute in data 26-29 novembre 2021 e 24-25 novembre 2022 e conseguito [ulteriori] certificazioni […]. Vale concludere precisando che, nell’ottica di miglioramento, in capo al Responsabile, del sistema di sicurezza e di mantenimento della capacità di porre in essere misure tecniche ed organizzative adeguate, alla data odierna, il Data Center gestito da LAZIOcrea per conto della Regione Lazio risulta anche accreditato presso l’Agenzia per la Cybersicurezza Nazionale (ACN). In assenza di un codice di condotta applicabile, si ritiene che l’adesione del Responsabile del Trattamento ai meccanismi di certificazione sopra richiamati, su input del Titolare, costituisca piena evidenza di sufficienti garanzie per l’attuazione di misure tecniche e organizzative in termini di conoscenze specialistiche, di competenze tecniche in materia di misure di sicurezza e di violazione dei dati e di grado di affidabilità”;

> “relativamente alle specifiche istruzioni che il Titolare fornisce al Responsabile del Trattamento, oltre alla designazione della società con DGR 797/2017 e DGR 840/2018 […], rilevino, nell’ambito del rapporto giuridico tra la Giunta Regionale e LAZIOcrea S.p.A., anche i progetti approvati e finanziati in tema cybersecurity contenuti nel Piano Operativo Annuale 2021 di cui alla DGR n. 1024/2020 […]. Con specifico riferimento alla DGR n. 840/2018 si evidenzia poi che nell’allegato G, […] il Titolare, nell’esercizio della sua funzione, ha provveduto a impartire specifiche istruzioni anche in tema di sicurezza del trattamento dati personali”;

con riferimento alla mancata adozione di misure adeguate a rilevare tempestivamente la violazione dei dati personali:

> LAZIOcrea, “per conto del Titolare, all’epoca dell’incidente accaduto a luglio 2021 si era già [dotata] della console Microsoft Windows Defender ATP e del Security Information and Event Management (SIEM) di Microsoft i quali hanno correttamente inviato “alert” in merito alla rilevazione di possibili attività malevole. Gli strumenti di rilevazione sopra richiamati erano già in esercizio all’epoca della violazione e sono stati adottati all’interno di una più ampia pianificazione delle attività relative alla cybersecurity che risale a periodo antecedente all’incidente e che, come previsto nell’Allegato B sezione B1 al POA per l’anno 2021 (DGR 1024/2020), avrebbe condotto all’implementazione del servizio denominato “CYBERSECURITY - Implementazione Servizio SOC Interno”; nella citata DGR la suddetta attività è stata finanziata ed è stato effettuato il relativo impegno sull’apposito capitolo di bilancio. […] Vale la pena sottolineare che il Titolare, nell’ottica di adottare misure sempre più adeguate a rilevare tempestivamente potenziali violazioni dei dati personali, ha cooperato con LAZIOcrea per accelerare la messa in operatività del SOC anticipando il completamento della progettazione preliminare degli interventi ai primi mesi del 2021, nonostante, per le pubbliche amministrazioni, l’ordinamento vigente a tutt’oggi ancora non preveda l’obbligo di attivazione di un SOC presidiato continuativamente h24. Pertanto, si intende sottolineare che il comportamento del Titolare e del Responsabile, basato sui principi della prudenza e della cautela, risulta rispondente al principio di conformità al sistema di protezione dati personali sin dalla progettazione e che quindi le azioni poste in essere possono ritenersi tempestive”;

> “nelle prime fasi dell’offensiva, il superamento delle misure di sicurezza in atto al momento dell’incidente da parte degli attaccanti non è avvenuto a causa dell’inadeguatezza delle stesse, ma piuttosto a causa dell’utilizzo di strumenti particolarmente sofisticati e non rilevabili in quanto sconosciuti agli antivirus, come avvenuto anche in altre circostanze simili […]. Tali elementi, evidentemente, non possono essere noti prima dell’individuazione della minaccia e, solo in seguito a questa, vengono inclusi nei test di rilevazione da parte degli strumenti di protezione, a seguito degli aggiornamenti rilasciati dal produttore degli stessi. […] Nel caso di incidenti di rilevante complessità, come nel caso di che trattasi, la rilevazione di una violazione di dati personali richiede approfondite e specifiche indagini tecniche prima della conclusione delle quali il titolare non può essere completamente a “conoscenza della violazione” (cfr. Linee guida sulla notifica, p. 12). Quanto sopra dichiarato, unitamente – come giova ripetere - alla tempestività della notifica avvenuta prima con PEC nella serata del XX e successivamente con la notifica preliminare attraverso la procedura on line dal sito istituzionale di codesta Autorità in data XX, dimostra inequivocabilmente l’adeguatezza delle misure adottate in ordine alla immediata rilevazione dell’incidente informatico ed alla successiva valutazione della violazione. Ciò anche a riprova della operatività delle procedure di rilevazione e della cooperazione e comunicazione tra Titolare e Responsabile”;

con riferimento alla mancata adozione di misure adeguate a garantire la sicurezza delle reti:

> “le misure di sicurezza in essere al momento dell’attacco hanno consentito un ripristino dei

dati a partire dai backup che, evidentemente, non erano stati compromessi in virtù proprio dei sistemi di segregazione in atto. In riferimento alla adeguatezza delle misure relative alla segmentazione e segregazione delle reti, in considerazione che trattasi di argomento di natura tecnica e peraltro di specifica competenza della società in house, come da norma statutaria di quest'ultima, si rinvia integralmente […] a quanto riportato nelle memorie del Responsabile";

"la separazione logica e la segregazione fisica delle reti, predisposte dal Responsabile del Trattamento, hanno impedito agli hacker di esfiltrare i dati presenti nel Data Center e che non si è determinata alcuna limitazione ai diritti ed alle libertà degli interessati e che l'incidente non ha arrecato danni materiali o immateriali";

"nell'ambito delle valutazioni sulla garanzia e adeguatezza delle misure adottate dal Responsabile in capo al Titolare si richiama quanto già evidenziato infra, al punto 3.1, in merito alla adesione del responsabile ai meccanismi di certificazione ISO 27001";

con riferimento all'obsolescenza dei software di base installati su alcuni sistemi di trattamento, nel rinviare sul punto a quanto riportato nelle memorie di LAZIOcrea, viene aggiunto che "nella valutazione del bilanciamento del rapporto costi/benefici, rispetto all'aggiornamento di servizi informatici in produzione, rientrano considerazioni in ordine all'importanza di assicurare continuità ai progetti in essere, tenuto conto delle risorse disponibili e che sarebbe necessario investire, nonché delle effettive disponibilità e del miglioramento che sarebbe possibile conseguire. Al contempo, il fatto di mantenere in esercizio un'applicazione gestita da un sistema che ha raggiunto il termine di "fine vita", per il quale non sono più disponibili patch o aggiornamenti di sistema, non costituisce in sé una violazione di sicurezza, poiché tale applicazione può opportunamente essere isolata all'interno di un perimetro volto ad assicurarne il funzionamento. Infatti, la vulnerabilità sfruttata dall'agente esterno in relazione alla "privileges escalation" non era esposta all'esterno della rete regionale, come dichiarato nelle memorie del Responsabile";

con riferimento alla mancata adozione di misure adeguate ad assicurare la disponibilità e la resilienza dei sistemi e dei servizi di trattamento, nel ritenere che "non si possa configurare, in capo al Titolare, la violazione delle disposizioni di cui agli artt. 5, par. 1, lettera f) e 32, par. 1, lettera b)":

anche in base a quanto emerso durante l'accertamento ispettivo presso la Società, "il backup dei dati veniva in realtà effettuato giornalmente";

"la certificazione degli standard di sicurezza per la tutela delle informazioni ISO 27001, che contiene specifici item relativi alla gestione dei backup, è stata conseguita dal Responsabile in epoca antecedente all'incidente di che trattasi e che appare evidente che l'Ente certificatore abbia ritenuto le procedure di backup, all'epoca in atto, conformi agli standard di sicurezza. Anche sul punto, pertanto, non può che ribadirsi che la Giunta Regionale, nella sua qualità di Titolare del trattamento dei dati personali, all'epoca dell'incidente avesse specifica evidenza dell'adeguatezza delle misure tecniche e organizzative adottate dal Responsabile volte a garantire la disponibilità e la resilienza dei sistemi. A riprova dell'efficacia dei sistemi di conservazione e recupero dei dati da parte del Responsabile si evidenzia che le procedure di backup in atto al momento dell'attacco si sono rivelate adeguate e funzionanti, tanto che gli applicativi coinvolti dall'incidente sono stati correttamente reinstallati e ripristinati. Per le specifiche misure adottate e per la descrizione dei sistemi di backup in atto, si rinvia integralmente alle memorie del Responsabile";

"il fatto che il Responsabile successivamente all'incidente si sia dotato di un nuovo sistema di backup non evidenzia affatto l'inadeguatezza di quello già in essere, ma piuttosto la capacità di adeguare, con continui interventi migliorativi, le misure tecniche ed organizzative

poste in essere a seguito di continue valutazioni del livello del rischio connesso al trattamento. L'implementazione di ulteriori misure di sicurezza tecniche e organizzative post incidente da parte di LAZIOcrea rientra invero in un più ampio progetto di adeguamento, peraltro, come già detto in prcedenza, in larga parte programmato ed affidato dal Titolare con tempistiche antecedenti all'incidente, che ricomprende tra l'altro sistemi e procedure di backup, disaster recovery e business continuity, volte a migliorare il livello di sicurezza al fine di proteggere le operazioni di trattamento effettuate sui propri sistemi e di mitigare i rischi";

con riferimento alla protezione dei dati fin dalla progettazione:

"la contestazione in relazione alla protezione dei dati fin dalla progettazione da parte di questa Autorità, non sia contestualizzata nella descrizione di specifici fatti, atti od omissioni ascrivibili ad eventuali condotte non adeguate del Titolare, ma piuttosto costituisca un richiamo alla normativa vigente in merito";

"il Titolare ha operato nei confronti del Responsabile, tramite l'acquisizione delle certificazioni più volte richiamate, valutazioni in merito all'adeguatezza dei sistemi ed alle misure di contrasto adottate […]. Il Titolare, in considerazione del fatto che l'incidente è avvenuto sfruttando una tipologia di malware non rilevabile dai sistemi/applicativi antivirus disponibili all'epoca (a riprova di ciò, si ricorda che lo stesso non è stato rilevato nemmeno dagli esperti nell'ambito dell'indagine forense quasi due settimane più tardi con sistemi di rilevazione aggiornati al 10 agosto 2021), ha adottato misure tecniche e organizzative che sono da ritenersi oggettivamente adeguate ad individuare tempestivamente possibili violazioni se rapportate al quadro noto all'epoca dei fatti, in tema di cybersecurity. Inoltre, i sistemi di sicurezza in essere presso il Responsabile risultavano idonei ad assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento, nel rispetto, di fatto, anche del principio della "protezione dei dati fin dalla progettazione" di cui all'art. 25, par. 1, del Regolamento. Vale al riguardo osservare che lo stesso art. 25, par 3, del Regolamento ammette che il meccanismo di certificazione possa essere utilizzato come elemento per dimostrare la conformità ai requisiti di cui ai paragrafi 1 e 2 del medesimo articolo";

"nonostante alcuni dei sistemi coinvolti nell'incidente fossero preesistenti all'entrata in vigore del Regolamento, il Titolare ed il Responsabile, ognuno per la propria competenza, si sono adoperati a revisionare e adeguare le misure di sicurezza in atto in relazione alla protezione dei dati personali. Rimandando alle motivazioni sopra esposte e sottolineando le limitate conseguenze post incidente, si ritiene di fatto che le verifiche e gli adeguamenti operati anche sui sistemi precedenti al RGPD abbiano dato prova di adeguate garanzie sui diritti degli interessati";

con specifico riferimento al dovere di valutare i rischi per la sicurezza dei dati personali, considerando l'impatto sui diritti e le libertà degli interessati, e contrastare efficacemente quelli identificati, "il sistema di valutazione dei rischi adottato dal Responsabile è da ritenersi adeguato se rapportato alle minacce note all'epoca dell'incidente; in particolare erano presenti sia sistemi antivirus che sistemi di alert. Tuttavia, si ribadisce che il malware, da cui ha avuto origine l'incidente, era di fatto non identificabile tanto da essere sfuggito ai migliori sistemi/applicativi antivirus disponibili nel periodo, anche a quelli adottati per l'indagine forense. […] Il Titolare del Trattamento, inoltre, nell'ambito della sua funzione di controllo, all'epoca dell'accadimento aveva evidenza del fatto che il Responsabile del Trattamento designato avesse adottato i più elevati standard di sicurezza al fine di non compromettere la riservatezza, l'integrità e la disponibilità dei dati personali trattati per suo conto", sottolineando ancora una volta l'elemento del conseguimento delle menzionate certificazioni da parte della Società;

con specifico riferimento al dovere di tenere conto non appena possibile dei requisiti di sicurezza nella progettazione e nello sviluppo del sistema, integrando e svolgendo costantemente test pertinenti, “la Giunta Regionale ha recepito prontamente le osservazioni contenute nella certificazione conseguita dal Responsabile del Trattamento in data 11 dicembre 2020 e le ha tradotte in concrete azioni di miglioramento nel Programma Operativo Annuale 2021 (POA 2021), approvato con D.G.R 1024 del 22 dicembre 2020”;

con specifico riferimento al dovere di definire il trattamento dei dati in modo tale che un numero minimo di persone abbia bisogno di accedere ai dati personali per svolgere le proprie funzioni, e limitare l’accesso di conseguenza, “l’autenticazione per l’accesso da remoto, tramite “VPN Pulse secure” a singolo fattore, risultava infatti adeguata al quadro generale noto all’epoca dei fatti relativamente alle possibili vulnerabilità dei sistemi ed ai possibili vettori di attacco. Non si rilevano da parte dell’ente certificatore per lo standard ISO 27001:2017 prescrizioni in relazione all’accesso alla VPN con singolo fattore di autenticazione. Come già noto, infatti, gli attaccanti, dopo aver avuto accesso alla rete interna, per poter sferrare l’attacco, hanno dovuto effettuare un movimento laterale per apprendere le credenziali di un utente che avesse i privilegi di amministratore e che consentisse loro l’accesso ad altre sottoreti. Come risulta dalle memorie del Responsabile gli accessi degli amministratori di sistema alla sottorete (diversa da quella degli utenti ordinari), avvenivano, all’epoca dell’incidente, attraverso l’utilizzo di password particolarmente robuste e complesse (20 caratteri contenenti lettere maiuscole, minuscole e caratteri speciali, da rinnovare ogni 30 giorni, e non coincidenza della password in uso con le ultime quattro utilizzate) e, inoltre, la configurazione della rete antecedente all’attacco prevedeva il necessario accesso diretto di tutti gli utenti al server di autenticazione nel dominio. Qualora le reti non fossero state adeguatamente configurate e segregate in termini di accessi e filtraggio le conseguenze dell’attacco avrebbero avuto un impatto rilevante sui diritti e le libertà degli interessati. È opportuno sottolineare che le misure di sicurezza minime previste dall’AgID, prevedono tre diversi livelli (Minimo, Standard, Alto) e, relativamente all’“Uso appropriato dei privilegi di amministratore”, classificano il doppio fattore di autenticazione per gli accessi degli AdS come una misura di livello “Alto”, (si ricorda che le misure obbligatorie sono quelle classificate di livello “Minimo”, cfr. Circolare AgID n. 2/2017 ABSC 5 - CSC 5). Sono considerate, tra l’altro, di livello “Alto” le password di almeno 14 caratteri: pertanto la password di 20 caratteri, prevista per l’accesso ai sistemi da parte degli Amministratori può essere considerata assolutamente ed indiscutibilmente robusta”;

con specifico riferimento al dovere di proteggere i dati personali da modifiche e accessi non autorizzati e accidentali, sia durante il loro trasferimento che durante la loro conservazione, “il Titolare aveva evidenza di adeguate garanzie da parte del Responsabile in particolare in relazione al possesso di certificazioni del sistema di gestione della sicurezza basate su standard internazionali (in particolare ISO 27001:2017 che si fonda su approfonditi controlli di sicurezza in ordine alla disponibilità, confidenzialità ed integrità del dato). In particolare, tutti gli accessi ai sistemi avvenivano tramite protocolli criptati (HTTPS/TLS) che garantiscono la crittografia dei dati in transito”;

con specifico riferimento al dovere di registrare gli eventi rilevanti ai fini della sicurezza delle informazioni e monitorandoli per rilevare in modo tempestivo eventuali incidenti di sicurezza, “il Responsabile all’epoca dell’incidente era dotato di misure adeguate a rilevare tempestivamente le violazioni di dati personali; nello specifico i sistemi relativi alla console Microsoft Windows Defender ATP e al SIEM di Microsoft hanno correttamente inviato alert in merito a possibili attività malevole”;

con specifico riferimento al dovere di garantire il ripristino dei sistemi informatici in caso di disastro e la continuità operativa, assicurando la disponibilità dei dati personali a seguito di incidenti di sicurezza rilevanti, “le misure di sicurezza adottate sia nella fase pre che nella

fase post-incidente hanno permesso di ripristinare gli applicativi tramite le copie dei back-up offline. Al riguardo si precisa che è stata garantita la continuità operativa delle applicazioni ed in particolare degli strumenti di supporto alla campagna vaccinale e alla prenotazione delle prestazioni sanitarie, come del resto già esplicitato nella documentazione in possesso di codesta Autorità. Tale ripristino è stato possibile grazie alla configurazione dei sistemi ed alla progettazione del data center che pertanto, sol per questo, rispettano i principi stabiliti dall'art. 25 del Regolamento. Si ritiene dover sottolineare che la temporanea indisponibilità del dato personale (limitata al tempo strettamente necessario al ripristino delle applicazioni) non ha comportato alcun pregiudizio per le libertà ed i diritti degli interessati ed è stata determinata dalla messa in atto da parte del Responsabile delle procedure necessarie a fronteggiare l'attacco al fine di evitare conseguenze peggiori. Non è da sottovalutare il fatto che il citato tempestivo ripristino è stato realizzato proprio perché, grazie alla configurazione dell'architettura dei sistemi ed alla progettazione del Data Center (nel rispetto dei principi dell'art. 25 RGPD), per il quale era prevista una suddivisione in reti e sale logicamente e/o fisicamente separate, i dati personali sono rimasti protetti";

con specifico riferimento al dovere di disporre di adeguate procedure per gestire le violazioni dei dati personali, comprese procedure per la loro documentazione, "la pronta attivazione da parte della Giunta Regionale e della Società ed il contenimento della potenziale portata dell'incidente, nonché il ripristino dei servizi temporaneamente sospesi (esclusivamente per le verifiche tecniche necessarie) sono tutti elementi che dimostrano ex se la conformità dei sistemi al requisito menzionato";

in merito agli elementi per le valutazioni di cui all'art. 83, par. 2, del Regolamento:

"l'incidente non ha comportato esfiltrazione di dati e non ha causato nessun danno ai diritti ed alle libertà degli interessati. Come più volte ricordato, l'incidente non ha determinato alcuna perdita di riservatezza ed integrità del dato. Riguardo alla disponibilità, si rileva che la stessa è stata circoscritta al tempo necessario all'Ente per la valutazione dell'incidente e per la messa in atto delle necessarie azioni di mitigazione e remediation. Pertanto, alla luce di quanto sopra, il quadro si riferisce senza dubbio ad una violazione non grave. La durata della violazione, inoltre, è da ritenersi estremamente contenuta rispetto al potenziale impatto che si sarebbe generato in assenza dell'adozione di tutte le operazioni di contenimento dei rischi ampiamente descritte. La temporanea indisponibilità dei servizi regionali non è infatti da inquadrare nell'ambito di una violazione dei diritti e delle libertà degli interessati, ma piuttosto nell'ambito di una necessaria e immediata azione di mitigazione dei possibili rischi proprio a tutela dei diritti e delle libertà degli interessati stessi. A riprova di quanto affermato si ribadisce che gli interventi post incidente non hanno determinato sospensioni ai servizi di emergenza (Ares 118, Protezione civile, NUE 112) e non hanno ostacolato in alcun modo la campagna vaccinale, in quanto la temporanea indisponibilità della piattaforma vaccinale non ha generato alcun ritardo nel sistema di prenotazione che, al momento della sua riattivazione, ha permesso di utilizzare gli slot di prenotazione già disponibili in fase pre-incidente";

"il fatto che l'attacco hacker sia originato esternamente all'Amministrazione, la natura del malware più volte evidenziata e le modalità di attacco supportano la tesi che gli elementi psicologici in esame non rilevino in alcun modo né in capo al Titolare e né in capo al Responsabile. Pertanto, nelle condotte adottate non si rilevano gli elementi di dolo o colpa";

"nonostante […] il virus fosse sconosciuto ai migliori e più aggiornati sistemi di rilevazione del periodo, le misure adottate si sono rivelate adeguate ed efficaci ad impedire l'ulteriore propagazione del malware. Pertanto, i fatti descritti supportano efficacemente la tesi dell'adeguatezza delle misure di sicurezza tecniche e organizzative messe in atto ai sensi degli artt. 25 e 32 del Regolamento, ivi comprese le misure di mitigazione post incidente";

“non risultano precedenti attacchi informatici contro i sistemi della Regione Lazio, pertanto non esistono precedenti violazioni pertinenti ed ascrivibili alla fattispecie di che trattasi”;

“il Titolare ha sempre adottato nei confronti di codesta Autorità un atteggiamento collaborativo e proattivo improntato ai principi di correttezza, lealtà, trasparenza. Valgano in proposito la prima e le successive notifiche inviate periodicamente a codesta Autorità”;

“il Titolare ha provveduto ad effettuate tempestiva segnalazione della violazione. A fronte della violazione avvenuta tra il 31 luglio ed il 1° agosto 2021, il Titolare, infatti nella serata del 1° agosto ha provveduto a mezzo PEC, per il tramite del proprio DPO pro tempore, ad informare codesta Autorità sull’incidente, ed in data XX, ha effettuato la notifica preliminare on line della violazione dei dati personali tramite il portale del Garante, senza ingiustificato ritardo e nel termine delle 72 ore prescritte dall’art. 33 del Regolamento”;

“non sono mai state notificate violazioni relative a questioni dello stesso oggetto, pertanto, non risultano disposti da parte di codesta Autorità i provvedimenti di cui all'articolo 58, paragrafo 2 né nei confronti del Titolare, né nei confronti del Responsabile”;

“in assenza di un codice di condotta approvato ed applicabile alla fattispecie, il Responsabile del Trattamento, su impulso del Titolare, ha conseguito in data 11 dicembre 2020 (data antecedente alla violazione in oggetto), la certificazione degli standard di sicurezza per la tutela delle informazioni UNI CEI EN ISO/IEC 27001:2017. Tale certificazione è stata confermata a seguito delle visite di mantenimento (post incidente) […]. Nel periodo successivo all’incidente, inoltre il Responsabile ha conseguito le ulteriori seguenti certificazioni: ISO 27017 in data 20 luglio 2022 (standard di riferimento per i controlli di sicurezza generali per gli utilizzatori e i fornitori di servizi cloud); ISO 27018 in data 20 luglio 2022 (standard per i controlli per i fornitori di servizi cloud pubblici che agiscono come responsabili del trattamento)”.

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);

in virtù del richiamato principio di “integrità e riservatezza” (art. 5, par. 1, lett. f), del Regolamento), il titolare deve (cfr. le “Linee guida 4/2019 sull’articolo 25 - Protezione dei dati fin dalla progettazione e per impostazione predefinita”, adottate dal Comitato europeo per la protezione dei dati – di seguito “Comitato” – il 20 ottobre 2020, spec. punto 85):

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

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

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

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

registrare gli eventi rilevanti ai fini della sicurezza delle informazioni e monitorandoli per rilevare in modo tempestivo eventuali incidenti di sicurezza;

garantire il ripristino dei sistemi informatici in caso di disastro e la continuità operativa, assicurando la disponibilità dei dati personali a seguito di incidenti di sicurezza rilevanti;

disporre di adeguate procedure per gestire le violazioni dei dati personali, comprese procedure per la loro documentazione;

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" (di seguito "Linee guida sulla notifica"), adottate dal Comitato il 28 marzo 2023, evidenziano che "un incidente di sicurezza che determina l'indisponibilità dei dati personali per un certo periodo di tempo costituisce una violazione, in quanto la mancanza di accesso ai dati può avere un impatto significativo sui diritti e sulle libertà delle persone fisiche" (sez. I.B.2);

art. 25, par. 1, del Regolamento prevede che "tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento [debba mettere] in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati" (cfr. anche conss. 75 e 78 del Regolamento);

sulla base del richiamato principio della "protezione dei dati fin dalla progettazione", i titolari dovrebbero effettuare revisioni periodiche delle misure di sicurezza poste a presidio e tutela dei dati personali, nonché della procedura per la gestione delle violazioni dei dati. L'obbligo di mantenere, verificare e aggiornare, ove necessario, il trattamento si applica anche ai sistemi preesistenti. Ciò implica che i sistemi progettati prima dell'entrata in vigore del Regolamento devono essere sottoposti a verifiche e manutenzione per garantire l'applicazione di misure e garanzie che mettano in atto i principi e i diritti degli interessati in

modo efficace. Tale obbligo si estende anche ai trattamenti svolti per mezzo di un responsabile del trattamento. Infatti, le operazioni di trattamento effettuate da un responsabile dovrebbero essere regolarmente esaminate e valutate dal titolare per garantire che continuino a rispettare i principi e permettano al titolare di adempiere gli obblighi previsti dal Regolamento (cfr. le citate “Linee guida 4/2019 sull’articolo 25 - Protezione dei dati fin dalla progettazione e per impostazione predefinita”, spec. punti 7, 38, 39 e 84).

Preso atto di quanto rappresentato dalla Regione nella documentazione in atti e nelle memorie difensive, si osserva che:

in generale, la titolarità dei trattamenti di dati personali comporta comunque una responsabilità in capo al soggetto che riveste tale ruolo e, quindi, nel caso di specie, alla Regione in ordine alle scelte effettuate con riferimento a finalità e mezzi degli stessi trattamenti. Infatti, come anche indicato nelle Linee guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR (adottate il 7 luglio 2021 dal Comitato), anche se il servizio offerto dal responsabile viene da quest’ultimo definito preliminarmente in modo specifico, spetta comunque al titolare adottare la decisione finale con cui si approvano le modalità di esecuzione del trattamento nonché chiedere eventuali modifiche (cfr. punto 30); inoltre, con specifico riferimento alle misure adottate dal responsabile, sulla base delle istruzioni impartite del titolare, al fine di assicurare il rispetto degli obblighi di sicurezza di cui all’art. 32 del Regolamento, resta comunque fermo che il titolare rimane responsabile dell’attuazione di misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al Regolamento, come richiesto dall’art. 24 del medesimo (cfr. punti 37 e 135). D’altronde, oltre agli imperativi obblighi di vigilanza, le responsabilità in capo al titolare non si esauriscono con la stipula dell’atto giuridico di cui all’art. 28, par. 3, del Regolamento e con la disposizione delle istruzioni relative al trattamento, ma durano per tutto il tempo in cui il responsabile tratta i dati per suo conto. Pertanto, sia il titolare che il responsabile possono essere oggetto di sanzioni in caso di inadempimento degli obblighi stabiliti dal Regolamento poiché entrambi sono direttamente tenuti ad assicurarne il rispetto (cfr. punto 9 delle citate Linee guida); in tal caso gli eventuali interventi correttivi sono modulati con differenti gradi di afflizione sulla base delle responsabilità effettive e del grado di autonomia decisionale nel caso concreto;

sempre in generale, con riferimento alle ricorrenti argomentazioni fondate sul possesso, da parte di LAZIOcrea, della certificazione del sistema di gestione per la sicurezza delle informazioni (SGSI) in conformità alla norma UNI CEI EN ISO/IEC 27001:2017, con estensione ai controlli della ISO 27017 e ISO 27018, si evidenzia che tale certificazione non rientra, al momento, tra quelle previste dall’art. 42 del Regolamento. In ogni caso, la certificazione ai sensi dell’art. 42 del Regolamento, seppur possa essere utilizzata, da titolari o responsabili, come elemento per dimostrare il rispetto degli obblighi del Regolamento, non ne implica automaticamente il rispetto. Inoltre, occorre considerare che la certificazione di un SGSI può essere limitata a specifici ambiti (servizi e/o sedi) dell’organizzazione (riportati sinteticamente nel certificato rilasciato dall’organismo di certificazione) e che il processo di certificazione di un SGSI, basato principalmente sui risultati degli audit (verifiche documentali e sul campo), contiene elementi di incertezza sia perché legato al concetto di rischio sia perché svolto su un campione dei processi che l’organizzazione, ferma restando la sua buona fede, sottopone a certificazione. La certificazione di un SGSI basato sulla ISO/IEC 27001, quindi, non garantisce, di per sé, livelli di sicurezza, controlli o misure di sicurezza stabiliti o fissati a priori, ma assicura l’adozione dei controlli che l'organizzazione ha identificato e ritenuto adeguati sulla base di una propria valutazione del rischio. Il titolare del trattamento, pertanto, quando si avvale di un responsabile del trattamento certificato, secondo meccanismi di certificazione, a prescindere che siano approvati o meno ai sensi

dell'art. 42 del Regolamento, dovrebbe sempre verificare se le garanzie offerte dal medesimo responsabile siano efficaci e adeguate ai trattamenti a quest'ultimo affidati;

con riferimento alla violazione del principio di cui all'art. 5, par. 1, lett. f), e degli obblighi di cui all'art. 32 del Regolamento:

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, anche sulla salute, di milioni di interessati assistiti. Ciò, tenendo altresì conto delle finalità dei trattamenti e della natura dei dati personali trattati, appartenenti anche a categorie particolari. Su tale base, gli obblighi di sicurezza imposti dal Regolamento richiedono l'adozione di rigorose misure tecniche e organizzative, includendo, oltre a quelle espressamente individuate dall'art. 32, par. 1, lett. da a) a d), tutte quelle necessarie ad attenuare i rischi che i trattamenti presentano. Al riguardo, si osserva che, con riferimento alle criticità relative ai trattamenti effettuati dalla Società per conto della Regione, spetta in ogni caso al titolare del trattamento "mettere in atto misure adeguate ed efficaci [e a …] dimostrare la conformità delle attività di trattamento con il […] Regolamento, compresa l'efficacia delle misure" adottate (cons. 74 del Regolamento), anche qualora si avvalga di un responsabile per lo svolgimento di alcune attività di trattamento, al quale deve impartire specifiche istruzioni, anche sotto il profilo della sicurezza (cons. 81 e art. 32, parr. 1, lett. d), e 4, del Regolamento). Infatti, il titolare rimane responsabile dell'attuazione delle misure tecniche e organizzative adeguate per garantire ed essere in grado di dimostrare che il trattamento è effettuato in conformità al Regolamento (artt. 5, par. 2, e 24 del Regolamento; cfr. le menzionate Linee guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR, spec. punto 41);

sulla mancata adozione di misure adeguate a rilevare tempestivamente la violazione di dati personali:

- il 31 luglio 2021, dalle ore 16:49 i soggetti malintenzionati hanno effettuato una serie di operazioni propedeutiche all'attacco informatico, a seguito delle quali, alle ore 21:12, "le piattaforme di sicurezza Microsoft generavano un incidente di sicurezza di severity High denominato Multi-stage incident involving Execution & Command and control on multiple endpoints reported by multiple sources, composto da un totale di 2189 allarmi. L'incidente segnalava la rilevazione, su molteplici sistemi, di attività malevole". Dalle ore 00:00 del 1° agosto 2021 è stata "avviata la routine di cifratura dei sistemi";

- la Società ha avuto "evidenza nelle prime ore della mattina del 1° agosto quando alcune macchine virtuali sono risultate inutilizzabili"; al riguardo, la stessa ha dichiarato che "a seguito del rilevamento di "attività ostili" (2.189 allarmi) da parte della "console Microsoft Windows Defender ATP" nella serata del 31 luglio 2021, […] tale strumento di monitoraggio non era presidiato H24" e, pertanto, "non si è potuto gestire tali allarmi con "maggiore" tempestività"". Ciò anche in quanto 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";

- risulta, pertanto, accertato che l'inadeguata gestione dei predetti allarmi non ha consentito alla Società, e quindi alla Regione, di venire tempestivamente a conoscenza della violazione dei dati personali occorsa; al riguardo, non rileva, infatti, quanto sostenuto dalla Regione nelle memorie difensive in ordine alla circostanza che "per le pubbliche amministrazioni, l'ordinamento vigente a tutt'oggi ancora non preveda l'obbligo di attivazione di un SOC presidiato continuativamente h24", in quanto, sotto il

profilo della protezione dei dati, il Regolamento, in ossequio al principio di responsabilizzazione, demanda al titolare e al responsabile il compito di individuare e adottare misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato ai rischi presentati dai trattamenti, che nel caso di specie risultavano elevati in ragione della natura dei dati trattati, della larga scala degli interessati, anche vulnerabili, coinvolti, nonché, in caso di violazione, delle possibili conseguenze negative nei confronti degli interessati con particolare riferimento all'esercizio del diritto all'accesso alle cure sanitarie;

con riguardo alla mancata adozione di misure adeguate a garantire la sicurezza delle reti:

- la Società non aveva adottato adeguate misure per segmentare e segregare le reti su cui erano attestate le postazioni di lavoro dei propri dipendenti, quelle dei dipendenti della Regione Lazio, nonché i sistemi (server) utilizzati per i trattamenti effettuati in qualità di titolare o di responsabile anche per conto della Regione. In particolare, le regole di filtering configurate sui sistemi firewall presenti nel data center gestito dalla Società, limitate solo a specifici sistemi o servizi critici, non hanno impedito la propagazione del malware su circa 180 sistemi;

- nell'ambito delle attività di analisi condotte da Leonardo S.p.a. in relazione alla violazione dei dati personali in esame, è stato definito un "Mitigation, Eradication & Improvement Plan" (di seguito "Piano") che prevede l'adozione, tra le altre, di specifiche azioni volte alla segregazione e messa in sicurezza dei diversi sistemi gestiti dalla Società. In particolare, tali azioni prevedono la "segmentazione delle reti evitando subnet eccessivamente ampie e limitando, di fatto, la possibilità per un potenziale attaccante di eseguire movimenti laterali", la "reinstallazione completa di tutti i sistemi server e contestuale posizionamento in segmenti di rete suddivisi per layer di sicurezza (Tier), ad accesso limitato e amministrabili solo da un numero limitato di workstation, a loro volta isolate dalle altre reti (PAW, Privileged Access Workstation)", nonché la "riprogettazione della network [...] favorendo il principio del privilegio minimo";

- peraltro, al momento in cui si è verificata la violazione dei dati personali, l'accesso remoto, tramite VPN, alla rete della Regione, avveniva mediante una procedura di autenticazione informatica basata solo sull'utilizzo di username e password. In relazione a tale aspetto, la Regione e la Società, a seguito dell'incidente, hanno ritenuto necessario attivare una procedura con doppio fattore di autenticazione, come previsto anche dal predetto Piano;

- quanto sostenuto dalla Regione nelle memorie difensive non consente di superare le criticità rilevate nell'atto di avvio del procedimento in quanto, anche se "la separazione logica e la segregazione fisica delle reti […] hanno impedito agli hacker di esfiltrare i dati presenti nel Data Center", questo non ha impedito a soggetti non autorizzati di accedere e compromettere, rendendoli indisponibili, molti sistemi server che, come dichiarato dalla Società nel corso dell'accertamento ispettivo, al momento della violazione, potevano essere raggiunti a partire dalla rete utilizzata per l'accesso VPN dei dipendenti della Regione Lazio;

con riguardo all'obsolescenza dei software di base istallati su alcuni sistemi di trattamento:

- dalla documentazione in atti è emerso che il server con hostname "RLWSIRIFT01" è stato "uno dei principali punti di snodo utilizzati dall'attaccante nella fase finale dell'attacco" informatico alla base della violazione dei dati personali in esame. La Società ha evidenziato che sul "server con hostname "RLWSIRIFT01" […] 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". In particolare, è emerso che sul sistema di trattamento in questione era installato un sistema operativo obsoleto (Windows Server 2008 R2 Standard) per il quale il produttore (Microsoft) aveva cessato la distribuzione degli aggiornamenti di sicurezza. Ciò rendeva particolarmente difficile il patching di tale sistema, richiedendo l'adozione, realisticamente non tempestiva, di eventuali accorgimenti ad hoc in grado di fronteggiare nuove vulnerabilità;

- solo a seguito della violazione dei dati personali, la Società "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";

- quanto riportato dalla Regione nelle memorie difensive non consente di superare i rilievi dell'Ufficio in ordine all'utilizzo di software di base obsoleti, per i quali non sono più disponibili aggiornamenti di sicurezza, anche in considerazione del fatto che i sistemi server su cui tali software erano installati, diversamente da quanto asserito, non erano adeguatamente isolati da altri sistemi server mediante i quali erano effettuati trattamenti di dati anche relativi alla salute degli assistiti del Servizio sanitario regionale;

con riguardo alla mancata adozione di misure adeguate ad assicurare la disponibilità e la resilienza dei sistemi e dei servizi di trattamento:

- la Società, al momento dell'incidente di sicurezza, utilizzava un sistema di gestione dei backup e che "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";

- la gestione dei backup veniva effettuata mediante una "tabella contenente l'elenco di progetti per cui era effettuato il backup con l'indicazione dei referenti, del nome dello schema, degli host e delle relative policy di retention";

- solo a seguito della violazione dei dati personali, la Società ha adottato un nuovo sistema di gestione dei backup che consente una più semplice gestione e monitoraggio del backup dei dati e dei sistemi sulla base di quanto indicato da ciascun referente di progetto, al momento del rilascio in esercizio;

- quanto affermato dalla Regione nelle memorie difensive non consente di superare i rilievi dell'Ufficio in ordine alle modalità adottate per assicurare la disponibilità e la resilienza dei sistemi e dei servizi di trattamento, inclusa la gestione del backup, in quanto le stesse risultavano non in linea con le migliori pratiche di settore e non adeguate al contesto dei trattamenti svolti dalla Società per conto della Regione Lazio;

- la violazione ha determinato l'impossibilità di utilizzare molti sistemi informativi della Regione, alcuni dei quali trattano dati sulla salute, tra cui si segnalano: ASUR – Anagrafe sanitaria unica regionale; nuovo RECUP – Gestione prenotazioni, accettazioni, disdette; ESCAPE, per la gestione dei referti relativi ad esami di laboratorio; pagamenti prestazioni afferenti attività specialistica ambulatoriale compreso pagamenti on line tramite PAGOPA; Sistema regionale invio flussi per debito informativo afferente prestazioni specialistiche in carico al SSN, prestazioni intramoenia, domiciliari e prestazioni effettuate presso i consultori, ricoveri ospedalieri, accessi di Pronto Soccorso; RICDIG – Sistema registrazione ricetta dematerializzata per prescrizione farmaci e prestazioni ambulatoriali; attività di screening

neonatali e oncologici; Piattaforma regionale di sorveglianza Covid-19; ADVICE – Sistema di teleconsulto per consulenze verso i DEA di secondo livello; Sistema AVR – Anagrafe Vaccinale Regionale;

- i predetti sistemi informativi, attraverso i quali sono trattati dati sulla salute degli assistiti del Servizio sanitario regionale, sono stati indisponibili per un arco temporale che si estende, in alcuni casi, per una durata di alcuni mesi; la società LAZIOcrea ha infatti provveduto a ripristinare gli stessi, in ambiente cloud, in via graduale dando priorità a quelli maggiormente critici (es. vaccinazione Covid-19) per completare il completo ripristino nel mese di ottobre 2021 (cfr. notifiche della società LAZIOcrea del 10 settembre e 29 ottobre 2021 – cui rinvia espressamente la Regione con la notifica del XX – nonché riserve del verbale degli accertamenti ispettivi del XX);

- la mancata disponibilità di accesso ai dati conservati sui predetti sistemi è stata determinata:

  i) direttamente dall'attacco informatico che, compromettendo lo strato applicativo del sistema di virtualizzazione, ha quindi reso indisponibili circa 180 sistemi server virtuali e inaccessibili i dati ivi trattati;

  ii) indirettamente dalla scelta di LAZIOcrea di spegnere tutti i sistemi server in quanto, al momento dell'attacco informatico, non era in grado né di determinare quali fossero compromessi, né di evitare un'ulteriore propagazione del malware stante l'assenza di una segregazione delle reti su cui gli stessi erano attestati;

- pertanto, qualora LAZIOcrea avesse provveduto a segregare adeguatamente le reti su cui erano attestati i sistemi server e le postazioni di lavoro dei propri dipendenti e della Regione Lazio, la stessa Società non avrebbe dovuto procedere allo spegnimento dei citati sistemi server, e quindi le strutture sanitarie non avrebbero subito l'indisponibilità di accesso a numerosi sistemi informativi e ai relativi dati;

- la segregazione delle reti è peraltro una delle più comuni misure adottate nell'ambito di data center che ospitano sistemi informatici deputati al trattamento di diverse categorie di dati personali, anche relativi allo stato di salute, che LAZIOcrea - in qualità di società che opera nel settore ICT secondo il modello in house providing - avrebbe senz'altro dovuto assicurare tenuto conto del contesto e delle caratteristiche dei trattamenti in relazione ai quali è stata designata responsabile dalla Regione e dalle strutture sanitarie;

con riferimento alla violazione del principio di cui all'art. 25, par. 1, del Regolamento:

l'art. 25 del Regolamento richiede che le misure e le garanzie individuate e adottate dal titolare siano specificamente connesse all'attuazione dei principi di protezione dei dati nell'ambito dei trattamenti in concreto svolti; le misure e le garanzie devono essere concepite per essere robuste e il titolare del trattamento deve essere in grado di attuarne ulteriori al fine di far fronte a un eventuale aumento dei rischi. L'efficacia o meno delle misure dipende dal contesto del trattamento e degli altri elementi che il titolare deve tenere in considerazione all'atto della determinazione dei mezzi del trattamento;

in merito alle argomentazioni fondate sul possesso, da parte di LAZIOcrea, della certificazione del (SGSI) in conformità alla norma UNI CEI EN ISO/IEC 27001:2017, si richiama quanto sopra osservato circa i doveri in capo al titolare del trattamento nell'adozione, fin dalla progettazione, di misure efficaci e adeguate ai trattamenti anche se affidati a un responsabile del trattamento; peraltro, anche nel caso in cui "un trattamento sia certificato ai sensi dell'articolo 42, il titolare è comunque tenuto a garantire il monitoraggio

costante e il miglioramento della conformità ai criteri della DPbDD" (cfr. "Linee guida 4/2019 sull'articolo 25 - Protezione dei dati fin dalla progettazione e per impostazione predefinita", punto 91);

la valutazione dei rischi effettuata dal responsabile può essere utilizzata, ma non è di per sé sufficiente, per consentire al titolare del trattamento di progettare adeguatamente i trattamenti al fine di integrare le garanzie a tutela dei diritti e delle libertà degli interessati e di adottare misure -anche organizzative- ulteriori rispetto a quelle individuate dal responsabile del trattamento;

quanto riportato dalla Regione nelle memorie difensive non consente di superare i rilievi dell'Ufficio in ordine alla violazione del principio di protezione dei dati fin dalla progettazione con particolare riferimento all'adeguatezza e all'efficacia delle misure adottate in relazione al contesto e all'ambito dei trattamenti svolti dal titolare.

3. Conclusioni.

Alla luce delle valutazioni sopra richiamate, tenuto conto delle dichiarazioni rese dalla Regione Lazio 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 rileva l'illiceità del trattamento di dati personali effettuato dalla Regione Lazio, nei termini di cui in motivazione, in violazione degli artt. 5, par. 1, lett. f), 25, par. 1, e 32 del Regolamento.
In tale quadro, considerato che sono state adottate misure volte a superare le criticità sopra descritte non ricorrono i presupposti per l'adozione delle misure correttive di cui all'art. 58, par. 2, 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 degli artt. 5, par. 1, lett. f), 25, par. 1, e 32 del Regolamento, causata dalla condotta posta in essere dalla Regione Lazio, è soggetta all'applicazione della sanzione amministrativa pecuniaria ai sensi dell'art. 83, parr. 3, 4 e 5, 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, 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.

Con specifico riguardo alla natura e alla gravità delle violazioni (art. 83, par. 2, lett. a), d) e g), del Regolamento), occorre considerare che la numerosità e delicatezza dei servizi colpiti e, in ragione di ciò, l'elevato numero di interessati coinvolti e le tipologie di dati personali oggetto di violazione (comprese categorie particolari di cui all'art. 9 del Regolamento, o altri dati connotati da particolare delicatezza quali dati retributivi e dati bancari), e ciò a prescindere dalla mancata esfiltrazione dei dati medesimi.

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

A ciò si aggiunga, ai sensi dell'art. 83, par. 2, lett. e), del Regolamento, che la Regione è già stata destinataria di alcuni provvedimenti correttivi e sanzionatori.

Inoltre, ai sensi dell'art. 83, par. 2, lett. h), del Regolamento, l'Autorità ha preso conoscenza dell'evento dalla tempestiva notifica della violazione trasmessa dalla Regione.

In senso favorevole al titolare occorre comunque considerare, ai sensi dell'art. 83, par. 2, lett. c) e f), del Regolamento, che la Regione ha cooperato con l'Autorità introducendo, nella concomitanza del contesto emergenziale da Covid-19, misure idonee a superare le criticità sopra evidenziate.

In ragione dei suddetti elementi, valutati nel loro complesso, si ritiene di determinare l'ammontare della sanzione pecuniaria prevista dall'art. 83, parr. 3, 4 e 5, del Regolamento, nella misura di euro 120.000,00 (centoventimila) per la violazione degli artt. 5, par. 1, lett. f), 25, par. 1, e 32 del Regolamento o, quale sanzione amministrativa pecuniaria ritenuta, ai sensi dell'art. 83, par. 1, del Regolamento, effettiva, proporzionata e dissuasiva.

Si ritiene, altresì, che debba applicarsi la sanzione accessoria della pubblicazione sul sito del Garante del presente provvedimento, prevista dall'art. 166, comma 7, del Codice e dall'art. 16 del Regolamento del Garante n. 1/2019, anche in considerazione del numero di interessati coinvolti, della tipologia di dati personali oggetto di violazione e dell'ampiezza e dell'impatto sulla disponibilità dei servizi colpiti.

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 dalla Regione Lazio per la violazione degli artt. 5, par. 1, lett. f), 25, par. 1, e 32, del Regolamento nei termini di cui in motivazione.

ORDINA

ai sensi degli artt. 58, par. 2, lett. i), e 83 del Regolamento, nonché dell'art. 166 del Codice, alla Regione Lazio, codice fiscale 80143490581, in persona del legale rappresentante pro-tempore, di pagare la somma di euro 120.000,00 (centoventimila) 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 Regione Lazio, in caso di mancata definizione della controversia ai sensi dell'art. 166, comma 8, del Codice, di pagare la somma di euro 120.000,00 (centoventimila) secondo le modalità indicate in allegato, entro 30 giorni dalla notificazione del presente provvedimento, pena l'adozione dei conseguenti atti esecutivi a norma dall'art. 27 della legge n. 689/1981.

DISPONE

ai sensi dell'art. 166, comma 7, del Codice, la pubblicazione per intero del presente provvedimento sul sito web del Garante e 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
Cerrina Feroni

IL SEGRETARIO GENERALE
Mattei

[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 "subìto 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 rispristinato 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", "comunicate 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 correttivi 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 dl cui si propone l'adozione, per porre rimedio alla violazione e attenuarne i possibili effetti negativi per gli interessati; misure tecniche organizzative adottate, o dl 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 Lazione 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 ella 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