Provvedimento del 18 giugno 2026 [10272529]

VEDI ANCHE Newsletter del 29 luglio 2026

[doc. web n. 10272529]

Provvedimento del 18 giugno 2026

Registro dei provvedimenti
n. 476 del 18 giugno 2026

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, componente e il dott. Luigi Montuori, 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");

VISTO il reclamo presentato ai sensi dell'art. 77 del Regolamento dal sig. XX e dalla sig.ra XX nei confronti di Piaggio & C. S.p.A.;

ESAMINATA la documentazione in atti;

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

RELATORE il dott. Agostino Ghiglia;

PREMESSO

1. I reclami presentati dinanzi al Garante e l'istruttoria avviata dall'Ufficio.

Con i reclami presentati a questa Autorità in data 17/07/2023, tramite i propri legali, il sig. XX e la sig.ra X hanno lamentato una violazione della disciplina in materia di protezione dei dati personali da parte di Piaggio & C. S.p.A. (di seguito "la Società"), alle cui dipendenze avevano svolto attività lavorativa, fino al licenziamento per giusta causa, comunicato loro con lettera datata 02/03/2023.

I reclamanti, in particolare, rappresentavano di aver chiesto alla Società conferma dell'avvenuta disattivazione degli account di posta elettronica aziendale di tipo individualizzato, utilizzati dagli stessi, nel corso del rapporto di lavoro, nell'ambito delle impugnazioni dei rispettivi licenziamenti, datate 26/04/2023.

Tali richieste venivano reiterate, con comunicazione pec del 31/05/2023 e, sebbene fossero state

regolarmente notificate all'indirizzo pec della Società, non ricevevano riscontro, nei termini indicati dall'art. 12, par. 3, del Regolamento.

Con successivi reclami, presentati all'Autorità in data 14/09/2023, i reclamanti lamentavano che la Società, nel corso del rapporto di lavoro, aveva effettuato degli accessi alla corrispondenza in transito sui propri account di posta elettronica aziendale di tipo individualizzato (XX e XX), e aveva acquisito numerose e-mail, transitate sui predetti account e sulle caselle di posta elettronica personale, per poi utilizzarle nell'ambito dei procedimenti disciplinari.

Precisamente, sulla base di quanto emerso dalle contestazioni disciplinari loro notificate (e prodotte in atti), risultava che la Società aveva "acquisito, trattato e utilizzato almeno 18 mail complessive (…) transitate sulla casella mail aziendale della reclamante nel periodo dal novembre 2020 al gennaio 2022" (reclamo della signora XX); che aveva "acquisito, trattato e utilizzato ben 94 mail complessive transitate sulla casella mail aziendale del reclamante" (reclamo del sig. XX). "Tale scambio di mail ha riguardato anche molti messaggi di posta elettronica transitati sulla … casella di posta elettronica personale" e scambiati con terzi.

L'Ufficio, pertanto, formulava nei confronti della Società una richiesta di informazioni, ai sensi dell'art. 157 del Codice, invitandola a fornire osservazioni in merito a quanto rappresentato nei reclami, con particolare riferimento ai presupposti di legittimità alla base dell'accesso eseguito sugli account di posta elettronica aziendale dei due reclamanti (nota del 19/12/2023).

La Società forniva riscontro con nota del 17/01/2024, rappresentando che:

- "gli account di posta elettronica aziendale dei reclamanti sono stati disattivati con impossibilità di accesso alle caselle di posta elettronica, in data 16 febbraio 2023, alle ore 08:54, in seguito alla contestazione dei comportamenti degli illeciti disciplinari e contestuale sospensione cautelare. Il 27 aprile 2023 le caselle di posta elettronica aziendale dei reclamanti sono state cancellate";

- "A partire dalla data di disattivazione delle caselle (16 febbraio 2023) nessuno ha avuto accesso agli account di posta aziendale dei reclamanti. I log di accesso agli account email aziendali sono conservati per 6 mesi, in ossequio al principio di limitazione della conservazione dei dati. I log relativi all'accesso alle caselle di posta aziendale dei reclamanti non sono pertanto disponibili, in quanto le stesse sono state disattivate e quindi non sono più accessibili da più di 6 mesi";

- "La Società ha adottato a livello di gruppo una specifica procedura per la gestione della cessazione del rapporto di lavoro dei collaboratori/dipendenti (allegato 2) nonché delle linee guida interne che specificano nel dettaglio il processo di "off-boarding" del personale aziendale (allegato 3)";

- "una volta cessato il rapporto di lavoro con un collaboratore/dipendente, l'indirizzo mail aziendale a questi assegnato viene immediatamente disattivato. Decorso il periodo massimo di giorni 30 dalla cessazione del rapporto di lavoro/collaborazione, gli account di posta elettronica vengono cancellati, con possibilità per ulteriori 30 gg e solo su richiesta del collaboratore/dipendente di recuperare il loro contenuto. Dopo i 30 giorni gli account sono definitivamente cancellati/eliminati";

- "Per quanto riguarda le caselle di posta elettronica dei due reclamanti, la relativa disattivazione è avvenuta in data 16 febbraio 2023, in seguito all'irrogazione della contestazione dei comportamenti degli illeciti disciplinari (…); dunque, non a seguito di ordinaria cessazione del rapporto di lavoro. La disattivazione delle caselle di posta elettronica aziendale è stata eseguita manualmente dalla funzione ICT aziendale e la

cancellazione delle stesse è avvenuta sempre manualmente il 27 aprile 2023, oltre i 30 giorni che sono calcolati in automatico dal sistema che gestisce la casella di posta elettronica aziendale in caso di ordinaria cessazione del rapporto di lavoro";

- con riferimento agli accessi eseguiti sugli account aziendali, "a seguito di alcune segnalazioni interne che lamentavano comportamenti scorretti tenuti dai due reclamanti, in data 24 novembre 2022, il Lead Independent Director, legale rappresentante della Società (…) si è consultato, tra gli altri, con il Data Protection Officer (…), al fine di definire l'opportunità di procedere a specifiche attività di indagine interna atte a verificare la fondatezza del sospetto di specifiche e gravi condotte illecite ascrivibili ai due reclamanti a danno della Società";

- pertanto, "si è deciso di ricorrere a controlli difensivi in senso stretto esclusivamente sugli account di posta elettronica aziendale dei due ricorrenti per finalità di tutela del patrimonio aziendale ex art. 4 L. 300/1970 ("Controlli difensivi"), previa definizione dei criteri e le modalità di azione (allegato 4), nonché previo test di bilanciamento (…)" al cui esito "si è ritenuto che la modalità più idonea al perseguimento delle finalità prefissate e più rispettosa del principio di minimizzazione consistesse nell'estrazione graduale dei dati dalle caselle di posta elettronica dei due reclamanti, circoscritta a filtri e parole chiavi (keywords) preventivamente identificati, ed entro un arco temporale limitato (…), al fine di delimitare l'oggetto operativo dell'indagine e di restringere la stessa ai soli dati rilevanti sulla base dei principi di proporzionalità e necessità, pertinenza, correttezza e non eccedenza";

- "I controlli difensivi, lungi dall'integrare una forma di monitoraggio sistematico o una forma di sorveglianza sull'esecuzione della prestazione lavorativa, sono stati disposti dalla Società successivamente alla commissione dell'illecito da parte dei due reclamanti, quindi ex post, al fine di accertarlo";

- "La materiale attività di recupero mirato delle mail dal server aziendale è avvenuta dando incarico ad XX in qualità di responsabile del trattamento ai sensi dell'art. 28 del GDPR. XX è stata incaricata dal titolare del trattamento di effettuare il trattamento con mail del 29 novembre 2023 (rectius 2022). La Società ha indicato al responsabile del trattamento le istruzioni e i criteri da adottare nell'estrazione dei dati dalle caselle di posta elettronica dei due reclamanti (…). L'accesso da parte di XX è avvenuto tramite server aziendale e ai soli account di e-mail aziendale: non è stato pertanto effettuato nessun accesso ai computer aziendali in uso ai due reclamanti";

- "Né la funzione ICT Piaggio, né tantomeno XX hanno avuto accesso al contenuto delle mail estratte. (…) I dati raccolti a seguito dell'accesso alle caselle di posta elettronica aziendale dei due reclamanti e ritenuti rilevanti ai fini dei controlli difensivi sono stati conservati, dalla funzione Internal Audit, per il solo tempo necessario all'effettuazione dei controlli difensivi e alla valutazione delle relative risultanze (3 mesi) e quindi irreversibilmente cancellati (…)".

Con riferimento al mancato riscontro alle istanze di esercizio dei diritti, formulate dai reclamanti e rimaste prive di riscontro, la Società ha inoltre dichiarato che:

- "la disattivazione e chiusura degli account era stata già implementata con le tempistiche previste (disattivazione account con impossibilità di accesso 16 febbraio 2023 e cancellazione definitiva account 27 aprile 2023)";

- "a fronte del contenzioso già in essere con i reclamanti (…) il riscontro alle summenzionate richieste dovesse essere gestito nell'ambito dei procedimenti giudiziari stessi".

Con riguardo, invece, alle modalità e ai tempi di conservazione dei messaggi in transito sugli

account aziendali, la Società rappresentava che:

- “i messaggi di posta elettronica sono salvati in backup per tutta la durata del contratto di lavoro e per ulteriori 5 (cinque) anni dalla cessazione dello stesso”, come documentato anche nelle Linee Guida Off-Boarding (allegato 3 alla citata nota);

- “Tutti i dipendenti della Società sono informati in modo chiaro e trasparente su: (i) regole, criteri e modalità di accesso e utilizzo del sistema informativo aziendale e relativi dati e applicazioni tramite la policy aziendale sul corretto utilizzo degli strumenti informatici; (ii) le condizioni, modalità e finalità che la Società si riserva per eseguire i controlli aziendali sugli strumenti e servizi aziendali messi a disposizione dei dipendenti per lo svolgimento della propria prestazione lavorativa a favore della Società; (iii) le regole e le metodologie volte alla prevenzione dei reati in materia informatica”, come documentato dalle “Policy per il corretto utilizzo degli strumenti Information & Communication Technology”.

Prima di proseguire le proprie valutazioni, l’Ufficio formulava, nei confronti dei reclamanti, una richiesta volta a verificare l’applicabilità, al caso di specie, della disposizione di cui all’art. 140-bis del Codice in considerazione della contestuale presentazione dei ricorsi dinanzi all’Autorità giudiziaria.

Gli interessati, con comunicazione del 03/05/2024, dichiaravano che i ricorsi presentati dinanzi al Tribunale di Pisa, sez. lavoro, riguardavano unicamente l’impugnazione dei rispettivi licenziamenti, con richiesta di declaratoria della nullità/annullamento del provvedimento espulsivo.

2. L’avvio del procedimento per l’adozione dei provvedimenti correttivi e sanzionatori dell’Autorità.

L’Ufficio, alla luce di quanto sopra, provvedeva a notificare alla Società l’atto di avvio del procedimento sanzionatorio, ai sensi dell’art. 166, comma 5, del Codice, per la violazione degli artt. 5, par. 1, lett. a), b), c) ed e), 6, 12, 13, 17 e 88 del Regolamento e dell’art. 114 del Codice (nota del 03/09/2024).

La Società, in data 18/10/2024, inviava le proprie memorie difensive sulla base dell’art. 18 della legge n. 689/1981, con cui rappresentava, con riferimento all’omesso riscontro all’istanza di esercizio dei diritti, come le richieste formulate dagli interessati non rientrassero nel campo di applicazione degli artt. 15 e ss. del Regolamento.

“Gli interessati non hanno infatti richiesto la cancellazione di specifici dati personali a loro riferibili, né la cessazione di un particolare trattamento avente ad oggetto i propri dati. Non hanno quindi esercitato il diritto alla cancellazione ai sensi dell’art. 17 GDPR. Il termine di 30 giorni per rispondere all’interessato previsto dall’art. 12 GDPR non trovava dunque applicazione nel caso di specie”.

In ogni caso, anche volendo ritenere che gli interessati avessero chiesto la cancellazione delle e-mail conservate sul server aziendale, “in ogni caso Piaggio non avrebbe potuto dare seguito alla richiesta, poiché l’esercizio del diritto alla cancellazione deve essere ponderato in ragione dell’adeguatezza e pertinenza dei dati rispetto alle finalità del trattamento”.

“Nel caso di specie, le email degli Ex Dipendenti costituiscono prova fondamentale nei giudizi del lavoro innanzi al Tribunale di Pisa. La cancellazione di tali email avrebbe dunque compromesso la possibilità di Piaggio di difendersi nel processo che gli Ex Dipendenti già dichiaravano di voler instaurare con l’impugnazione stragiudiziale dei licenziamenti”.

Rispetto, invece, alla gestione e alla conservazione dei log della posta elettronica, la Società ha osservato, preliminarmente, che la posta elettronica aziendale costituisce “uno strumento utilizzato

dal lavoratore per rendere la prestazione lavorativa" e, come tale, rientra nell'ambito di applicazione del secondo comma dell'art. 4 Statuto dei lavoratori.

Pertanto, considerato che "La posta elettronica è oggi il principale strumento di lavoro di tutti coloro che svolgono lavori d'ufficio (…), Una cancellazione continua della posta elettronica impedirebbe agli stessi lavoratori di svolgere serenamente le proprie mansioni (…). Dunque la posta elettronica deve essere conservata durante tutto il rapporto di lavoro senza alcuna necessità di accordo sindacale".

Premesso, quindi, che la Società ha individuato, in un'ottica di accountability, un tempo di conservazione della posta elettronica dei dipendenti pari a 5 anni, successivamente alla cessazione del rapporto di lavoro, la stessa ha argomentato che tale termine risponde alle finalità di tutelare la sicurezza delle informazioni aziendali e garantire l'operatività aziendale, allo stesso tempo consente alla Società "di rispondere a eventuali contestazioni e/o a richieste delle autorità e quindi difendersi anche in giudizio".

Inoltre, come indicato nel documento recante le Linee Guida Off Boarding (all. 4 alle memorie difensive, pag. 2), i messaggi di posta che i dipendenti cancellano definitivamente dal cestino, vengono cancellati anche dal server di backup di Piaggio dopo un anno.

Mentre, per quanto riguarda le e-mail non cancellate dai dipendenti, nella Policy IT (all. 3 alle memorie) è chiarito che tutti i messaggi composti, spediti o ricevuti sul sistema di posta elettronica, inerenti allo svolgimento delle mansioni lavorative, sono e rimangono di proprietà dell'Azienda e che la casella di posta aziendale può essere soggetta a controllo da parte della Società.

In particolare, "Piaggio si riserva di effettuare attività di verifica e controlli sulle Risorse ICT per le seguenti finalità: a) finalità di produzione, organizzazione, gestione delle Risorse ICT, gestione dell'attività commerciale di Piaggio; b) per finalità di sicurezza informatica, verifica della funzionalità delle Risorse ICT; c) per garantire il corretto utilizzo delle Risorse ICT, il rispetto della normativa applicabile, delle policies aziendali e del Codice Etico; d) per attività di investigazione interna esclusivamente mirate all'accertamento di condotte illecite dell'utente; e) per far valere o difendere un diritto in sede giudiziaria" (pag. 16 delle Policy).

Con riferimento al backup della corrispondenza in transito sugli account aziendali, assegnati ai dipendenti, la Società ha precisato che questo "è completamente segregato rispetto alle altre informazioni aziendali ed è gestito dal fornitore (…), appositamente nominato responsabile del trattamento" (all. 11 alle memorie), e che "la procedura prevede che il fornitore non possa mai accedere alle mail se non su istruzione specifica di Piaggio, fornita alla luce e nei limiti di quanto previsto dalla normativa privacy e dalla Policy IT. Gli amministratori di sistema della Società non possono accedere al backup se non tramite il fornitore".

Considerato, quindi, che la Società non utilizza la posta elettronica come repository documentale, bensì esclusivamente come strumento di lavoro dei propri dipendenti, la Società ha precisato di non aver mai effettuato accessi alle e-mail dei dipendenti, dopo la cessazione del rapporto di lavoro.

Infatti, anche nel caso in esame, "l'accesso è stato effettuato in costanza di rapporto di lavoro, nel rispetto della normativa privacy e solo successivamente ad una valutazione della Società, in concerto con il DPO, degli eventuali rischi ed impatti per gli interessati", come risultante dalla DPIA allegata alle memorie.

La Società, pur ritenendo che la conservazione oltre la cessazione del rapporto di lavoro sia un'attività legittima, perché supportata da esigenze di sicurezza aziendale e senza alcun danno

per gli interessati, ha comunicato, con le memorie difensive, di aver ridotto il termine quinquennale di conservazione della posta elettronica, riducendolo a 3 mesi dalla cessazione del rapporto, “termine minimo necessario per la procedura di lay-off e per consentire all’interessato di richiedere l’accesso e/o contestare l’eventuale licenziamento”.

Con riguardo all’ipotizzata violazione dell’art. 4 della legge n. 300/1970, la Società ha escluso che “la conservazione della posta elettronica oltre la cessazione del rapporto può rilevare ai fini della suddetta norma, la quale si occupa della tutela del lavoratore e del possibile monitoraggio dello stesso in costanza del rapporto di lavoro”.

Rispetto al tempo di conservazione dei log di accesso alla posta elettronica, la Società ha osservato che, a seguito della pubblicazione del Documento di indirizzo recante “Programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati”, adottato dal Garante il 06/06/2024 (provv. n. 364, in doc web n. 10026277), i tempi di conservazione sono stati ridotti in linea con le indicazioni fornite, implementando una nuova prassi aziendale la quale prevede ora la cancellazione dei log ogni 21 giorni.

In ultimo, con riferimento alla violazione relativa alla mancanza di informativa e trasparenza sui trattamenti di conservazione dei log della posta elettronica e della posta stessa, la Società ha osservato come, sia le Linee Guida sulla trasparenza che i provvedimenti adottati dall’Autorità in circostanza simili, “non richiedono che nelle informative agli interessati sia indicata la specifica ragione della scelta del periodo di conserva zione e quindi nel dettaglio il percorso logico che ha guidato tale scelta”. Per cui, ritiene di aver rispettato gli obblighi di trasparenza di cui all’art. 5, par. 1, lett. a) e all’art. 13 del Regolamento.

In ogni caso, “al fine di garantire un’ancor maggiore trasparenza nei confronti dei propri dipendenti relativamente al trattamento dei dati di quest’ultimi, Piaggio ha integrato il proprio Regolamento per l’Utilizzo di Internet e della Posta Elettronica”, “indicando il termine di ciclo automatico del backup (i.e. 8 ore), spiegando che qualora una mail venga cancellata definitivamente entro l’intervallo di 8 ore, la stessa non sarà inclusa nel backup e non sarà più recuperabile” e che laddove venga eliminata definitivamente una e-mail dal proprio cestino di posta elettronica “la stessa verrà eliminata anche dal backup aziendale dopo 1 anno dalla cancellazione”.

In data 06/12/2024, veniva svolta l’audizione della Società, nel corso della quale veniva ribadito quanto già ampiamente argomentato nelle memorie difensive.

3. L’esito dell’istruttoria e del procedimento per l’adozione dei provvedimenti correttivi e sanzionatori di cui all’art. 58, par. 2, del Regolamento.

All’esito dell’esame delle dichiarazioni rese dalla parte nel corso del procedimento, nonché della documentazione acquisita, risulta accertato che la Società, individuata quale titolare del trattamento ai sensi dell’art. 4, n. 7, del Regolamento, ha effettuato operazioni di trattamento non conformi alla disciplina in materia di protezione dei dati personali.

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”.

3.1. Violazione degli artt. 12, par. 3, e 17 del Regolamento.

In primo luogo, risulta accertato che i reclamanti hanno chiesto alla Società, in due distinte occasioni, la conferma dell’avvenuta disattivazione degli account di posta elettronica aziendale di tipo individualizzato, a seguito dell’interruzione dei rapporti di lavoro.

Tali richieste erano motivate dalla necessità di conoscere lo stato dei suddetti account, avendo constatato che la Società aveva effettuato degli accessi finalizzati all'acquisizione di e-mail per muovere nei loro confronti degli addebiti disciplinari.

Le prime richieste venivano quindi formulate nell'ambito delle impugnazioni dei licenziamenti (con lettere datate 23/04/2023), mentre le successive venivano ripresentate, in data 31/05/2023, con espresso avvertimento che una eventuale persistente attivazione degli account, successiva alla cessazione dei rapporti di lavoro, potesse configurare una "evidente, gravissima e ingiustificata (ulteriore) lesione della privacy".

Ciò comporta, da un lato, che le richieste, sebbene non contenessero espliciti richiami alle disposizioni del Regolamento in tema di esercizio dei diritti, dovessero in ogni caso essere lette alla luce delle disposizioni vigenti in materia di trattamento dei dati personali, proprio in considerazione delle violazioni derivanti da un persistente trattamento di dati personali afferenti alla posta elettronica dei reclamanti.

Tra l'altro, alla luce dei chiarimenti forniti dall'EDPB nelle Linee guida 1/2022 sui diritti degli interessati, datate 28/03/2023, "Il titolare del trattamento non può quindi rifiutarsi di fornire i dati richiamandosi all'omessa indicazione della base giuridica della richiesta, in particolare alla mancanza di un riferimento specifico al diritto di accesso o al GDPR", considerato anche che "il GDPR non impone requisiti agli interessati per quanto riguarda la forma della richiesta di accesso ai dati personali" (si vedano a tal proposito il par. 3.1.1, punto 50, e par. 3.1.2, punto 52 delle citate Linee guida).

D'altro lato, deve considerarsi che, contrariamente a quanto ritenuto dalla parte, le richieste aventi ad oggetto la disattivazione degli account aziendali di tipo individualizzato rientrano, a pieno titolo, nell'ambito dei diritti riconosciuti agli interessati dagli artt. 15 e ss. del Regolamento.

Ciò in quanto, l'indirizzo di posta elettronica aziendale individualizzato (ovvero assegnato a uno specifico lavoratore), così come il contenuto della posta elettronica presente nell'account, costituiscono dati personali relativi al lavoratore stesso. In particolare, le comunicazioni in transito su un account di tipo individualizzato sono inevitabilmente riconducibili a dati personali dell'assegnatario dell'account stesso.

Pertanto, come ormai costantemente riconosciuto dall'Autorità nei propri provvedimenti, la richiesta di disattivazione di un account di tipo individualizzato (accompagnata o meno dalla richiesta di cancellazione delle e-mail presenti) si traduce nella richiesta di cessazione di ogni attività di trattamento che sia stata svolta, fino a quel momento, sui dati personali dell'interessato (si vedano, tra i più recenti, il provv. n. 427 del 17 luglio 2025, doc web n. 10182762; provv. n. 754 del 18 dicembre 2025, doc web n. 10213574; provv. n. 82 del 12 febbraio 2026, doc web n. 10230220).

Nel caso in esame, tra l'altro, le istanze presentate dagli interessati avevano come esclusivo oggetto la conferma della disattivazione degli account aziendali individualizzati e non anche la cancellazione delle e-mail che erano state acquisite dalla Società mediante l'attività di investigazione.

Ne deriva, quindi, l'infondatezza dell'argomentazione addotta dalla Società secondo cui, in ogni caso, la richiesta di cancellazione non poteva essere soddisfatta, perché avrebbe comportato una compressione del legittimo esercizio del diritto di difesa nell'ambito dei procedimenti seguiti all'impugnazione dei licenziamenti; diritto di difesa che si basava proprio sull'utilizzo, in sede giudiziaria, della corrispondenza intrattenuta dai reclamanti mediante gli account di posta aziendale.

Tuttavia, con riferimento alle limitazioni ai diritti dell'interessato, l'art. 2-undecies del Codice, conformemente a quanto previsto dall'art. 23 del Regolamento, prevede che "I diritti di cui agli articoli da 15 a 22 del Regolamento non possono essere esercitati con richiesta al titolare del trattamento ovvero con reclamo ai sensi dell'articolo 77 del Regolamento qualora dall'esercizio di tali diritti possa derivare un pregiudizio effettivo e concreto: […] e) allo svolgimento delle investigazioni difensive o all'esercizio di un diritto in sede giudiziaria".

In tale ipotesi "L'esercizio dei medesimi diritti può […] essere ritardato, limitato o escluso con comunicazione motivata e resa senza ritardo all'interessato, a meno che la comunicazione possa compromettere la finalità della limitazione, per il tempo e nei limiti in cui ciò costituisca una misura necessaria e proporzionata, tenuto conto dei diritti fondamentali e dei legittimi interessi dell'interessato".

Anche in base all'art. 12, par. 4, del Regolamento "se non ottempera alla richiesta dell'interessato, il titolare del trattamento informa l'interessato senza ritardo, e al più tardi entro un mese dal ricevimento della richiesta, dei motivi dell'inottemperanza e della possibilità di proporre reclamo a un'autorità di controllo e di proporre ricorso giurisdizionale".

Pertanto, alla luce di quanto sopra richiamato e soprattutto delle disposizioni del Regolamento, deve confermarsi la violazione in capo alla Società della disposizione di cui all'art. 12, par. 3, in relazione all'art. 17 del Regolamento.

3.2. Violazione degli artt. 5, par. 1, lett. a), b), c), ed e), 88 del Regolamento e 114 del Codice.

Risulta accertato che la Società abbia effettuato degli accessi alla posta elettronica dei reclamanti, in costanza del rapporto di lavoro, che abbia acquisito e raccolto "almeno 18 mail complessive (…) transitate sulla casella mail aziendale della reclamante nel periodo dal novembre 2020 al gennaio 2022" e "ben 94 mail complessive transitate sulla casella mail aziendale del reclamante", a partire da aprile 2020.

In base a quanto rappresentato dalla Società nell'ambito dell'istruttoria, tale attività è stata svolta al fine di "verificare la fondatezza del sospetto di specifiche e gravi condotte illecite ascrivibili ai due reclamanti a danno della Società" (nota del 17/01/2024) e, dunque, nell'ambito dei cd. controlli difensivi, i quali sono stati effettuati, dopo aver individuato criteri e modalità di azione e aver svolto un test di bilanciamento (all. 5 alla nota del 17/01/2024 e all. 2 alle memorie difensive del 18/10/2024).

La Società ha, in ogni caso, ritenuto legittima tale attività di controllo, che è prevista e disciplinata nei propri documenti interni per il perseguimento di diverse finalità (tra cui quella di "investigazione interna esclusivamente mirate all'accertamento di condotte illecite dell'utente" Policy IT, par. 9.3), in quanto svolta nel rispetto dei principi in materia di protezione dei dati personali, nonché del divieto di controllo dell'attività lavorativa di cui all'art. 4 della legge n. 300/1970.

Rispetto all'attività di investigazione sugli account di posta elettronica individualizzata dei due reclamanti, effettuata dalla Società nell'ambito dei cd. controlli difensivi e finalizzata a recuperare e-mail che fornissero prova delle condotte illecite, premesso che non rientra nelle competenze dell'Autorità pronunciarsi sulla cd. teoria dei controlli difensivi, di pura creazione giurisprudenziale e tra l'altro oggetto di applicazioni non univoche (si vedano sull'argomento il provv. n. 137 del 15/04/2021, doc. web n. 9670738, il provv. n. 409 del 01/12/2022, doc web n. 9833530), si richiama il principio ribadito in diverse pronunce giurisprudenziali in base al quale "in tema di cd. sistemi difensivi, sono consentiti, anche dopo la modifica dell'art. 4 St. Lav. ad opera dell'art. 23 del D. Lgs. n. 151 del 2015, i controlli anche tecnologici posti in essere dal datore di lavoro finalizzati alla tutela di beni estranei al rapporto di lavoro o ad evitare comportamenti illeciti, in presenza di un fondato sospetto circa la commissione di un illecito, purché sia assicurato un

corretto bilanciamento tra le esigenze di protezione di interessi e beni aziendali, correlate alla libertà di iniziativa economica, rispetto alle imprescindibili tutele della dignità e della riservatezza del lavoratore, sempre che il controllo riguardi dati acquisiti successivamente all'insorgere del sospetto" (si vedano Cass. n. 25732 del 22/9/2021; Cass. n. 18168 del 26/6/2023; Cass. n. 32283 dell'11/12/2025).

L'elemento decisivo per l'ammissibilità del controllo, secondo gli orientamenti della Suprema Corte, consiste dunque nel fatto che il controllo si svolga ex post, ovvero su comportamenti posti in essere successivamente all'insorgenza del sospetto dell'illecito (sul punto anche Cass. n. 34092 del 12/11/2021).

È evidente che, nel caso di specie, tale condizione non ricorre, in quanto risulta accertato come i dati acquisiti dalla Società siano cronologicamente precedenti all'insorgere del sospetto dell'illecito compiuto: infatti la raccolta dei dati relativi alla corrispondenza intrattenuta dai due reclamanti è stata svolta a ritroso nel tempo, fino a circa 2 anni prima.

Sotto il profilo della protezione dei dati personali, l'attività di controllo eseguito dalla Società sugli account di posta elettronica dei due reclamanti è stata resa possibile in virtù della sistematica raccolta e conservazione dei dati relativi alla posta elettronica dei dipendenti che, come previsto nelle Linee guida off boarding prodotta in atti, viene effettuata su backup per tutta la durata del rapporto di lavoro fino a 5 anni successivi alla cessazione del rapporto stesso.

Come dichiarato dalla Società nell'ambito dell'istruttoria, la conservazione non attiene solo ai messaggi di posta elettronica, ma anche dei log della posta stessa conservati per un periodo di 6 mesi (nota del 17/01/2024).

Quanto alle specifiche ragioni per le quali è stato disposto un periodo di conservazione così esteso, in assenza di precise indicazioni nei documenti informativi predisposti riguardo alle finalità perseguite, la Società ha dichiarato che la posta elettronica non è utilizzata come repository documentale, bensì esclusivamente come strumento di lavoro dei propri dipendenti; mentre, la conservazione dei log generati dalla posta elettronica per 6 mesi è stata motivata con l'esigenza di garantire la sicurezza dei sistemi informatici (v. nota del 18/10/2024).

Con le memorie difensive del 18/10/2024, la Società ha comunicato di aver apportato, dopo l'avvio del procedimento, sostanziali modifiche ai tempi di conservazione di tali categorie di dati.
In particolare, la conservazione dei dati relativi alla posta elettronica è stata ridotta da cinque anni a tre mesi, dopo la cessazione del rapporto di lavoro.

L'Autorità prende atto con favore delle modifiche apportate, ricordando in ogni caso che la conservazione della posta elettronica deve essere strettamente legata alla possibilità di accesso solo da parte dell'intestatario.

Pertanto, devono essere adottate misure di tipo organizzativo e tecnologico tali da impedire l'accesso all'archivio da parte di soggetti diversi dall'intestatario, a meno che questi non ne faccia esplicitamente richiesta, per finalità di assistenza (si veda in tal senso il provv. n. 613 del 09/10/2025, doc. web n. 10185435; e provv. n. 153 del 01/02/2018, doc. web n. 8159221).

Ciò in quanto il contenuto dei messaggi di posta elettronica, così come i dati esteriori delle comunicazioni (quindi anche i log della posta elettronica, comprensivi degli indirizzi e-mail del mittente e del destinatario, gli indirizzi IP dei server o dei client coinvolti nell'instradamento del messaggio, gli orari di invio, di trasmissione o di ricezione, la dimensione del messaggio, la presenza di eventuali allegati, l'oggetto del messaggio spedito o ricevuto) riguardano forme di corrispondenza assistite da garanzie di segretezza tutelate anche costituzionalmente (artt. 2 e 15 Cost.), rispetto alle quali quindi il Garante ha ritenuto che, nel contesto lavorativo, sia pubblico che

privato, sussiste una legittima aspettativa di riservatezza in relazione ai messaggi oggetto di corrispondenza (v. punto 5.2 lett. b), del provvedimento n. 13 del 01/03/2007, recante Linee guida per posta elettronica e internet, doc web n. 1387522; e in relazione a casi specifici, tra gli ultimi, il provv. n. 613 del 09/10/2025, doc web n. 10185435).

Ciò tenendo conto anche dell'orientamento giurisprudenziale espresso dalla Corte europea dei diritti dell'uomo secondo cui la protezione della vita privata si estende anche all'ambito lavorativo, considerato che proprio in occasione dello svolgimento di attività lavorative e/o professionali si sviluppano relazioni dove si esplica la personalità del lavoratore.

Tenuto anche conto che la linea di confine tra ambito lavorativo/professionale e ambito strettamente privato non sempre può essere tracciata con chiarezza, la Corte ritiene applicabile l'art. 8 della Convenzione europea dei diritti dell'uomo posto a tutela della vita privata senza distinguere tra sfera privata e sfera professionale (v. Niemietz c. Allemagne, 16/12/1992 (ric. n. 13710/88), spec. par. 29; Copland v. UK, 03/04/2007 (ric. n. 62617/00), spec. par. 41; Barbulescu v. Romania [GC], 05/09/2017 (ric. n. 61496/08), spec. par. 70-73; Antovi and Mirkovi v. Montenegro, 28/11/ 2017 (ric. n. 70838/13), spec. par. 41-42).

Proprio alla luce dei principi sopra richiamati, non può essere condiviso quanto previsto nel par. 9.3. delle Policy, in cui si afferma che gli interessati in qualità di utenti "non devono avere aspettativa di confidenzialità in relazione a qualsiasi comunicazione, messaggio, file o materiale che siano creati, archiviati, ricevuti od inviati attraverso le Risorse ICT anche tramite dispositivi personali".

Tale impostazione risente anche dell'interpretazione fornita dalla parte in relazione alla natura della posta elettronica, intesa come "strumento di lavoro" e, come tale, sottratta all'ambito di applicazione delle garanzie di maggior tutela di cui all'art. 4, comma 1, della legge n. 300/1970 (a fronte della disposizione di cui al comma 2 secondo cui "la disposizione di cui al comma 1 non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa […]").

Su questo aspetto, si ribadisce l'orientamento dell'Autorità, già espresso in diversi provvedimenti, in base al quale i sistemi e i programmi che consentono la raccolta, la conservazione e l'elaborazione dei dati tratti dall'utilizzo della posta elettronica e della connessione ad internet (quest'ultimo non emerso nel caso in esame) non sono indispensabili per rendere la prestazione lavorativa e operano in modo del tutto indipendente rispetto alla normale attività dell'utilizzatore (cioè senza alcun impatto o interferenza sul lavoro del dipendente) (sul punto si veda: provv. n. 613 del 09/10/2025, doc web n. 10185435; provv. n. 384 del 28/10/2021, doc. web n. 9722661; provv. n. 190 del 13/5/2021, doc. web n. 9669974; provv. n. 479 del 16/11/2017, doc. web n.7355533; si vedano altresì le circolari INL n. 4/2017 del 26/7/2017 e n. 2/2016 del 7/11/2016).

Per quel che riguarda i tempi di conservazione dei log della posta elettronica, anche in tal caso la Società, nelle citate memorie difensive, ha comunicato che, in ottemperanza alle indicazioni rese dall'Autorità nel provvedimento recante "Documento di indirizzo. Programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati", adottato il 06/06/2024 (doc web n. 10026277), ha implementato una nuova prassi aziendale la quale prevede la cancellazione dei log ogni 21 giorni.

Si prende atto con favore anche di questa ulteriore modifica delle policy aziendali e delle misure tecniche e organizzative implementate, tenuto conto del fatto che, in osservanza del principio generale di limitazione della conservazione, di cui all'art. 5, par. 1, lett. e), del Regolamento, il titolare del trattamento deve individuare un arco temporale congruo rispetto all'obiettivo di rilevare e mitigare eventuali incidenti di sicurezza, adottando tempestivamente le opportune contromisure.

Resta fermo, in ogni caso, che le attività di trattamento poste in essere prima delle modifiche citate

sono avvenute in assenza di idonei presupposti di liceità ai sensi dell'art. 6 del Regolamento, e in violazione dei principi di limitazione delle finalità, di minimizzazione dei dati e di limitazione della conservazione di cui all'art. 5, par. 1, lett. b), c) ed e) del Regolamento.

Tenuto conto, infatti, che il datore di lavoro, in qualità di titolare del trattamento, può trattare i dati personali dei dipendenti, di regola, solo se il trattamento è necessario per la gestione del rapporto di lavoro stesso oppure se è necessario per adempiere a specifici obblighi o compiti posti dalle discipline di settore applicabili (v. artt. 5, par. 1, lett. a), 6 e 9, del Regolamento), nel caso in esame risulta accertato che le attività di trattamento sono state svolte in assenza di un idoneo presupposto di liceità del trattamento.

Bisogna, inoltre, considerare il fatto che i dati in questione erano trattati dalla Società per un considerevole periodo di tempo e in assenza di finalità predeterminate, in violazione del principio generale di minimizzazione in base al quale i dati personali devono essere "adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati" (art. 5, par. 1, lett. c) del Regolamento) e che costituisce espressione del principio di proporzionalità.

In ultimo, si fa presente che, sempre nella Policy, a integrazione di quanto riportato nelle Linee guida a proposito della gestione della posta elettronica a seguito della cessazione del rapporto di lavoro, la Società informa gli interessati che, previo consenso dell'utente, è possibile mantenere attivo l'indirizzo della casella di posta elettronica del dipendente uscente per un periodo non superiore a 30 giorni inoltrando le e-mail su un'altra casella di posta indicata dal responsabile dell'utente, o trasferire il contenuto della casella di posta a un altro utente, per comprovate esigenze di servizio.

Tale attività, tenuto conto anche della estrema genericità delle esigenze di servizio richiamate, risulta contraria alle disposizioni in materia di protezione dei dati personali come ribadito dall'Autorità in molteplici occasioni, non soltanto con provvedimenti di carattere generale (fra tutti le citate Linee guida per posta elettronica e internet), ma in numerosi provvedimenti adottati in relazione a casi concreti (v. provv. n. 758 del 18/12/2025, doc. web n. 10213574; n. 140 del 07/03/2024, doc. web n. 10009004; provv. n. 732 del 27/11/2024, doc web n. 10101221; provv. n. 263 del 22/06/2023, doc. web n. 9920814, provv. n. 255 del 21/07/2022, doc. web n. 9809466) in cui viene sottolineato che, a tutela di possibili e legittime esigenze di continuità dell'attività aziendale, dopo la cessazione del rapporto di lavoro il titolare deve provvedere alla rimozione dell'account, previa disattivazione dello stesso e contestuale adozione di sistemi automatici volti ad informare i terzi mittenti e a fornire, a questi ultimi, indirizzi alternativi riferiti alla sua attività professionale, provvedendo altresì ad adottare misure idonee a impedire la visualizzazione dei messaggi in arrivo, durante il periodo in cui tale sistema automatico è in funzione.

Ciò detto, non può ritenersi corretta la ricostruzione interpretativa fornita dalla Società nelle memorie difensive, quando ha escluso che la mera conservazione della posta elettronica e dei log potesse realizzare una forma di controllo dell'attività lavorativa, tenuto conto di quanto poi si è verificato nel caso specifico.

Infatti, la documentazione predisposta dalla Società (tra cui le citate Policy per il corretto utilizzo degli strumenti information & communication tecnology), contiene una regolamentazione dettagliata sulle modalità di effettuazione dei controlli, che vengono svolti "periodicamente" sull'utilizzo della posta elettronica, della rete e dei PC "per verificarne un uso equilibrato e coerente con l'attività aziendale, il rispetto della normativa applicabile, delle policies aziendali e del Codice Etico" (7.1.2. e 7.1.3 delle Policy).

In maniera più specifica e dettagliata, al par. 9 delle citate Policy, la Società informa gli interessati che le attività di verifica e controlli sulle Risorse ICT vengono svolte per diverse finalità, tra cui "finalità di produzione, organizzazione, gestione delle Risorse ICT", "per finalità di sicurezza

informatica, verifica della funzionalità delle Risorse ICT", ma anche "per attività di investigazione interna" e "per far valere o difendere un diritto in sede giudiziaria".

Quanto alle modalità con cui i controlli vengono disposti, il disciplinare interno prevede "accesso agli strumenti aziendali ed estrazione di file e/o messaggi di posta elettronica a fini investigativi e di difesa giudiziaria tramite l'utilizzo di chiavi di ricerca, filtri e/o altri strumenti di e - Discovery che garantiscano riservatezza e gradualità", "accesso agli strumenti aziendali tramite appositi software di verifica", "monitoraggio di comportamenti e attività sospette" (v. Policy IT, par. 9).

Nell'ambito dei controlli, la Società si riserva finanche "il diritto di rivedere i file e i messaggi conservati nelle Risorse ICT o già cancellati" (…), per diverse finalità, tra cui "per l'accertamento di condotte illecite e per esercitare o difendere un diritto in sede giudiziaria" (par. 9 citate Policy).

Alla luce di quanto accertato con il presente provvedimento, nonché sulla base della prassi aziendale riportata nei documenti in atti, si ritiene quindi che le attività di trattamento sopra descritte, realizzate attraverso la sistematica raccolta e conservazione delle e-mail aziendali e dei relativi log siano state realizzate in violazione del principio di liceità del trattamento di cui all'art. 5, par. 1, lett. a), del Regolamento.

Ciò in quanto, attraverso le operazioni sopra descritte, il titolare può ricostruire (come di fatto poi accaduto) l'attività dei propri dipendenti ed effettuare un controllo sulla stessa, in assenza delle garanzie stabilite nell'ambito del rapporto di lavoro, ai sensi dell'art. 88 del Regolamento, che rinvia alle norme più specifiche e di maggior tutela previste in materia lavoristica dall'ordinamento nazionale.

Nello specifico, l'art. 114 del Codice ("Garanzie in materia di controllo a distanza"), individua la disposizione di cui all'art. 4 della legge n. 300/1970 quale condizione di liceità dei trattamenti di dati personali effettuati nel contesto del rapporto di lavoro (in proposito si vedano alcuni provvedimenti adottati in relazione a casi concreti: provv. 21/07/2022, n. 255, doc. web n. 9809466; provv. 13/05/2021, n. 190, doc. web n. 9669974; provv. n. 53 del 01/02/2018, doc. web n. 8159221; provv. 13/07/2016, n. 303, doc. web n. 5408460).

Considerato, quindi, che l'art. 4, comma 1, della legge n. 300/1970, individua tassativamente le finalità (ovvero quelle organizzative, produttive, di sicurezza del lavoro e di tutela del patrimonio aziendale) per le quali gli strumenti, dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere impiegati nel contesto lavorativo, stabilendo precise garanzie procedurali (accordo sindacale o autorizzazione pubblica), si rileva che nel caso in esame i trattamenti siano stati effettuati in violazione di quanto previsto dalla normativa.

3.3. Violazione degli artt. 5, par. 1, lett. a) e 13 del Regolamento.

Risulta, inoltre, che la Società abbia predisposto, a partire dal 2022, alcuni documenti informativi che sono stati prodotti nell'ambito dell'istruttoria, consistenti nelle Linee guida Off Boarding e nella Policy per il corretto utilizzo degli strumenti information & communication tecnology.

Non è stato, invece, fornito nessun chiarimento rispetto a precedenti versioni di tali testi e delle modalità con cui i due reclamanti siano stati informati dei trattamenti posti in essere.

Si rileva, a tal proposito, che, in base all'art. 13 del Regolamento, l'informativa deve invece essere fornita agli interessati "nel momento in cui i dati personali sono ottenuti". Tale modalità è coerente con l'obbligo, posto in capo al titolare, di indicare, previamente e in modo trasparente, le attività di controllo che possono essere effettuate; ciò allo scopo di consentire all'interessato di essere pienamente consapevole della tipologia di operazioni di trattamento che potranno essere effettuate dal titolare del trattamento, anche attingendo, in un quadro di liceità e proporzionalità, ai dati raccolti nel corso dell'attività lavorativa.

In ogni caso, dall'esame congiunto di tali documenti, in cui vengono descritte le operazioni di trattamento effettuate anche sugli strumenti informatici messi a disposizione dei dipendenti da parte della Società, non risultano indicate le finalità dei trattamenti stessi, ovvero in maniera più specifica le finalità e i presupposti della conservazione della posta elettronica e dei relativi log.

A tal proposito, le Linee guida sulla trasparenza, adottate il 29 novembre 2017 dal Gruppo Articolo 29 per la protezione dei dati, chiariscono che "Oltre a definire le finalità del trattamento cui sono destinati i dati personali, dev'essere specificata la relativa base giuridica addotta ai sensi dell'articolo 6".

Nei casi in cui il trattamento venga effettuato sulla base del legittimo interesse del titolare, tale specifico interesse "dev'essere individuato a beneficio dell'interessato. La migliore prassi prevede che il titolare del trattamento possa anche fornire all'interessato le informazioni tratte dal test di bilanciamento, che dev'essere svolto come base giuridica del trattamento prima di raccogliere i dati personali degli interessati per poter addurre l'articolo 6, paragrafo 1, lettera f)".

Rispetto al periodo di conservazione dei dati, questo (o i criteri per determinarlo) "potrebbe essere dettato da fattori quali gli obblighi di legge o le linee guida di settore, ma dovrebbe essere indicato in maniera tale da consentire all'interessato di stabilire quale sarà, in base alla sua specifica situazione, il periodo previsto per i dati/fini specifici. Non è sufficiente che il titolare del trattamento affermi in maniera generica che i dati personali saranno conservati finché sarà necessario per le finalità legittime del trattamento. Ove pertinente, dovrebbero essere fissati periodi di conservazione diversi per le diverse categorie di dati personali e/o finalità del trattamento, inclusi, se del caso, i periodi di archiviazione".

Il "Regolamento per l'utilizzo di internet e della posta elettronica" prodotto con le memorie difensive a integrazione della precedente Policy, pur indicando in maniera coincisa e sufficientemente chiara i periodi di conservazione dei dati relativi alla posta elettronica e ai log, risulta ancora carente dell'informazione relativa alle finalità di tali attività di trattamento.

Pertanto, si conferma la violazione di quanto stabilito dagli artt. 5 par. 1, lett. a), e 13 del Regolamento, in base ai quali il titolare è tenuto a fornire preventivamente all'interessato tutte le informazioni relative alle caratteristiche essenziali del trattamento.

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

Per i suesposti motivi, l'Autorità ritiene che le dichiarazioni rese 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, con riferimento a tali profili, alcuno dei casi previsti dall'art. 11 del Regolamento del Garante n. 1/2019.

Il trattamento dei dati personali effettuato da Piaggio & C. S.p.A. risulta illecito, nei termini su esposti, in quanto posto in essere in violazione degli artt. 5, par. 1, lett. a), b), c) ed e), 6, 12, 13, 17 e 88 del Regolamento e dell'art. 114 del Codice.

La violazione accertata nei termini di cui in motivazione non può essere considerata "minore", tenuto conto della natura della violazione che hanno riguardato i principi generali del trattamento dei dati (liceità, minimizzazione, limitazione della conservazione) e le disposizioni più specifiche in materia di controlli a distanza, oltre ai diritti riconosciuti agli interessati.

Pertanto, visti i poteri correttivi attribuiti dall'art. 58, par. 2 del Regolamento, si dispone il divieto del trattamento dei dati raccolti illecitamente e l'irrogazione di una sanzione amministrativa pecuniaria ai sensi dell'art. 83 del Regolamento, commisurata alle circostanze del caso concreto (art. 58, par.

2, lett. f) e i) Regolamento).

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

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 Piaggio & C. S.p.A. s.r.l. ha violato gli artt. 5, par. 1, lett. a), b), c) ed e), 6, 12, 13, 17 e 88 del Regolamento, nonché l'art. 114 del Codice. Per la violazione delle predette disposizioni è prevista l'applicazione della sanzione amministrativa pecuniaria prevista dall'art. 83, par. 5, lett. a) e d) del Regolamento.

Il Garante, ai sensi dell'art. 58, par. 2, lett. i) del Regolamento e dell'art. 166 del Codice, ha il potere di infliggere una sanzione amministrativa pecuniaria prevista dall'art. 83 del Regolamento, mediante l'adozione di una ordinanza ingiunzione (art. 18. legge 24 novembre 1981 n. 689), in relazione al trattamento dei dati personali posto in essere da Piaggio & C. S.p.A. di cui è stata accertata l'illiceità, nei termini sopra esposti.

Ritenuto di dover applicare il paragrafo 3 dell'art. 83 del Regolamento che 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 dell' 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 e alla gravità della violazione, sono state considerate rilevanti le violazioni commesse che hanno riguardato le disposizioni in materia di esercizio dei diritti, i principi generali del trattamento e disposizioni più specifiche in materia di controlli a distanza; in particolare, è stata presa in considerazione la natura del trattamento che ha riguardato la sistematica registrazione e conservazione di comunicazioni effettuate dai dipendenti (interessati vulnerabili) mediante la posta elettronica e dei relativi log;

- con riguardo alla durata della violazione, è stata considerata la circostanza che il riscontro all'istanza di esercizio dei diritti è pervenuta solo a seguito dell'avvio dell'istruttoria da parte dell'Autorità; mentre è stata considerata rilevante la estesa durata della conservazione della posta elettronica e dei log (l'intera durata del rapporto di lavoro più un ulteriore periodo dopo la cessazione dello stesso);

- 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 ha previsto in via generale la conservazione dei dati contenuti nella posta elettronica dei propri dipendenti con possibilità di accedervi per una pluralità di scopi;

- a favore della Società, si è tenuto conto della cooperazione fornita nel corso del procedimento, finalizzata a porre rimedio alle violazioni riscontrate e ad attenuarne gli effetti negativi; in particolare, sono state positivamente valutate le modifiche apportate ai propri sistemi informatici rispetto al periodo di conservazione dei dati, l'adozione di ulteriori misure

tecniche, le revisioni ai documenti informativi per i dipendenti;

- è stata altresì considerata l'assenza di precedenti violazioni pertinenti commesse dal titolare.

Si ritiene inoltre che assumano 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 al volume d'affari della Società, di cui al bilancio di esercizio per l'anno 2025.

Alla luce degli elementi sopra indicati e delle valutazioni effettuate, si ritiene, nel caso di specie, di applicare nei confronti di Piaggio & C. S.p.A. la sanzione amministrativa del pagamento di una somma pari ad euro 460.000,00 (quattrocentosessantamila).

In tale quadro si ritiene, altresì, che, ai sensi dell'art. 166, comma 7, del Codice e dell'art. 16, comma 1, del Regolamento del Garante n. 1/2019, si debba procedere alla pubblicazione del presente capo contenente l'ordinanza ingiunzione sul sito internet del Garante.

Ciò in considerazione della condotta particolarmente lesiva dei diritti dell'interessato, avvenuta in violazione dei principi generali in materia di protezione dei dati personali.

TUTTO CIÒ PREMESSO, IL GARANTE

ai sensi dell'art. 57, par. 1, lett. f), del Regolamento, rileva l'illiceità del trattamento effettuato da Piaggio & C. S.p.A., in persona del legale rappresentante pro tempore, con sede legale in Pontedera (PI) Viale Rinaldo Piaggio, P.I. 01551260506, per la violazione degli artt. 5, par. 1, lett. a), b), c), e), 6, 12, 13, 17 e 88 del Regolamento e 114 del Codice;

ORDINA

alla predetta Società, ai sensi dell'art. 58, par. 2, lett. f) del Regolamento, il divieto dell'accesso al contenuto dei dati raccolti e conservati sui sistemi aziendali relativi alla posta elettronica aziendale;

ai sensi dell'art. 58, par. 2, lett. i) del Regolamento alla medesima Società di pagare la somma di euro 460.000,00 (quattrocentosessantamila) a titolo di sanzione amministrativa pecuniaria per le violazioni indicate nel presente provvedimento;

INGIUNGE

quindi alla medesima Società di pagare la predetta somma di euro 460.000,00 (quattrocentosessantamila), 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 rappresenta che ai sensi dell'art. 166, comma 8 del Codice, resta salva la facoltà per il trasgressore di definire la controversia mediante il pagamento - sempre secondo le modalità indicate in allegato - di un importo pari alla metà della sanzione irrogata entro il termine di cui all'art. 10, comma 3, del d. lgs. n. 150 del 1° settembre 2011 previsto per la proposizione del ricorso come sotto indicato.

DISPONE

- ai sensi dell'art. 166, comma 7, del Codice e dell'art. 16, comma 1, del Regolamento del

Garante n. 1/20129, la pubblicazione dell'ordinanza ingiunzione sul sito internet del Garante;

- ai sensi dell'art. 154-bis, comma 3, del Codice e dell'art. 37 del Regolamento del Garante n. 1/20129, la pubblicazione del presente provvedimento sul sito internet del Garante;

- ai sensi dell'art. 17 del Regolamento n. 1/2019, l'annotazione delle violazioni e delle misure adottate in conformità all'art. 58, par. 2 del Regolamento, nel registro interno dell'Autorità previsto dall'art. 57, par. 1, lett. u) del Regolamento.

Ai sensi dell'art. 78 del Regolamento, 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, 18 giugno 2026

IL PRESIDENTE
Stanzione

IL RELATORE
Ghiglia

IL SEGRETARIO GENERALE
Montuori