Provvedimento del 14 maggio 2026 [10255494]

VEDI ANCHE Comunicato stampa del 28 maggio 2026

[doc. web n. 10255494]

Provvedimento del 14 maggio 2026

Registro dei provvedimenti
n. 342 del 14 maggio 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, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE, "Regolamento generale sulla protezione dei dati" (di seguito "Regolamento");

VISTO il d.lgs. 30 giugno 2003, n. 196 recante "Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE (di seguito "Codice");

VISTO il Regolamento n. 1/2019 concernente le procedure interne aventi rilevanza esterna, finalizzate allo svolgimento dei compiti e all'esercizio dei poteri demandati al Garante per la protezione dei dati personali, approvato con deliberazione n. 98 del 4 aprile 2019, pubblicato in G.U. n. 106 dell'8 maggio 2019 e in www.gpdp.it, doc. web n. 9107633 (di seguito "Regolamento del Garante n. 1/2019");

Vista la documentazione in atti;

Viste le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del Regolamento del Garante n. 1/2000 sull'organizzazione e il funzionamento dell'ufficio del Garante per la protezione dei dati personali, doc. web n. 1098801;

Relatore la prof.ssa Ginevra Cerrina Feroni;

PREMESSO

1. Introduzione.

Alla luce di talune notizie di stampa, l'Autorità ha avviato d'ufficio specifici accertamenti ispettivi

nei confronti di Myndoor S.r.l. (di seguito anche solo “Myndoor” o “Società”), ai sensi dell’art. 58, par. 1, del Regolamento e degli artt. 157 e 158 del Codice, in relazione ai trattamenti effettuati mediante il sistema plug-in, sviluppato dalla medesima Società, il quale prevede il ricorso alla c.d. sentiment analysis dei messaggi scambiati dagli individui che decidano di utilizzarlo nello svolgimento della propria attività lavorativa nell’ambito delle chat Slack e Teams (v. verbali delle operazioni compiute nei giorni 3 e 4 giugno 2025).

Al riguardo, occorre preliminarmente dare atto che tali iniziative ispettive sono state avviate sul presupposto che, in base a quanto appreso dalle predette notizie di stampa, il sistema plug-in Myndoor sarebbe stato in uso presso numerosi enti della pubblica amministrazione - tra cui, in particolare, XX – con la conseguenza che, pertanto, gli stessi avrebbero dato corso a siffatti trattamenti di dati personali riferibili ai propri dipendenti, operando in qualità di datori di lavoro e titolari del trattamento.

In merito a tale circostanza, con dichiarazioni rese anche ai sensi dell’art. 168 del Codice nell’ambito dell’attività istruttoria, la Società ha tuttavia rappresentato che “XX […] non ha acquistato, allo stato, […] i [predetti] plugin per le chat aziendali” (v. verbale del 3 giugno 2025).

Il presente provvedimento riguarda, pertanto, unicamente i trattamenti che, in generale, nell’attuale configurazione del sistema Myndoor, potrebbero essere effettuati, in relazione ai dati delle persone che decidano di farne uso, dagli enti e dalle imprese che, avendo acquistato tale servizio, agirebbero in tale quadro in qualità di datori di lavoro delle persone predette e titolari del trattamento dei rispettivi dati personali.

2. L’attività istruttoria.

Nel corso delle menzionate verifiche ispettive, sono emersi elementi circa il funzionamento dell’applicativo e dettagli sulle soluzioni commerciali assunte dalla Società e, in particolare, per quanto rilevante ai fini del presente provvedimento:

- quanto al “servizio che viene reso alle aziende (attualmente, una soltanto) qualora venga richiesto anche l’invio di uno specifico report contenente dati aggregati relativi ai livelli di stress nel contesto lavorativo dei propri dipendenti […], il report viene in tal caso generato con cadenza settimanale solo qualora almeno 10 lavoratori abbiano contemporaneamente attivato il plugin. La Società si interfaccia in questi casi con un referente del cliente-datore di lavoro” (v. verbale del 4 giugno 2025); “questo report, esclusivamente in riferimento a Teams, riguarda l’intera platea dei dipendenti del cliente e non invece una realtà organizzativa più ristretta (es. dipartimento, articolazione) al fine di non rendere identificabile il lavoratore” (v. verbale del 3 giugno 2025);

- in ogni caso, la Società non ha “mai effettuato l’abbinamento del nominativo del lavoratore con i dati contenuti nel proprio database” (v. verbale del 4 giugno 2025).

Successivamente, con nota del 2 luglio 2025, la Società ha fornito specifici elementi informativi a scioglimento delle riserve formulate in occasione dei predetti accertamenti ispettivi, mettendo a disposizione dell’Autorità l’informativa resa agli interessati ai sensi dell’art. 13 del Regolamento (v. allegati nn. 1 e 2 della citata nota del 2 luglio 2025), in cui risultava previsto che:

- “il titolare del trattamento dei dati è: Myndoor S.r.l. […]”;

- i dati trattati per il tramite del sistema Myndoor consistono nei:

  - “dati di elaborazione”: “l'Applicazione utilizza un modello di intelligenza artificiale per analizzare i contenuti testuali dei messaggi inviati dall'Interessato all'interno di Slack. Questi dati vengono elaborati per valutare i Parametri di stress degli utenti. I dati di

analisi, trattandosi di informazioni integralmente e discrezionalmente fornite dall'utente, possono includere: - Dati comuni: quali, a titolo esemplificativo, nome e cognome, e-mail, numero di telefono, luogo e data di nascita, residenza. - Categorie di dati particolari, ai sensi dell'art. 9 del Regolamento UE n. 679/2016. Tali dati sono comunque analizzati in forma anonima o pseudonimizzata e non conservati dall'Applicazione. Una volta effettuata l'analisi ed elaborata la risposta, infatti, i dati vengono cancellati";

- "dati di utilizzo": "dati anonimi riguardanti l'utilizzo dell'Applicazione, come il numero di messaggi analizzati e le valutazioni di stress generate";

- "i dati di elaborazione vengono utilizzati per finalità di medicina preventiva, diagnosi e assistenza. In particolare, i dati saranno utilizzati al fine della valutazione dei Parametri Di stress finalizzati all'individuazione dei livelli generali di benessere o di stress dell'Interessato. Suddetti Parametri Di stress saranno individuati tramite l'analisi dei contenuti testuali immessi dall'interessato all'interno di Slack [o Teams], nell'ambito dell'attività di lavoro quotidiana";

- "nel caso in cui il Servizio venga attivato da un'azienda cui l'interessato è parte, ulteriore finalità del trattamento dei dati sarà la fornitura alla stessa azienda di un report con i risultati dell'analisi effettuata, avente ad oggetto il solo dato aggregato risultato di tale analisi […]".

A seguire, con nota del 24 dicembre 2025, la Società, facendo pervenire ulteriori elementi e precisazioni necessari per la definizione del quadro istruttorio, ha evidenziato, in particolare, che:

- "a seguito di opportune e definitive valutazioni, [… la] Società ha ritenuto di operare in qualità di Titolare del trattamento dei dati degli utenti del servizio"; ciò anche "indipendentemente dalla modalità di commercializzazione o dal rapporto con l'azienda cliente/contraente";

- "le imprese e gli enti che hanno acquistato il servizio per metterlo a disposizione dei propri dipendenti non dispongono della possibilità di accedere ai dati personali degli interessati, i quali sono trattati direttamente e unicamente da Myndoor S.r.l. in qualità di titolare del trattamento"; "unico scopo del servizio in oggetto è mettere a disposizione degli utenti/interessati uno strumento che consenta di favorire il benessere mentale degli stessi, rilevando condizioni di potenziale stress e restituendo appositi suggerimenti. Per tale ragione, non avendo il servizio ulteriori finalità, si esclude categoricamente l'accesso ai dati da parte delle imprese o enti acquirenti del servizio";

- "a seguito della recente ottimizzazione dell'infrastruttura tecnologica, l'attuale architettura del sistema non prevede più l'acquisizione di dati personali da parte di Myndoor per l'erogazione del Servizio. L'attivazione del plugin avviene infatti mediante l'utilizzo esclusivo di un identificativo univoco (ID) che, in linea con i principi di minimizzazione, non consente di risalire all'identità dell'interessato, garantendo così l'erogazione delle prestazioni in regime di anonimato per il fornitore";

- "il Report con i risultati dell'analisi effettuata, avente ad oggetto il solo dato aggregato risultato di tale analisi è stato reso disponibile ad una sola azienda […] e non vi è stata alcuna richiesta né spontanea comunicazione da parte di Myndoor S.r.l. di dati personali direttamente riconducibili a singoli individui alle aziende acquirenti";

- "non è avvenuta alcuna ulteriore comunicazione o trasmissione di report aggregati […] al di fuori del caso citato"; inoltre, "a seguito della diminuzione della base utenti attivi presso l'azienda sopra indicata […], il sistema ha automaticamente inibito la generazione di nuovi

report e l'accesso alle visualizzazioni storiche. Tale misura di sicurezza tecnica garantisce l'impossibilità di estrapolare dati, anche indirettamente, in contesti in cui il campione numerico ridotto potrebbe compromettere l'anonimato degli interessati";

- "il modello di trattamento adottato da Myndoor è strutturato per garantire che l'unico output accessibile al cliente (Titolare del trattamento) sia un report di natura esclusivamente statistico-aggregata, derivante dall'analisi di dati preventivamente pseudonimizzati. Al fine di mitigare il rischio di single-out (isolamento) e garantire la riservatezza degli interessati, sono state implementate le seguenti misure tecniche e organizzative:

  - Soglia Minima di Popolazione Statistica: La generazione del report è subordinata alla presenza di un campione minimo di almeno 10 utenti attivi su base settimanale. Tale misura garantisce un livello di aggregazione sufficiente a impedire la re-identificazione per inferenza; qualora la base utenti dovesse scendere sotto tale soglia, il sistema provvede all'immediata inabilitazione della generazione di nuovi report e alla sospensione dell'accesso alla pagina di consultazione.

  - Accesso in sola visualizzazione: Il report è reso disponibile esclusivamente tramite la Piattaforma Myndoor, all'interno dell'account aziendale protetto. Non sono previsti flussi di trasmissione automatica o download di dati grezzi, né l'inclusione di identificativi o codici che possano consentire l'associazione dei risultati a singoli individui.

  - Assenza di dati semi-aggregati: La procedura di analisi esclude la fornitura di micro-dati o dati semi-aggregati, limitando la visibilità del cliente al solo dato statistico finale prodotto dall'algoritmo".

3. Il trattamento di dati personali mediante il plug-in Myndoor.

All'esito dell'attività istruttoria è emerso, in particolare, che il plug-in Myndoor può essere acquistato da enti e imprese al fine di consentire alle persone che decidano di farne uso mentre prestano la propria attività lavorativa di verificare il proprio livello di stress psicologico alla luce dell'analisi della semantica dalle stesse impiegata nei messaggi scambiati nell'ambito delle chat Slack e Teams.

Nell'erogazione di tale servizio in favore delle predette persone, la Società, tenuto conto delle finalità perseguite e dei mezzi utilizzati in concreto, raccoglie e tratta i relativi dati personali nel contesto di una relazione dialettica che intercorre unicamente tra la Società medesima e i soli interessati che abbiano espressamente scelto di utilizzare il predetto servizio, operando dunque in relazione ai dati di questi ultimi in qualità di titolare del trattamento (artt. 4, n. 7, e 24 del Regolamento), come indicato anche nell'informativa resa agli interessati, in atti (art. 13 del Regolamento).

Il sistema plug-in Myndoor, trattandosi di un servizio acquistato dal datore di lavoro a beneficio del proprio personale che intenda fruirne, si configura, quindi, come un applicativo messo a disposizione dei dipendenti e altro personale a vario titolo operante nella realtà organizzativa, unici soggetti che, in concreto, possono scegliere se utilizzarlo, o meno, per proprie personali esigenze, restando tecnicamente inibito al datore di lavoro accedere ai dati necessari all'erogazione del servizio da parte della Società ai soli interessati (sia quelli attinenti al contenuto dei messaggi scambiati nelle chat sia quelli concernenti il prodotto delle elaborazioni effettuate dal sistema e relativi alla sfera emotiva delle persone che utilizzano il servizio).

Ciò secondo un'impostazione che, sotto tale profilo, risulta analoga a quanto, nella prassi, avviene con la stipulazione, da parte di enti e imprese datori di lavoro, di contratti di servizio per

l’erogazione di benefici e prestazioni in favore dei dipendenti (ad esempio, contratti di assicurazione sanitaria, accesso a servizi di assistenza psicologica in favore dei lavoratori, convenzioni con esercizi commerciali e altri fornitori di beni e servizi). In tale scenario, sotto il profilo della protezione dei dati, indipendentemente dalla configurazione civilistica dei contratti sottostanti (ad esempio, contratti a favore di terzo, art. 1411 c.c.), alcun trattamento di dati derivanti dall’erogazione dello stesso servizio viene infatti posto in essere dai datori di lavoro né, peraltro, potrebbe essere effettuato, difettando idonei presupposti di liceità a fondamento del trattamento in questione da parte del datore di lavoro (ad esempio, in merito alla tipologia di prestazioni sanitarie di cui il lavoratore richieda all’assicurazione il rimborso; la tipologia di beni e servizi acquistati presso enti convenzionati; l’accesso o meno al servizio di assistenza psicologica).

In tale quadro, occorre, tuttavia, far presente che, come specificato anche nell’informativa resa agli interessati (art. 13 del Regolamento), in atti, gli enti e le imprese che abbiano acquistato il servizio possono richiedere alla Società di mettere a loro disposizione un report recante un resoconto di natura aggregata in merito al livello di stress psicologico calcolato dal sistema Myndoor in relazione ai dipendenti che ne abbiano fatto uso, a condizione che questi ultimi siano più di dieci.

Alla luce delle dichiarazioni della Società, in atti, siffatto report è stato reso disponibile, in un unico caso, ad una sola società, la quale, peraltro, non risulta aver richiesto o, comunque, non disponeva di ulteriori riferimenti o dettagli che le consentissero, in concreto, di risalire all’identità delle persone che, nell’ambito della propria realtà aziendale, avevano fatto uso del sistema Myndoor e a cui si riferiva l’analisi aggregata contenuta nel report.

4. Il quadro normativo in materia di protezione dei dati personali e tutela della dignità dei lavoratori.

Nel sistema normativo in materia di protezione dei dati personali, sul titolare del trattamento incombe una “responsabilità generale” in merito al trattamento effettuato, essendo lo stesso chiamato a mettere in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente alla disciplina in materia di protezione dei dati personali, riesaminando e aggiornando dette misure qualora necessario, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche (cfr. art. 24 del Regolamento; v. anche considerando 74 del Regolamento).

In questa prospettiva, con particolare riguardo alla “fase di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali o che trattano dati personali per svolgere le loro funzioni”, è previsto che “i produttori dei prodotti, dei servizi e delle applicazioni dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi e applicazioni” (v. considerando 78 del Regolamento).

Si osserva, dunque, che, nel caso dei servizi e delle applicazioni che richiedono il trattamento di dati personali, come il sistema Myndoor, l’osservanza della disciplina di protezione dei dati deve essere assicurata, fin dalla fase della relativa progettazione, anche sotto il profilo della corretta impostazione delle scelte di fondo del trattamento, quale in particolare la definizione dei ruoli sul piano del trattamento dei dati personali, se del caso anche attuando specifiche misure idonee a prevenire in radice il rischio della messa a disposizione di dati in favore di terzi non legittimati (nel caso di specie, il datore di lavoro che ha acquistato il servizio in favore dei dipendenti).

Alla luce di quanto sopra, occorre ricordare che, in generale, con riferimento ai trattamenti effettuati nel contesto lavorativo, i datori di lavoro devono, tra l’altro, rispettare le norme nazionali, che “includono misure appropriate e specifiche a salvaguardia della dignità umana, degli interessi

legittimi e dei diritti fondamentali degli interessati in particolare per quanto riguarda la trasparenza del trattamento […] e i sistemi di monitoraggio sul posto di lavoro" (artt. 6, par. 2, e 88, par. 2, del Regolamento).

Sul punto, si fa in particolare presente che l'art. 113 del Codice ("Raccolta dati e pertinenza"), confermando l'impianto anteriore alle modifiche apportate dal d.lgs. 10 agosto 2018, n. 101, fa espresso rinvio alle disposizioni nazionali di settore che tutelano la dignità delle persone sul luogo di lavoro e che vietano al datore di lavoro di raccogliere dati non pertinenti rispetto all'attività lavorativa (artt. 8 della l. 20 maggio 1970, n. 300, e 10 del d.lgs. n. 297/2003, la cui violazione è peraltro penalmente sanzionata, cfr. art. 171 del Codice), la cui osservanza, per effetto di tale rinvio e tenuto conto dell'art. 88, par. 2, del Regolamento, costituisce una condizione di liceità del trattamento.

Nella cornice normativa sopra delineata, le informazioni riguardanti la sfera emotiva dei dipendenti, dunque il relativo stato di benessere o stress psicologico, costituiscono informazioni riconducibili all'ambito di applicazione dell'art. 113 del Codice, la cui conoscibilità è dunque preclusa al datore di lavoro.

Analogamente, il perseguimento della dichiarata finalità "di medicina preventiva, diagnosi e assistenza" (v. informativa resa agli interessati) deve ritenersi radicalmente precluso al datore di lavoro, non solo in ragione delle richiamate disposizioni che vietano l'acquisizione di informazioni non pertinenti rispetto all'attività lavorativa e del tradizionale divieto incombente sul datori di lavoro di assumere in via autonoma iniziative di accertamento sanitario sui dipendenti (v. art. 5 della l. 20 maggio 1970, n. 300), ma anche tenuto conto della stessa circostanza che la predetta finalità è caratterizzata da una dimensione di natura pubblicistica che, nel quadro della disciplina sulla tutela della salute e della sicurezza sul luogo di lavoro, costituisce nel contesto lavorativo espressione di una competenza propria del solo medico competente (v. d. lgs. n. 81/2008; v. anche, più in generale, art. 5 della l. 20 maggio 1970, n. 300).

Tanto, anche nel rispetto di quel tradizionale riparto di competenze e separazione di ruoli tra il medico competente e il datore di lavoro, in cui risiede il principale elemento di garanzia delle norme che, nel disciplinarne compiti e funzioni, prevedono limiti, condizioni e presupposti per il trattamento dei dati nell'ambito di tale specifico contesto (cfr., per analoghe considerazioni, Documento di indirizzo del 14 maggio 2021 recante "Il ruolo del "medico competente" in materia di sicurezza sul luogo di lavoro, anche con riferimento al contesto emergenziale", doc. web n. 958536).

Ciò anche tenuto conto, sotto altro ma connesso profilo, dell'esigenza di assicurare la conformità del prodotto commercializzato anche al separato quadro normativo in materia di intelligenza artificiale e, in particolare, al divieto previsto dall'art. 5, par. 1, lett. f), del Regolamento (UE) 2024/1689 del 13 giugno 2024, cd. "Regolamento sull'intelligenza artificiale" (che vieta espressamente "l'immissione sul mercato, la messa in servizio per tale finalità specifica o l'uso di sistemi di IA per inferire le emozioni di una persona fisica nell'ambito del luogo di lavoro […]"). In tale quadro, anche alla luce dei principi di protezione dei dati e delle disposizioni nazionali più specifiche e di maggior tutela della dignità delle persone nel proprio contesto lavorativo e professionale (artt. 88 del Regolamento e 113 del Codice), tale principio impone e conferma che l'impiego di siffatti sistemi non deve comportare la messa a disposizione dei datori di lavoro di informazioni, inferite tramite sistemi di intelligenza artificiale, riguardanti il proprio personale. Ne consegue che, anche in applicazione dei principi di protezione dei dati "fin dalla progettazione" e "per impostazione predefinita" (art. 25 del Regolamento), dovranno svolgersi valutazioni circa la disattivazione di funzioni che non hanno una base giuridica, non sono compatibili con le finalità del trattamento ovvero, come nel caso di specie, potrebbero porsi verosimilmente in contrasto con specifiche norme di settore previste dall'ordinamento nazionale e sovranazionale.

Più in generale, si ritiene opportuno evidenziare che l'utilizzo di sistemi di intelligenza artificiale richiede di considerare anche le implicazioni sostanziali derivanti dalla capacità di tali tecnologie di generare inferenze ulteriori, talvolta anche non immediatamente prevedibili o controllabili, rispetto ai dati originariamente trattati. Tale capacità inferenziale – propria dei modelli di machine learning e, in particolare, dei sistemi basati su analisi semantica e modelli linguistici – impone un approccio particolarmente cauto, soprattutto nei casi in cui i risultati derivino da processi di correlazione e classificazione caratterizzati da ridotta interpretabilità, che rendono il percorso logico-decisionale dell'algoritmo non immediatamente comprensibile o verificabile.

In questa prospettiva, l'affidabilità dei modelli, la qualità e la rappresentatività dei dati, nonché la trasparenza e la spiegabilità (explainability) delle logiche di funzionamento non costituiscono meri aspetti tecnici ma rappresentano condizioni essenziali per prevenire forme di trattamento invasive e non conformi alla disciplina di protezione dei dati. L'assenza di tali garanzie produce, infatti, il rischio di un affidamento sugli output algoritmici, generati attraverso pattern statistici e modelli predittivi, che, ove non adeguatamente verificato, è foriero di possibili effetti distorsivi, amplificazione dei bias e margini di errore non sempre agevolmente rilevabili, in particolare laddove il sistema presenti profili di opacità o limitata spiegabilità. Ciò, peraltro, in taluni contesti di trattamento contraddistinti da particolare delicatezza e dalla presenza di interessati vulnerabili, può comportare effetti pregiudizievoli nonché discriminazione, con conseguenze, talvolta irrimediabili, in relazione all'identità e alla dignità della persona.

Ne consegue che l'adozione di tali tecnologie richiede un approccio prudente e consapevole, fondato su una valutazione concreta delle implicazioni derivanti dal loro utilizzo, sulla robustezza dei modelli, sulla qualità dei dati di addestramento e sulla verificabilità degli output, assicurando in ogni caso garanzie informative adeguate e un controllo umano effettivo, in grado di intervenire e incidere sul processo decisionale, idoneo a mitigare i rischi connessi all'automatizzazione dei processi decisionali.

D'altra parte, anche lo stesso Regolamento (UE) 2024/1689 del 13 giugno 2024, sopra citato, espressamente prevede che i sistemi di intelligenza artificiale ad alto rischio siano contraddistinti da un adeguato livello di trasparenza, mediante specifiche informazioni e istruzioni per l'uso, anche con riguardo alle caratteristiche, alle capacità e ai limiti delle prestazioni dei sistemi in questione, ivi inclusi "la finalità prevista", "il livello di accuratezza che ci si può attendere, comprese le metriche, di robustezza e cibersicurezza", i "rischi per la salute e la sicurezza o per i diritti fondamentali" nonché "le capacità e caratteristiche tecniche del sistema di IA ad alto rischio connesse alla fornitura di informazioni pertinenti per spiegarne l'output" (art. 13 del Regolamento (UE) 2024/1689 del 13 giugno 2024).

5. Considerazioni conclusive.

Alla luce di quanto precede, in disparte da ogni valutazione sull'attendibilità scientifica delle elaborazioni prodotte dal sistema Myndoor e messe a disposizione dell'utenza, si prende favorevolmente atto dell'impostazione adottata dalla Società, per cui risulta esclusa qualsivoglia forma di trattamento dei dati trattati tramite il sistema Myndoor da parte degli enti e delle imprese che hanno acquistato il servizio e che si pongono come datori di lavoro delle persone destinate a scegliere se utilizzarlo.

Tanto considerato, preso atto che, nell'unico caso in cui la Società ha dichiarato di aver messo a disposizione di un proprio cliente il predetto report aggregato, è emerso che lo stesso non disponeva di ulteriori informazioni sufficienti a permettergli di re-identificare in concreto gli interessati, deve concludersi che, allo stato degli atti, non risulta comprovato che siffatti trattamenti siano stati effettivamente posti in essere dagli enti e dalle imprese che hanno acquistato il servizio in favore dei propri dipendenti, non avendo Myndoor in concreto comunicato loro dati personali delle persone che ne hanno fatto individualmente uso.

Anche tenuto conto, pertanto, che, in ogni caso, la normativa in materia di protezione dei dati personali trova applicazione nel caso in cui il trattamento di dati personali sia stato effettivamente posto in essere (cfr. art. 2 del Regolamento), non si ravvisano sotto tale profilo specifiche responsabilità in capo alla Società.

6. Adozione del provvedimento di avvertimento ai sensi dell'art. 58, par. 2, lett. a), del Regolamento e dell'art. 154, comma 1, lett. f), del Codice.

Posto che il Garante, ai sensi dell'art. 58, par. 2, lett. a), del Regolamento, ha il potere di rivolgere avvertimenti al titolare del trattamento o al responsabile del trattamento sul fatto che i trattamenti previsti possono verosimilmente violare le disposizioni di cui al Regolamento e, in tale quadro, ai sensi dell'art. 154, comma 1, lett. f), del Codice, è chiamato ad assicurare la tutela dei diritti e delle libertà fondamentali degli individui dando idonea attuazione al Regolamento e al Codice, si evidenzia quanto segue.

In base ad una valutazione complessiva degli atti istruttori, considerando la delicatezza dei dati trattati e del contesto di riferimento e stante, in particolare, l'impossibilità di escludere in via assoluta l'evenienza che, in futuro, gli enti e le imprese che facciano richiesta del predetto report aggregato possano risalire all'identità dei propri dipendenti che abbiano scelto di utilizzare individualmente il servizio, si rappresenta, per i profili di competenza, che emerge dagli atti il rischio che la trasmissione del predetto report, da parte di Myndoor agli enti e alle imprese che eventualmente lo richiedano, possa verosimilmente determinare una violazione del quadro normativo in materia di protezione dei dati personali e tutela della dignità della persona che lavora (cfr., in particolare, artt. 5, 6, 9, 24, 25 e 88 del Regolamento e 2-ter e 113 del Codice). Ciò, in particolare, tenuto conto delle specificità delle singole realtà organizzative datoriali (ad esempio, sotto il profilo dimensionale o della numerosità e delle caratteristiche del personale impiegato).

Ricorrendo, pertanto, i presupposti di cui all'art. 58, par. 2, lett. a), del Regolamento, si ritiene necessario che, nel contesto di riferimento, la Società assicuri l'adozione di misure e accorgimenti intesi a prevenire qualsiasi forma di messa a disposizione, anche mediante il predetto report, dei dati delle persone che decidano di fruire del plug-in Myndoor in favore degli enti e delle imprese che ne costituiscono i rispettivi datori di lavoro, al fine di evitare che gli stessi vengano in qualsiasi modo, anche in via indiretta, a conoscenza delle informazioni trattate mediante il sistema in questione.

TUTTO CIÒ PREMESSO IL GARANTE

- ai sensi dell'art. 58, par. 2, lett. a), del Regolamento e dell'art. 154, comma 1, lett. f), del Codice, avverte Myndoor S.r.l., con sede legale in via Aldo Moro 5/3 - 20088 Rosate (MI) – P. IVA 12097060961, che, nei termini di cui sopra, i trattamenti previsti possono verosimilmente violare il quadro normativo in materia di protezione dei dati personali e tutela della dignità della persona che lavora (cfr., in particolare, artt. 5, 6, 9, 24, 25 e 88 del Regolamento e 2-ter e 113 del Codice);

- ai sensi dell'art. 154-bis, comma 3, del Codice e dell'art. 37 del Regolamento del Garante n. 1/2019, dispone la pubblicazione del presente provvedimento sul sito internet dell'Autorità

Ai sensi degli artt. 78 del Regolamento, 152 del Codice e 10 del d.lgs. n. 150/2011, avverso il presente provvedimento è possibile proporre ricorso dinnanzi all'autorità giudiziaria ordinaria, a pena di inammissibilità, entro trenta giorni dalla data di comunicazione del provvedimento stesso ovvero entro sessanta giorni se il ricorrente risiede all'estero.

Roma, 14 maggio 2026

IL PRESIDENTE

Stanzione

IL RELATORE
Cerrina Feroni

IL SEGRETARIO GENERALE
Montuori