Provvedimento del 4 luglio 2024 [10063782]

VEDI ANCHE Newsletter del 22 ottobre 2024

[doc. web n. 10063782]

Provvedimento del 4 luglio 2024

Registro dei provvedimenti
n. 572 del 4 luglio 2024

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, alla quale hanno preso parte il prof. Pasquale Stanzione, 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 (di seguito, "Regolamento");

VISTO il Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al Regolamento (UE) 2016/679 (d.lgs. 30 giugno 2003, n. 196, come modificato dal d.lgs. 10 agosto 2018, n. 101, di seguito "Codice");

VISTA la violazione di dati personali notificata da Postel S.p.A. all'Autorità il 17 agosto 2023, ai sensi dell'art. 33 del Regolamento, più volte integrata dalla Società, fino al 4 ottobre 2023, relativa a un attacco informatico ai propri sistemi;

ESAMINATA la documentazione in atti;

VISTE le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

RELATORE il prof. Pasquale Stanzione;

PREMESSO

1. La violazione di dati personali e l'attività istruttoria.

In data 17 agosto 2023, Postel S.p.A. (di seguito, la Società) ha notificato al Garante, ai sensi dell'art. 33 del Regolamento, una violazione dei dati personali, più volte integrata dalla stessa fino all'invio della versione definitiva il 4 ottobre 2023.

Con la predetta segnalazione, la Società ha comunicato di avere subito "un attacco informatico di tipo ransomware oggetto di successiva rivendicazione da parte della cybergang denominata Medusa. Tale attacco ha comportato il blocco di alcuni server e di alcune postazioni di lavoro [della Società], con conseguente attivazione delle procedure di recovery/restore".

In particolare, l'attacco ha comportato l'esfiltrazione (e la successiva pubblicazione nel dark web)

di file contenenti dati personali afferenti ai lavoratori dell'azienda (inclusi lavoratori cessati), ai congiunti dei lavoratori, ai titolari di cariche societarie (membri del consiglio di amministrazione, del collegio sindacale e dell'organismo di vigilanza), a candidati a posizioni lavorative, nonché a esponenti delle imprese intrattenenti rapporti commerciali con la Società.

Per alcuni file presenti nelle cartelle di rete, la Società non è stata in grado di provvedere al ripristino e, di conseguenza, limitatamente a tali dati si è verificata anche la perdita di disponibilità.

Sulla base di quanto dichiarato dalla Società nella notifica al Garante, la violazione ha riguardato, nel complesso, circa 25.000 interessati e le categorie di dati personali oggetto di violazione sono state molteplici: dati anagrafici; dati di contatto; dati di accesso e di identificazione; dati di pagamento; dati relativi a condanne penali e ai reati; dati relativi a documenti di identificazione/riconoscimento; dati che rivelano l'appartenenza sindacale; dati relativi alla salute.

In data 13 ottobre 2023, considerata l'assenza, all'interno della notifica definitiva inviata dalla Società, di elementi ritenuti necessari per l'esercizio, da parte dell'Autorità, dei compiti e dei poteri previsti dal Regolamento, sono state richieste informazioni alla Società in merito, in particolare, alle vulnerabilità utilizzate per portare a compimento l'attacco subito e alle informazioni fornite, in qualità di responsabile del trattamento, ad altri titolari i cui dati erano stati coinvolti nella violazione.

In data 23 ottobre 2023, la Società ha fornito riscontro alla richiesta dell'Autorità e, in tale occasione, ha rappresentato che:

> "tramite le […] vulnerabilità [CVE-2022-41080 e CVE-2022-41082] l'attaccante, a seguito di penetrazione nei sistemi della Società, è stato in grado di creare un'utenza la quale è stata contestualmente aggiunta al gruppo degli amministratori di dominio, al fine di ottenere la persistenza dell'attore malevolo sulla piattaforma informatica aziendale" (v. nota 23/10/2023 cit., p. 1);
>
> "il perimetro dell'incidente di sicurezza non ha riguardato le piattaforme di produzione dedicate all'erogazione dei servizi in favore della clientela della Società, bensì esclusivamente alcuni sistemi utilizzati per lo svolgimento di attività ad uso interno. Cionondimeno, sono stati esfiltrati dati personali trattati dalla Società in veste di responsabile del trattamento afferenti ad alcuni documenti, eccezionalmente presenti nei predetti sistemi utilizzati per lo svolgimento di attività ad uso interno, riconducibili a 22 [società] clienti rispetto al totale dei documenti gestiti dalla Società per conto di circa 4.000 clienti" (v. nota cit., p. 1);
>
> "i suddetti clienti sono stati tutti resi edotti dell'evento da parte della scrivente tramite comunicazioni formali ex art.33, par. 2, GDPR" (v. nota cit., p. 2).

La Società ha fornito l'elenco dei titolari del trattamento, per i quali svolge il ruolo di responsabile del trattamento, coinvolti nel data breach in oggetto i quali hanno regolarmente notificato la violazione dei dati personali ai sensi degli artt. 33 e 34 del Regolamento.

È stato inoltre verificato che la Società, per i dati oggetto di data breach per i quali svolge il ruolo di titolare del trattamento, ha provveduto alla comunicazione della violazione agli interessati coinvolti, ritenendo che il rischio per i diritti e le libertà di questi ultimi fosse elevato.

2. L'avvio del procedimento e le deduzioni della Società.

Il 15 dicembre 2023, l'Ufficio ha effettuato, ai sensi dell'art. 166, comma 5, del Codice, la notificazione alla Società delle presunte violazioni del Regolamento riscontrate, con riferimento agli artt. 5, par. 1, lett. f), 25, 28, par. 3, lett. f), 32, 33, del Regolamento.
In data 12 gennaio 2024, la Società ha presentato i propri scritti difensivi e in tale occasione ha

evidenziato che:

> “Postel […] si è dotata di uno strutturato sistema di gestione volto a proteggere i diritti e le libertà delle persone fisiche che potrebbero essere impattati dai trattamenti di Dati che essa svolge” (v. nota 12/01/2024 cit., p. 1);
>
> “quanto al profilo della sicurezza dei Dati, sono implementate misure organizzative e tecniche volte a: - gestire i rischi di violazione degli stessi; - attuare le azioni richieste dalla vigente normativa ove cionondimeno delle violazioni dovessero verificarsi” (v. nota cit., p. 1);
>
> “a fronte della violazione dei Dati subita (la “Violazione”), Postel ha introdotto tutte le azioni necessarie a: - adempiere alle prescrizioni di cui agli artt. 33 e 34 del […] Regolamento […]; - mitigare per quanto possibile l’impatto della Violazione stessa sui diritti e sulle libertà delle persone fisiche, nonché degli altri portatori d’interesse coinvolti” (v. nota cit., p. 2);
>
> “la stessa Postel è la prima vittima della condotta criminale di Medusa, stante i gravissimi danni economici connessi ai rallentamenti dell’infrastruttura tecnologica resisi necessari per mitigare le conseguenze della Violazione, nonché l’esigenza di destinare parte rilevante delle proprie risorse umane, economiche e tecnologiche per un consistente periodo di tempo alla gestione della Violazione stessa” (v. nota cit., p. 2);
>
> “ha analizzato le vicende connesse alla Violazione […] e conseguentemente segnala che: - sono in corso una serie di ulteriori misure organizzative e tecniche volte a rafforzare la sicurezza dei Dati trattati; - si stanno definendo azioni di rafforzamento dei propri protocolli di gestione delle violazioni dei Dati a norma degli artt. 33 e 34 del Regolamento, anche per quanto attiene alla gestione dei rapporti con eventuali committenti titolari del trattamento, ex art. 28, par 3, lett. f) del Regolamento” (v. nota cit., p. 3);
>
> “Postel desidera manifestare il proprio spirito di massima collaborazione con l’Autorità stessa, dichiarandosi disponibile ad aderire a eventuali prescrizioni aggiuntive che la medesima intenda raccomandare” (v. nota cit., p. 3);
>
> “sull’asserita insufficienza della notifica della Violazione […] Postel ritiene tale valutazione giuridicamente infondata, oltre che non corrispondente ai fatti, e pertanto non condivisibile. Infatti, nell’adempiere ai propri obblighi ex art. 33 del Regolamento, Postel ha compilato tutti i campi del modulo standard di notifica presente sul sito Internet istituzionale di codesta spettabile Autorità: tale compilazione, per quanto completa, ha avuto carattere necessariamente sintetico” (v. nota cit., p. 3, 4);
>
> “inoltre, l’elemento informativo di cui codesta spettabile Autorità contesta l’omissione – cioè, il tipo di vulnerabilità utilizzate dall’attaccante - non risulta espressamente menzionato tra gli elementi obbligatori della notifica ai sensi del Regolamento (neanche nel considerando 87 citato da codesta spettabile Autorità). Né esplicite indicazioni sul punto si rinvengono nel Codice e/o in provvedimenti del Comitato Europeo per la Protezione dei Dati e/o di codesta spettabile Autorità” (v. nota cit., p. 4);
>
> “la contestata omissione dell’elemento informativo indicato da[ll’] Autorità non è certo frutto di una mancanza di trasparenza da parte di Postel […] a fronte di una successiva precipua richiesta sul punto da parte di codesta spettabile Autorità, Postel non ha esitato a fornire tutte le informazioni richieste” (v. nota cit., p. 4, 5);
>
> “l’affermazione d[ell’] Autorità secondo cui la notifica inviata da Postel non avrebbe indicato «[…] il dettaglio delle misure di sicurezza che erano applicate ai sistemi coinvolti nell’attacco […]» non è conforme al vero, avendo la scrivente diligentemente compilato il campo F.9 […] del modulo standard di notifica predisposto dall’Autorità medesima” (v. nota cit., p. 5);

“Postel intende prendere positivamente e proattivamente atto delle osservazioni di codesta spettabile Autorità, impegnandosi ad attuare attività di sensibilizzazione, esercitazioni e simulazioni inerenti ai propri protocolli di gestione delle violazioni di Dati, specie con riguardo all’implementazione di un maggiore livello di dettaglio e granularità delle informazioni trasmesse all’autorità di controllo ex art. 33 del Regolamento. Con l’occasione, s’implementeranno anche azioni volte a ridurre i tempi di gestione delle eventuali violazioni di Dati” (v. nota cit., p. 5);

“nel caso de quo i tempi di gestione sono ampiamente giustificati dalla complessità e portata della Violazione medesima […]. Peraltro, la Violazione è avvenuta durante il periodo estivo di parziale chiusura aziendale, con conseguente accresciuta difficoltà di attivazione delle procedure di contingenza” (v. nota cit., p. 5);

in merito alla contestazione relativa alla “mancata adozione di misure di mitigazione delle vulnerabilità” “la menzionata vulnerabilità non costituisc[e] la [causa profonda] della Violazione, da identificarsi solo ed esclusivamente nell’azione criminale di Medusa. Conseguentemente, non è rinvenibile un nesso di causalità diretta tra l’esistenza della vulnerabilità software e il verificarsi della Violazione” (v. nota cit., p. 6);

“la mancata rimozione delle vulnerabilità in esame non è derivata dall’assenza di procedure e protocolli aziendali in materia di «patch and vulnerability management» o dall’inadeguatezza delle procedure e dei protocolli stessi. Infatti, sull’infrastruttura di Postel è implementato uno strutturato processo di early warning, di rilevazione ed emissione di security critical alert e di scansione e patching dei propri sistemi informativi. Tale processo è stato attivato anche con riguardo alle menzionate vulnerabilità e, in particolare, a seguito dell’early warning, le stesse erano state temporaneamente gestite applicando dei workaround. Purtroppo, però, a causa di un errore umano nella configurazione delle attività di scansione, il server Exchange oggetto dell’attacco era rimasto escluso dalla scansione medesima: ciò ha accidentalmente determinato il mancato patching delle citate vulnerabilità, esclusivamente con riguardo a tale sistema. Pertanto, anche con riguardo alla gestione delle menzionate vulnerabilità sono state implementate delle misure di sicurezza conformi ai requisiti di cui agli artt. 5, par. 1, lett. f), 25 e 32 del Regolamento, che solo a causa di un’isolata e sfortunata anomalia non sono state in grado di operare efficacemente” (v. nota cit., p. 7);

“è stato ritenuto opportuno implementare delle azioni di miglioramento della postura di sicurezza aziendale e si sta quindi implementando uno strutturato piano di azione a tale fine […] esso comprende, tra l’altro, la revisione e il miglioramento del processo gestionale dei security critical alert. Peraltro, tale Cybersecurity Improvement Plan si affianca a uno strutturato e preesistente sistema di misure organizzative e tecniche” (v. nota cit., p. 8);

in merito alla contestazione relativa al “mancato supporto ai titolari del trattamento da parte del responsabile” “Postel ritiene tali valutazioni difformi dalla realtà fattuale […]. [le dichiarazioni di alcuni titolari], rese in assenza di contraddittorio, provengono peraltro non già da soggetti terzi e imparziali, bensì controinteressati e che trarrebbero unicamente vantaggi dall’imputazione alla sola Postel dell’eventuale omesso e/o ritardato adempimento dei propri obblighi in materia di protezione dei dati personali (in primis, quelli ex artt. 33 e 34 del Regolamento). Peraltro, tali dichiarazioni promanano solo da tre dei ventidue clienti di Postel impattati dalla Violazione” (v. nota cit., p. 8);

“relativamente al titolare Coop Italia S.p.A., il coinvolgimento dello stesso nella Violazione era comunicato da Postel a ridosso della relativa scoperta, prima per vie brevi e poco dopo con comunicazione via PEC. Il 22 settembre [2023], completate le analisi necessarie, Postel inviava a Coop Italia la relazione di dettaglio inerente alla Violazione, fermo restando che

nelle more erano sempre rimasti aperti i canali d'interlocuzione con il cliente […]. Peraltro, anche dopo l'invio della citata relazione, Postel è rimasta a disposizione del titolare con riguardo a ulteriori richieste di supporto" (v. nota cit., p. 9);

"quanto al titolare SAT S.p.A., a fronte della prima comunicazione inviata il 30 agosto [2023] e alle richieste di chiarimenti ulteriori sottoposte dallo stesso titolare il giorno successivo, Postel forniva i risconti richiesti dopo pochi giorni, cioè il 7 settembre [2023], e comunque dopo avere completato le necessarie attività istruttorie" (v. nota cit., p. 9);

"considerazioni analoghe possono svolgersi con riguardo a quanto riportato dal titolare Nexi S.p.A., a cui Postel trasmetteva le informazioni rilevanti ex art. 28, par. 3, lett. f) del Regolamento l'8 settembre [2023], cioè appena scoperto il coinvolgimento del titolare stesso nella Violazione, circostanza non emersa in precedenza a fronte del fatto che le analisi del perimetro dell'incidente erano ancora in via di svolgimento. Le interlocuzioni con tale cliente sono comunque proseguite nei giorni successivi, con anche la produzione di una relazione ulteriormente dettagliata sulle dinamiche della Violazione" (v. nota cit., p. 9);

"i tempi di trasmissione delle informazioni rilevanti ex art. 28, par. 3, lett. f) del Regolamento da parte di Postel nei confronti dei tre committenti sopra menzionati non sono stati in alcun modo dovuti a inerzia o mancanza di collaborazione, bensì sono imputabili agli stessi tempi tecnici di analisi e raccolta delle informazioni, da parametrare alla portata dell'attacco informatico perpetrato da Medusa" (v. nota cit., p. 9);

con riferimento all'art. 83 par. 2 lett. a) del Regolamento "la Violazione è connessa alla perdita di riservatezza e disponibilità di alcuni Dati detenuti da Postel, causata da un attacco informatico perpetrato dalla cybergang professionale Medusa. Gli interessati coinvolti nella violazione sono circa 24.800: tuttavia, solo con riguardo a 2.161 interessati (pari quindi a circa l'8,71% del totale) è stato rilevato un livello di rischio elevato per i diritti e le libertà delle persone fisiche tale da determinare la necessità d'inviare una comunicazione ex art. 34 del Regolamento. Quanto invece ai Dati detenuti da Postel quale responsabile del trattamento, la Violazione ha impattato sui Dati riconducibili a soli ventidue clienti, rispetto al totale dei documenti gestiti da Postel per conto di circa 4.000 clienti" (v. nota cit., p. 10, 11);

con riferimento all'art. 83 par. 2 lett. b) del Regolamento "la Violazione è stata causata dall'attacco informatico di natura criminale dolosamente perpetrato da Medusa […]. Conseguentemente, alcuna infrazione del Regolamento può essere imputabile a Postel" (v. nota cit., p. 11);

con riferimento all'art. 83 par. 2 lett. c) del Regolamento "per attenuare le conseguenze della Violazione, si è immediatamente attivata la procedura aziendale di gestione degli eventi e incidenti di sicurezza informatica, con: apertura di un ticket per la gestione dell'incidente; convocazione dell'unità di crisi tecnica; svolgimento di analisi continuative inerenti alla dinamica e al perimetro dell'incidente; implementazione di azioni di contenimento dell'attacco; sanificazione e successivo ripristino dei sistemi informativi. Inoltre, Postel ha: implementato attività di comunicazione, collaborazione, supporto e assistenza nei confronti degli interessati (conformi, come riconosciuto anche da codesta spettabile Autorità, all'art. 34 GDPR), dei committenti (specie quelli per cui Postel opera come responsabile del trattamento), nonché degli altri rilevanti portatori d'interesse; presentato denuncia alle competenti autorità di polizia" (v. nota cit., p. 11);

con riferimento all'art. 83 par. 2 lett. d) del Regolamento "al momento della Violazione risultavano - tra le altre - implementate le seguenti misure di sicurezza (tuttora presenti) a tutela dei sistemi informativi: procedure di autenticazione sicura; sistemi antivirus; sistemi antimalware; sistemi del tipo «Defender for Identity»; sistemi di prevenzione delle intrusioni;

sistemi firewall; procedure e sistemi di «security information and event management»; procedure di backup; procedure di business continuity e disaster recovery" (v. nota cit., p. 11, 12);

"successivamente alla Violazione […] è stato implementato un Cybersecurity Improvement Plan che, per quanto attiene al tema della gestione delle vulnerabilità, prevede la revisione e il miglioramento del processo gestionale dei security critical alert. In particolare, è stata prevista l'integrazione tra gli strumenti di scansione, asset management e trouble ticketing, facendo sì che i ticket di sicurezza siano generati e inoltrati automaticamente alla funzione competente ogni volta che i sistemi di scansione rilevano una vulnerabilità oggetto di security critical alert, onde consentirne la relativa presa in carico e risoluzione, la quale è disciplinata da service level agreement concordati tra le funzioni di sicurezza e quelle operative" (v. nota cit., p. 12);

"il […] Cybersecurity Improvement Plan comprende le seguenti ulteriori azioni di miglioramento […]: - rafforzamento delle attività di sensibilizzazione verso i dipendenti e organizzazione di corsi di formazione sulla gestione sicura dei dati; - rafforzamento del processo di upgrade dei sistemi operativi e middleware; - migrazione verso sistemi di file sharing in cloud (SharePoint); - migrazione delle caselle di posta elettronica ancora presenti su sistema on premises verso piattaforma in cloud" (v. nota cit., p. 12, 13);

"sono in via d'implementazione attività di sensibilizzazione, esercitazioni e simulazioni inerenti ai protocolli di gestione delle violazioni di Dati, specie per quanto attiene: - all'implementazione di un maggiore livello di dettaglio e granularità delle informazioni trasmesse all'autorità di controllo ex art. 33 del Regolamento; - all'assistenza nei confronti di eventuali titolari del trattamento per conto dei quali Postel agisce quale responsabile del trattamento stesso" (v. nota cit., p. 13);

con riferimento all'art. 83, par. 2, lett. f), del Regolamento "sin dalla rilevazione della Violazione, Postel ha prestato la più ampia cooperazione per rimediare all'evento stesso e attenuarne i possibili effetti negativi […] Altresì, Postel ha proceduto alla notifica a codesta spettabile Autorità ex art. 33 del Regolamento e a riscontrare puntualmente le richieste di chiarimenti della stessa" (v. nota cit., p. 13);

con riferimento all'art. 83, par. 2, lett. g), del Regolamento "la Violazione ha riguardato principalmente Dati anagrafici e di contatto, nonché talora Dati di pagamento e inerenti a documenti identificativi e/o di riconoscimento. In un numero ancora minore di casi, sono stati anche impattati Dati rivelanti l'appartenenza sindacale e relativi alla salute" (v. nota cit., p. 13);

con riferimento all'art. 83, par. 2, lett. h), del Regolamento "[l'] Autorità è venuta a conoscenza della Violazione per effetto della notifica […] effettuata dalla stessa Postel ex art. 33 del Regolamento subito dopo la scoperta della Violazione medesima e successivamente oggetto d'integrazione" (v. nota cit., p. 13);

con riferimento all'art. 83, par. 2, lett. i), del Regolamento "non risultano specifici provvedimenti correttivi già adottati da codesta spettabile Autorità con riferimento alla specifica violazione contestata" (v. nota cit., p. 14);

in relazione all'art. 83 par. 2 lett. k) del Regolamento "[dalla violazione alla Società] è derivata una perdita economica" (v. nota cit., p. 14);

"l'eventuale irrogazione di una sanzione amministrativa pecuniaria da parte di codesta spettabile Autorità aggraverebbe ulteriormente l'impatto economico della Violazione in capo

alla scrivente, con potenziale pregiudizio anche per i portatori d'interesse nei confronti della stessa (lavoratori, fornitori, ecc.)" (v. nota cit., p. 15).

In data 31 gennaio 2024, a seguito di specifica richiesta della Società, si è tenuta l'audizione della stessa. In tale occasione la parte ha rappresentato che:

"la Società è certificata ISO9001 e ISO27001";

"le policy aziendali in tema di privacy, anche in virtù della composizione societaria pubblica del gruppo, sono basate su un'articolata strutturazione, suddivisa in 14 aree di intervento declinate in apposite linee guida privacy di gruppo che definiscono ruoli, procedure e azioni. Oltre a ciò, a partire dal GDPR la Società ha avviato un'azione di miglioramento continuo in tema di privacy che ha riguardato anche attività di formazione del personale e di audit mirati";

"la Società ritiene che l'evento non sia ascrivibile a un problema strutturale e sistemico, ma a un episodio isolato. Per questo motivo, si evidenzia come la Società non abbia agito mossa da una logica di vantaggio nella imperfetta applicazione di misure di sicurezza, non avendo la stessa generato alcun risparmio di costi in capo alla Società medesima";

"una recente sentenza della CGUE (causa C-340 del 2021) […] ha stabilito che il verificarsi di un data breach non è prova in re ipsa di una inadeguatezza strutturale delle misure di sicurezza implementate dal titolare del trattamento";

"con riferimento alla gestione del data breach si sottolinea come l'attacco abbia comportato la necessità di effettuare una ricognizione manuale e puntuale dei sistemi e dei dati coinvolti in ragione dell'ampiezza della violazione. L'analisi ha coinvolto tutti i livelli aziendali e ha richiesto un tempo significativo";

"ad oggi la Società sta valutando lo svolgimento di attività di formazione specifiche dedicate ai data breach per sensibilizzare ulteriormente il personale e migliorare la capacità di risposta in casi analoghi";

"la Società, a partire dal periodo pandemico e fino agli eventi bellici recenti e agli eventi atmosferici che hanno riguardato lo stabilimento di Melzo, è stata interessata da congiunture economiche avverse. Inoltre, a seguito dell'attacco informatico subito, la Società ha scelto di bloccare, per ragioni di sicurezza, i sistemi di produzione e, di conseguenza, alcuni clienti si sono rivolti ad altri concorrenti".

3. Esito del procedimento.

3.1 Fatti accertati e osservazioni sulla normativa in materia di protezione dei dati personali.

All'esito dell'esame degli elementi acquisiti nel corso dell'istruttoria e delle successive valutazioni dell'Autorità, sulla base delle risultanze delle specifiche relazioni tecniche redatte nel corso del procedimento, è emerso che la Società ha posto in essere delle condotte che risultano non conformi alla disciplina in materia di protezione dei dati personali.

In particolare, risulta accertato che la Società, nonostante la rilevanza del data breach subito, ha trasmesso all'Autorità una notifica delle violazioni incompleta; è stato altresì accertato che la Società non ha tenuto una condotta conforme alla disciplina di protezione dei dati neanche relativamente alle misure di sicurezza che avrebbe dovuto adottare nei termini che verranno indicati.

In proposito si evidenzia 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”.

L’art. 5, par. 1, lett. f), del Regolamento stabilisce che i dati personali devono essere “trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali”.

In proposito, 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).

In base all’art. 25, par. 1, del Regolamento il titolare del trattamento “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 [deve] mette[re] 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” (principio di protezione dei dati fin dalla progettazione).

L’art. 25, par. 2, del Regolamento dispone inoltre che il titolare del trattamento deve “mette[re] in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento” con riferimento a “la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità”, garantendo, in particolare, “che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica” (principio della protezione dei dati per impostazione predefinita).

L’art. 33 del Regolamento dispone che “in caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 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 “la notifica di cui al paragrafo 1 deve almeno: a) descrivere 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; b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni; c) descrivere le probabili conseguenze della violazione dei dati personali; d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi” (par. 3).

3.2 Violazioni accertate.

3.2.1 Insufficienza delle informazioni contenute nella notifica della violazione.

È stato in primo luogo accertato, tenuto conto anche delle risultanze delle specifiche relazioni tecniche redatte dall'Autorità, che la Società, a seguito di un data breach che ha interessato alcuni server e alcune postazioni di lavoro della Società, ha effettuato una notifica delle violazioni, ai sensi dell'art. 33 del Regolamento, priva degli elementi ritenuti necessari per l'esercizio, da parte del Garante, dei compiti e dei poteri previsti dal Regolamento.

L'art. 33, par. 3, del Regolamento richiede che la notifica di un data breach, tra gli elementi che deve necessariamente contenere, riporti, tra l'altro ("almeno"), la descrizione della natura della violazione (comprensiva di, ove possibile, categorie e numero approssimativo di interessati, categorie e numero approssimativo di registrazioni dei dati personali oggetto di breach) nonché la descrizione delle misure adottate o di cui si propone l'adozione per porre rimedio alla violazione e, se del caso, per attenuarne i possibili effetti negativi.

Il paragrafo 5 dell'articolo citato dispone, inoltre, che, al verificarsi di qualsiasi violazione di dati, il titolare del trattamento deve documentare la stessa, tenendo traccia anche delle "circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo".

Il considerando 87 del Regolamento, richiamato dalle Guidelines 9/2022 on personal data breach notification under GDPR (adottate il 28 marzo 2023, v. punto 26), precisa in proposito che la notifica di un data breach "può dar luogo a un intervento dell'autorità di controllo nell'ambito dei suoi compiti e poteri previsti dal presente regolamento".

Dal tenore letterale delle norme citate nonché dalla loro lettura sistematica emerge chiaramente che la segnalazione prevista dall'art. 33 del Regolamento deve contenere informazioni idonee ed esaustive in riferimento all'evento di violazione. Risulta essenziale, cioè, che la segnalazione includa tutte quelle informazioni necessarie per individuare le caratteristiche dell'incidente informatico da cui ha avuto origine la violazione dei dati. Questi elementi sono necessari per consentire al Garante, al verificarsi di una violazione di dati, di esercitare i suoi poteri - e appurare che siano state messe in atto le misure tecnologiche e organizzative adeguate alla fattispecie concreta, anche nell'ottica di ripristinare un adeguato livello di protezione dei dati personali violati.

Per quanto riguarda, quindi, la segnalazione presentata dalla Società, si ritiene invece che la stessa sia priva di tali elementi fondamentali e, quindi, non sia conforme a quanto previsto dall'art. 33 del Regolamento: in particolare, nella segnalazione non vi è l'indicazione dei server impattati (nello specifico i server Exchange), della tipologia di vulnerabilità sfruttata dall'attaccante e di alcuni elementi in merito alla kill chain dell'attacco. Tali informazioni, assenti nella prima segnalazione, non si rinvengono nemmeno nelle successive integrazioni, seppure l'attività di integrazione della segnalazione originaria abbia coperto un lungo periodo di tempo (tra la prima comunicazione del 17/08/2023 fino all'invio della versione definitiva, il 4/10/2023), tanto che la predetta attività ha inevitabilmente comportato l'allungamento dei tempi per la verifica, da parte dell'Autorità, del rispetto della disciplina di protezione dei dati.

La mera compilazione di "tutti i campi del modulo standard di notifica presente sul sito Internet istituzionale d[ell'] Autorità" (v. scritti difensivi del 12/01/2024, p. 4) con informazioni generiche (tra cui, per esempio, "Tale attacco ha comportato il blocco di alcuni server e postazioni di lavoro", v. notifica integrativa del 4/10/2023, sezione F.7), non può ritenersi di per sé condizione sufficiente a fornire informazioni adeguate in riferimento all'evento di violazione, vista proprio la vaghezza del contenuto di tali informazioni.

Ciò anche avuto riguardo al fatto che, nell'indicare le misure applicate ai sistemi al momento dell'evento (v. sezione F.9 del modulo), la Società non ha fatto alcun riferimento alle attività di patching delle vulnerabilità indicate, ovvero alle azioni di mitigazione/eliminazione della vulnerabilità eseguite, ma si è limitata ad elencare le misure genericamente adottate ("I server e

gli endpoint erano e sono protetti tramite sistemi di autenticazione, antivirus, antimalware, defender for identity, IPS, firewall e SIEM. Sono presenti sistemi di backup e business continuity e disaster recovery"; v. notifica integrativa del 4/10/2023, sezione F.9).

Le informazioni relative al tipo di vulnerabilità utilizzate dall'attaccante e il dettaglio delle misure di sicurezza che erano applicate ai sistemi coinvolti nell'attacco sono state fornite, infatti, solo in risposta a una specifica richiesta di informazioni dell'Autorità (in particolare richiesta di informazioni del 13/10/2023).

Le citate Guidelines 9/2022 on personal data breach notification under GDPR in proposito chiariscono che, in ogni caso, oltre alle informazioni di cui espressamente il Regolamento chiede la presenza, il titolare del trattamento, valutato il caso di specie, deve proattivamente fornire tutte quelle ulteriori informazioni necessarie per spiegare pienamente le circostanze di ciascun caso di violazione di dati (v. punto 54 "Article 33(3) GDPR states that the controller «shall at least» provide this information with a notification, so a controller can, if necessary, choose to provide further details. Different types of breaches (confidentiality, integrity or availability) might require further information to be provided to fully explain the circumstances of each case").

Per le ragioni indicate, la condotta tenuta dalla Società non è conforme all'art. 33 del Regolamento.

3.2.2 Inadeguatezza delle misure di sicurezza: mancata adozione di misure di mitigazione e di risoluzione delle vulnerabilità.

È stato accertato, inoltre, che la Società non ha tenuto una condotta conforme agli obblighi previsti dalla disciplina di protezione dei dati, relativamente all'adozione di misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio.

In particolare, è emerso che il soggetto che ha posto in essere l'attacco informatico nei confronti della Società ha sfruttato due vulnerabilità della piattaforma Microsoft Exchange (CVE-2022-41040 e CVE-2022-41082) utilizzata dalla Società.

La combinazione delle predette vulnerabilità, considerate le caratteristiche delle stesse (la prima consente l'escalation dei privilegi utente, la seconda permette l'esecuzione di codice remoto sulla macchina target dell'attacco), ha permesso, in termini generali, a un attaccante di assumere privilegi di amministratore sulla macchina attaccata ed eseguire un codice malevolo remoto, prendendo così il pieno controllo della piattaforma.

Nel caso di specie, come evidenziato dalla stessa Società, l'attaccante, a seguito di penetrazione nei sistemi, è stato in grado di creare un'utenza che è stata contestualmente inserita nel gruppo degli "amministratori di dominio", al fine di assicurarsi la persistente possibilità di condurre attività fraudolente sulla piattaforma informatica della Società.

Rileva il fatto che le predette vulnerabilità erano già state rese note, a settembre 2022, dal Microsoft Security Response Center che aveva altresì pubblicato le opportune azioni di mitigazione; inoltre, a novembre 2022, Microsoft aveva reso disponibili gli aggiornamenti necessari da apportare alla piattaforma Exchange per superare proprio le vulnerabilità indicate (per di più considerato che erano state valutate ad alta criticità).

Tra l'altro, anche in Italia, diversi mesi prima dell'evento, l'esistenza della predetta vulnerabilità era stata opportunamente segnalata dall'Agenzia per la Cybersicurezza nazionale (v. bollettino del Computer Security Incident Response Team dell'Agenzia per la Cybersicurezza nazionale di novembre 2022, cfr. https://www.csirt.gov.it/contenuti/vulnerabilita-0-day-in-exchage-server-al03-220930-csirt-ita).

Nonostante ciò, ad agosto 2023, mese in cui la Società ha subito l'attacco informatico, la stessa non aveva ancora adottato sui propri sistemi alcuna delle azioni specificatamente raccomandate da Microsoft ("We recommend that customers protect their organizations by applying the updates immediately to affected systems"), non avendo provveduto ad effettuare i necessari aggiornamenti della piattaforma Microsoft Exchange.

Per tali ragioni, esaminata nel concreto la mancata adozione tempestiva delle misure di protezione dagli attacchi sulla piattaforma Microsoft Exchange, valutato l'effetto pratico della predetta mancanza sul trattamento in concreto effettuato, la condotta della Società si pone in contrasto con le disposizioni di cui all'art. 5, par. 1, lett. f), e all'art. 32 del Regolamento.

Tale condotta si pone, inoltre, in contrasto anche con i principi della protezione dei dati fin dalla progettazione e della protezione dei dati per impostazione predefinita di cui all'art. 25 del Regolamento, in quanto le predette misure - rese note e debitamente annunciate alla platea dei soggetti utilizzatori della piattaforma Microsoft Exchange, tra l'altro molto tempo prima, rispetto alla violazione di dati che ha interessato la Società, rientrano proprio tra le misure che un titolare del trattamento deve adottare per attuare i principi di protezione dei dati e per integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del Regolamento, nonché per garantire che siano trattati, per impostazione predefinita, solo i dati necessari per ogni specifica finalità del trattamento.

La valutazione effettuata dall'Autorità, quindi, non si è limitata a prendere in considerazione il verificarsi, in quanto tale, della violazione di dati (che, come sottolineato dalle Linee guida 4/2022 sul calcolo delle sanzioni amministrative pecuniarie ai sensi del GDPR, adottate il 24 maggio 2023, "non implica necessariamente una violazione del GDPR", v. punto 5.6, nota 37), ma, muovendo dalla violazione di dati oggetto dell'indagine, si è proceduto a verificare se la Società avesse adottato tutte quelle misure tecniche e organizzative che avrebbero potuto evitare la violazione di dati personali.

In proposito, quindi, l'operato dell'Autorità è stato assolutamente conforme a quanto indicato nella sentenza, richiamata dalla Società, della Corte di Giustizia dell'Unione europea del 14 dicembre 2023 (causa C-340 del 2021), in particolare laddove viene precisato, con riferimento alle misure di cui all'art. 32 del Regolamento, che "l'adeguatezza di siffatte misure tecniche e organizzative deve essere valutata in due tempi. Da un lato, occorre individuare i rischi di violazione dei dati personali indotti dal trattamento di cui trattasi e le loro eventuali conseguenze per i diritti e le libertà delle persone fisiche. Tale valutazione deve essere effettuata in concreto, prendendo in considerazione il grado di probabilità dei rischi individuati e il loro grado di gravità. Dall'altro lato, occorre verificare se le misure attuate dal titolare del trattamento siano adeguate a tali rischi, tenuto conto dello stato dell'arte, dei costi di attuazione nonché della natura, della portata, del contesto e delle finalità di tale trattamento" (punto 42).

Inoltre, sempre nella citata sentenza, la Corte di Giustizia ha precisato che "dal disposto dell'articolo 5, paragrafo 2, dell'articolo 24, paragrafo 1, e dell'articolo 32, paragrafo 1, del RGPD risulta senza ambiguità che l'onere di provare che i dati personali sono trattati in modo tale da garantire una loro adeguata sicurezza ai sensi dell'articolo 5, paragrafo 1, lettera f), e dell'articolo 32 di detto regolamento incombe al titolare del trattamento in parola" (punto 52), e ancora sul punto, "da un lato, poiché il livello di protezione di cui al RGPD dipende dalle misure di sicurezza adottate dai titolari del trattamento di dati personali, questi ultimi devono essere indotti, sopportando l'onere di dimostrare l'adeguatezza di tali misure, a fare tutto il possibile per prevenire operazioni di trattamento non conformi a tale regolamento" (punto 55).

Dall'esame di quanto dichiarato e dalla documentazione prodotta dalla Società, è risultato evidente come la stessa non abbia fatto tutto quanto poteva per evitare la violazione di dati, considerato che, come già ampiamente chiarito, la Società non ha adottato quelle misure di

mitigazione che, pubblicamente diffuse, in primis Microsoft e, a livello nazionale, anche l'Agenzia per la Cybersicurezza nazionale avevano fortemente raccomandato.

In proposito si osserva come quanto esposto dalla Società non possa ritenersi idoneo a giustificare il mancato aggiornamento completo e tempestivo dei sistemi da parte della stessa.

Di nessun pregio, infatti, l'affermazione della Società secondo cui "a causa di un errore umano nella configurazione delle attività di scansione il server Exchange oggetto dell'attacco era rimasto escluso dalla scansione medesima" (v. scritti difensivi del 12/01/2024, p. 7): considerata la criticità delle vulnerabilità in questione (valutate, come già rilevato, da Microsoft ad alto rischio per la perdita di integrità, disponibilità e riservatezza dei dati ricollegati, cfr. https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2022-41040, e https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2022-41082) e la delicatezza dei sistemi impattati, le attività di patching e di aggiornamento avrebbero dovuto essere sottoposte a controlli ripetuti e necessariamente ridondanti da parte della Società e non eseguite a partire da un'attività manuale non oggetto di alcuna successiva verifica.

Con riferimento ai propri sistemi, la Società, per un periodo molto lungo di tempo (quasi 12 mesi), non è stata in grado di garantire la necessaria protezione rispetto alla perdita e alla diffusione dei dati personali trattati, se non parzialmente attraverso degli workaround, per loro natura da considerarsi una soluzione temporanea e di emergenza, tra l'altro e comunque non applicati a tutti i server Exchange.

In proposito si osserva come la mancata attività di aggiornamento di tutti i sistemi, nonostante non sia stata direttamente la causa dell'attacco perpetrato dalla cybergang Medusa, ha senz'altro reso vulnerabili i sistemi e i dati da questi trattati, rendendoli non adeguatamente protetti rispetto ai rischi incombenti.

Per tali motivi la Società non è stata dunque in grado di assicurare su base permanente la riservatezza, l'integrità e la resilienza dei sistemi e dei servizi di trattamento e non ha adottato una procedura finalizzata a verificare regolarmente l'efficacia delle misure tecniche applicate ad essi.

In relazione al complesso delle motivazioni sopra riportate, si ritiene pertanto che la Società abbia violato gli artt. 5, par. 1, lett. f), 25 e 32 del Regolamento.

Per quanto invece riguarda la contestazione, formulata in sede di avvio del procedimento, in merito alla violazione dell'art. 28, par. 3, lett. f), del Regolamento in relazione alle supposte carenze nell'assistenza prestata ai titolari del trattamento coinvolti nell'evento di violazione dei dati, si ritiene che quanto rappresentato dalla Società negli scritti difensivi del 12 gennaio 2024 abbia messo in luce come la stessa abbia posto in essere un'adeguata e tempestiva attività di assistenza nei confronti dei titolari del trattamento coinvolti nell'evento; ciò tenute in considerazione le necessarie azioni di analisi dell'incidente informatico che la Società ha dovuto espletare.

Per tali ragioni non si ritiene che sussistano, nel caso di specie, gli estremi per adottare provvedimenti in relazione alla violazione dell'art. 28, par. 3, lett. f), del Regolamento, contenuta nella notifica delle violazioni del 15 dicembre 2023 che si ritiene, dunque, di archiviare nella parte riguardante tale specifico profilo oggetto di contestazione.

4. Conclusioni: dichiarazione di illiceità del trattamento. Provvedimenti correttivi ex art. 58, par. 2, Regolamento.

Per i suesposti motivi, l'Autorità ritiene che le dichiarazioni, la documentazione e le ricostruzioni fornite dal titolare del trattamento nel corso dell'istruttoria non consentono di superare i rilievi notificati dall'Ufficio con l'atto di avvio del procedimento e che risultano pertanto inidonee a

consentire l'archiviazione del presente procedimento, non ricorrendo peraltro alcuno dei casi previsti dall'art. 11 del Regolamento del Garante n. 1/2019.

Le condotte poste in essere dalla Società - segnatamente l'invio all'Autorità di una segnalazione di data breach priva degli elementi fondamentali e la mancata adozione di attività di aggiornamento dei propri sistemi - risultano infatti illecite, nei termini su esposti, in relazione agli artt. 5, par. 1, lett. f), 25, 32 e 33 del Regolamento.

La violazione, accertata nei termini di cui in motivazione, non può essere considerata "minore", tenuto conto della natura e della gravità della violazione stessa e del grado di responsabilità (v. Considerando 148 del Regolamento).

L'Autorità ha altresì tenuto conto del livello medio di gravità della violazione alla luce di tutti i fattori rilevanti nel caso concreto, e in particolare la natura, la gravità e la durata della violazione, tenendo in considerazione la natura, l'oggetto o la finalità del trattamento in questione nonché il numero di interessati lesi dal danno e il livello del danno da essi subito.

L'Autorità ha altresì preso in considerazione i criteri relativi al carattere doloso o colposo della violazione e le categorie di dati personali interessate dalla violazione (v. art. 83, par. 2 e Considerando 148 del Regolamento).

Pertanto, visti i poteri correttivi attribuiti dall'art. 58, par. 2 del Regolamento, alla luce del caso concreto:

a. si ingiunge al titolare:

- di effettuare una tempestiva verifica delle vulnerabilità nei propri sistemi e la rapida risoluzione delle stesse, tenuto conto del livello di rischio che deriva dalla inadeguata protezione dei dati personali trattati;

- la predisposizione di una procedura formalizzata per la gestione delle vulnerabilità, che preveda, in particolare la pianificazione del controllo di tutti gli asset IT dell'organizzazione al fine di rilevare l'eventuale presenza di vulnerabilità note o potenziali nonché l'individuazione delle relative procedure di correzione e mitigazione;

- l'individuazione, per i diversi asset IT attraverso cui la società tratta dati personali, dei valori relativi al tempo medio di rilevamento delle vulnerabilità (MTTD) e al tempo medio di risposta (MTTR), che siano adeguati tenuto conto del rischio per i diritti e le libertà delle persone fisiche.

b. si dispone l'applicazione di una sanzione amministrativa pecuniaria ai sensi dell'art. 83 del Regolamento, commisurata alle circostanze del caso concreto (art. 58, par. 2, lett. i) Regolamento).

5. 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).

All'esito del procedimento risulta che Postel S.p.A. ha violato gli artt. artt. 5, par. 1, lett. f), 25, 32 e 33 del Regolamento. Per la violazione delle predette disposizioni, è prevista l'applicazione della sanzione amministrativa pecuniaria prevista dall'art. 83, par. 4, lett. a), e 5, lett. a) del Regolamento, mediante adozione di un'ordinanza ingiunzione (art. 18, l. 24.11.1981, n. 689).

Ritenuto di dover applicare il paragrafo 3 dell'art. 83 del Regolamento laddove prevede che "Se, in relazione allo stesso trattamento o a trattamenti collegati, un titolare del trattamento […] viola, con

dolo o colpa, varie disposizioni del presente regolamento, l'importo totale della sanzione amministrativa pecuniaria non supera l'importo specificato per la violazione più grave", l'importo totale della sanzione è calcolato in modo da non superare il massimo edittale previsto dal medesimo art. 83, par. 5.

Con riferimento agli elementi elencati dall'art. 83, par. 2 del Regolamento ai fini della applicazione della sanzione amministrativa pecuniaria e la relativa quantificazione, tenuto conto che la sanzione deve "in ogni caso [essere] effettiva, proporzionata e dissuasiva" (art. 83, par. 1 del Regolamento), si rappresenta che, nel caso di specie, sono state considerate le seguenti circostanze:

in relazione alla natura della violazione, questa ha riguardato, tra l'altro, fattispecie punite più severamente ai sensi dell'art. 83, par. 5, del Regolamento (principi generali del trattamento, in particolare il principio di integrità e riservatezza);

in relazione alla gravità della violazione, è stata presa in considerazione la circostanza del rilevante numero di interessati i cui dati personali sono stati coinvolti nella violazione (circa 25.000), la perdita di disponibilità di una parte dei dati oggetto della violazione e dell'impatto elevato che la violazione può aver determinato sugli interessati (in termini di perdita di controllo dei dati, furti di identità, frodi, rischi reputazionali);

con riguardo alla durata della violazione, è stata considerata rilevante la durata della violazione considerato che, da quando erano state rese note le vulnerabilità sfruttate per l'attacco (settembre 2022), la Società, quasi dodici mesi dopo (agosto 2023), non aveva ancora provveduto ad aggiornare i propri sistemi;

il grado di responsabilità del titolare o del responsabile del trattamento, tenendo conto delle misure tecniche e organizzative messe in atto ai sensi degli artt. 25 e 32 del Regolamento oggetto di specifico rilievo nell'ambito del procedimento;

con riferimento al carattere doloso o colposo della violazione e al grado di responsabilità del titolare, è stata presa in considerazione la condotta della Società che non ha provveduto ad adottare idonee misure tecniche a protezione dei dati personali trattati sui propri sistemi, nonostante gli avvisi pubblici sulle vulnerabilità e le contromisure da adottare, provenienti dal fornitore del software e dall'ACN;

a favore della Società si è tenuto conto della cooperazione con l'Autorità di controllo dimostrata nel corso del procedimento e della decisione di aggiornare i sistemi e di implementare un Cybersecurity Improvement Plan al fine di aggiornare e migliorare il processo gestionale dei security critical alert.

Si ritiene inoltre che assuma rilevanza, nel caso di specie, tenuto conto dei richiamati principi di effettività, proporzionalità e dissuasività ai quali l'Autorità deve attenersi nella determinazione dell'ammontare della sanzione (art. 83, par. 1, del Regolamento), in primo luogo le condizioni economiche del contravventore, determinate in base ai ricavi conseguiti dalla Società con riferimento al bilancio ordinario d'esercizio per l'anno 2023. Da ultimo si tiene conto dell'entità delle sanzioni irrogate in casi analoghi.

Nella quantificazione della sanzione si è anche tenuto conto che, nel caso di specie, la sanzione pecuniaria si aggiunge ad altre misure correttive ingiunte con il provvedimento.

Alla luce degli elementi sopra indicati e delle valutazioni effettuate, si ritiene, nel caso di specie, di applicare nei confronti di Postel S.p.A. la sanzione amministrativa del pagamento di una somma pari ad euro 900.000 (novecentomila).

In tale quadro si ritiene, altresì, in considerazione della tipologia delle violazioni accertate che hanno riguardato i principi generali del trattamento nonché le misure di sicurezza e il contenuto della segnalazione di violazione di dati, che ai sensi dell'art. 166, comma 7, del Codice e dell'art. 16, comma 1, del Regolamento del Garante n. 1/2019, si debba procedere alla pubblicazione del presente provvedimento sul sito Internet del Garante.

Si ritiene, altresì, che ricorrano i presupposti di cui all'art. 17 del Regolamento n. 1/2019.

TUTTO CIÒ PREMESSO, IL GARANTE

rileva l'illiceità del trattamento effettuato da Postel S.p.A., in persona del legale rappresentante pro-tempore, con sede legale in Viale Europa, 175, Roma, C.F. 04839740489, ai sensi dell'art. 143 del Codice, per la violazione degli artt. 5, par. 1, lett. f), 25, 32 e 33 del Regolamento;

DETERMINA

di archiviare la contestazione adottata nei confronti di Postel S.p.A. in persona del legale rappresentante pro-tempore, con atto del 15 dicembre 2023, limitatamente alla violazione dell'art. 28, par. 3, lett. f), del Regolamento;

INGIUNGE

a Postel S.p.A.:

a. ai sensi dell'art. 58, par. 2, lett. d) del Regolamento:

- di effettuare una verifica delle vulnerabilità nei propri sistemi e la rapida risoluzione delle stesse, tenuto conto del livello di rischio che deriva dalla inadeguata protezione dei dati personali trattati, entro 90 giorni dalla notifica del presente provvedimento;

- di predisporre una procedura formalizzata per la gestione delle vulnerabilità, che preveda, in particolare la pianificazione del controllo di tutti gli asset IT dell'organizzazione al fine di rilevare l'eventuale presenza di vulnerabilità note o potenziali nonché l'individuazione delle relative procedure di correzione e mitigazione, entro 90 giorni dalla notifica del presente provvedimento;

- di individuare, per i diversi asset IT attraverso cui la società tratta dati personali, dei valori relativi al tempo medio di rilevamento delle vulnerabilità (MTTD) e al tempo medio di risposta (MTTR), che siano adeguati tenuto conto del rischio per i diritti e le libertà delle persone fisiche, entro 90 giorni dalla notifica del presente provvedimento.

b. di pagare la predetta somma di euro 900.000 (novecentomila), secondo le modalità indicate in allegato, entro 30 giorni dalla notifica del presente provvedimento, pena l'adozione dei conseguenti atti esecutivi a norma dell'art. 27 della legge n. 689/1981. Si ricorda che resta salva la facoltà per il trasgressore di definire la controversia mediante il pagamento – sempre secondo le modalità indicate in allegato - di un importo pari alla metà della sanzione irrogata, entro il termine di cui all'art. 10, comma 3, del d. lgs. n. 150 dell'1.9.2011 previsto per la proposizione del ricorso come sotto indicato (art. 166, comma 8, del Codice);

ORDINA

ai sensi dell’art. 58, par. 2, lett. i) del Regolamento a Postel S.p.A., di pagare la somma di euro 900.000 (novecentomila) a titolo di sanzione amministrativa pecuniaria per le violazioni indicate nel presente provvedimento;

DISPONE

la pubblicazione del presente provvedimento sul sito web del Garante ai sensi dell’art. 166, comma 7, del Codice e dell’art. 16, comma 1, del Regolamento del Garante n. 1/20129, e ritiene che ricorrano i presupposti di cui all’art. 17 del Regolamento n. 1/2019.

Richiede a Postel S.p.A. di comunicare quali iniziative siano state intraprese al fine di dare attuazione a quanto disposto con il presente provvedimento e di fornire comunque riscontro adeguatamente documentato ai sensi dell’art. 157 del Codice, entro il termine di 120 giorni dalla data di notifica del presente provvedimento; l’eventuale mancato riscontro può comportare l’applicazione della sanzione amministrativa prevista dall’art. 83, par. 5, lett. e) del Regolamento.

Ai sensi dell’art. 78 del Regolamento, nonché degli articoli 152 del Codice e 10 del d.lgs. n. 150/2011, avverso il presente provvedimento può essere proposta opposizione all'autorità giudiziaria ordinaria, con ricorso depositato al tribunale ordinario del luogo individuato nel medesimo art. 10, entro il termine di trenta giorni dalla data di comunicazione del provvedimento stesso, ovvero di sessanta giorni se il ricorrente risiede all'estero.

Roma, 4 luglio 2024

IL PRESIDENTE
Stanzione

IL RELATORE
Stanzione

IL SEGRETARIO GENERALE
Mattei