Provvedimento del 25 settembre 2025 [10184744]

[doc. web n. 10184744]

Provvedimento del 25 settembre 2025

Registro dei provvedimenti
n. 534 del 25 settembre 2025

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, alla quale hanno preso parte il prof. Pasquale Stanzione, presidente, la prof.ssa Ginevra Cerrina Feroni, vicepresidente, il dott. Agostino Ghiglia e l'avv. Guido Scorza, componenti e il cons. Angelo Fanizza, 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 nei confronti di Vimar S.p.A.;

ESAMINATA la documentazione in atti;

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

RELATORE il dott. Agostino Ghiglia;

PREMESSO

1. Il reclamo nei confronti della Società e l'attività istruttoria.

In data 25 maggio 2023, il sig. XX ha presentato un reclamo nei confronti di Vimar S.p.A. (di seguito, la Società) ai sensi dell'art. 77 del Regolamento e degli artt. 142 e ss. del Codice.

Il reclamo è stato regolarizzato, in data 17 luglio 2023, a seguito di invito a regolarizzare inviato dall'Autorità.

Con il reclamo, sono state lamentate presunte violazioni del Regolamento e in particolare: l'attivazione dell'account XX, in assenza di alcuna informativa fornita al reclamante; che il predetto account sia "aperto in un computer accessibile a chiunque (dipendenti e non dipendenti) con nome utente e password di accesso ben visibili e in quanto riportati in bella evidenza in un adesivo con l'aggiunta […] della dicitura «non rimuovere»"; che il predetto account sia stato utilizzato da soggetti terzi come se invece fosse usato dal reclamante che non era neanche a conoscenza

dell'esistenza dell'account stesso, fino a tempi recenti.

In data 7 settembre 2023, il Dipartimento ha inviato una richiesta di informazioni ai sensi dell'art. 157 del Codice e il 21 settembre 2023 la Società ha inviato il proprio riscontro nel quale ha dichiarato che:

> "l'account di posta elettronica XX è stato attivato il 19/10/2019. Il suddetto account fu creato per mere finalità organizzative e produttive. La sua creazione si rese necessaria perché, all'epoca dell'avvio delle operazioni di stoccaggio nel magazzino sito a Marostica […], le licenze «non nominative» non erano contemplate nell'offerta Microsoft, impedimento venuto meno solo da qualche mese, dopo che la fornitrice del software di posta elettronica ha accordato una modifica contrattuale […] che consente la creazione di caselle di posta elettronica «non nominative» per un massimo di 40 utenti" (v. nota cit., 21.9.2023, p. 1);
>
> "la casella di posta elettronica XX ha sempre avuto una operatività limitata alle comunicazioni relative alle modalità di esecuzione delle operazioni di magazzino e alle comunicazioni tra i reparti aziendali" (v. nota cit., p. 1);
>
> "l'account di posta elettronica [in esame] è stato disattivato in data 23/02/2023, una volta accertato che dell'esistenza del suddetto account il [reclamante] non era a conoscenza. Come comunicato ai difensori del [reclamante], infatti, dopo una verifica effettuata a seguito della richiesta del dipendente di disporre di una casella di posta elettronica aziendale al fine di inviare i calendari delle assemblee sindacali ai lavoratori, la Direzione Risorse Umane, constatato che un account di posta elettronica a nome del dipendente era già presente nei server aziendali, ma che di detto account il dipendente non era informato, ne ha senza indugio richiesto la disattivazione" (v. nota cit., p. 1);
>
> "nella fattispecie, la posta elettronica [riferita al reclamante] era utilizzata per l'organizzazione e la gestione dei turni degli addetti, per l'organizzazione delle spedizioni dei prodotti e, in generale, per tutte le comunicazioni aventi ad oggetto lo svolgimento delle operazioni logistiche dello specifico reparto. I soggetti autorizzati ad accedere e ad utilizzare l'account erano i dipendenti di Vimar S.p.A. ed i collaboratori della società appaltatrice di servizi logistici" (v. nota cit., p. 2);
>
> "la società si è dotata, fin dal 2015, di un Regolamento aziendale ([…] ultima versione del 27 settembre 2018) che disciplina l'utilizzo dei sistemi informatici, della posta elettronica aziendale ed in generale di tutti gli strumenti che l'azienda mette a disposizione dei lavoratori per lo svolgimento delle proprie mansioni lavorative" (v. nota cit., p. 2);
>
> "tutti i lavoratori di Vimar S.p.A. ricevono una informativa, conforme al dettato dell'articolo 13 del Regolamento […], relativa alle finalità, alle modalità del trattamento dei dati personali raccolti dall'azienda durante l'esecuzione del rapporto di lavoro oltre che sui diritti che possono essere esercitati in connessione al trattamento medesimo" (v. nota cit., p. 2).

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

Il 16 novembre 2023, l'Ufficio ha effettuato, ai sensi dell'art. 166, comma 5, del Codice, la notificazione alla Società delle presunte violazioni del Regolamento riscontrate, con riferimento agli artt. 5, par. 1, lett. a), b), c), d), 6, 13, 25, 32 del Regolamento.
In data 15 dicembre 2023, la Società ha presentato i propri scritti difensivi e in quell'occasione ha evidenziato che:

> "alla luce delle contestazioni di codesta Autorità e a compimento di un processo di aggiornamento delle proprie procedure privacy già in essere al momento del reclamo formulato dal [reclamante] (di seguito "Interessato") avanti alla medesima Autorità, la Società

comunica di aver avviato l'aggiornamento del regolamento per il corretto utilizzo degli strumenti informatici e l'informativa privacy destinata al personale" (v. nota 15/12/2023, p. 1);

"la Società si è infatti già attivata durante il presente procedimento per superare le criticità oggetto del reclamo" (v. nota cit., p. 1);

"la Società non ha in alcun modo agito con l'intento di eludere o violare le disposizioni legali vigenti in danno dei propri dipendenti. Questo si riflette anche nel caso dell'Interessato, evidenziando la buona fede della Società. […] la Società non ha in alcun modo occultato l'errore relativo all'attivazione dell'account aziendale di posta elettronica personalizzato dell'Interessato; anzi, ha prontamente intrapreso azioni correttive per porre fine al trattamento non conforme dei dati in questione" (v. nota cit., pp. 1, 2);

in merito alla "asserita carenza di liceità del trattamento" "seppur riconoscendo che nella fattispecie oggetto di contestazione non siano stati rispettati appieno i requisiti dettati dalla normativa in materia di protezione dei dati personali, pur tuttavia, la Società rileva come l'accaduto costituisca […] un caso isolato frutto di un errore nella gestione di un account email (dedicato in ogni caso a comunicazioni lavorative relative alle operazioni di magazzino), al quale la Società ha prontamente posto rimedio, provvedendo subito alla sua disattivazione" (v. nota cit., p. 2);

"trattandosi, nel caso di specie, di un account e-mail aziendale creato esclusivamente per la gestione delle operazioni di magazzino, l'Interessato non ha subito, né avrebbe potuto subire, danni derivanti dalla creazione del suddetto account e-mail, né, per i medesimi motivi, alcun soggetto avrebbe potuto violarne la riservatezza la Società ha immediatamente cancellato l'indirizzo di posta elettronica in oggetto una volta scopertane l'erronea attivazione" (v. nota cit., p. 2);

"non si è mai verificato alcun caso analogo, né la Società ha mai ricevuto contestazioni lato privacy e/o diritto del lavoro in relazione alla gestione della posta elettronica aziendale" (v. nota cit., p. 2);

"sull'asserita assenza di informativa" "la Società ha […] fornito sia l'informativa che il regolamento aziendale già agli atti. Ne consegue che, sulla base dei principi stabiliti nel citato provvedimento da codesta Autorità, la contestazione della violazione dell'obbligo informativo non è fondata" (v. nota cit., p. 3);

"sull'asserita violazione dei principi dell'art. 5 GDPR" "la Società non può che ribadire come l'accaduto sia frutto di un errore […] rileva di non avere mai effettuato accessi alla posta elettronica dei dipendenti, specie quelli cessati e che la disattivazione degli account è sempre avvenuta in tempi più ristretti di quelli indicati nel citato regolamento (massimo 180 giorni) in essere al momento dei fatti in oggetto. Per quanto riguarda le contestazioni circa gli Amministratori di sistema, si precisa che gli accessi possono avvenire ("facoltà") solo per motivi di sicurezza e tutela del patrimonio, come espressamente indicato proprio nel citato regolamento. La Società, quindi, non opera alcun controllo abusivo sui propri lavoratori, né tantomeno sulla loro corrispondenza" (v. nota cit., p. 3);

"la versione aggiornata del regolamento [aziendale] tiene conto delle osservazioni espresse da codesta Autorità in relazione al procedimento in corso" (v. nota cit., p. 4);

"in ottica di miglioramento è stata altresì aggiornata anche l'informativa privacy al personale ai sensi dell'art. 13 GDPR" (v. nota cit., p. 4);

"la Società riconosce l'errore commesso e, nell'intento di tutelare i propri dipendenti e prevenire incidenti simili a quello in questione, ha agito con sollecitudine per rafforzare le

proprie procedure. Questo intervento mira a risolvere le criticità sottolineate da codesta Autorità, dimostrando proattività, trasparenza e uno spirito di collaborazione assoluta, al fine di assicurare il corretto trattamento dei dati personali" (v. nota cit., p. 4);

"sull'asserita violazione del "principio di privacy by design" nel processo di creazione ed assegnazione delle e-mail ai lavoratori" "la Società ritiene infondata anche la contestazione relativa al mancato rispetto dell'art. 25 GDPR. La Società dispone infatti di regole per la gestione dell'attivazione di nuovi servizi, tra cui la corretta creazione di account e-mail al personale (vedi art. 13 Regolamento aziendale […]): in particolare, l'attivazione di nuovi account o le modifiche dei profili di accesso vengono richieste dal Responsabile Risorse Umane o dal Responsabile gerarchicamente superiore dell'utente attraverso l'apertura di ticket mediante software dedicato. Nel caso di specie tale sistema di attivazione non ha funzionato correttamente: tuttavia la Società evidenzia come ciò costituisca un caso isolato, non certamente un modus operandi consolidato della Società. E ciò anche in quanto la dinamica di attivazione (e poi di cessazione) della e-mail aziendale dell'Interessato è stato talmente singolare da non potersi spiegare in altro modo che un errore difficilmente ripetibile. Il sistema di regole adottato dalla Società è adeguato al rischio: l'attivazione di email aziendali non può infatti che passare da regole pre-stabilite e da un intervento umano. Purtroppo, nel caso di specie il sistema non ha funzionato" (v. nota cit., p. 4);

"sull'asserita violazione della sicurezza dei dati" "tale contestazione non è fondata dal momento che non è mai stato consentito l'accesso alla email aziendale personale dell'Interessato, bensì vi è stata solo una attivazione non corretta di una casella e-mail con nome e del cognome di quest'ultimo. L'e-mail in oggetto è stata originariamente assegnata ai dipendenti operanti presso il magazzino di Marostica […]. L'indirizzo e-mail è stato utilizzato come un contatto generico, rendendo improbabile che contenga dati personali dell'Interessato, al di là del suo nome e cognome, ai quali soggetti terzi avrebbero potuto accedere. La posta elettronica è peraltro protetta (aspetto mai contestato) da diverse misure di sicurezza (es. password, antivirus, antispam, MFA system, controllo phishing e antimalware, regolamento aziendale, istruzioni art. 29 GDPR, formazione, data breach policy, ecc.) e non è mai stata oggetto di accessi abusivi, per cui non si può dire che la Società non abbia implementato misure ex art. 32 GDPR adeguate. La Società coglie l'occasione per comunicare anche l'intervenuto e progressivo avvio di un processo di limitazione degli accessi ai servizi Office365 dai soli device aziendali" (v. nota cit., p. 5);

con riferimento agli elementi di cui all'art. 83 par. 2 del Regolamento si sottolinea che "il caso in oggetto è unico e isolato e ha coinvolto esclusivamente dati personali c.d. comuni (nella specie, nome e cognome) di un (1) solo interessato, per il solo tempo intercorrente tra la data di erronea attivazione e di cassazione dell'account email contestato" (v. nota cit., pp. 5, 6);

"la Società evidenzia che l'interessato non ha – ne avrebbe potuto – subire danni (es. contestazioni disciplinari) a causa dell'attivazione erronea dell'account email in oggetto. Infatti, qualora la Società avesse voluto contestare – cosa che non è mai accaduta – qualcosa all'Interessato si sarebbe ben presto accorta dell'errore che ha condotto al presente reclamo, errore che avrebbe inficiato qualsiasi procedimento disciplinare e/o causa giudiziaria" (v. nota cit., p. 6);

"la Società i) ha aggiornato il proprio regolamento aziendale (aggiornamento peraltro già avviato prima dell'avvio del presente procedimento), ii) ha riscritto le informative destinate ai lavoratori, iii) ha superato il problema di attivazione di e-mail generiche […]. […] dallo scorso mese di ottobre, prima quindi della notifica [delle violazioni], la Società ha avviato un aggiornamento formativo in materia privacy destinato ai lavoratori, tra cui i responsabili dell'ufficio IT, che si inserisce all'interno dei programmi di formazione in materia che

periodicamente vengono organizzati a cura della Società" (v. nota cit., p. 6);

"la Società non è stata condannata per alcuna violazione privacy" (v. nota cit., p. 6);

si tratta di un "procedimento originato da un reclamo dell'interessato" (v. nota cit., p. 7).

In data 5 febbraio 2024, a seguito di specifica richiesta della Società, si è tenuta l'audizione della stessa. In tale occasione la parte ha rappresentato che:

- "è stata la Società ad avvisare il reclamante dell'esistenza dell'account dopo che lo stesso aveva fatto richiesta alla Società di attivarne uno a suo nome per le comunicazioni sindacali";

- "vorremo sottolineare la prontezza con cui, una volta emerso il problema, è stata disattivata la casella di posta oggetto di reclamo";

- "la revisione del regolamento aziendale relativo agli strumenti informatici è cominciata prima della presentazione del reclamo e ad oggi è stata completata";

- "la Società allo stato ha attivato un account generalizzato per comunicazioni operative, logistiche che può essere utilizzato da quaranta utenze".

3. Esito del procedimento.

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

In base agli elementi acquisiti nel corso dell'attività nonché delle successive valutazioni di questo Dipartimento, risulta accertato che la Società ha creato un indirizzo di posta elettronica aziendale contenente il nome e il cognome del reclamante ("XX"), senza informarlo di ciò e mettendo il predetto account a disposizione di terzi, nello specifico ai dipendenti di Vimar S.p.A. e ai collaboratori della società appaltatrice di servizi logistici (v. nota del 21/9/2023, p. 2), e non al reclamante.

L'account, in particolare, sulla base di quanto dichiarato dalla stessa Società, è stato attivato il 19/10/2019 ed è stato disattivato in data 23/02/2023, tra l'altro, solo a seguito della "richiesta del dipendente di disporre di una casella di posta elettronica aziendale al fine di inviare i calendari delle assemblee sindacali ai lavoratori" e della conseguente constatazione, da parte della Direzione Risorse Umane, dell'esistenza di un account con il nominativo del reclamante.

La Società, nel confermare la condotta tenuta, ha manifestato l'esigenza di fare quanto descritto perché l'offerta sottoscritta con Microsoft non prevedeva la messa a disposizione di account generalizzati.

Dunque, la condotta della Società è consistita nell'attivazione di un indirizzo di posta, formalmente individualizzato intestato al reclamante, ma reso, di fatto, un account condiviso tra una molteplicità indefinita di soggetti (anche terzi rispetto alla Società) che per più di tre anni l'hanno utilizzato, per esigenze che la Società ha definito "organizzative/produttive" (v. nota 21/9/2023).

In tal modo, la Società ha effettuato un trattamento di dati personali del reclamante non conforme alla disciplina di protezione dei dati per i motivi che verranno indicati.

In proposito, si evidenzia che, salvo che il fatto non costituisca più grave reato, chiunque, in un procedimento dinanzi al Garante, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi ne risponde ai sensi dell'art. 168 del Codice "Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante".

Si rammenta, in termini generali, che il dato personale, oggetto di trattamento, è “qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale” (v. art. 4 punto 1 del Regolamento).

L’art. 5 par. 1 lett. a) del Regolamento dispone che i dati personali sono “trattati in modo lecito, corretto e trasparente nei confronti dell'interessato” (principio di liceità, di correttezza e di trasparenza»).

L’art. 5, par. 1, lett. b) e c), del Regolamento prevede che i dati personali sono “raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità” (principio di limitazione delle finalità) e che sono “adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati” (principio di minimizzazione dei dati).

L’art. 5, par. 1, lett. d), del Regolamento prevede che i dati personali devono essere “esatti e, se necessario, aggiornati” (principio di esattezza).

L’art. 13 del Regolamento prevede che il titolare è tenuto a fornire all’interessato tutte le informazioni relative alle caratteristiche essenziali del trattamento prima che questo abbia inizio. Nell’ambito del rapporto di lavoro l’obbligo di informare il dipendente è altresì espressione del principio generale di correttezza dei trattamenti (art. 5, par. 1, lett. a) del Regolamento).

Con riferimento alle condizioni di liceità dei trattamenti effettuati mediante sistemi di posta elettronica e della rete Internet nel contesto del rapporto di lavoro, il Garante ha adottato le "Linee guida del Garante per posta elettronica e Internet", Provv. 1.3.2007, in G. U. n. 58 del 10.3.2007.

Il trattamento di dati c.d. comuni, per essere lecito, deve essere effettuato, tra l’altro, in presenza di una delle condizioni di liceità individuate nell’art. 6 del Regolamento.

3.2 Violazioni accertate

3.2.1 Violazione del principio di liceità del trattamento.

La condotta della Società che è consistita nell’attivare un indirizzo di posta formalmente individualizzato intestato al reclamante, ma rendendolo, di fatto, un account condiviso tra una molteplicità indefinita di soggetti che, per più di tre anni, lo hanno utilizzato per esigenze che la Società ha definito “organizzative/produttive” (v. nota 21/9/2023) è stata posta in essere in assenza di una idonea condizione di liceità del trattamento: l’account in esame, infatti, non è stato creato affinché venisse utilizzato dal reclamante, nell’ambito dell’attività lavorativa (trattamento che, in astratto, sarebbe stato lecito), ma impiegato da soggetti terzi, rispetto al rapporto intercorrente tra il reclamante e la Società, tra l’altro, non comunicandolo al reclamante stesso.

La Società ha pertanto violato gli artt. 5 par. 1 lett. a) e 6 del Regolamento.

In proposito la Società si è limitata a riconoscere come nel caso di specie “non siano stati rispettati appieno i requisiti dettati dalla normativa in materia di protezione dei dati personali” e che quanto accaduto sia “frutto di un errore nella gestione di un account email” (v. nota 15/12/2023, p. 2).

Relativamente a ciò, dunque, la stessa Società è consapevole di avere posto in essere una condotta non conforme alla disciplina di protezione dei dati personali.

Peraltro tale condotta, protrattasi per oltre tre anni e nota a numerosi soggetti all'interno della Società — come dimostra il numero di persone che facevano uso dell'account nel contesto lavorativo — non può essere considerata un semplice errore.

3.2.2 Violazione del principio di correttezza.

Il trattamento posto in essere dalla Società non è stato conforme neppure al principio di correttezza posto che, anche nell'ambito del rapporto di lavoro, l'esecuzione del contratto deve essere conforme ai principi di buona fede e correttezza (art. 1375 c.c.).

Nel caso di specie, ciò non è avvenuto considerato che un account riferito a uno specifico soggetto è stato utilizzato da altri, come se fossero il titolare dell'account senza, tra l'altro, come già precisato, che di quanto posto in essere venisse informato il reclamante.

Il principio di correttezza che deve guidare la condotta delle parti anche per quanto riguarda i trattamenti collegati a contratti, è da intendersi come canone di condotta leale e corretta reciproca, che riguarda dunque entrambe le parti del rapporto.

La condotta della Società si pone in contrasto con l'art. 5 par. 1 lett. a) del Regolamento.

3.2.3 Violazione del principio di minimizzazione.

Il trattamento della Società è stato effettuato altresì in violazione del principio di minimizzazione (art. 5 par. 1 lett. c) del Regolamento) in quanto l'utilizzo dell'account in esame non è stato adeguato e pertinente, rispetto alle finalità per le quali era necessario e lecito avvenisse.

Il datore di lavoro, in qualità di titolare del trattamento, infatti, può creare account di posta elettronica individualizzati da assegnare ai lavoratori, nell'ambito del rapporto di lavoro, ma gli account individualizzati - quindi quelli che sono ricollegati a uno specifico interessato - costituiscono dati personali ai sensi dell'art. 4 (1) del Regolamento ai quali si applica la disciplina di protezione dei dati personali.

Pertanto, il datore di lavoro non può utilizzare i dati personali di un dipendente (quali, per esempio, nome e cognome) per creare account condivisi, utilizzati da una molteplicità di soggetti differenti rispetto al dipendente stesso.

Un uso quale quello posto in essere dalla Società, nel caso di specie, comporta dunque un trattamento di dati personali non adeguati, non pertinenti e non limitati alle finalità per le quali l'account individualizzato avrebbe potuto essere utilizzato.

3.2.4 Violazione del principio di limitazione delle finalità e del principio di esattezza.

Il trattamento in esame è stato inoltre posto in essere in violazione del principio di limitazione della finalità (art. 5 par. 1 lett. b) del Regolamento) considerato che un account di posta elettronica aziendale individualizzato deve essere utilizzato, in quanto dato personale dell'intestatario, dal soggetto al quale si riferisce e non da terzi, come, invece, è accaduto nel caso di specie. Ciò anche a tutela, tra l'altro, di coloro che vi entrano in contatto scambiando corrispondenza con l'account in questione.

Il trattamento è stato pertanto effettuato in violazione anche del principio di esattezza (art. 5 par. 1 lett. d) del Regolamento), considerato che l'account riferito al reclamante, in quanto contenente il suo nome e cognome, è stato utilizzato da soggetti diversi dallo stesso, secondo una modalità di utilizzo definita dalla Società.

In proposito, si sottolinea come la spiegazione del trattamento fornita dalla Società, ricollegata alla

mancanza, nell'offerta di Microsoft, della possibilità di ricorrere ad account generalizzati - circostanza che comunque non è stata provata nel corso del procedimento - non risulta dirimente posto che la Società, in quanto titolare del trattamento, avrebbe potuto, viste le proprie esigenze, trovare offerte che prevedessero, tra l'altro, la possibilità di ricorrere ad account non individualizzati.

In ogni caso, l'impossibilità, tramite l'offerta del tempo, di utilizzare account generalizzati non può giustificare la violazione della disciplina di protezione dei dati.

Inoltre, con il "Regolamento per l'utilizzo del sistema informativo fornito dalla Società", aggiornato al 26 luglio 2018 (quindi prima del verificarsi dei fatti oggetto di reclamo), consegnato dalla Società in allegato al riscontro del 21 settembre 2023, quest'ultima ha fornito agli interessati informazioni sul trattamento dei dati degli account di posta elettronica aziendale non aderenti alla condotta tenuta nel caso di specie e a quanto dichiarato in merito alla impossibilità di attivare utenze generalizzate: nel citato regolamento aziendale, infatti, vi è la precisazione che "Attivazione di utenze generiche: caso di più persone che utilizzano lo stesso PC e utilizzano lo stesso ambiente di lavoro. Nel caso ci sia la necessità di far usare lo stesso PC a più persone, sarà possibile creare delle utenze generiche con la nomenclatura "X-…..". Per questa tipologia di utenti, l'utilizzo della mail sarà riservato solo a indirizzi non riconducibili ad un utilizzo nominativo, come ad esempio: X-CP1 con email XX" (v. p. 4, punto 6).

Quanto riportato nel regolamento aziendale relativamente alle "utenze generiche", non risulta corrispondere alla condotta tenuta dalla Società: in base a quanto dichiarato dalla Società, infatti, fino alla modifica contrattuale con Microsoft (avvenuta in una data non meglio precisata, ma comunque "qualche mese" prima del riscontro del 21/9/2023), la Società stessa non aveva attivato account non individualizzati, ma anzi aveva fatto utilizzare un account, formalmente individualizzato, a una molteplicità di soggetti diversi dall'interessato.

3.2.5 Violazione dell'obbligo di fornire l'informativa.

La Società ha inoltre effettuato il trattamento descritto, senza fornire all'interessato un'idonea informativa e, quindi, in violazione dell'art. 13 e dell'art. 5 par. 1 lett. a) del Regolamento (principio di correttezza) posto che, nell'ambito del rapporto di lavoro, fornire al lavoratore un'adeguata informativa è espressione del generale principio di correttezza.

Premesso comunque e in ogni caso che nei documenti contenenti le informazioni in merito al trattamento dei dati devono essere descritte operazioni di trattamento conformi alla disciplina di protezione dei dati personali (in quanto non è sufficiente informare gli interessati di un trattamento perché quest'ultimo possa considerarsi di per sé solo lecito), nel caso di specie né il "Regolamento per l'utilizzo del sistema informatico" (nella versione "Rev. 2 approvato dalla Direzione aziendale il 26 luglio 2018", all. 2 al riscontro del 21/09/2023 che è stato oggetto del procedimento avviato dinanzi alla Autorità) né il documento contenente "Informativa e dichiarazione di consenso al trattamento dei dati personali" (all. 3 al riscontro del 21/09/2023 che è stato oggetto di esame nel corso del procedimento avviato dinanzi alla Autorità) forniti dalla Società, possono considerarsi documenti attraverso i quali la Società abbia adempiuto, con riferimento alla fattispecie oggetto di esame, all'obbligo del titolare del trattamento di fornire la c.d. informativa.

Si osserva, inoltre e in ogni caso, come il predetto "Regolamento per l'utilizzo del sistema informativo fornito dalla Società" nella versione consegnata dalla Società con il riscontro del 21 settembre 2023 non risulti conforme all'art. 5 del Regolamento, in particolare al principio di minimizzazione, nella parte in cui precisa che, in caso di dimissioni, "Su specifica richiesta del diretto responsabile, l'account di rete del dimissionario può essere mantenuto attivo fino ad un massimo di 180 gg dalla data di cessazione. La sua email potrà essere indirizzata a un altro

indirizzo esistente in azienda. […] Su richiesta del responsabile, possono venire consegnati l'archivio di posta e gli eventuali dati personali archiviati nel PC del dimissionario".

Allo stesso modo, non è conforme al principio di minimizzazione la disposizione secondo la quale, in caso di maternità o di malattia prolungata, "può essere impostato un inoltro automatico ad un indirizzo di posta elettronica alternativo. In questo caso, la persona oggetto dell'assenza deve attivare – prima dell'uscita dall'azienda – un inoltro automatico a un indirizzo concordato con il proprio responsabile. Su specifica richiesta del responsabile, l'inoltro della mail nel caso il diretto interessato sia impossibilitato ad effettuarlo potrà essere impostato da DSI".

Sempre per quanto riguarda la posta elettronica, non risulta conforme al principio di liceità del trattamento (art. 5 par. 1 lett. a) del Regolamento) la previsione secondo cui "L'Amministratore del Sistema per l'espletamento delle sue funzioni, ha la facoltà, per ragioni di sicurezza e tutela del patrimonio aziendale, in qualunque momento di accedere ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica" (v. regolamento aziendale p. 1, punto 2, "Utilizzo del personal computer").

Non risulta individuabile, infatti, la condizione di liceità del trattamento in presenza della quale l'amministratore di sistema potrebbe accedere, in ogni momento, agli interi archivi di posta elettronica, quindi anche alle comunicazioni scambiate con account di posta elettronica individualizzati, considerato anche 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; un'ulteriore protezione deriva dalle norme penali a tutela dell'inviolabilità dei segreti (artt. 2 e 15 Cost.; Corte cost. 17 luglio 1998, n. 281 e 11 marzo 1993, n. 81; art. 616, quarto comma, c.p.; art. 49 Codice dell'amministrazione digitale; v. Provv. 1° marzo 2007, n. 13 "Linee guida per posta elettronica e internet", in G. U. n. 58 del 10.3.2007).

In proposito si osserva, inoltre, come, dal riferimento contenuto nel regolamento aziendale agli "archivi di posta elettronica", non è chiaro se il titolare del trattamento raccolga sistematicamente le comunicazioni elettroniche scambiate dai propri dipendenti nel corso del rapporto di lavoro e che trattamento ulteriore eventualmente effettui.

In proposito la Società, a seguito della notifica delle violazioni del 16 novembre 2023, ha sostenuto di "non avere mai effettuato accessi alla posta elettronica dei dipendenti, specie quelli cessati e che la disattivazione degli account è sempre avvenuta in tempi più ristretti di quelli indicati nel citato regolamento (massimo 180 giorni) in essere al momento dei fatti in oggetto. Per quanto riguarda le contestazioni circa gli Amministratori di sistema, si precisa che gli accessi possono avvenire ("facoltà") solo per motivi di sicurezza e tutela del patrimonio, come espressamente indicato proprio nel citato regolamento. La Società, quindi, non opera alcun controllo abusivo sui propri lavoratori, né tantomeno sulla loro corrispondenza" (v. nota 15/12/2023, p. 3)".

Posto che in proposito non è stata fornita alcuna evidenza, in ogni caso, il fatto che nei documenti citati sarebbero descritte operazioni di trattamento non in linea con quanto in concreto effettuato dalla Società conferma, a maggiore ragione, che il contenuto dei documenti citati non fosse corretto e, dunque, non conforme alle disposizioni normative.

Con riferimento alle versioni riviste del regolamento aziendale e dell'informativa allegati agli scritti difensivi, in merito alle quali la Società ha dichiarato di avere tenuto conto di quanto rilevato dalla Autorità, e ha comunicato che "si trasmette in allegato la versione aggiornata del regolamento […]. In assenza di ulteriori commenti o indicazioni da parte di codesta Autorità, il regolamento menzionato verrà diffuso tra i dipendenti unitamente all'informativa sul trattamento dei dati

personali allegata allo stesso"), si invita la Società, nel revisionarli, a tenere conto di quanto l'Autorità ha già deciso in relazione a specifici casi concreti sui temi relativi alla gestione ed eventuale conservazione della posta elettronica, anche in relazione al raccordo ai profili relativi alla disciplina sui controlli a distanza (v. es., tra i tanti, provv. n. 171 del 27 aprile 2023, doc. web n. 9909235 in www.garanteprivacy.it; provv. 21 dicembre 2023, n. 602, doc. web n. 9978536).

Per quanto riguarda invece la contestazione, formulata in sede di avvio del procedimento, in merito alla violazione degli artt. 25 e 32 del Regolamento in relazione al principio di protezione dei dati fin dalla progettazione e alla mancata adozione delle misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, si ritiene che quanto rappresentato dalla Società negli scritti difensivi del 15 dicembre 2023 abbia messo in luce come la stessa non abbia, con la condotta esaminata, violato gli articoli appena indicati, considerato il trattamento nello specifico posto in essere e considerato che i rilievi di non conformità alla disciplina di protezione dei dati personali accertati dall'Autorità rientrano negli altri profili sopra indicati.

Per tali ragioni non si ritiene che sussistano, nel caso di specie, gli estremi per adottare provvedimenti in relazione alla violazione degli artt. 25 e 32 del Regolamento, contenuta nella notifica delle violazioni del 16 novembre 2023 che si ritiene, dunque, di archiviare nella parte riguardante tali specifici profili oggetto di contestazione.

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

Per i suesposti motivi, l'Autorità ritiene che le dichiarazioni, la documentazione e le ricostruzioni fornite dal titolare del trattamento nel corso dell'istruttoria non consentono di superare i rilievi notificati dall'Ufficio con l'atto di avvio del procedimento e che risultano pertanto inidonee a consentire l'archiviazione del presente procedimento, non ricorrendo peraltro alcuno dei casi previsti dall'art. 11 del Regolamento del Garante n. 1/2019.

Il trattamento dei dati personali effettuato dalla Società e segnatamente l'attivazione di un indirizzo di posta formalmente individualizzato intestato al reclamante, ma rendendolo, di fatto, un account condiviso tra una molteplicità indefinita di soggetti che, per più di tre anni, lo hanno utilizzato per esigenze che la Società ha definito "organizzative/produttive", risulta non conforme alla disciplina di protezione dei dati personali e in particolare in violazione degli artt. 5, par. 1, lett. a), b), c), d), 6, 13, 25, 32 del Regolamento.

La violazione, accertata nei termini di cui in motivazione, non può essere considerata "minore", tenuto conto della natura e della gravità della violazione stessa che ha riguardato, tra l'altro, i principi generali del trattamento, la maniera in cui l'autorità di controllo ha preso conoscenza della violazione (v. Considerando 148 del Regolamento).

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

L'Autorità ha preso in considerazione i criteri relativi al carattere doloso o colposo della violazione e le categorie di dati personali interessate dalla violazione nonché la maniera in cui l'autorità di controllo ha preso conoscenza della violazione (v. art. 82, par. 2, e Considerando 148 del Regolamento).

Pertanto, visti i poteri correttivi attribuiti dall'art. 58, par. 2, del Regolamento si dispone la predisposizione dei documenti contenenti le informazioni sui trattamenti relativi agli account di

posta elettronica aziendale in modo che il contenuto descriva operazioni di trattamento conformi alla disciplina di protezione dei dati personali 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), g) e i) del Regolamento

5. Adozione dell'ordinanza ingiunzione per l'applicazione della sanzione amministrativa pecuniaria e delle sanzioni accessorie (artt. 58, par. 2, lett. i), e 83 del Regolamento; art. 166, comma 7, del Codice).

La violazione degli artt. 5, par. 1, lett. a), b), c), d), 6, 13 del Regolamento comporta l'applicazione della sanzione amministrativa dall'art. 83, par. 5, lett. a) e d) del Regolamento, mediante adozione di un'ordinanza ingiunzione (art. 18, l. 24.11.1981, n. 689).

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 Vimar 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 laddove prevede che "se, in relazione allo stesso trattamento o a trattamenti collegati, un titolare del trattamento […] viola, con dolo o colpa, varie disposizioni del presente Regolamento, l'importo totale della sanzione amministrativa pecuniaria non supera l'importo specificato per la violazione più grave", l'importo totale della sanzione è calcolato in modo da non superare il massimo edittale previsto dal medesimo art. 83, par. 5.

Con riferimento agli elementi elencati dall'art. 83, par. 2 del Regolamento ai fini dell'applicazione della sanzione amministrativa pecuniaria e della relativa quantificazione, tenuto conto che la sanzione deve essere "in ogni singolo caso effettiva, proporzionata e dissuasiva" (art. 83, par. 1 del Regolamento), si rappresenta che, nell'ipotesi in esame, sono state tenute in considerazione le circostanze sotto riportate:

la rilevante gravità della violazione, infatti questa ha riguardato anche fattispecie punite più severamente in ragione dell'interesse protetto dalle norme violate (riguardanti i principi di liceità, correttezza, limitazione della finalità, minimizzazione, esattezza; il diritto di informativa);

la durata della violazione relativa all'utilizzo dell'account di posta elettronica individualizzato da parte di una pluralità di soggetti all'insaputa del reclamante che si è protratta dal 19/10/2019 al 23/02/2023 per quanto riguarda il trattamento dell'account di posta elettronica aziendale contenente nome e cognome del reclamante;

con riferimento al carattere doloso o colposo della violazione e al grado di responsabilità del titolare, sono stati presi in considerazione gli elementi oggettivi della condotta della Società e il grado di responsabilità della stessa che ha violato l'obbligo di diligenza, previsto dall'ordinamento, e non si è conformata alla disciplina in materia di protezione dei dati, relativamente a una pluralità di disposizioni;

si è tenuto conto della cooperazione con l'Autorità di controllo; si è tenuto anche conto del fatto che la Società in data 23/02/2023 ha cancellato l'account in esame.

Si ritiene inoltre che assumano rilevanza nel caso di specie, in ragione 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), le condizioni economiche del contravventore, determinate in base ai ricavi conseguiti dalla Società con riferimento al bilancio

ordinario d’esercizio per l’anno 2024 (ultimo disponibile).

Alla luce degli elementi sopra indicati e delle valutazioni effettuate, si ritiene, nel caso di specie, di applicare nei confronti di Vimar S.p.A. la sanzione amministrativa del pagamento di una somma pari ad euro 15.000 (quindicimila/00).

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 delle caratteristiche concrete della fattispecie esaminata, in particolare posto che il trattamento ha violato anche principi generali del trattamento, tra cui liceità, correttezza, limitazione della finalità, minimizzazione, esattezza, e considerato che per un lungo periodo di tempo un account di posta elettronica aziendale che, pur avendo i caratteri di un account individualizzato, è stato utilizzato come account generalizzato da una pluralità di soggetti anche facenti parte di una diversa compagine aziendale.

TUTTO CIÒ PREMESSO, IL GARANTE

ai sensi dell’art. 57, par. 1, lett. f) e 83, del Regolamento rileva l’illiceità del trattamento effettuato da Vimar S.p.A., con sede legale in Marostica (VI), viale Vicenza, 14, 36063, C.F. 01587170307, descritto nei termini di cui in motivazione, per la violazione degli artt. 5, par. 1, lett. a), b), c), d), 6, 13 del Regolamento;

DETERMINA

di archiviare la contestazione adottata nei confronti di Vimar S.p.A. in personale del legale rappresentante pro-tempore, con atto del 16 novembre 2023, limitatamente alla violazione degli artt. 25 e 32 del Regolamento;

ORDINA

a Vimar S.p.A.:

- ai sensi dell’art. 58, par. 2, lett. d) di predisporre documenti contenenti le informazioni sui trattamenti relativi agli account di posta elettronica aziendale che siano conformi alla disciplina di protezione dei dati personali;

- ai sensi dell’art. 58, par. 2, lett. i) del Regolamento di pagare la somma di euro 15.000 (quindicimila/00) a titolo di sanzione amministrativa pecuniaria per le violazioni indicate nel presente provvedimento.

INGIUNGE

quindi a Vimar S.p.A. di pagare la predetta somma di euro 15.000 (quindicimila/00), secondo le modalità indicate in allegato, entro trenta giorni dalla notifica del presente provvedimento, pena l’adozione dei conseguenti atti esecutivi a norma dall'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. 1/2019, 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. 1/2019, la pubblicazione del presente provvedimento sul sito internet dell’Autorità;

ai sensi dell’art. 17 del Regolamento del Garante 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, 25 settembre 2025

IL PRESIDENTE
Stanzione

IL RELATORE
Ghiglia

IL SEGRETARIO GENERALE
Fanizza