Provvedimento del 12 marzo 2026 [10233328]

VEDI ANCHE Newsletter del 15 aprile 2026

[doc. web n. 10233328]

Provvedimento del 12 marzo 2026

Registro dei provvedimenti
n. 165 del 12 marzo 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, componenti e il dott. Claudio Filippi, Vice 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 dal sig. XX, ai sensi dell'art. 77 del Regolamento nei confronti di ITAS Mutua;

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 la prof.ssa Ginevra Cerrina Feroni;

PREMESSO

1. L'avvio dell'istruttoria preliminare a seguito della presentazione del reclamo.

Con il reclamo presentato a questa Autorità in data 20/07/2023, il Sig. XX segnalava una violazione della disciplina in materia di protezione dei dati personali posta in essere da ITAS Mutua (di seguito "la Società"), ex datore di lavoro, consistente, in particolare, nel riscontro ritenuto non idoneo all'istanza di esercizio dei diritti formulata ai sensi dell'art. 15 del Regolamento.

In particolare, il reclamante rappresentava che, a seguito della cessazione del rapporto di lavoro con la Società, chiedeva alla stessa di poter accedere ai documenti e alle cartelle personali presenti sul pc e nella casella di posta elettronica aziendale di tipo individualizzato, utilizzata nel corso del rapporto di lavoro (pec del 02/05/2022 e del 09/05/2022).

Nel corso degli incontri avvenuti presso la sede della Società il 06/05/2022 e il 26/05/2022, la Società consentiva l'accesso al desktop e il recupero dei documenti personali, mentre l'accesso alla posta elettronica non veniva eseguito, a causa di non meglio precisate ragioni tecniche.

Nel corso dell'incontro svoltosi il 16/06/2022, la Società consegnava "la posta solamente personale quali scambi con famigliari, CU personali, rimborsi spese", mentre non venivano consegnati "altri messaggi di posta elettronica afferenti all'attività lavorativa e/o documenti ritenuti dai referenti ITAS non a contenuto personale" (verbale della riunione del 16/06/2022).

Il reclamante, pertanto, formulava un'istanza di esercizio dei diritti ai sensi dell'art. 15 del Regolamento, chiedendo formalmente alla Società di ricevere "copia di tutte le e-mail presenti nella casella di posta elettronica (…) dal 1° marzo 2021 in poi" oltre ad altra documentazione inerente al rapporto lavorativo (istanza del 15/07/2022).

Veniva quindi fissato un ulteriore incontro nel corso del quale la Società "consegna[va] all'interessato una chiavetta USB contenente la documentazione richiesta (…)", riservandosi di fornire le e-mail individuate nel corso della riunione in un momento successivo "debitamente anonimizzate relativamente ai dati personali attinenti soggetti terzi" (verbale del 22/09/2022).

La corrispondenza presente sull'account di posta elettronica veniva, infine, consegnata al reclamante, in data 29/09/2022, "epurata di molti elementi".

Alla luce di quanto sopra, l'Ufficio formulava una richiesta di informazioni, nei confronti della Società, ai sensi dell'art. 157 del Codice (nota dell'08/11/2023), a cui la Società forniva riscontro con nota del 06/12/2023, rappresentando che:

- "in data 11/04/2022 l'account di posta elettronica aziendale attribuito all'interessato è stato disattivato con l'attivazione del messaggio di risposta automatico rivolto a terzi, per poi essere definitivamente cancellato in data 25.04.2022";

- "In data 26/05/2022 e 16/06/2022, sono avvenuti specifici incontri in cui il [reclamante] ha avuto modo non solo di recuperare i propri effetti personali, ma anche di accedere alla casella email (…). A tal fine, la Società ha effettuato un restore dal sistema di backup su un laptop dedicato";

- "Ciononostante, in data 15/07/2022 l'interessato presentava per il tramite del proprio legale istanza di accesso ai dati personali ai sensi dell'art. 15 del RGPD, chiedendo copia di documentazione varia. (…).";

- "In data 22/09/2022 si svolgeva un ulteriore appuntamento per consentire al [reclamante] di accedere alla casella email, informando lo stesso che tale incontro sarebbe avvenuto in affiancamento per garantire che il reclamante non entrasse in possesso di dati e informazioni aziendali riservate, consentendo l'accesso e la copia dei soli dati personali riguardanti l'interessato stesso".

Con riferimento alle modalità e ai tempi di conservazione dei messaggi che transitano sulle caselle di posta elettronica aziendale, la Società osservava che:

- "a fronte della cessazione del rapporto di lavoro, i database di posta elettronica vengono disattivati tramite un apposito sistema informatico automatizzato di Identity & Access Management. La disabilitazione della casella attiva un messaggio automatico verso tutti i mittenti. La casella di posta elettronica rimane in uno stato di disattivazione per 14 giorni per poi, attraverso un automatismo, essere definitivamente cancellata dai sistemi online, rimanendo salvati nel sistema di backup per 5 anni";

- “in qualità di dipendente della Società, il reclamante ha ricevuto al momento dell’assunzione l’informativa sul trattamento dei dati personali, in conformità all’allora vigente disciplina in materia”;

- “oltre all’informativa privacy il reclamante riceveva altresì l’atto di nomina ad incaricato del trattamento ai sensi dell’art. 30 del Codice (…); in ragione del particolare ruolo ricoperto dal [reclamante], in data 20 ottobre 2021, la Società forniva al reclamante l’atto di nomina a “Referente interno a supporto del DPO” ricevendo ulteriori istruzioni specifiche in relazione alle attività di trattamento dei dati assegnati allo stesso”.

Con la nota, venivano trasmessi, in allegato, l’informativa, sottoscritta dal reclamante il 23/01/2012, la nomina a incaricato del trattamento, ai sensi dell’art. 30 del Codice (nella formulazione antecedente alle modifiche introdotte con il d.lgs. del 10 agosto 2018 n. 101), e la nomina a “Referente interno a supporto del DPO”, datata 20/10/2021, oltre al documento recante “Regole utilizzo strumenti aziendali” del 28/06/2019.

In particolare, dall’esame del documento ad oggetto “Regole utilizzo strumenti aziendali” (all. 4 alla nota del 06/12/2023), emergeva che:

- “A conclusione del rapporto di lavoro, la casella elettronica verrà bloccata in entrata e in uscita. Il contenuto della posta elettronica verrà bloccato e l’accesso permesso al solo titolare del trattamento o su suo mandato l’assistente tecnico informatico solo per l’accesso a dati per l’eventuale tutela dei diritti dell’interessato o del titolare” (punto 5.22 delle Regole cit.);

- “per questo si informa l’incaricato/autorizzato al trattamento che la trasmissione è controllata dal titolare e che i messaggi inviati e ricevuti vengono automaticamente salvati sui sistemi IT aziendali per il tempo necessario ad adempiere alle finalità indicate. Successivamente saranno conservati e non ulteriormente trattati, secondo quanto viene documentato nel nostro Registro di trattamento. Il periodo di conservazione può variare in modo significativo in base a: finalità, il tipo di dati trattato, gli obblighi di legge (…)” (punto 5.23 delle Regole cit.);

- “ITAS, in conformità ai provvedimenti del Garante privacy (…) e dell’art. 4 dello Statuto dei lavoratori (…), potrà effettuare controlli sugli strumenti elettronici concessi in uso (PC e dati archiviati, posta elettronica, accessi ad Internet, telefono, ecc.) qualora sia necessario” (par. 7, n. 1, Regole cit.)

Alla luce di quanto emerso, l’Ufficio formulava un’ulteriore richiesta di informazioni, ai sensi dell’art. 157 del Codice, chiedendo di conoscere le finalità, le modalità (con particolare riferimento ai tempi) e i presupposti di legittimità alla base della conservazione dei messaggi che transitano sugli account di posta elettronica aziendale, assegnati ai dipendenti, nonché l’eventuale rispetto della disciplina di settore in materia di controlli a distanza di cui all’art. 4 della legge n. 300 del 1970 richiamato dall’art. 114 del Codice (nota del 03/04/2024).

La Società, con la nota del 02/05/2024, rappresentava che:

- “I messaggi che transitano sugli account di posta elettronica dei dipendenti vengono conservati con misure di sicurezza adeguate in esito all’analisi del rischio, come documentate nel Registro dei trattamenti. Il backup della casella e-mail viene conservato per un periodo massimo di cinque anni. Il titolare (…) ha inteso operare una conservazione entro i termini indicati, ritenendoli congrui al rispetto dei principi di necessità, pertinenza e non eccedenza”;

- “Le finalità per le quali si è ritenuto di individuare il tempo di conservazione di cinque anni

trovano fondamento nella necessità di preservare il patrimonio informativo della società in relazione all'attività di vigilanza a cui la stessa è sottoposta, considerati i termini di prescrizione di legge derivanti dal core business di un'impresa assicurativa";

- "I messaggi di posta, avendo rilevanza giuridico-commerciale, sono quindi solamente conservati, senza che sia realizzato alcun ulteriore diverso trattamento (…) per il tempo necessario ad assicurare la possibilità, laddove richiesto dal Titolare del trattamento, di adempiere alle finalità rappresentate. La sola conservazione in sistemi non on-line, senza ulteriori trattamenti, infatti, garantisce che il contenuto dei messaggi di posta elettronica, così come gli allegati, in quanto forme di corrispondenza assistite da garanzia di segretezza costituzionale, non siano oggetto di accesso, a meno che non ricorrano le necessità di cui alle finalità indicate (…)";

- "Con riferimento ai controlli sugli account di posta elettronica (…) si precisa che pur avendone prevista nelle policy aziendali (vedasi paragrafo 7, punto 2, lettera a. e successivi del documento Regole di utilizzo degli strumenti informatici) la possibilità, non sono mai stati effettuati controlli a distanza volti a verificare l'attività dei lavoratori né in costanza di rapporto di lavoro né successivamente alla conclusione".

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 (nota del 26/08/2024), per la violazione degli artt. 5, par. 1, lett. a) e 88 in relazione all'art. 114 del Codice, 5, par. 1, lett. a) in relazione all'art. 13, 5, par. 1, lett. b), c) ed e), 12, par. 3 e 15 del Regolamento.

La Società, in data 24/09/2024, inviava le proprie memorie difensive sulla base dell'art. 18 della legge n. 689/1981, con cui osservava che:

- "ITAS ritiene che il diritto di accesso ai dati, come formulato in data 15.7.2022 sia stato adeguatamente riscontrato entro il termine di un mese come previsto dall'art. 12 del Regolamento, con pec del 10.8.2022, poi seguita dall'incontro in presenza del 22.9.2022 necessario per la grande mole di dati richiesta dall'istante";

- "Durante il mese di maggio 2022, il [reclamante] non più in forza in azienda, chiedeva di poter recuperare unicamente le dotazioni personali tra cui le "cartelle elettroniche personali presenti sul desk e sulla posta elettronica" (si veda pec del 23.05.2022);in data 26/05/2022 e 16/06/2022 sono avvenuti specifici incontri in cui il [reclamante] ha avuto modo non solo di recuperare i propri effetti personali, ma anche le sue email personali mediante un restore dal sistema di backup aziendale effettuato dall'Amministratore di Sistema (…) con il fornitore XX il quale ha proceduto al recupero del database di posta (non totalmente andato a buon fine in data 26 maggio 2022 ma poi completato con successo il 16 giugno 2022) tramite restore direttamente sul server Microsoft Exchange (…)";

- "Pertanto, l'accesso e la copia della "sola corrispondenza di carattere strettamente personale" è avvenuta, nella fase ante istanza ex art. 15 del Regolamento, poiché il [reclamante] aveva egli stesso, in un primo momento, limitato la sua richiesta alle sole "cartelle elettroniche personali presenti sul desk e nella posta elettronica" (…); nessuna esclusione è stata dunque adottata da ITAS né è avvenuta una "previa individuazione della [corrispondenza] da parte di personale interno dell'azienda" poiché il [reclamante] ha avuto accesso, durante i predetti incontri, alla casella email potendo selezionare e individuare lui stesso le email di interesse";

- “Solo in data 15/07/2022 l’interessato presentava, per il tramite del proprio legale, istanza di accesso ai dati personali ai sensi dell’art. 15 del RGPD, chiedendo copia di tutta la casella email aziendale dal 1° marzo 2021 (…)”;

- “ITAS, in virtù dei principi citati nelle Linee Guida [sui diritti degli interessati n. 1/2022], della notevole quantità di dati richiesti (i.e. copia della casella email) e del fatto che si trattava anche di informazioni aziendali riservate (…), dell’esistenza del backup aziendale, ha legittimamente proposto un incontro in presenza, nella data scelta dal reclamante (…). È stato avvisato il reclamante che tale incontro sarebbe avvenuto in affiancamento per garantire che non entrasse in possesso di informazioni aziendali riservate, ciò in linea con il Regolamento e l’EDPB”;

-“Il tutto è stato regolarmente verbalizzato e firmato in fede dal [reclamante] che mai ha contestato nulla in merito alle modalità di accesso nemmeno a verbale e che ha atteso fuori dalla riunione, qualche minuto, solo perché i delegati di ITAS all’operazione dovevano valutare se e cosa anonimizzare per tutelare i diritti di terzi e i segreti aziendali, come espressamente previsto dal Considerando 63 del Regolamento e anche dalle Linee guida”;

- “ITAS non ha posto in essere alcun illecito controllo sul dipendente. (…) Ci si permette di precisare che la scrivente società ha avuto accesso ai dati del [reclamante] solo per riscontrare la richiesta di accesso e mai ha effettuato attività di controllo sulle attività del dipendente che peraltro è un ex dipendente dall’08.04.2022 (antecedente alla richiesta di accesso privacy di luglio 2022 e ai fatti di settembre 2022) senza quindi alcuna violazione dell’art. 4 dello Statuto dei lavoratori. (…) Si precisa che mai è stato effettuato un controllo sull’account in transito (…)”;

- con riguardo alla conservazione dei log e delle e-mail in transito, “ITAS è consapevole della necessità di applicare in modo più stringente il principio di minimizzazione e, come già indicato nelle due memorie ha avviato un processo finalizzato ad aggiornare sia diverse procedure aziendali in materia di protezione dei dati personali (…) sia nuovamente l’informativa ai sensi dell’art. 13 del RGPD (doc. 12 già depositato con la prima memoria di dicembre 2023) e l’autorizzazione al trattamento ai sensi dell’art. 29 del RGPD (doc. 8 già depositato con la prima memoria di dicembre 2023) rilasciate a tutti i dipendenti”.

Con comunicazione del 16/01/2026, la Società ha inteso rinunciare all’audizione inizialmente richiesta ai sensi dell’art. 18 della legge n. 689/1981.

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 e 15 del Regolamento.

Con riferimento alla violazione degli artt. 12 e 15 del Regolamento, occorre esaminare, preliminarmente, l’oggetto dell’istanza presentata dal reclamante, in data 15/07/2022, e i riscontri forniti dalla Società, sia per mezzo delle comunicazioni del 10/08/2022 e del 21/09/2022, sia nel

corso dell'incontro che si è svolto, presso la sede societaria, di cui al verbale del 22/09/2022.

Viene correttamente osservato dalla Società che le iniziali richieste del reclamante erano limitate al recupero dei soli documenti personali presenti sul pc e sulla posta elettronica (si vedano le e-mail del 2, 9 e 23 maggio 2022); tuttavia, deve anche rilevarsi che tali richieste furono solo parzialmente accolte, in quanto l'accesso alla casella di posta elettronica del reclamante non fu possibile, a causa di problematiche di carattere tecnico (come risulta dal verbale dell'incontro del 26/05/2022).

Per questo motivo, l'interessato formulò un'ulteriore richiesta, il 01/06/2022, chiedendo una copia di tutta la posta elettronica, a cui seguì l'incontro del 16/06/2022, nel corso del quale, invece, al reclamante "viene consegnata la posta solamente personale quali scambi con famigliari, CU personali, rimborsi spese. Non sono consegnati altri messaggi di posta elettronica afferenti all'attività lavorativa e/o contenente documenti ritenuti dai referenti ITAS non a contenuto personale" (verbale della riunione del 16/06/2022).

La scelta della Società di circoscrivere l'ambito dei documenti da consegnare al reclamante alle sole e-mail di carattere personale viene ulteriormente ribadita nella e-mail del 21/09/2022 quando, in vista dell'incontro del giorno successivo, la Società chiarisce all'istante che "la richiesta di ricevere copia di "tutte le email presenti nella casella di posta" [oggetto dell'istanza del 15/07/2022] esula dal diritto di accesso ex art. 15 del GDPR. (…) i dati e le informazioni presenti nella casella di posta elettronica sono di proprietà di ITAS e la richiesta del Vostro assistito deve essere limitata ai suoi dati personali contenuti nella casella email".

La Società ha, poi, fatto presente che, nel corso degli incontri tenuti presso la sede aziendale, "l'interessato ha avuto accesso alla casella email potendo selezionare e individuare lui stesso le email di interesse". Risulta, in ogni caso, documentato che la corrispondenza non è stata immediatamente consegnata al reclamante, avendo la Società proceduto a una approfondita verifica, volta a individuare e anonimizzare i dati di terzi e i segreti aziendali che vi erano eventualmente contenuti.

Tanto premesso, occorre fare alcune precisazioni, rispetto all'oggetto dell'istanza di esercizio dei diritti, che, nel caso di specie, attiene principalmente al contenuto della casella di posta elettronica aziendale, di tipo individualizzato, utilizzata dal reclamante, nel corso del rapporto di lavoro.

A tal proposito, è opportuno richiamare il costante orientamento della Corte europea dei diritti dell'uomo che, in alcune pronunce (richiamate anche nei provvedimenti dell'Autorità), ha osservato come la linea di confine tra ambito lavorativo/professionale e ambito strettamente privato non sempre può essere tracciata con chiarezza, motivo per cui deve ritenersi applicabile, anche all'ambito lavorativo, l'art. 8 della CEDU posto a tutela della vita privata.

Anche le comunicazioni di tipo elettronico scambiate sul luogo di lavoro rientrano, quindi, nelle nozioni di "vita privata" e di "corrispondenza", di cui al citato articolo 8 (si vedano le pronunce 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; Brbulescu 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).

La protezione della vita privata si estende, dunque, 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 (v. artt. 2 e 41, comma 2, Cost.).

Pertanto, il trattamento dei dati, effettuato mediante tecnologie informatiche, nell'ambito del rapporto di lavoro, deve conformarsi al rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, a tutela di lavoratori e di terzi (v. Raccomandazione CM/Rec (2015)5 del

Comitato dei Ministri agli Stati Membri sul trattamento di dati personali nel contesto occupazionale, spec. punto 3).

Coerentemente con questa impostazione, nel provvedimento recante “Linee guida per posta elettronica e Internet” l’Autorità ha osservato che “Il contenuto dei messaggi di posta elettronica –come pure i dati esteriori delle comunicazioni e i file allegati– riguardano forme di corrispondenza assistite da garanzie di segretezza tutelate anche costituzionalmente, la cui ratio risiede nel proteggere il nucleo essenziale della dignità umana e il pieno sviluppo della personalità nelle formazioni sociali” (provvedimento del 01/03/2007, n. 13, doc. web n. 1387522, punto 5.2, lett. b). Orientamento che è stato ribadito anche in provvedimenti adottati dall’Autorità nell’ambito di specifiche istruttorie su casi concreti (si vedano provv.ti: n. 8 del 16/01/2025, doc web n. 10110927; n. 732 del 27/11/2024, doc web n. 10101221; n. 353 del 29/09/2021, doc web n. 9719914).

Alla luce di quanto sopra, deve quindi ritenersi contraria ai principi in materia di protezione dei dati personali la condotta, posta in essere dalla Società, consistente nella decisione di esaminare preventivamente il contenuto delle e-mail presenti sull’account di posta elettronica individualizzato dell’interessato, al fine di limitare l’accesso dello stesso alle sole comunicazioni di carattere “strettamente personale”, sull’erroneo convincimento che lo scambio di corrispondenza, intrattenuto sull’account aziendale, sia di piena ed esclusiva disponibilità dell’azienda.

Su questo aspetto, infatti, alla luce delle definizioni di “dato personale” e “trattamento”, di cui all’art. 4, n. 1 e 2, del Regolamento, che ricomprendono necessariamente anche i dati relativi all’attività lavorativa, le comunicazioni in transito su un account individualizzato sono inevitabilmente riconducibili a dati personali dell’assegnatario dell’account.

Deve ritenersi illecita peraltro anche l’ulteriore attività di oscuramento e anonimizzazione effettuata dalla Società sul contenuto della corrispondenza del reclamante, per rispondere all’esigenza di tutelare i diritti dei terzi e i segreti aziendali contenuti nelle e-mail.

Infatti, viste le ipotesi tassativamente previste dal Regolamento in cui il diritto di accesso può essere limitato solo in caso di richieste manifestamente infondate o eccessive (art. 12, par. 5, del Regolamento) e di tutela dei diritti dei terzi (art. 15, par. 4, del Regolamento), si rileva come nel caso di specie non ricorra nessuna delle circostanze previste dalla norma.

In particolare, per quel che riguarda la tutela dei diritti e delle libertà altrui, il considerando 63 precisa che tra questi va compreso anche il segreto industriale e aziendale e la proprietà intellettuale, segnatamente i diritti d’autore che tutelano il software.

Tuttavia, “la generica preoccupazione che, dando seguito alla richiesta di accesso, i diritti e le libertà altrui possano essere lesi non è sufficiente per fare appello all'articolo 15, paragrafo 4, GDPR. Il titolare del trattamento dev'essere in grado di dimostrare che, nella situazione concreta, i diritti o le libertà altrui sarebbero effettivamente lesi” (Linee guida 1/2022 sui diritti degli interessati - Diritto di accesso, punto 172).

Nel caso di specie, tra l’altro, si osserva come i dati riferiti ai terzi erano contenuti nelle comunicazioni ricevute e conosciute dallo stesso interessato, motivo per cui l’attività di oscuramento, effettuata su tali informazioni, appare non necessaria; per quel che riguarda la conoscibilità dei segreti aziendali, si evidenzia come la Società non abbia prodotto alcun elemento di fatto utile a dimostrare che, dall’accesso alla corrispondenza da parte dell’interessato, potesse effettivamente derivare un pregiudizio serio per i diritti e le libertà, quali appunto la conoscibilità o la sottrazione di segreti aziendali.

Deve, pertanto, confermarsi in capo alla Società la violazione delle disposizioni di cui agli artt. 12 e

15 del Regolamento, tenuto conto del fatto che tuttora non sono stati forniti all'interessato riscontri idonei e completi in relazione ai dati contenuti nella propria casella di posta elettronica aziendale individualizzata, tuttora nella disponibilità della Società.

3.2 Violazione degli artt. 5, par. 1, lett. a), b) c), e), e 13 del Regolamento.

Nell'ambito dell'istruttoria svolta, è emerso che la Società effettua una conservazione delle e-mail che transitano sugli account aziendali dei propri dipendenti, mediante un backup della posta elettronica disposta per un periodo di cinque anni, al fine di "preservare il patrimonio informativo della società in relazione all'attività di vigilanza a cui la stessa è sottoposta" (nota del 02/05/2024 e meglio specificato nelle memorie difensive del 24/09/2024).

Occorre innanzitutto osservare che la specifica attività di backup, disposta dalla Società sul contenuto delle caselle di posta elettronica assegnate ai dipendenti, non è stata contemplata e disciplinata in nessuno dei documenti informativi predisposti nei confronti dei dipendenti.

Ne deriva, quindi, che gli interessati non sono stati messi in condizione di conoscere l'attività di trattamento effettivamente svolta sulla posta elettronica in transito sui propri account, né i tempi di conservazione, le finalità di tale trattamento e i relativi presupposti di legittimità.

Tale condotta risulta quindi contraria al principio di correttezza e trasparenza (art. 5, par. 1, lett. a) del Regolamento) che, nell'ambito dei rapporti di lavoro, si esplica mediante la predisposizione di un'idonea informativa (art. 13 del Regolamento).

Nel caso di specie, infatti, le informative prodotte in atti (all. 6 e 12 alla nota del 06/12/2023) e il documento recante "Regole di utilizzo degli strumenti informatici" (all. 4 alla citata nota) contengono solo informazioni relative alla conservazione della posta elettronica che, tra l'altro, presentano tra loro evidenti difformità, rispetto ai tempi di conservazione dei dati raccolti e alle finalità in concreto perseguite.

In particolare, nell'informativa resa ai dipendenti (all. 6 alla nota del 06/12/2023), è indicato, in maniera assai generica, che "la società conserva, di regola, i dati del dipendente per un periodo di dieci anni dall'estinzione del rapporto di lavoro, salvo che sia previsto un periodo di conservazione diverso (ad esempio nel caso di contenzioso o per adempiere ad un obbligo di legge) che potrebbe essere inferiore o superiore a detto termine".

Invece, nel documento recante "Regole di utilizzo degli strumenti informatici", si legge che "il periodo di conservazione [della posta elettronica] può variare in modo significativo in base a: finalità, tipo di dato trattato, obblighi di legge (…)", oltre alla circostanza che l'accesso al contenuto della posta elettronica di un dipendente cessato è previsto "per l'eventuale tutela dei diritti dell'interessato o del titolare" (cap. 5, par. 22-23 del documento cit.).

Con specifico riguardo al backup del contenuto della posta elettronica, previsto per un periodo di tempo particolarmente esteso (pari a 5 anni), la Società ha motivato tale scelta in ragione della necessità di salvaguardare il patrimonio informativo in relazione all'attività di vigilanza a cui è sottoposta.

Tuttavia, come già ribadito dall'Autorità in altri provvedimenti, "la legittima necessità di assicurare la conservazione di documentazione necessaria per l´ordinario svolgimento e la continuità dell´attività aziendale, anche in relazione ai rapporti intrattenuti con soggetti privati e pubblici, nonché in base a specifiche disposizioni dell´ordinamento, è assicurata, in primo luogo, dalla predisposizione di sistemi di gestione documentale con i quali attraverso l´adozione di appropriate misure organizzative e tecnologiche individuare i documenti che nel corso dello svolgimento dell´attività lavorativa devono essere via via archiviati con modalità idonee a garantire le caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità prescritte dalla disciplina

di settore applicabile. I sistemi di posta elettronica, per loro stessa natura, non consentono di assicurare tali caratteristiche" (v. provv. n. 732 del 27 novembre 2024, doc web n. 10101221, n. 263 del 22/06/2023, doc. web n. 9920814, provv. n. 53 del 01/02/2018, doc. web n. 8159221 e provv. n. 214 del 29/10/2020 doc. web 9518890).

È opportuno quindi che la Società predisponga delle misure e tecniche che garantiscano una ordinaria ed efficiente gestione dei flussi documentali aziendali, in conformità alle disposizioni vigenti, che siano meno invasive per il diritto alla riservatezza degli interessati, con ciò evitando di effettuare attività di accesso al contenuto delle comunicazioni pervenute sugli account assegnati ai dipendenti e collaboratori.

Ciò, anche sul presupposto che lo scambio di corrispondenza elettronica, estranea o meno all'attività lavorativa, su un account aziendale di tipo individualizzato è un'operazione che consente di conoscere anche informazioni personali relative all'interessato e ai terzi mittenti delle comunicazioni la cui aspettativa di riservatezza è, nel caso concreto, non adeguatamente tutelata (v. "Linee guida del Garante per posta elettronica e Internet", cit., spec. punto 5.2, lett. b).

L'attività di conservazione della posta elettronica aziendale mediante backup del contenuto delle e-mail, contrariamente a quanto ritenuto, costituisce un'operazione di trattamento dei dati personali, sulla base della definizione di "trattamento" che si ricava dall'art. 4, n. 2 del Regolamento ("qualsiasi operazione o insieme di operazioni, quale la raccolta, la registrazione, l'organizzazione, …, la conservazione, …la consultazione, …").

Ritenere, quindi, che la conservazione della posta elettronica in modalità "non on-line" non rappresenti un trattamento di dati personali, è un'interpretazione errata che non tiene conto della nozione più ampia di trattamento che è data dal Regolamento.

Ciò posto, considerato che tale trattamento viene effettuato dalla Società per un esteso periodo di tempo (pari a 5 anni), si deve rilevare l'illiceità dello stesso per violazione dei principi di minimizzazione, di limitazione delle finalità e di limitazione della conservazione (art. 5, par. 1, b), c) ed e) del Regolamento), in quanto, come detto, trattasi di un'attività, protrattasi per un periodo di tempo notevole, che non è necessaria né proporzionata rispetto allo scopo di garantire la continuità dell'attività (v. provv. n. 53 del 01/02/2018, doc. web 8159221).

Tutto quanto sopra esposto deve ritenersi applicabile anche all'ulteriore attività di trattamento effettuata dalla Società sui log della navigazione in Internet. In tal caso, le citate Regole aziendali prevedono un periodo di conservazione dei file di log relativi alla navigazione in Internet per un periodo di 12 mesi, per finalità connesse al corretto funzionamento del sistema informatico, per la tutela del patrimonio aziendale, ma anche "per la difesa dei propri diritti contro gli abusi previsti dalla legge", oltre la possibilità di accedervi da parte di personale autorizzato (cap. 7, par. 2, lett. b) delle Regole cit.).

Come messo in evidenza in numerose circostanze dal Garante (in ultimo si veda il provv. del 09/10/2025 n. 613, doc web n. 10185435), laddove la conservazione dei file di log sia finalizzata ad assicurare la sicurezza informatica, il titolare del trattamento, in applicazione del principio di limitazione della conservazione (art. 5, par. 1, lett. e) del Regolamento), deve individuare un arco temporale congruo, rispetto all'obiettivo di rilevare e mitigare eventuali incidenti di sicurezza, adottando tempestivamente le opportune contromisure (si veda al tal proposito anche "Documento di indirizzo. Programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati", provv. del 06/06/2024, doc web. n. 10026277).

Nel caso di specie, tra l'altro, in base a quanto rilevato nelle Regole aziendali, tale trattamento viene realizzato per il perseguimento anche di finalità di difesa dei diritti, ovvero rispetto a finalità ulteriori rispetto a quelle necessarie a garantire la sicurezza informatica. La conservazione dei file

di log finalizzata alla difesa dei diritti in giudizio, invece, rappresenta uno strumento a disposizione del datore di lavoro idoneo a realizzare un controllo sull'attività dei dipendenti (si veda infra par. 3.3).

Alla luce del quadro complessivo di tutela dei dati personali, risulta altresì illecito, in quanto contrario ai principi di minimizzazione, di limitazione delle finalità e di limitazione della conservazione di cui all'art. 5, par. 1, lett. b), c) ed e) del Regolamento anche il trattamento effettuato dalla Società in relazione alla conservazione dei file di log della navigazione in Internet.

3.3. Violazione degli artt. 5, par. 1, lett. a), e 88 del Regolamento e dell'art. 114 del Codice.

La regolamentazione della gestione della posta elettronica e dell'utilizzo di Internet così come regolamentata dalla Società nelle policy interne rileva anche sotto il profilo del rispetto della disciplina di settore di cui alla legge n. 300/1970.

In diversi passaggi del documento recante le "Regole di utilizzo degli strumenti informatici", si dà atto di un accesso al contenuto della posta elettronica e ai log della navigazione in Internet che lo stesso titolare del trattamento (o gli assistenti informatici designati) può effettuare, per il perseguimento di varie finalità (si vedano i cap. 5, par. 22-23, e 7).

Sebbene la Società, nelle memorie difensive, abbia escluso di aver svolto qualsiasi controllo sul contenuto della posta elettronica del reclamante (e in generale dei propri dipendenti) e di aver effettuato l'accesso, al solo fine di riscontrare l'istanza di accesso dello stesso, tali circostanze di per sé non sono sufficienti a escludere l'applicabilità al caso di specie della disciplina sui controlli a distanza di cui alla legge n. 300/1970, proprio in virtù di quanto rappresentato nelle policy aziendali.

L'art. 4 della legge n. 300/1970, come noto, prevede una specifica procedura di garanzia in caso di impiego di "strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori", i quali "possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale", "previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali" o, in mancanza di accordo, "previa autorizzazione della sede territoriale dell'Ispettorato nazionale del lavoro".

Nel caso in esame, sia il backup della posta elettronica sia la conservazione dei log della navigazione in Internet rappresentano degli strumenti che sono potenzialmente idonei a realizzare un controllo sull'attività dei dipendenti in quanto consentono di trattare (ovvero di raccogliere nell'ambito del rapporto di lavoro e di conservare per un esteso periodo di tempo) informazioni e dati personali riferiti ai lavoratori, in assenza delle garanzie stabilite dalla legge.

Considerato, quindi, che, a fronte dei trattamenti descritti nelle "Regole di utilizzo degli strumenti informatici", non risulta che la Società abbia verificato la sussistenza, in concreto, delle tassative finalità indicate dall'art. 4 della legge n. 300/1970 (con particolare riferimento ai cd. scopi difensivi) né che abbia, all'esito di tale verifica, attivato la procedura di garanzia prevista dalla richiamata disciplina di settore, deve ritenersi confermata la violazione degli artt. 5, par. 1, lett. a) e 88 del Regolamento, che è richiamata dall'art. 114 del Codice ("Garanzie in materia di controllo a distanza") come condizione di liceità dei trattamenti di dati personali effettuati nel contesto del rapporto di lavoro.

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 ITAS Mutua risulta illecito, nei termini su esposti, in quanto posto in essere in violazione degli artt. 5, par. 1, lett. a), b), c), e), 13, 12, 15, 88 del Regolamento e 114 del Codice.

La violazione accertata nei termini di cui in motivazione non può essere considerata "minore", tenuto conto della natura delle plurime violazioni accertate, che hanno riguardato i principi generali del trattamento dei dati e le disposizioni più specifiche in materia di controlli a distanza, della gravità e della durata della violazione stessa, del grado di responsabilità e della maniera in cui l'autorità di controllo ha preso conoscenza della violazione (v. Considerando 148 del Regolamento).

Visti i poteri correttivi attribuiti dall'art. 58, par. 2, del Regolamento, alla luce delle circostanze del caso concreto, si dispone di:

- consentire al reclamante l'accesso integrale al contenuto della corrispondenza presente sull'account di posta elettronica aziendale, di tipo individualizzato, utilizzato nel corso del rapporto di lavoro;

- conformare le policy aziendale e i trattamenti descritti alla disciplina in materia di protezione dei dati personali come richiamata nei par. 3.2 e 3.3;

- 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), del 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 ITAS Mutua ha violato gli artt. 5, par. 1, lett. a), b), c) ed e), 13, 12, 15 e 88 del Regolamento, e art. 114 del Codice. Per la violazione delle predette disposizioni è prevista l'applicazione della sanzione amministrativa pecuniaria prevista dall'art. 83 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. L. 24 novembre 1981 n. 689), in relazione al trattamento dei dati personali posto in essere da ITAS Mutua 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, gravità e durata della violazione è stata considerata rilevante la natura della violazione che ha riguardato disposizioni poste a tutela dell'esercizio di diritti in materia di protezione dei dati e disposizioni più specifiche a tutela degli interessati nell'ambito dei rapporti di lavoro; quanto alla durata della violazione, deve considerarsi rilevante la circostanza che i dati relativi al contenuto della posta elettronica e della navigazione in Internet siano conservati per un considerevole periodo di tempo, e che il reclamante non abbia ricevuto riscontro completo all'istanza di accesso presentata il 15/07/2022;

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, il grado di responsabilità della stessa che non risulta tuttora conforme alla disciplina in materia di protezione dei dati, con specifico riferimento alla conservazione dei dati relativi al contenuto della posta elettronica e della navigazione in Internet;

a favore della parte si è tenuto conto del grado di cooperazione fornita nel corso dell'istruttoria e dell'assenza di precedenti specifici.

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 2024.

Alla luce degli elementi sopra indicati e delle valutazioni effettuate, si ritiene, nel caso di specie, di applicare nei confronti di ITAS Mutua la sanzione amministrativa del pagamento di una somma pari ad euro 50.000,00 (cinquantamila).

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 LT S.p.A., in persona del legale rappresentante pro tempore, con sede legale in Trento, Piazza delle donne lavoratrici n. 2, P.I. 00110750221, per la violazione degli artt. 5, par. 1, lett. a), b), c), e), 13, 12, 15 e 88 del Regolamento e dell'art. 114 del Codice;

ai sensi dell'art. 58, par. 2, lett. d), del Regolamento, prescrive alla Società di conformarsi, entro 90 giorni dalla data di notifica del presente provvedimento, alle prescrizioni formulate al par. 4 della presente decisione, richiedendo al contempo di fornire, entro il predetto termine, un riscontro adeguatamente motivato ai sensi dell'art. 157 del Codice; l'eventuale mancato riscontro può comportare l'applicazione della sanzione amministrativa pecuniaria prevista dall'art. 83, par. 5, lett. e) del Regolamento;

ORDINA

ai sensi dell’art. 58, par. 2, lett. i) del Regolamento alla medesima Società di pagare la somma di euro 50.000,00 (cinquantamila) 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 50.000,00 (cinquantamila), 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, 12 marzo 2026

IL PRESIDENTE
Stanzione

IL RELATORE

IL VICE SEGRETARIO GENERALE
Filippi