GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

DIPARTIMENTO SANITÀ E RICERCA

Ordine Provinciale dei Medici Chirurghi e Odontoiatri

Via Pec

DSR/CdS/CL/160291
(All. n.1)
Oggetto: trasmissione provvedimento

Si trasmette il provvedimento sanzionatorio adottato dal Garante in data 1° giugno 2023, reg. n. 226, ai sensi dell'art. 58, par. 2 lett. d) e i) del Regolamento (UE) 2016/679 nei confronti della società Thin s.r.l., con preghiera di darne la più ampia diffusione presso i propri iscritti.

In particolare, la Società ha avviato un progetto avente ad oggetto la raccolta presso i Medici di medicina generale di dati erroneamente considerati "*anonimizzati*" necessari alla realizzazione dell'"*Health Improvement Network -THIN*", ossia "*un progetto internazionale di raccolta e analisi di dati clinici anonimi 'real life' che ha l'obiettivo di garantire progressi nella cura del paziente e negli outcome clinici ed accrescere la comprensione del percorso di cura del paziente*" nell'ambito del quale l'Autorità, con l'allegato provvedimento, ha accertato specifiche violazioni della disciplina in materia di protezione dei dati personali, da parte del titolare del trattamento.

IL VICE SEGRETARIO GENERALE
E DIRIGENTE DEL DIPARTIMENTO
Claudio Filippi
(documento sottoscritto con firma digitale)

Piazza Venezia, 11 - 00187 Roma
Tel. +39 06 69677.1
protocollo@gpdp.it - protocollo@pec.gpdp.it
www.gpdp.it

Omettere le informazioni indicate nel TAG in caso di pubblicazione (art. 24 reg. Garante 1.8.2013)

IL SEGRETARIO GENERALE
f.to Mattei

Registro dei provvedimenti
n. 226 del 1° giugno 2023

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 cons. Fabio Mattei, 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* (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 del n. 98 del 4/4/2019, pubblicato in G.U. n. 106 dell'8/5/2019 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, in www.gpdp.it, doc. web n. 1098801;

RELATORE il dott. Agostino Ghiglia;

PREMESSO

1. Il progetto Thin

Un medico di medicina generale ha segnalato una presunta violazione della disciplina in materia di protezione dei dati personali da parte della Società Thin Srl, con sede legale in Piazza Vetra 17 - Milano (di seguito la "Società" o "Thin") trasmettendo al Garante copia del contratto predisposto dalla Società, avente ad oggetto la raccolta presso i Medici di medicina generale (MMG, individuati come parte del contratto) di dati "*anonimizzati*" necessari alla realizzazione dell'"*Health Improvement Network -THIN*", presentato nel contratto medesimo come "*un progetto internazionale di raccolta e analisi di dati clinici anonimi 'real life' che ha l'obiettivo di garantire progressi nella cura del paziente e negli outcome clinici ed accrescere la comprensione del percorso di cura del paziente*" (di seguito il "Progetto").

A tal fine, è prevista la partecipazione dei MMG, utilizzatori del *software* Medico 2000 -attualmente in uso in Italia da circa settemila medici di base- di cui è proprietaria e fornitrice la società Mediatec Informatica S.r.l., con la quale la Società ha avviato una collaborazione.

In particolare, per i MMG aderenti al Progetto è prevista la fornitura di un modulo aggiuntivo (cd *add-on*) alla versione *standard* del gestionale di Medico 2000, che consentirebbe di effettuare automaticamente il processo di anonimizzazione dei dati e la conseguente trasmissione degli stessi verso la Società.

In tale ambito è prevista, altresì, per i medici che aderiscono all'iniziativa, attraverso l'utilizzo del *software* Medico 2000, la fornitura di servizi aggiuntivi che consentirebbero a questi ultimi "*di avere costantemente a disposizione un complesso di informazioni, completo ed aggiornato, sulle condizioni di salute dei propri pazienti e sull'andamento delle prescrizioni ad essi dispensate, al fine di seguire, tra l'altro, l'evoluzione dei trattamenti farmacologici già disposti ed in corso*". Inoltre, i MMG avranno a disposizione un "*sistema esperto avanzato*" in supporto dello svolgimento della loro attività professionale e che consentirebbe altresì di accedere a *report* scientifici per diventare "medici ricercatori".

2. L'attività istruttoria e procedimentale

L'Ufficio, con specifico riferimento ai profili di protezione dei dati personali relativi al Progetto, ha avviato un'istruttoria preliminare nei confronti della Società, la quale in riscontro alle prime due richieste di informazioni, formulate ai sensi dell'art. 157 del Codice (cfr. note del 22 febbraio 2021, prot. n. 10583 e del 20 luglio 2021, prot. n. 38067), ha rappresentato in particolare quanto segue (cfr. note del 29 marzo 2021, del 6 agosto, del 3 e del 23 settembre 2021).

In relazione alla base giuridica dei trattamenti effettuati, la Società ha dichiarato che:

- "*Thin S.r.l. riceve solo dati anonimi*";
- "*Il processo di anonimizzazione che permetterà la generazione dei dati de-identificati che verranno utilizzati per creare il database "THIN" viene*

necessariamente svolto dal Medico il quale è il soggetto che ha raccolto e tratta tali dati nell'ambito della sua attività professionale (…) e del "*rapporto intercorrente tra Medico e Paziente in funzione delle attività svolte e descritte nell'informativa che il Medico stesso fornisce al Paziente*";

- di conseguenza THIN "*non interviene nella fase di definizione della base giuridica del processo di anonimizzazione stesso*";
- qualora il "*Paziente, dopo essere stato adeguatamente informato dal Medico sulle attività che il Medico stesso intende svolgere partecipando al progetto Thin, dichiari di non voler partecipare al progetto stesso, i suoi dati non verranno trattati dall'add-on presente nel software Medico 2000 e saranno quindi esclusi*".

La Società ha dichiarato che il Progetto è volto a consentire il perseguimento di molteplici finalità per il miglioramento delle cure del paziente e di ricerca scientifica, sia epidemiologica che di farmacovigilanza.

Con riferimento al processo di anonimizzazione la Società ha chiarito che:

- il Progetto THIN "*costituisce una fonte di dati anonimi medico scientifici ampiamente riconosciuta, rispettata e affidabile nel campo della ricerca e degli studi accademici" e "promuove la raccolta di dati anonimizzati forniti dai Medici Ricercatori che volontariamente decidono di aderire al progetto*";
- "*la componente software aggiuntiva (o add-on), cosiddetto "estrattore" dei dati, sviluppata dalla società Mediatec S.r.l. ad integrazione della suite Medico 2000, effettua una serie di elaborazioni sui dati personali finalizzate a renderli anonimi, evitando il rischio di de-identificazione*";
- le tecniche di anonimizzazione applicate nel progetto "(…) *sono quelle raccomandate nell' "Opinion 05/2014 on Anonymisation Techniques" emessa dal Gruppo di Lavoro ex 29*".

È stato altresì evidenziato che la Società ha messo in atto molteplici misure volte a garantire la minimizzazione dei dati attraverso tecniche di generalizzazione degli stessi: ad es. la residenza verrebbe indicata solo con riferimento alla Regione, mentre la data di nascita ed eventuale morte, solo con riferimento all'anno.

La Società si è inoltre impegnata a mettere in atto un processo di verifica costante sulle tecniche adottate, in modo tale da valutarle periodicamente unitamente al rischio di re-identificazione degli interessati "*mettendo eventualmente in campo altre tecniche quali ad esempio le permutazioni o l'aggiunta di rumore statistico che non sono state valutate come necessarie allo stato attuale*". Per tali attività, la Società ha dichiarato di avvalersi del supporto tecnico della società terza e indipendente Bl4ckSwan S.r.l.

La Società ha inoltre dichiarato di aver concluso il "*10 settembre 2021 l'attività di assessment sul livello di protezione dei dati personali nell'ambito del Progetto commissionato alla Società Bl4ckwan, condotta al fine di definire miglioramenti e azioni volte a prevenire ogni rischio nella gestione dei dati anonimizzati*" la quale avrebbe ritenuto che "*La situazione rilevata in merito alla protezione dei dati personali (…) è risultata complessivamente adeguata"* e raccomandato *"due possibili azioni di ulteriore miglioramento del livello di protezione dei dati personali*".

La Società, pertanto, ha realizzato ulteriori misure sulla componente *software* aggiuntiva (*add-on*) cd "estrattore dei dati", consistenti nella rimozione o riduzione nella raccolta di specifici attributi quali quelli relativi al "*Patient Marital e Patien Education*".

La Società ha poi dichiarato che "*i tempi pianificati per il* (…) *progetto prevedono il prossimo avvio delle attività di trattamento* (…) *che avverrà secondo l'attuale stato degli interventi che la nostra società ha posto in essere*".

In relazione ai ruoli dei soggetti coinvolti nel progetto, la Società ha precisato che Thin e Mediatec Informatica "*operano autonomamente, ognuna nel proprio ambito nei rapporti con il Medico che utilizza il software Medico 2000. Il Medico utilizzatore del software Medico 2000, si configura come Titolare del trattamento dei dati dei suoi pazienti tramite il software Medico 2000. Mediatec Informatica S.r.l. opera quale Responsabile del trattamento designato dal Medico, ai sensi dell'art. 28 del Reg. UE 2016/679 per le attività di supporto tecnico sulla base del contratto stipulato con il Medico per la fruizione del software stesso. Mediatec Informatica* (…) *provvede autonomamente ad informarlo* [il Medico] *di tale potenziale ulteriore funzionalità aggiuntiva del software connesso al Progetto THIN e segnala al Medico che, nel caso in cui fosse interessato a ricevere informazioni sul progetto, può segnalarlo e chiedere di essere contattato da Thin S.r.l. e ricevere informazioni dettagliate sul progetto stesso*".

La Società ha inoltre chiarito che "*al fine di gestire il contatto che Mediatec Informatica S.r.l. svolge con i medici per accertare il loro interesse a ricevere informazioni sul progetto THIN e gestire la successiva attivazione dell'Add- On, THIN Italia, ha provveduto a designare Mediatec Informatica S.r.l., in relazione a tale specifico trattamento, quale proprio responsabile del trattamento"* e che *"ha cura di fornire al medico stesso una propria informativa sul trattamento dei dati personali e qualora il medico aderisca al progetto gli precisa che, nel suo ruolo di Titolare del trattamento dei dati dei pazienti, è tenuto a informare gli interessati del fatto che i dati del paziente potranno essere dal medico stesso anonimizzati per trasferire tali dati anonimi a Thin S.r.l.*".

In relazione all'applicazione del principio di trasparenza la Società ha ribadito che:

- "*il trattamento dei dati che precede l'anonimizzazione*, (…), *è svolto in piena autonomia dal Medico che raccoglie questi dati nell'ambito del suo rapporto con l'interessato. L'obbligo del Medico di fornire un'adeguata informativa agli*

interessati in relazione al trattamento dei dati non è solo genericamente definito in relazione agli accordi che vengono sottoscritti con i Medici che decidono di partecipare al progetto "The Health Improvement Network — THIN" ma costituisce un obbligo diretto che grava sul Medico, per effetto della normativa vigente. Inoltre tale previsione forma l'oggetto di un formale impegno che il Medico assume nei confronti della nostra società aderendo all'iniziativa";

- "*Pur non ricoprendo noi il ruolo di Titolari del trattamento di questi dati personali, a garanzia della corretta informazione al paziente, abbiamo comunque predisposto un'informativa scaricabile dal software Medico 2000 che deve essere fornita dal medico al paziente. Evidenziamo inoltre che in qualsiasi momento il soggetto interessato può chiedere che i suoi dati vengano esclusi da quelli da rendere anonimi per partecipare al progetto "The Health Improvement Network — THIN" e che tale intervento sui dati del Paziente è gestito direttamente dal Medico tramite apposita semplice funzionalità del software*".

Alla luce degli elementi pervenuti, l'Ufficio ha formulato un'ulteriore richiesta di informazioni (cfr. nota del 2 dicembre 2021, prot. n. 60239), volta ad acquisire maggiori e più specifici elementi in ordine al progetto e in particolare sul funzionamento dell'*add-on*, sulla minimizzazione dei dati e sui presupposti giuridici del trattamento.

La Società in riscontro alla prima delle due ulteriori richieste di informazioni, ha rappresentato, con nota del 22 dicembre 2021, che:

- "*l'oggetto d*[el] *contratto* [con i MMG] è *la trasmissione da parte del Medico Ricercatore alla nostra Società di informazioni relative alla sua attività di visita dei pazienti, previa la totale anonimizzazione non reversibile di tali dati*";
- "*La partecipazione del Medico Ricercatore al progetto, fornendo tali dati anonimi, gli garantisce una delle seguenti opzioni di incentivazione, in funzione delle sue preferenze: Opzione 1 - Contributo annuo pari ad € 260 + IVA (importo che corrisponde al costo medio annuo di informatizzazione software di base di uno studio medico non associato); Opzione 2 - Contributo annuo pari ad € 60 + IVA ed utilizzo gratuito, finanziato da Thin S.r.L., del 'Sistema Esperto Avanzato' ('SEA') (…)"* che *"é un supporto informatico finalizzato ad agevolare la gestione della routinaria attività ambulatoriale medica (…). Si tratta quindi di un beneficio offerto ai Medici Ricercatori per gratificarli per la loro decisione di partecipare e sostenere il progetto ma chiariamo che tale strumento non riveste invece nessun ruolo nel processo di anonimizzazione, selezione ed invio dei dati relativi al progetto THIN*";
- "*I dati personali, fino a quando non sono resi anonimi, sono gestiti esclusivamente dal Medico, senza alcun intervento, nemmeno potenziale, di THIN. Tale trattamento viene svolto dal Medico nel contesto del suo rapporto di cura con il paziente (...). Il Medico Ricercatore è tenuto ad informare il paziente del fatto che ha aderito al Progetto THIN, illustrandone finalità e*

modalità di svolgimento, chiarendo che il progetto si basa esclusivamente sull'utilizzo di dati anonimi";

- "*lo stato attuale del progetto ha comportato che si procedesse ad una iniziale raccolta dei dati attraverso l'add-on di Medico 2000, sulla base delle confortanti conclusioni contenute nella relazione di assessment svolta dalla Società indipendente e specializzata Bl4ckswan S.r.l.*";
- al momento tale raccolta è tuttavia rimasta in una fase preliminare di valutazione "*evitandone qualsiasi utilizzo che non sia funzionale a tale valutazione e alle ulteriori validazioni dell'efficacia dei processi di anonimizzazione, a nostro avviso necessarie per consolidare la definizione di soglie di k-anonimity adeguate* (…). *il database*, (…) *non é stato creato nella sua struttura definitiva, né diffuso o comunicato a terze parti*"
- "*il nostro progetto si inserisce nel solco di iniziative oggi ampiamente diffuse sia in Italia che in Europa e svolte da diversi operatori del settore* [sin dagli anni 90]" e che "*contribuiscono a vario titolo a questa area importante di ricerca (…) si tratta di attività che sono assolutamente allineate alla nostra in relazione alla modalità di raccolta dati anonimi, al ruolo assunto dai professionisti sanitari e alle finalità perseguite con queste raccolte di dati dopo la loro anonimizzazione*";
- *Lo conferma il fatto che, (...) la valenza scientifica dello stesso progetto è tale che l'Agenzia europea per i medicinali (EMA), a seguito di una gara aperta (ref. EMA/2021/01/TDA 'Real World Data Subscription' Lot 1: Primary health care or claims database from a Southern European country), ha selezionato, relativamente al territorio italiano, proprio il database THIN per lo sviluppo nei prossimi sei anni delle analisi di efficacia e safety basate sulla popolazione che riceve cure primarie, avendone presumibilmente valutato, sia sul piano di compliance normativa che di adeguatezza scientifica, le modalità di creazione, il livello di anonimizzazione e la qualità dei dati*";
- *"su un universo stimato di 47.000 Medici di Medicina Generale convenzionati con il Servizio sanitario nazionale, 507 Medici Ricercatori hanno sottoscritto un accordo contrattuale con la Società Thin S.r.l. per partecipare all'osservatorio epidemiologico THIN*" chiarendo inoltre che "*non tutti hanno ad oggi già installato l'add on per l'anonimizzazione, selezione e trasmissione dei dati*".

In relazione al funzionamento del cd "*add-on*", la Società ha dichiarato che:

- i "*Medici Ricercatori, titolari del trattamento dei dati dei pazienti e del trattamento che porta alla loro anonimizzazione* (…), *inviano a Thin S.r.l. solo un sottoinsieme di dati già precedentemente anonimizzati*";
- il medico autorizza l'invio dei dati anonimizzati spuntando una specifica casella, dopo "*questa autorizzazione l'invio avviene in modo automatico. Il modulo aggiuntivo contiene una funzionalità che consente al*

Medico Ricercatore di escludere l'invio dei dati anonimi di quei pazienti che ne negano l'autorizzazione";

- "*i dati estratti e anonimizzati vengono criptati in un file compresso e trasferiti in modalità incrementale, tramite connessione protetta, al server del progetto Thin*" localizzato in Francia;
- "*Il processo di anonimizzazione si realizza direttamente sulla postazione del medico con modalità tali da garantire e assicurare la non identificabilità e re-identificabilità dell'interessato, implementando una serie di tecniche di de-identificazione strutturate, prendendo come riferimento l'"Opinion 05/2014 on Anonymisation Techniques*";
- "*Un elemento chiave per l'anonimizzazione è la sostituzione non reversibile dell'identificatore del paziente con un identificatore (GUID) ottenuto utilizzando l'hash calcolato tramite l'algoritmo sicuro SHA-256 di un valore estratto in modo randomico* (…)";
- "*nessuna informazione sull'identità dei pazienti (c.d. identificatori) verrà quindi trasmessa a THIN*".

La Società ha infine rappresentato di aver implementato ulteriori generalizzazioni dei dati per ridurre il rischio di re-identificazione dei pazienti, tra cui la "*sostituzione di valori esatti come il luogo di residenza con la regione di residenza; data di nascita riportata al primo giorno dell'anno; data di decesso con la stessa logica riportata al primo giorno dell'anno; il peso del paziente è stato limitato a 220kg; l'altezza del paziente è stata raggruppata in intervalli di 5cm e il valore massimo è stato limitato a 2mt*". Sono inoltre stati eliminati dal tracciato record alcuni attributi quali i "*marital status (single, coniugato, celibe, nubile ecc) e la motivazione del congedo da lavoro per malattia, con l'esclusione dello stato di maternità*".

In data 17 gennaio 2022, si è svolto un incontro richiesto dalla Società a seguito del quale la Società, in riscontro a una nuova richiesta di elementi dell'Ufficio, del 18 gennaio 2022, prot. n. 3568, ha ulteriormente dichiarato che (cfr. nota del 2 febbraio 2022):

- "*a livello europeo il progetto THIN è presente a partire dagli anni 90 nel Regno Unito, in Francia, Belgio, Romania e Spagna, con identica metodologia di anonimizzazione e trasmissione dei dati*";
- "*in Italia la soluzione LPD/Health Search di IQVIA Italia, con una metodologia di raccolta e anonimizzazione dati del tutto sovrapponibile, per logica e modalità, a quella implementata per il progetto THIN, è presente dai primi anni 2000 (ed è stata direttamente gestita dal Gruppo Cegedim nel periodo 2004-2015) ed è attualmente il riferimento scientifico per molte Istituzioni di Sanità Pubblica, in particolare in collaborazione con l'Agenzia italiana del Farmaco (AIFA) è utilizzata per la realizzazione del rapporto Osmed, è riconosciuta come una delle fonti di dati di riferimento per la*

popolazione italiana dall'ISTAT, il Ministero della Salute, attraverso l'Ufficio di Programmazione Sanitaria, utilizza Health Search per realizzare progetti di analisi dei dati e flussi amministrativi integrati con i dati clinico-assistenziali della Medicina Generale";

- "*in aggiunta a questo progetto,* (...) *molti altri progetti con metodologia di raccolta dati speculare a quella di THIN, e anche con garanzie significativamente inferiori, sono presenti da svariati anni in Italia sia sulla medicina di famiglia che sulla specialistica. Tutti questi progetti, ampiamente diffusi nel contesto nazionale ed internazionale e di interesse pubblico rilevante per il settore della ricerca medica e scientifica, si basano sulla gestione di dati anonimizzati, escludendo in radice l'utilizzo di dati personali*".

La Società ha ribadito la robustezza delle tecniche implementate e ha dichiarato di aver studiato "*un ulteriore affinamento al processo di anonimizzazione in grado di garantire in particolare il rispetto del principio di non singolarità del dato, modificando il paradigma operativo dell'anonimizzazione da distribuito a centralizzato. Tale affinamento prevede l'aggiunta di una base di dati di servizio centralizzata, raggiungibile dai MMG partecipanti al progetto e gestita da una terza parte in qualità di responsabile del trattamento dei MMG che si farà carico centralmente di misurare e di garantire l'efficacia del processo di anonimizzazione prima che i dati vengano trasmessi a Thin S.r.l., scartando o effettuando operazioni aggiuntive sui record che dovessero, per le loro caratteristiche statistiche, presentare rischi significativi di re-identificazione. La terza parte individuata è in possesso di formali qualifiche conferite dalle autorità francesi competenti per l'effettuazione di attività di questo tipo*".

Merita inoltre sottolinearsi come la Società abbia ribadito che il MMG effettua autonomamente "*il processo di anonimizzazione il quale, nella sua qualità di professionista sanitario soggetto al segreto professionale e al rispetto delle norme deontologiche che regolano il suo rapporto con il paziente e con i terzi, agisce, ai fini del GDPR, quale autonomo titolare del trattamento. I MMG, infatti, in fase di raccolta dei dati si assicurano che tutti i trattamenti di dati personali, ivi compresi quelli relativi alla salute, siano conformi ai principi in materia di trattamento di cui all'articolo 5 del RGPD e ad uno dei fondamenti di liceità e alle deroghe specifiche indicati rispettivamente all'articolo 6 e all'articolo 9 del RGPD affinché sia assicurata la liceità del trattamento di tale categoria particolare di dati personali. Questa fase è dunque presidiata dai singoli MMG in via del tutto autonoma*". Ciò premesso, la Società non sarebbe tenuta all'individuazione di idonea base giuridica (ex artt. 5, par. 1 lett. a) e 9, par. 2, del GDPR) a fondamento dell'attività di raccolta dati svolta presso gli stessi MMG.

Da ultimo, l'Ufficio ha rilevato la persistenza di criticità in ordine, in particolare, alle tecniche impiegate nonché al coinvolgimento della cd "terza parte" e ha pertanto richiesto (cfr. nota del 4 aprile 2022, prot. n. 18425) ulteriori specifici elementi di valutazione in ordine a:

1. gli interventi posti in essere per eliminare ogni singolarità dal *dataset* anonimizzato;
2. le tecniche di generalizzazione e randomizzazione impiegate;
3. gli accorgimenti adottati per impedire che eventuali codici univoci, conosciuti dai MMG, possano essere resi noti alla "*terza parte*" centralizzata che dovrà "*garantire l'efficacia del processo di anonimizzazione*".

La Società in riscontro alla predetta richiesta di informazioni e a integrazione di quanto già rappresentato, con riferimento al punto sub 1 ha fornito una tabella descrittiva delle informazioni sottoposte a tecniche di generalizzazione, a quelle codificate e a quelle che non possono essere utilizzate "*in alcun modo per la reidentificazione*" differenziando tra "*azioni effettuate sulla postazione del MMG*"; "*azioni effettuate dalla terza parte*" e "*azioni effettuate in fase finale di aggregazione*". In particolare, risulta che l'attributo "ID paziente" venga sostituito con un codice GUID randomico di cui viene calcolato un *hash* irreversibile (SHA256) di 64 caratteri e, quindi, sostituito con un codice progressivo.

È stato inoltre specificato che "*la generalizzazione viene usata come tecnica sui dati di: altezza del paziente* (…), *data di nascita* (…), *data di contatto del medico da parte del paziente* (…) e che la Società non ha previsto tecniche di randomizzazione "*in quanto intaccherebbero direttamente il valore dei dati rispetto alle finalità di ricerca scientifica né sarebbero impiegabili in modo efficace sul modello di dati in questione*".

"*L'installazione dell'add-on di anonimizzazione è sempre rimessa a una libera valutazione del MMG, titolare del trattamento, che, valutata l'affidabilità del fornitore, aderisce al progetto di ricerca, nella sua interezza, installando l'add-on. La terza parte, ai fini della fase di centralizzazione del processo di anonimizzazione e dell'eliminazione di ogni singolarità del dataset, agisce pertanto in qualità di sub-responsabile del trattamento per conto di Mediatec Informatica SrL, responsabile del trattamento. Nel quadro delle attività di trattamento svolte da Mediatec, la terza parte è stata selezionata tra coloro che possono offrire le maggiori garanzie di corretta implementazione del processo di anonimizzazione, anche in ottica di garanzia del rispetto dei principi di privacy by design e di accountability, e tenendo in considerazione le suggestioni ricevute dal confronto con Codesta Autorità*".

"*I MMG hanno la possibilità di valutare in piena autonomia l'idoneità delle garanzie offerte dal responsabile e dalla catena di subresponsabili nel momento in cui decidono di aderire al progetto di ricerca, in conformità al disposto dell'art. 28 parr. 2 e 4 GDPR che conferiscono al Titolare la facoltà di autorizzare o meno il subresponsabile individuato dal responsabile*".

Sulla base degli elementi acquisiti nell'ambito dell'istruttoria preliminare, l'Ufficio, -con atto del, 23 giugno 2022 (prot. n. 34136), notificato in pari data

mediante posta elettronica certificata, che qui deve intendersi integralmente riprodotto- ha avviato, ai sensi dell'art. 166, comma 5 del Codice, con riferimento alle specifiche situazioni di illiceità in esso richiamate, un procedimento per l'adozione dei provvedimenti di cui all'art. 58, par. 2 del Regolamento, nei confronti della Società invitandola a produrre al Garante scritti difensivi o documenti ovvero a chiedere di essere sentita dall'Autorità (art. 166, commi 6 e 7, del Codice, nonché art. 18, comma 1, l. n. 689 del 24 novembre 1981).

Con il predetto atto l'Ufficio ha rilevato che la Società ha effettuato, in qualità di autonomo titolare del trattamento, una raccolta di dati personali ivi inclusi quelli sulla salute in assenza di un valido presupposto giuridico e in violazione del principio di correttezza (art. 5, par. 1 lett. a) e 9, par. 2 del Regolamento). Nello specifico, la Società si è sostanzialmente inserita nel rapporto contrattuale tra MMG e la società Mediatec (responsabile del trattamento dei medici che acquistano il gestionale Medico 2000) per avere accesso alle informazioni da essi raccolte nello svolgimento dell'attività di cura della salute dei propri assistiti, sull'erroneo presupposto della natura anonima dei dati trattati attraverso il cd *add-on.*

La Società inoltre, fondandosi sull'erroneo presupposto di trattare informazioni anonimizzate, ha effettuato un trattamento di dati personali senza fornire preventivamente agli interessati un'idonea informativa, ai sensi dell'art. 13 del Regolamento.

Da ultimo l'Ufficio ha contestato la violazione di quanto previsto dall'art. 36 del Regolamento in ordine all'obbligo di effettuare una consultazione preventiva del Garante, avendo riscontrato che la Società si è limitata a chiedere la consulenza di una società privata.

3. Le memorie difensive

Con nota del 21 luglio 2022, la Società ha fatto pervenire, le proprie memorie difensive, chiedendo altresì di essere sentita, ai sensi dell'art. 166, comma 5 del Codice (nota del 5 luglio 2022). Nei richiamati atti con specifico riferimento alle contestazioni mosse dall'Ufficio nell'atto di avvio del procedimento sanzionatorio ai sensi dell'art. 166 comma 5 del Codice, la Società ha ribadito in particolare quanto segue.

3.1. Sulla violazione dei principi di liceità, correttezza e trasparenza

In relazione ai principi di liceità, correttezza e trasparenza la Società ha dichiarato che:

- tratta esclusivamente dati anonimizzati attraverso *l'add-on* realizzato da Mediatec e che "*i trattamenti che sono a monte di tale attività sono tutti basati su scelte autonome operate dal singolo medico di medicina generale che liberamente decide se partecipare o meno all'attività che Thin intende perseguire basandosi esclusivamente su dati anonimi*";

- la contestazione infatti, non terrebbe conto del fatto che il trattamento dei dati dei pazienti è svolto dal Medico che decide liberamente se aderire al Progetto Thin finalizzato alla creazione di *data base* contenente informazioni anonimizzate, nel rispetto del principio di minimizzazione per consentire "*(…) agli operatori del settore medico e sanitario di disporre di dati necessari per la ricerca scientifica e la cura dei pazienti*";
- il medico, nel ruolo di titolare dei dati dei pazienti gestisce il rapporto con questi ultimi e definisce le finalità e i mezzi del trattamento;
- Thin non avrebbe titolo ad intervenire nel trattamento dei dati relativi alla salute dei pazienti del medico in quanto non avrebbe titolo a trattarli in qualità di autonomo titolare del trattamento non svolgendo attività di cura;
- la titolarità del trattamento di anonimizzazione dei dati dei pazienti deriva dall'adesione, totalmente libera e volontaria, al Progetto da parte del Medico che ha già prescelto di utilizzare la Piattaforma Medico 2000 per la gestione dei dati dei propri pazienti;
- "*non ha alcun rapporto diretto con i pazienti e non intende raccogliere direttamente dati personali relativi a tali soggetti perseguendo come propria unica finalità la creazione* [della richiamata banca dati]". Il soggetto che propone il Progetto opera autonomamente a valle di tale processo di anonimizzazione ricevendo elaborazioni di tali dati solo dopo che sono stati resi anonimi dal Medico.

La Società ha inoltre dichiarato che:

- "*Questo schema ampiamente utilizzato nell'ambito della ricerca scientifica comporta l'utilizzo cosiddetto "secondario" delle informazioni sanitarie*";
- "*Come ha chiarito lo stesso Comitato Europeo per la protezione dei dati personali nelle proprie Linee guida 3/2020 sul trattamento dei dati sulla salute a fini di ricerca scientifica nel contesto dell'emergenza legata al Covid-19* (…) *in questo contesto siamo in presenza di quello che viene definito un "Trattamento ulteriore" che costituisce uno dei due possibili utilizzi di dati personali*";
- "*In particolare le suddette linee guida chiariscono che: Infine, rispetto al "trattamento di dati sanitari a fini di ricerca scientifica" occorre distinguere fra due tipologie di dati: 1. Ricerca su dati personali (relativi alla salute) consistente nell'impiego di dati raccolti direttamente per scopi di studio scientifico ("utilizzo primario"). 2. Ricerca su dati personali (relativi alla salute) consistente nel trattamento ulteriore di dati inizialmente raccolti per altre finalità ("utilizzo secondario")*";

- *"Thin svolge il proprio progetto unicamente utilizzando dati anonimi frutto di un processo di anonimizzazione effettuato dal medico titolare del trattamento nell'ambito dell'"uso secondario" dei dati sanitari svolto da quest'ultimo entro i limiti che le suddette Linee guida descrivono"*;
- "(…) *i trattamenti che formano oggetto della notifica di violazione avvengono nell'ambito di tale utilizzo secondario dei dati e il presupposto per lo svolgimento di tale attività ulteriore è appunto il fatto che sia il Medico di medicina generale, nel suo ruolo di titolare del trattamento dei dati a decidere se procedere o meno con tale utilizzo secondario e qualora assuma tale decisione gestisca il processo di anonimizzazione utilizzando i mezzi che liberamente ha scelto di utilizzare per gestire i dati dei pazienti*";
- "*Il Medico* (…) *che aderisce al Progetto ha, prima di aderire al progetto, scelto di utilizzare il software Medico 2000 (…) non può quindi dirsi che sia Thin a proporre al Medico di utilizzare questo software per procedere all'anonimizzazione dei dati. Semmai è vero il contrario* (...) *è il medico che aderendo al progetto Thin per l'utilizzo secondario dei dati dei suoi pazienti sceglie di avvalersi dell'add-on che Mediatec* (…) *ha predisposto per la gestione del processo di anonimizzazione dei dati prima del loro trasferimento a Thin per la realizzazione del data base*";
- "(…) *Entrambi i richiamati utilizzi primario e secondario dei dati sono totalmente in capo al medico di medicina generale che è l'unico soggetto legittimato a disporre dei dati generati dal suo rapporto con i pazienti*".
- *"Thin ritiene* (…) *che questo sia un ulteriore elemento di garanzia* (…) *e riterrebbe improprio tenuto conto della natura dei dati trattati dal medico, qualificarsi come titolare del trattamento di questi dati prima della loro anonimizzazione e troverebbe ingiustificata e contraria ai principi generali del trattamento dei dati la consegna di una propria informativa ai pazienti dei medici per qualificarsi come titolare del trattamento dell'uso secondario dei dati generati dal rapporto tra medico e paziente*";
- "*La scelta fatta da Thin è quella di rispettare tale rapporto e di tutelare la protezione dei dati dei pazienti, ricevendoli solo dopo che l'unico soggetto legittimato a trattarli, cioè il medico, ha provveduto ad anonimizzarli per sua scelta a cura e adottando mezzi che ha autonomamente individuato per trattare dati dei pazienti*".

3.2. Sull'anonimizzazione dei dati personali

La Società ha ribadito che:

- "*il Progetto è stato disegnato per incorporare tutti gli opportuni ed adeguati presidi che permettano ulteriormente di rafforzare i processi di anonimizzazione svolti dal medico di medicina generale utilizzando l'add-on messo a disposizione tramite il software Medico 2000*";

- "*Per essere certi in ultima analisi che ogni singolarità venga rimossa e verificata l'efficacia dell'anonimizzazione, Edgewhere, la terza parte indipendente ed accreditata agendo i qualità di sub responsabile dei medici di medicina generale si fa carico a livello centralizzato di misurare e garantire* (…) *l'efficacia del processo di anonimizzazione prima che i dati vengano trasmessi a Thin S.r.l. eliminando ogni possibile rischio residuo di singolarità dal dataset anonimizzato*";
- "*In particolare i record che dovessero presentare una frequenza inferiore a 10 vengono sistematicamente bloccati e quindi Thin non avrà accesso a tali record*".
- A tale riguardo la Società ha altresì prodotto in atti una dichiarazione della predetta Società Edgewhere che parimenti alle precedenti di Lucerna Iuris del 2019 e di BL4CKSWAN nel 2021 ritiene impossibile che si possa procedere alla re-identificazione irreversibile dei dati contenuti nel data base Thin.

La Società ha inoltre rappresentato che:

- l'impostazione di qualificare il medico come titolare del trattamento dei dati dei pazienti, appare confermata anche dal Codice di condotta per l'utilizzo dei dati sulla salute a fini didattici e di pubblicazione scientifica della Regione Veneto approvato dal Garante con provvedimento del 14 gennaio 2021 che attribuisce sempre al medico e alle strutture in cui il medico eventualmente operi il ruolo di titolare affidando a tali soggetti le responsabilità e gli obblighi in materia di protezione dei dati personali;
- il processo di anonimizzazione descritto nel suddetto codice è ampiamente assimilabile a quello che Thin presidia con l'introduzione di un ulteriore *layer* di sicurezza affidato ad una terza parte. Ciò anche in quanto i risultati delle proprie attività sono messe a disposizione dei professionisti del settore sanitario per finalità di ricerca scientifica.

3.3. Sulla violazione dell'obbligo di effettuare la consultazione preventiva dell'Autorità ai sensi dell'art. 36 del Regolamento

La Società ha, in via preliminare, rappresentato che l'obbligo di effettuare la consultazione preventiva grava su chi opera in qualità di titolare del trattamento solo laddove "*nella valutazione del titolare, il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolate del trattamento per attenuare il rischio*". Nel caso specifico le valutazioni condotte dalla Società "*hanno permesso di concludere che il processo di raccolta dei dati, basandosi sull'aninimizzazione dei medesimi dati escludeva l'esistenza di impatti che possano determinare un elevato rischio*". Nello specifico "*Le misure di sicurezza adottate sono conformi a quelle che*

nelle prassi operative da molto tempo vengono adottate dalle numerose organizzazioni che danno luogo a utilizzo secondario di dati personali e questo rendeva non necessaria la consultazione preventiva. Inoltre di tale consultazione preventiva non viene fatta menzione né nelle richiamate Linee del Comitato europeo per la protezione dei dati, né tantomeno nel richiamato Codice di condotta.

La Società infatti ha ritenuto non necessaria tale consultazione preventiva in mancanza, nella fattispecie in esame, dei presupposti soggettivi (non essendo Thin il titolare del trattamento dei dati personali) che oggettivi (non essendoci i presupposti per considerare esposti a rischio i diritti e le libertà degli interessati che sono ampiamente e compiutamente gestiti dal medico che è l'unico titolare del trattamento dei dati dei pazienti).

La Società alla luce di quanto sopra esposto, ha chiesto, che il Garante voglia ritenere non sussistenti i motivi che portino a ritenere che siano stati violati gli artt. 5, par. 1, 9, 13 e 36 del Regolamento stesso rendendosi al contempo disponibile a "*introdurre misure integrative ulteriori per consolidare adeguatamente il processo di anonimizzazione dei dati*" ottenendo *"l'indicazione di metriche, algoritmi o procedure oggettive finalizzate a valutare l'adeguatezza della soluzione di anonimizzazione implementata in modo da poter fornire evidenze rilevanti il linea con le aspettative dell'Autorità e ciò in continuità con lo spirito proattivo sempre dimostrato da parte della società* (…)".

4. L'audizione

In data 6 settembre 2022, si è svolta l'audizione nel corso della quale la Società -nel riservarsi di produrre ulteriore documentazione- ad integrazione di quanto già in atti, ha in particolare ribadito che:

- "*Nel febbraio 2021, ormai oltre un anno e mezzo fa, è iniziata l'interlocuzione con la vostra Autorità a cui abbiamo risposto sempre con la massima trasparenza e sollecitudine, illustrando tutti gli aspetti del nostro modello di business, fermando anche i trattamenti finché non siamo stati in grado di valutare oltre che qualitativamente anche quantitativamente la bontà del processo di anonimizzazione (…)*";
- *A gennaio di quest'anno finalmente abbiamo avuto la possibilità di incontrarvi e di confrontarci sul modello di anonimizzazione implementato. Abbiamo colto* (…) *l'importanza di integrare nel modello implementato uno step di verifica della non singolarità del dato che correttamente i vostri tecnici hanno suggerito avvenisse a livello centralizzato. Abbiamo chiesto a Mediatec, Responsabile del trattamento dei MMG, la società che produce il sw Medico 2000 utilizzato da circa 8000 MMG e che ha sviluppato il tool di anonimizzazione, di integrare questo passaggio, ed é stata identificata una terza parte referenziata con le autorità francesi, il Cnil in particolare,*

Edgewhere, per implementare questo ulteriore layer, agendo Edgewhere come subresponsabile di Mediatec.

– "*L'esperienza accumulata in oltre 30 anni a livello locale ed internazionale, e le valutazioni di tre società indipendenti specializzate ed accreditate in data protection, ci supportano nella nostra convinzione che non esista un rischio significativo di reidentificazione dei nostri dati (…);*

- la Società ha avanzato al Garante la richiesta di identificare delle metriche per valutare il livello di adeguatezza del processo di anonimizzazione implementato, dichiarandosi disponibile ad apportare ulteriori misure al processo di anonimizzazione, come dichiarano di avere già più volte fatto nel corso dell'" *interlocuzione che ormai dura da oltre un anno e mezzo, senza però che il Progetto venga stravolto e soprattutto i dati raccolti perdano valore*";

- la Società ha inoltre richiesto che non sia messo in discussione il valore del progetto e la correttezza del proprio operato anche al fine di non intaccare la credibilità della società nei confronti degli *stakeholders;*

– "*il trattamento di dati oggetto dell'odierno procedimento è stato valutato da Thin in sede di analisi progettuale del trattamento stesso, sulla scorta delle esperienze e delle prassi diffuse come standard internazionali*";

– "*Thin ritiene di aver tenuto conto dello stato dell'arte, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, valutando anche i rischi per i diritti e le libertà delle persone fisiche (art. 25 del Regolamento)*";

– "*l'attività svolta da Thin si basa su una prassi internazionale diffusa da tempo nel settore sanitario: tale prassi consiste nell'utilizzo di dati e di prove cliniche derivate dal mondo reale, ciò che nel gergo internazionale viene definito con le espressioni anglosassoni "real world data" (RWD) e "real world evidence" (RWE). Sono informazioni ed evidenze cliniche raccolte e condivise nell'ambito medico con lo scopo di favorire l'efficienza e l'efficacia dell'assistenza sanitaria nell'interesse generale*";

– "*I real world data servono per integrare i dati delle sperimentazioni cliniche randomizzate e sono essenziali per colmare il divario di conoscenze tra le sperimentazioni cliniche e la pratica clinica, fornire nuove informazioni sui modelli di malattia e contribuire a migliorare la sicurezza e l'efficacia degli interventi sanitari*";

– "*Si tratta di un settore di analisi estremamente rilevante e da molti anni ampiamente riconosciuto e praticato sia da parte di organismi istituzionali (ad esempio la European Medicine Agency – EMA) che da istituti di ricerca ed enti*";

- "*A tale fine va tenuto presente che le sperimentazioni cliniche non permettono di rilevare l'effettiva efficacia e il rischio di complicanze o effetti avversi dei farmaci di nuova approvazione nella popolazione reale. La modalità che il mondo della ricerca medica ha individuato per superare questo problema è di utilizzare i RWD che sono i dati osservazionali generati routinariamente durante l'erogazione dell'assistenza sanitaria. I RWD sono quindi, per definizione, dati relativi alla salute generati dal rapporto tra il medico e il paziente, rapporto che è essenziale nella logica dei RWD. Uno degli elementi qualificanti dei Real World Data è quindi il fatto che, per essere rappresentativi del mondo reale, diversamente dai dati generati dalle sperimentazioni cliniche, non possono essere oggetto di una rielaborazione dei dati raccolti da parte di uno sperimentatore o di un soggetto diverso dal medico che li raccoglie e li tratta*";
- "*nell'ambito del Progetto Thin, solo un medico può essere titolare del trattamento di "real world data". Doverosamente Thin, nel definire gli elementi organizzativi del Progetto, ha considerato questo elemento (che è ineludibile per gli studi che si basano sui Real world data) trovandosi nella necessità di prendere atto del fatto che solo i medici che gestiscono il rapporto diretto con il paziente possono essere titolari del trattamento dei RWD*".
- "*Thin si è posta, in relazione ai dati generati dal rapporto tra medico e paziente, rispettando le prassi condivise in tale ambito ed ha agito, nel rispetto del rapporto tra l'esercente la professione sanitaria e l'interessato cui si riferiscono i dati, ponendosi fuori da tale relazione ed intervenendo, come ritiene sia doveroso nel rispetto delle metodologie delle ricerche basata sui "real world data", solo nella fase successiva all'anonimizzazione dei dati stessi, per garantirne la corretta gestione al fine di permetterne l'utilizzo nell'ambito del Protetto Thin*";
- "*Thin ha adottato ogni cautela necessaria volta a verificare la robustezza del processo di anonimizzazione e per trovarsi quindi nelle condizioni necessarie per poter legittimamente ricevere i suddetti real world data solo dopo averne verificato l'effettiva e irreversibile natura anomima*";
- "*In questi termini l'attività svolta da Thin, in fase progettuale, ha mirato a presidiare, da un lato la corretta natura dei dati rilevanti per il Progetto in modo da garantire il fatto che siano effettivamente "real world data*" (…) *e dall'altro che i dati ricevuti da Thin siano stati effettivamente resi anonimi dal titolare che li ha raccolti e generati (il medico) prima che Thin stessa li riceva*";
- "*la condotta tenuta da Thin nel quadro del suo effettivo ruolo che non è quello di titolare del trattamento, posto che per le ricerche svolte utilizzando real world data, è il medico che, nell'ambito del suo rapporto con il paziente, decide la finalità e i mezzi del trattamento per permettere ad un soggetto terzo (in*

questo caso Thin) di ricevere dati anonimizzati per elaborarli e metterli a disposizione della comunità degli operatori del settore sanitario, per fini di rilevante interesse sociale";

- *"L'aggiunta di Edgewhere S.A.S. come terza parte porti con sé le garanzie di efficacia di anonimizzazione tipiche di un modello centralizzato evidenziate come desiderabili durante le precedenti interazioni con il personale tecnico di codesta Autorità";*
- *"La re-identificazione dei dati anonimizzati è stata resa ulteriormente improbabile dall'inserimento di Edgewhere S.A.S. nel processo anche attraverso l'ulteriore passaggio di separazione dei dati sopra descritto che garantisce di fatto una k-anonimity minima di 10";*
- *"THIN Srl ha più volte* [richiesto] *a codesta Autorità di ricevere specifiche in merito alla produzione di analisi e metriche per poter dimostrare la bontà del metodo di anonimizzazione implementato";*
- *"A febbraio di quest'anno sono stati prodotti e presentati spontaneamente alcuni risultati derivanti dall'analisi del database di pre-produzione ed ottenuti grazie all'utilizzo del software open source ARX riconosciuto come strumento completo sia per l'ampia gamma di metodi di analisi dei dati in uscita, sia per la completezza dei modelli di privacy, rischio e metodi di trasformazione dei dati";*
- *"I risultati ottenuti a febbraio dimostravano già allora l'efficacia del metodo di anonimizzazione in essere. I dataset analizzati riportavano totale assenza di record unici ed un livello di rischio di re-identificazione dei dati anonimizzati estremamente ridotto con valori sempre molto vicini allo 0%".*
- *In questi mesi THIN S.r.l.,* (…)*, ha accolto il suggerimento ricevuto dal gruppo tecnico che opera per codesta Autorità e ha quindi introdotto un secondo livello di anonimizzazione a livello centralizzato";*
- *per questo motivo come richiesto anche nelle nostre precedenti comunicazioni chiediamo a codesta Autorità di ricevere indicazioni per poter produrre le evidenze sui risultati del metodo di anonimizzazione attuato nel progetto THIN Srl.*
- *Ritenendo fondamentale che la nostra attività ed il nostro progetto sia valutato su elementi oggettivi (…), Thin produrrà all'Autorità autonomamente le evidenze in oggetto supportati dai migliori esperti in materia".*

Da ultimo, è stato ribadito che:

- *"La direzione intrapresa da Thin è coerente anche con i contenuti della proposta di Regolamento sull'EHDS, con il Codice di Condotta della Regione Veneto e con il Codice di Condotta per il trattamento dei dati personali nel*

campo della sperimentazione clinica e di altre ricerche cliniche e farmacovigilanza approvato dall'AEPD che ritiene coerente l'introduzione di un ulteriore layer di sicurezza affidato a un soggetto terzo.

- "(…) *il processo di anonimizzazione, a quanto ci consta, irreversibile, tale da rendere impossibile a Thin anche l'eventuale riscontro all'esercizio dei diritti da parte degli interessati*";
- "*Il modello del 2013 è stato già oggetto di verifica senza rilievi da parte dell'Autorità. È necessario, pertanto, tenere conto della natura anonimizzata dei dati oggetto del trattamento da parte di Thin e considerare, tra gli elementi soggettivi, che Thin ha collaborato fattivamente con gli uffici del Garante fin dagli inizi*".

5. La documentazione integrativa

Con nota del 20 settembre 2022 la Società ha dichiarato di aver "*avviato autonomamente, in collaborazione con esperti in materia, la produzione delle evidenze in oggetto, con l'obiettivo di consegnarvi una prima reportistica* (…)" e che è intenzione della predetta Società "(…) *monitorare nel corso del tempo tali evidenze e condividere periodicamente con codesta Autorità i risultati aggiornati*". In data 26 settembre 2022, la Società ha trasmesso in atti un documento denominato "*Risultati dei test di anonimizzazione effettuati su dataset THIN*" (elaborato con il supporto della società Bl4ckswan S.r.l.), recante i "*risultati delle analisi condotte su 3 dataset creati utilizzando come fonte il Database THIN con la finalità principale di valutare il rischio di re-identificazione risultante a valle dell'applicazione di tutte le tecniche e i passaggi di de-identificazione già ampiamente descritti a Codesta Autorità*" e rispetto al quale sono state applicate non solo le regole di anonimizzazione già in essere ma anche "*un valore di filtro K=10 (principio di k-anonimity) così come specificato nella nostra ultima comunicazione e confermato durante l'audizione del 6 settembre 2022*". In particolare, il documento riporta:

- "*le specifiche relative ai 3 dataset creati ad hoc per l'effettuazione dei test, estratti a partire dalle tabelle costitutive del dataset complessivo di THIN*" in quanto "*lo strumento lavora su singole tabelle e non su insiemi delle stesse, motivo per cui si è deciso di combinare le tabelle contenenti gli identificatori e i quasi-identificatori in modo da incrociarli come farebbe un attaccante che volesse operare una re-identificazione del dato*";
- le tecniche impiegate al fine di analizzare il rischio di re-identificazione dei *dataset* indicati nel documento che sono quelle messe a disposizione dal *software* ARX (*prosecutor attack model* – in cui l'attaccante prende di mira un individuo specifico assumendo che i suoi dati siano contenuti nel dataset; *journalist attack model* – in cui l'attaccante prende di mira un individuo specifico senza avere informazioni sulla presenza dei suoi dati all'interno del *dataset*; e *marketer attack model* – in cui l'attaccante non

prende di mira un individuo specifico ma a re-identificare un numero elevato di individui);

– i livelli massimi di rischio evidenziati per ogni modello di attacco.

La Società pertanto ha rappresentato che "*I risultati riportati in questo documento e relativi alle analisi condotte sui dataset confermano: la totale assenza di record unici; un livello di rischio estremamente ridotto a fronte delle principali tipologie di attacchi utilizzati per effettuare re-identificazione dei dati anonimizzati, con valori molto uniformi e comunque sempre molto vicini allo 0%*, e che *"il livello di rischio effettivamente misurato sui dataset THIN (v. Tabella 1) risulta essere ampiamente accettabile"* alla luce della letteratura specifica in materia, *"come ad esempio riporta il documento EMA/90915/2016, 15/10/2018 "External guidance on the implementation of the European Medicines Agency policy on the publication of clinical data for medicinal products for human use"* che "*suggerisce di prendere conservativamente come soglia di accettabilità di un rischio di re-identificazione un valore di 0.09,"*. Tanto premesso la Società ritiene efficaci le misure di anonimizzazione poste in essere ed adottate nella raccolta dei dati utili alla creazione del Database THIN.

6. Quadro giuridico di riferimento

Preso atto di quanto rappresentato dalla Società nella documentazione in atti e nelle memorie difensive, si osserva, in primo luogo, che il trattamento di dati personali deve avvenire nel rispetto della normativa applicabile in materia di protezione dei dati personali e, in particolare, del Regolamento e del Codice.

6.1. Anonimizzazione e pseudonimizzazione dei dati personali

Per "*dato personale*" si intende "*qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato")*". Inoltre, "*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*" (art. 4, paragrafo 1, n. 1 del Regolamento).

Per pseudonimizzazione si intende: "*il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile*" (art. 4 punto 5). La pseudonimizzazione costituisce una misura di estremo rilievo nel settore della ricerca scientifica in particolare al fine di garantire effettiva applicazione al principio di minimizzazione (art. 5, par. 1, lett. c) e 89 del Regolamento).

I dati pseudonimizzati sono quindi dati personali che devono essere trattati nel rispetto del Regolamento. A tale riguardo, il Gruppo di lavoro Articolo 29 ha

evidenziato che "*la pseudonimizzazione non è un metodo di anonimizzazione. Si limita a ridurre la correlabilità di un insieme di dati all'identità originaria di una persona interessata, e rappresenta pertanto una misura di sicurezza utile*" (Parere 05/2014 sulle tecniche di anonimizzazione adottato il 10 aprile 2014).

Il dato anonimizzato, al quale non si applica la disciplina in materia di protezione dei dati personali, è tale solo se non consente l'identificazione diretta o indiretta di una persona tenuto conto di tutti i mezzi ragionevoli (economici, informazioni, risorse tecnologiche, competenze, tempo) nella disponibilità di chi (titolare o altro soggetto) provi a utilizzare tali mezzi per identificare un interessato. Il descritto processo, qualificato come anonimizzazione, deve pertanto impedire che si possa:

1. isolare una persona in un gruppo (*single-out*);

2. collegare un dato anonimizzato a dati riferibili a una persona presente in un distinto insieme di dati (*linkability*);

3. dedurre nuove informazioni riferibili a una persona da un dato anonimizzato (*inference*).

Sempre in riferimento all'anonimizzazione dei dati, sotto altro profilo, si sottolinea che il Comitato europeo per la protezione dei dati e il Garante hanno evidenziato, altresì, come essa già di per sé rappresenti un trattamento di dati personali e che, in quanto tale, deve essere svolta in conformità con la normativa vigente in materia di protezione dei dati personali (cfr. *Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research*, adottato il 2 febbraio 2021).

6.2. Principio di responsabilizzazione e di *privacy by design*

Il titolare del trattamento deve conformarsi ed essere in grado di comprovare sia il rispetto dei principi e degli adempienti previsti dal Regolamento, sia di avere effettivamente tutelato il diritto alla protezione dei dati personali degli interessati fin dalla progettazione (artt. 5, par. 2, 24 e 25 par. 1 del Regolamento).

In base al rinnovato quadro normativo in materia di protezione dei dati personali, si richiede, infatti, una valutazione ponderata di tutte le scelte connesse ai trattamenti di dati personali, dimostrabile sul piano logico attraverso specifiche motivazioni, volte all'individuazione di misure necessarie e proporzionate rispetto alla concreta efficacia del principio di volta in volta tutelato. In ossequio all'obbligo della protezione dei dati sin dalla progettazione, i titolari devono, inoltre, assumere una condotta attiva nell'applicazione dei principi, ponendosi l'obiettivo di ottenere un reale effetto di tutela. Non si richiede, quindi, la mera applicazione di misure generiche, non direttamente correlate allo scopo di tutela, ma di misure qualitativamente e quantitativamente efficaci rispetto all'obiettivo e progettate per essere, all'occorrenza, revisionate in relazione ad eventuali aumenti o riduzioni dei rischi per gli interessati.

Tali misure dovranno, ove possibile, includere specifici indicatori volti a dimostrarne in modo inequivoco l'efficacia. In tale ottica, il richiamato obbligo di documentazione delle scelte inerenti al trattamento dei dati personali si intende compiutamente adempiuto solo laddove il titolare sia in grado di dimostrare, attraverso indicatori di prestazione (qualitativi e ove possibile, quantitativi), l'efficacia delle misure (cfr. *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default Adopted on 13 November 2019 by the EDPB;* provv. del Garante del 23 gennaio 2020 doc. *web* 9261093).

6.3. I principi applicabili al trattamento: liceità, correttezza e trasparenza

In base al Regolamento, i dati personali devono essere trattati "*in modo lecito, corretto e trasparente nei confronti dell'interessato*" (principio di «liceità, correttezza e trasparenza»)" (art. 5, par. 1, lett. a) del Regolamento).

Con specifico riferimento alle particolari categorie di dati, tra cui rientrano i dati sulla salute, l'art. 9 del Regolamento sancisce un generale divieto al trattamento di tali dati a meno che non ricorra una delle specifiche esenzioni a tale divieto (art. 9, par. 2).

A tale riguardo, si segnalano le ipotesi in cui:

- l'interessato abbia prestato il proprio consenso esplicito, salvo nei casi in cui il diritto dell'Unione o degli Stati membri disponga diversamente (art. 9, par. 2, lett. a) del Regolamento);

- il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità (art. 9, par. 2, lett. h) e par. 3 del Regolamento e 75 del Codice; provv. del Garante recante Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario del 7 marzo 2019 doc. web 9091942).

I dati personali devono inoltre essere trattati nel rispetto del principio di trasparenza (art. 5, par. 1 lett. a) del Regolamento), fornendo preventivamente agli interessati -in caso di dati raccolti direttamente presso di essi- le informazioni di cui all'art. 13 del Regolamento. Tale principio impone che le informazioni e le comunicazioni relative al trattamento dei dati personali siano rese in una forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro (cons. 39, 58 e art. 12 del Regolamento).

6.4. L'individuazione dei ruoli in materia di protezione dei dati personali

Nell'ambito delle operazioni di trattamento dei dati personali occorre poi individuare correttamente i ruoli di titolare (artt. 4, n. 7 e 24) e, se del caso, di

responsabile (art. 4, n. 8 e 28), rispetto ai quali il Regolamento si pone in linea di continuità con il quadro normativo previgente.

Infatti, il Regolamento, da un lato, definisce quale «titolare del trattamento» "*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali*" (art. 4, n. 7) e, dall'altro, quale «responsabile del trattamento» "*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento*" (art. 4, n. 8).

Alla luce delle definizioni sopra riportate, pertanto, il titolare è il soggetto sul quale ricadono le decisioni di fondo relativamente alle finalità e ai mezzi del trattamento dei dati personali degli interessati nonché la responsabilità generale (cd. "*accountability*") sui trattamenti posti in essere dallo stesso o da altri "*per* [suo] *conto*", in qualità di responsabili ai sensi dell'art. 28 del Regolamento.

Il ruolo del responsabile del trattamento è, invece, caratterizzato dallo svolgimento di attività delegate dal titolare il quale, all'esito di proprie scelte organizzative, può individuare uno o più soggetti particolarmente qualificati allo svolgimento delle stesse - in termini di conoscenze specialistiche, di affidabilità, risorse e sicurezza del trattamento (cfr. cons. 81 del Regolamento) -, delimitando l'ambito delle rispettive attribuzioni e fornendo specifiche istruzioni sui trattamenti da effettuare (cfr. Linee guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR Versione 2.0, Adottate il 7 luglio 2021).

Ai fini della individuazione in concreto del ruolo svolto, in termini di titolare o responsabile, delle figure che effettuano trattamenti di dati personali è, quindi, essenziale esaminare sul piano sostanziale e non formale le attività in concreto svolte da tali soggetti. In tal senso, si è più volte espressa questa Autorità sotto la previgente e vigente normativa di riferimento (cfr. a titolo esemplificativo, provvedimenti del 16 febbraio 2006, punto 6 [doc. *web* n. 1242592], 4 ottobre 2011, punto 5 [doc. *web* 1850581], del 19 luglio 2018 [doc. *web* 9039945], 14 gennaio 2021 [doc. *web* n. 9542136, doc. *web* n. 9542113], 7 luglio 2022 [doc. *web* 9809998]; del 20 ottobre 2022, n. 342 in corso di pubblicazione; 10 novembre 2022, n. 368, in corso di pubblicazione, Linee guida per il trattamento di dati dei dipendenti privati del 23 novembre 2006 [doc *web* n. 1364099],).

6.5 L'"uso secondario" dei dati sulla salute per scopi di ricerca scientifica

L'eventuale ulteriore trattamento e conservazione dei dati personali per scopi di ricerca scientifica sono ammessi nei limiti del quadro normativo di riferimento (cons. 50, artt. 5, par. 1, lett. b) ed e), 6, par. 4 del Regolamento, punto 5.6 delle Prescrizioni per il trattamento dei dati personali per scopi di ricerca scientifica; si vedano anche *A Preliminary Opinion on data protection and scientific research,* adottata il 6 gennaio 2020 dall'*European data protection Supervisor,* (EDPS) e il Parere 3/2019 relativo alle domande e risposte sull'interazione tra il

regolamento sulla sperimentazione clinica e il regolamento generale sulla protezione dei dati (articolo 70, paragrafo 1, lettera b), del 23 gennaio 2019 e il *Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research*, del 2 febbraio 2021, adottati dall'*European data protection Board* (EDPB).

7. L'esito dell'attività istruttoria: le violazioni accertate

In tale quadro, risulta accertato che la Società Thin ha effettuato, in qualità di autonomo titolare del trattamento, una raccolta di dati personali in assenza di un valido presupposto giuridico e in violazione del principio di liceità, correttezza e trasparenza (art. 5, par. 1 lett. a) e 9, par. 2 del Regolamento) ciò in quanto essa ha trattato dati personali, riferiti ai pazienti dei MMG attraverso l'*add-on* del *software* Medico 2000 da questi ultimi hanno utilizzato per la gestione sanitaria dei propri pazienti.

7.1. Considerazioni di carattere preliminare

7.1.a I cd "*real world data*" in ambito sanitario e di ricerca scientifica

I cd *real world data* (RWD), in ambito sanitario sono considerati *big data*, che si riferiscono specificamente a qualsiasi tipo di dati non raccolti attraverso uno studio clinico. Questi dati possono integrare i dati delle sperimentazioni cliniche per colmare il divario di conoscenze scientifiche tra le sperimentazioni cliniche e la pratica clinica, fornire nuove informazioni sui modelli di malattia e contribuire a migliorare la sicurezza e l'efficacia degli interventi sanitari.

Le fonti di RWD sono sempre più utilizzate per integrare le fonti tradizionali di dati sanitari al fine di fornire informazioni più ampie su popolazioni eterogenee di pazienti in contesti reali. La crescente maturità delle fonti e dei metodi di utilizzo dei RWD, unita ai progressi tecnologici, contribuisce ad aumentare l'interesse ma anche l'accessibilità di tali dati per svariati scopi, ivi inclusi quelli di ricerca; ciò soprattutto a seguito della pandemia da Covid-19 (cfr. Commisione europea "*Study on the use of real-world data (RWD) for research, clinical care, regulatory decision-making*" del 2021; Istituto Superiore di Sanità "*decentralized clinical trial*: nuovo approccio alla sperimentazione clinica per facilitare il paziente e velocizzare la ricerca" Rapporti SISTAN 22/4 IT: *EMA Regulatory Science to 2025 Strategic reflection*).

La Commissione europea ha licenziato nel 2021, lo studio sopra richiamato sull'uso dei RWD evidenziando, tra le altre criticità, l'esigenza che sia garantita un'interpretazione e un'applicazione coerente del Regolamento per l'uso di tali dati.

La rilevanza e l'interesse dei ricercatori in ordine a tale tipologia di dati sono note e all'attenzione delle istituzioni nazionali e comunitarie anche deputate alla protezione dei dati personali (cfr. Proposta di Regolamento del parlamento

europeo e del consiglio sullo spazio europeo dei dati sanitari, del 3.5.2022 sulla quale il EDPB-EDPS hanno adottato la *Joint Opinion* 03/2022).

Il Garante se ne è di recente occupato nel Parere sui lavori statistici IST 02834 Studio dei Mobile Network Data a fini statistici e IST 02829 *La violenza raccontata dai social* del 9 giugno 2022 (doc. *web* 9802796).

Si ribadisce, pertanto, come la disciplina in materia di protezione dei dati personali non sia volta ad ostacolare iniziative che mirano ad integrare nel mondo della ricerca fonti di dati e strumenti nuovi, ma è deputata ad assicurare che tali iniziative siano realizzate garantendo una adeguata tutela ai diritti e alle libertà fondamentali degli interessati, anche in relazione ai profili di trasparenza nei confronti degli interessati stessi, in linea con quanto stabilito dalla Carta dei diritti fondamentali dell'Unione Europea e dal Regolamento, auspicando altresì l'introduzione di una disciplina omogenea a livello europeo.

7.1.b La struttura sinallagmatica creata

In relazione alla trattazione in esame, in via preliminare occorre ricostruire la struttura sinallagmatica creata.

Essa prevede che la società Thin, per il tramite della società Mediatec, proponga ai MMG di aderire al progetto Thin, ossia di accettare che sul proprio gestionale, Medico 2000, venga aggiunta una funzionalità (*add-on*) che anonimizza i dati dei pazienti e li trasmettere a Thin per la realizzazione del proprio progetto volto al miglioramento delle cure del paziente e di ricerca scientifica, sia epidemiologica che di farmacovigilanza. In cambio il medico oltre a ricevere non meglio definiti vantaggi nella gestione dei propri pazienti e il titolo di "*medico ricercatore*", ottiene altresì un beneficio economico.

In estrema sintesi, Thin offre ai MMG un corrispettivo economico a fronte dall'impegno di questi ultimi di installare l'*add-on*, fornire i dati dei propri pazienti e di occuparsi, se del caso, di escludere dal processo di (ipotetica) anonimizzazione i dati dei pazienti che hanno manifestato il proprio dissenso (*opt-out*).

Tutto ciò assicurando ai MMG, sempre per il tramite della società Mediatec, che attraverso l'*add-on* sia realizzata l'anonimizzazione dei dati. Inoltre, i MMG dovrebbero altresì essere chiamati a nominare la società individuata da Thin come parte terza -deputata a rafforzare il predetto ipotetico processo di anonimizzazione dei dati- quale responsabile del trattamento.

Si rileva sin da subito, che ciò dimostra inequivocabilmente che i dati dei pazienti trasferiti dai MMG alla terza parte indicata da Thin sono di natura personale, altrimenti tale nomina non avrebbe alcun senso dal punto di vista della disciplina in materia di protezione dei dati personali.

Sul falso presupposto di acquisire dati anonimi, Thin fa quindi dei dati personali dei pazienti la merce di scambio a fronte della quale offrire ai MMG sia taluni non ben precisati servizi, sia un contributo economico.

Tale circostanza determina rilevanti criticità, non solo sotto il profilo civilistico, in relazione al rispetto degli obblighi di correttezza e buona fede nelle relazioni contrattuali (art. 1175 e 1375 cc), ma anche sotto il profilo della protezione dei dati personali, in particolare in relazione ai principi di liceità, correttezza, trasparenza e tutela dell'autodeterminazione informativa del paziente, in quanto determina una sostanziale intromissione della società Thin nei rapporti giuridici tra il medico e il paziente e tra il medico e la società fornitrice del richiamato gestionale, utilizzato da questi ultimi per erogare le prestazioni di cura ai propri pazienti.

La disciplina in materia di protezione dei dati personali non è volta ad ostacolarne il trattamento, né la libertà di iniziativa economica privata o l'attività di ricerca, che fondano parte del loro buon esito proprio sull'uso di dati anche di carattere personale, ma ad assicurare che tali attività vengano svolte nel rispetto dei diritti e delle libertà fondamentali degli interessati e soprattutto nel rispetto dell'autodeterminazione informativa degli interessati ai quali deve essere assicurato, in piena trasparenza, il controllo e la gestione del proprio patrimonio informativo (cfr. cons 41 del Regolamento).

Ciò posto, tale ricostruzione sinallagmatica risulta particolarmente critica in relazione alla disciplina sulla protezione dei dati personali, per svariate ragioni. Il prodotto offerto ai MMG è presentato in maniera diversa da quello che effettivamente è, cioè strumento per l'anonimizzazione, laddove l'*add-on* non è in grado (per le ragioni tecniche di seguito illustrate) di conseguire tale obiettivo. Cionondimeno, la rilevanza della società Thin e le specifiche competenze tecniche che le misure di anonimizzazione di ingenti quantità di dati sulla salute richiedono, hanno giustificato il legittimo affidamento dei MMG sulle funzionalità dell'*add-on,* ritenuto effettivamente in grado di anonimizzare i dati.

D'altro canto, la buona fede contrattuale e, in particolare, l'uso di tecnologie avanzante impongono un elevato grado di *accountability* non solo da parte dell'utente (MMG) ma anche da parte del fornitore delle stesse (THIN) (si veda, a titolo meramente esemplificativo, il capo 3 della *Proposta di Regolamento del parlamento europeo e del consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'unione* del 21 aprile 2021).

Sotto altro profilo, si rileva come estremamente critica la riscontrata patrimonializzazione di dati personali (per altro inerenti allo stato di salute) che il richiamato sinallagma produce a vantaggio di soggetti terzi e nella sostanziale ignoranza degli interessati (pazienti dei MMG).

7.2. Il titolare del trattamento

Nello scenario sopra illustrato, fermo restando che i MMG sono gli unici titolari del trattamento dei dati personali, relativi alla salute dei propri pazienti necessari per finalità di cura (art. 9, par. 2, lett. h), par. 3 del Regolamento e provv. del Garante recante *Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario* del 7 marzo 2019 doc. *web* 9091942), medesime considerazioni non possono essere formulate, nel caso di specie, in relazione all'ulteriore trattamento (erroneamente ritenuto) di "anonimizzazione" dei dati.

In relazione al caso di specie, le modalità di realizzazione dell'anonimizzazione (risultata in concreto inefficace) sono decise in ogni loro fase dalla società THIN (che le ha commissionate alla società Mediatec, che a sua volta ha sviluppato per il perseguimento di finalità della predetta Società il richiamato *add-on*, parte integrante della suite del gestionale "Medico 2000"), cosi come lo scopo di tale operazione. Tale trattamento viene posto in essere da THIN per il perseguimento di una propria specifica finalità che la stessa Società definisce allo scopo di "*generare una base di conoscenza per la ricerca medica fondata su elementi oggettivi che consenta di realizzare progressi nei percorsi di cura dei pazienti attraverso un 'analisi di dati anonimi relativi alla cura dei pazienti dei medici*". È quest'ultima Società infatti che esercita effettivamente un'influenza determinante sulle finalità e sui mezzi del trattamento stesso e che quindi deve riconoscersi per le operazioni di trattamento in esame quale autonomo titolare.

A tale riguardo, si evidenzia che il Comitato europeo per la protezione dei dati, nelle richiamate linee *Linee guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR*, del 7 luglio 2021, raccomanda di interpretare il concetto di «titolare del trattamento» in modo sufficientemente estensivo alla luce di un'analisi fattuale delle vicende esaminate e non formale (*cfr*. part. 1 n. 14, part. 2 punto 21).

La duttilità della disciplina in materia di protezione dei dati personal rende, inoltre, impossibile la definizione aprioristica del ruolo di titolare del trattamento "*semplicemente redigendo il contratto in un determinato modo, laddove ciò non corrisponda alle circostanze di fatto*" (*cfr*. part. 2 punto 28, delle richiamate linee guida). Il Comitato evidenzia infatti come, a prescindere da quanto indicato nell'ambito di uno specifico contratto, "*se una parte decide di fatto le finalità e le modalità del trattamento di dati personali, essa sarà il titolare del trattamento*" (part. 2 punto 29, delle richiamate linee guida).

Pertanto, rispetto a tale operazione di (presunta) anonimizzazione, nel caso di specie, non può certamente essere ritenuto il Medico titolare del trattamento. Quest'ultimo è infatti deputato a svolgere esclusivamente trattamenti finalizzati alla cura del paziente. L'operazione di "anonimizzazione" verrebbe infatti in concreto realizzata solo ed esclusivamente a beneficio di Thin che, con il richiamato progetto, intende raccogliere dai MMG i dati personali dei pazienti in

cura presso di essi, ritenuti erroneamente anonimizzati, esclusivamente per il perseguimento delle proprie finalità volte a "*generare una base di conoscenza per la ricerca medica fondata su elementi oggettivi che consenta di realizzare progressi nei percorsi di cura dei pazienti attraverso un 'analisi di dati anonimi relativi alla cura dei pazienti dei medici*".

Ciò risulta comprovato dalla determinante ingerenza che Thin ha avuto proprio sulla definizione delle tecniche di anonimizzazione/pseudonimizzazione implementate e migliorate nel corso del procedimento istruttorio avviato dall'Ufficio del Garante.

A titolo non esaustivo, si segnala al riguardo che è la Società che ha sin da subito descritto le misure implementate per provare (seppur senza un risultato del tutto soddisfacente) ad anonimizzare i dati; è stata la Società a descrivere quelli che sono ritenuti gli elementi chiavi dell'anonimizzazione; è stata la Società ad aver implementato ulteriori generalizzazioni dei dati per ridurre il rischio di re-identificazione dei pazienti; è la Società che ha modificando il paradigma operativo dell'anonimizzazione da distribuito a centralizzato; la Società da ultimo ha individuato una "terza parte" "*che si farà carico centralmente di misurare e di garantire l'efficacia del processo di anonimizzazione prima che i dati le vengano trasmessi*"; è la Società che ha verificato l'affidabilità di questa terza parte che dovrebbe agire quale responsabile del trattamento dei MMG; è la Società che ha chiarito le caratteristiche del codice randomico sostituivo dell'ID del paziente; è la Società che da ultimo ha elaborato il documento contenente i risultati dei test di anonimizzazione da quest'ultima effettuato con il supporto di esperti tecnici, effettuati su *dataset*.

Sotto altro profilo, la raccolta di queste informazioni risulta necessaria solo ed esclusivamente al perseguimento delle attività di Thin volte a "*generare una base di conoscenza per la ricerca medica fondata su elementi oggettivi che consenta di realizzare progressi nei percorsi di cura dei pazienti attraverso un 'analisi di dati anonimi relativi alla cura dei pazienti dei medici*".

A nulla rileva, quindi, ai fini della qualificazione del titolare del trattamento, la circostanza che i dati siano materialmente forniti a Thin dai MMG, in quanto ciascun MMG altro non fa che, su richiesta e dietro corrispettivo di Thin, e con le modalità predisposte dalla stessa Thin, pseudonimizzare e trasferire i dati alla stessa Società. Ciò, seppur ritenendo in buona fede di trasferire dati anonimizzati.

D'altro canto, è proprio il Codice di deontologia medica, approvato dalla federazione nazionale degli ordini dei medici chirurghi e degli odontoiatri, a disporre, all'art. 11, che "*il medico non collabora alla costituzione, alla gestione o all'utilizzo di banche di dati relativi a persone assistite in assenza di garanzie sulla preliminare acquisizione del loro consenso informato e sulla tutela della riservatezza e della sicurezza dei dati stessi*".

Costituisce quindi una non condivisibile *fictio iuris* quella per cui nel caso in esame sarebbero i medici i soli titolari dell'operazione di anonimizzazione dei dati dei propri pazienti, realizzata nei termini sopra descritti.

7.3. La natura personale dei dati trattati

L'operazione di trattamento che Thin realizza attraverso l'*add-on*, non è tale da consentire di anonimizzare le informazioni acquisite dai MMG.

A tale riguardo, si rileva che la mera sostituzione dell'ID del paziente con un codice *hash* irreversibile da questo ottenuto non costituisce, in alcuna circostanza, misura idonea rispetto al requisito della rimozione delle singolarità (*single out*) necessario a qualificare il trattamento come un'anonimizzazione: ciò è ribadito dall'affermazione del Gruppo di lavoro Articolo 29 in virtù della quale "*affidarsi semplicemente alla solidità del meccanismo di crittografia quale misura del grado di "anonimizzazione" di un insieme di dati è fuorviante, in quanto molti altri fattori tecnici e organizzativi incidono sulla sicurezza generale di un meccanismo di crittografia o di una funzione di hash*" (Parere 05/2014 sulle tecniche di anonimizzazione).

Inoltre, dai documenti in atti, risulta che il mantenimento dell'univocità dei *record* è un requisito del trattamento in quanto ritenuto indispensabile per osservare la storia clinica di uno specifico paziente nel tempo (ad es. se l'assunzione di un determinato farmaco abbia generato particolari effetti, ovvero se una determinata patologia sia correlabile ad altre patologie, etc..).

L'ulteriore affinamento previsto dalla Società che sarebbe "*in grado di garantire in particolare il rispetto del principio di non singolarità del dato, modificando il paradigma operativo dell'anonimizzazione da distribuito a centralizzato*" e che prevederebbe "*l'aggiunta di una base di dati di servizio centralizzata, raggiungibile dai MMG partecipanti al progetto e gestita da una terza parte in qualità di responsabile del trattamento dei MMG che si farà carico centralmente di misurare e di garantire l'efficacia del processo di anonimizzazione prima che i dati vengano trasmessi a Thin S.r.l., scartando o effettuando operazioni aggiuntive sui record che dovessero, per le loro caratteristiche statistiche, presentare rischi significativi di re-identificazione*" e la successiva sostituzione dell'*hash* con un codice progressivo non rimuove l'associazione univoca tra un individuo e il codice con cui questo è rappresentato all'interno della base dati. Esso infatti introduce unicamente un'ulteriore separazione di responsabilità nell'identificazione dell'interessato tramite un intervento di carattere meramente organizzativo non in grado di scongiurare la presenza di singolarità del *data set* finale presso la terza parte.

Pertanto, l'introduzione di una terza parte, pur rappresentando un'ulteriore misura tecnica e organizzativa volta a rendere la re-identificazione dell'interessato semplicemente più complessa, vista l'ulteriore separazione delle responsabilità, non modifica la natura del dato trattato che continua a mantenere il carattere di "dato personale" e quindi, in quanto tale, soggetto alla disciplina in materia di protezione dei dati personali.

Infine, l'accorgimento da ultimo adottato dalla Società di introdurre tale identificativo univoco e legato all'identità della persona ottenuto mediante tecnica di *hash,* anche in presenza di *salt,* che non variano nel tempo per un determinato paziente, sortisce l'effetto di associare univocamente un *record* della tabella a uno specifico paziente vanificando, in radice, il beneficio della generalizzazione dei dati dei pazienti in classi di equivalenza (ad es. caratterizzati dalla stessa età e localizzazione), come previsto dalla tecnica di *k-anonymity* a cui la Società si è ispirata.

In altre parole, la tecnica di *k-anonimity*, che consiste nel raggruppare gli interessati sulla base di specifiche combinazioni di attributi, opportunamente generalizzati, in modo che in ciascun raggruppamento siano inclusi almeno *k* soggetti non distinguibili tra loro, perde efficacia laddove, come nel caso in esame, a ciascun individuo sia associato un *hash* univoco (codice crittografico) seppur reso più complesso dalla presenza di un elemento di disturbo ignoto (*salt*).

Si rileva, quindi, che il trattamento in esame risulta qualificabile come una forma di pseudonimizzazione ai sensi dell'art. 4, punto 5 del Regolamento e che l'introduzione della terza parte costituisce una misura organizzativa idonea a irrobustire la sicurezza del trattamento, rendendo più complessa la ricongiunzione tra l'identità del paziente e la sua storia clinica, senza tuttavia far venir meno la natura di dati personali che, dunque, sono stati oggetto di trattamento da parte di Thin.

7.4. La base giuridica del trattamento

Le operazioni di trattamento in questione (in particolare la raccolta e la pseudonimizzazione dei dati personali dei pazienti dei MMG) sono pertanto svolte da Thin in assenza di una idonea base giuridica.

La base giuridica di tale trattamento non può invero rinvenirsi nel contratto con i MMG, atteso che il contratto può costituire idonea condizione di liceità quando il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte (art. 6, par. 2, lett. b) del Regolamento). Ebbene nel caso esaminato gli interessati non sono parte del contratto ma i loro dati ne sono l'oggetto. Inoltre, nel caso di specie, tale condizione avrebbe dovuto essere affiancata da una delle esenzioni dal divieto di trattamento dei dati di cui all'art. 9, par. 2 del Regolamento che, allo stato non sembra sussistere in capo alla Società Thin.

Né può ritenersi che il trattamento si possa basare sul consenso degli interessati ai quali sarebbe stata offerta la possibilità di esprimere solo il proprio diniego alla partecipazione al progetto.

Come sopra riportato è previsto, infatti che "*il Paziente, dopo essere stato adeguatamente informato dal Medico sulle attività che il Medico stesso intende svolgere*

partecipando al progetto Thin, dichiari di non voler partecipare al progetto stesso, i suoi dati non verranno trattati dall'add-on presente nel software Medico 2000 e saranno quindi esclusi".

Il progetto prevede, quindi, per il paziente la facoltà di esercitare un *opt-out*, ossia di opporsi alla presunta (inesistente) anonimizzazione dei propri dati.

La normativa e la giurisprudenza in materia di protezione dei dati personali sono costanti nel ritenere l'*opt-out* una forma di manifestazione della volontà inadeguata ad integrare un consenso valido, ciò con particolare riferimento ai dati inerenti alle particolari categorie, nel caso di specie relativi alla salute, dove il consenso deve essere esplicito, in quanto esso costituisce una deroga al divieto espresso di trattare tali tipologie di dati personali (cfr. Sentenza della Corte di Giustizia, Causa C-673/17, del 1 ottobre 2019; Linee guida 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679, Versione 1.1 adottate il 4 maggio 2020, punto 81: provv. del 31 gennaio 2011, doc. *web* n. 1784528; provv. del 5 maggio 2013 doc. *web* n. 2543820).

In base al Regolamento il trattamento delle particolari categorie di dati può essere svolto se l'interessato abbia prestato il proprio consenso esplicito, salvo nei casi in cui il diritto dell'Unione o degli Stati membri disponga diversamente (art. 9, par. 2, lett. a) del Regolamento).

Tale manifestazione di volontà deve essere libera, specifica, informata, inequivocabile, revocabile ed esplicita e non può essere resa nella forma dell'opposizione. Deve trattarsi, invece, di una dichiarazione o di un'«azione positiva inequivocabile» che renda manifesta l'intenzione dell'interessato ad accettare un trattamento di dati personali che lo riguarda e che il titolare dovrà dimostrare di aver acquisito.

Nella fattispecie in esame, pertanto, risulta erroneamente individuata la modalità di raccolta del consenso, attraverso la forma del diniego (*opt-out*) al trattamento, piuttosto che tramite una manifestazione espressa, libera specifica ed informata.

Tanto premesso, nel caso di specie, dalla documentazione in atti risulta accertata la violazione del principio di liceità del trattamento in quanto la Società, in qualità di titolare ha trattato dati personali dei pazienti dei MMG in assenza di un idoneo presupposto giuridico (artt. 5, par. 1 lett. a) e 9 del Regolamento).

7.5 Gli oneri informativi

La Società di conseguenza ha omesso di fornire una idonea informativa agli interessati sull'erroneo presupposto di trattare solo dati anonimi e che i titolari del trattamento nella fattispecie in esame fossero soltanto i MMG. Nel paragrafo che precede si è evidenziato come questo assunto sia infondato e come il titolare del trattamento necessario all'operazione di anonimizzazione dei dati dei pazienti dei MMG non possa che essere la Società.

Atteso che la Società stessa ha dichiarato che, "*Pur non ricoprendo noi il ruolo di Titolari del trattamento di questi dati personali, a garanzia della corretta informazione al paziente, abbiamo comunque predisposto un'informativa scaricabile dal software Medico 2000 che deve essere fornita dal medico al paziente. Evidenziamo inoltre che in qualsiasi momento il soggetto interessato può chiedere che i suoi dati vengano esclusi da quelli da rendere anonimi per partecipare al progetto "The Health Improvement Network*", non può ritenersi tale adempimento compiuto.

Risulta pertanto accertata la violazione degli artt. 5, par. 1 lett. a), e 13 del Regolamento.

8. Trattamenti da parte dei MMG

Il presente provvedimento, per tutto quanto sopra esposto, disvela che per effetto della complessa struttura sinallagmatica posta in essere da Thin, quest'ultima, pur proponendo uno strumento per l'anonimizzazione dei dati, confidando sul legittimo affidamento dei MMG, in realtà raccoglie -attraverso l'*add on* (estrattore dei dai) del *software* gestionale "*Medico 2000*"-, dai MMG informazioni di carattere personale riferite ai loro pazienti in forma pseudonimizzata, in assenza di un idoneo presupposto giuridico.

I MMG in quanto titolari del trattamento dei dati personali, relativi alla salute dei propri pazienti in particolare per finalità di cura sono tenuti a trattarli in conformità alle specifiche disposizioni del Regolamento, del Codice e dei rilevanti provvedimenti in materia (art. 9, par. 2, lett. h), par. 3 del Regolamento e provv. del Garante recante Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario del 7 marzo 2019 doc. *web* 9091942).

Si ritiene pertanto necessario avvertire i MMG, che utilizzano il gestionale "Medico 2000", che l'adesione al Progetto Thin, nelle modalità attualmente proposte dalla Società e sopra descritte, e in assenza di idonei accorgimenti per anonimizzare effettivamente i dati dei propri pazienti, può verosimilmente determinare una violazione anche da parte di questi ultimi, in qualità di titolari del trattamento, delle disposizioni del Regolamento.

9. Conclusioni

Alla luce delle valutazioni sopra richiamate, tenuto conto delle dichiarazioni rese dal titolare nel corso dell'istruttoria - della cui veridicità si può essere chiamati a rispondere ai sensi dell'art. 168 del Codice- gli elementi forniti dal titolare del trattamento nella memoria difensiva, seppure meritevoli di considerazione, non consentono di superare gran parte dei rilievi notificati dall'Ufficio con l'atto di avvio del procedimento, non ricorrendo, peraltro, alcuno dei casi previsti dall'art. 11 del Regolamento del Garante n. 1/2019.

Per tali ragioni si rileva l'illiceità del trattamento di dati personali effettuato dalla Società in violazione degli articoli 5, par. 1 lett. a), 9 e 13 del

Regolamento. La violazione delle predette disposizioni rende, altresì, applicabile la sanzione amministrativa prevista dall'art. 83, par. 4 e 5, del Regolamento, ai sensi degli artt. 58, par. 2, lett. i), e 83, par. 3, del Regolamento medesimo.

L'art. 58, par. 2, del Regolamento prevede in capo al Garante una serie di poteri correttivi, di natura prescrittiva e sanzionatoria, da esercitare nel caso in cui venga accertato un trattamento illecito di dati personali.

Tra questi poteri, l'art. 58, par. 2, lett. d) del Regolamento, prevede il potere di "*ingiungere al titolare del trattamento o al responsabile del trattamento di conformare i trattamenti alle disposizioni del presente regolamento, se del caso, in una determinata maniera ed entro un determinato termine*".

Alla luce delle valutazioni sopra richiamate, si ritiene di dover ingiungere alla Società, ai sensi del richiamato art. 58, par. 2, lett. d) Regolamento, di conformare i trattamenti alle disposizioni del Regolamento, secondo quanto indicato ai paragrafi 7.2, 7.3, 7.4 e 7.5 del presente provvedimento.

Tra i richiamati poteri di cui all'art. 58, vi è quello di "*rivolgere avvertimenti al titolare del trattamento o al responsabile del trattamento sul fatto che i trattamenti previsti possono verosimilmente violare le disposizioni del presente Regolamento*" (par. 2, lett. a)). Alla luce delle valutazioni sopra richiamate, si ritiene necessario avvertire i Medici di medicina generale, che utilizzano il gestionale "*Medico 2000*" ai sensi del richiamato art. 58, par. 2, lett. a) Regolamento, che l'adesione al Progetto Thin, nelle modalità attualmente proposte dalla Società e sopra descritte e in assenza di idonei accorgimenti per anonimizzare effettivamente i dati dei propri pazienti, può verosimilmente determinare una violazione da parte di questi ultimi delle disposizioni del Regolamento.

10. 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), 9, e 13 del Regolamento, causata da Thin Srl è soggetta all'applicazione della sanzione amministrativa pecuniaria, ai sensi dell'art. 83, par. 5, lett. a) e b) del Regolamento.

Il Garante, ai sensi degli artt. 58, par. 2, lett. i) e 83 del Regolamento, nonché dell'art. 166 del Codice, ha il potere di "*infliggere una sanzione amministrativa pecuniaria ai sensi dell'articolo 83, in aggiunta alle* [altre] *misure* [correttive] *di cui al presente paragrafo, o in luogo di tali misure, in funzione delle circostanze di ogni singolo caso*" e, in tale quadro, "*il Collegio* [del Garante] *adotta l'ordinanza ingiunzione, con la quale dispone altresì in ordine all'applicazione della sanzione amministrativa accessoria della sua pubblicazione, per intero o per estratto, sul sito web del Garante ai sensi dell'articolo 166, comma 7, del Codice*" (art. 16, comma 1, del Regolamento del Garante n. 1/2019).

La predetta sanzione amministrativa pecuniaria inflitta, in funzione delle circostanze di ogni singolo caso, va determinata nell'ammontare tenuto conto dei principi di effettività, proporzionalità e dissuasività, indicati nell'art. 83, par. 1, del Regolamento, alla luce degli elementi previsti all'art. 83, par. 2 del Regolamento. Al riguardo, si osserva che:

1. il trattamento effettuato ha riguardato informazioni idonee a rilevare lo stato di salute dei pazienti di circa 547 medici di medicina generale, (art. 4, par. 1, n. 15 del Regolamento e art. 83, par. 2, lett. a) e g) del Regolamento);
2. sotto il profilo riguardante l'elemento soggettivo non emerge alcun atteggiamento intenzionale da parte del titolare del trattamento dovendosi ritenere che le violazioni accertate siano avvenute in buona fede (art. 83, par. 2, lett. b) del Regolamento);
3. non risultano precedenti violazioni pertinenti commesse dal titolare del trattamento, né sono stati precedentemente disposti provvedimenti di cui all'art. 58 del Regolamento (art. 83, par. 2, lett. e) del Regolamento);
4. la Società ha posto in essere alcune misure correttive in relazione al trattamento dei dati personali effettuato, tuttavia persistono i profili di non conformità al quadro normativo vigente in materia di protezione dei dati personali sopra evidenziati. (art. 83, par. 2, lett. c) del Regolamento;
5. l'ultimo bilancio della Società risulta in perdita.

In ragione dei suddetti elementi, valutati nel loro complesso, si ritiene di determinare l'ammontare della sanzione pecuniaria prevista dall'art. 83, par. 5, lett. a) del Regolamento, nella misura di € 15.000 (quindicimila) per la violazione degli artt. 5, par. 1 lett. a), 9, par. 2, e 13 del Regolamento, quale sanzione amministrativa pecuniaria ritenuta, ai sensi dell'art. 83, par. 1 e 3, del Regolamento, effettiva, proporzionata e dissuasiva.

Si ritiene, altresì, che debba applicarsi la sanzione accessoria della pubblicazione sul sito del Garante del presente provvedimento, prevista dall'art. 166, comma 7 del Codice e art. 16 del Regolamento del Garante n. 1/2019, anche in considerazione della tipologia di dati personali oggetto di illecito trattamento.

Si rileva, infine, che ricorrono i presupposti di cui all'art. 17 del Regolamento n. 1/2019 concernente le procedure interne aventi rilevanza esterna, finalizzate allo svolgimento dei compiti e all'esercizio dei poteri demandati al Garante.

Si ritiene, infine, opportuno trasmettere il presente provvedimento alla Federazione Nazionale degli Ordini dei Medici Chirurghi e degli Odontoiatri

(FNOMCeO) al fine di favorire la sensibilizzazione della categoria dei medici in ordine alle problematiche affrontate nel provvedimento stesso in relazione al trattamento dei dati personali dei pazienti.

TUTTO CIO' PREMESSO IL GARANTE

ai sensi dell'art. 58, par. 2, lett. a) Regolamento, avverte i Medici di medicina generale, che utilizzano il gestionale "*Medico 2000*", che l'adesione al Progetto Thin, nelle modalità attualmente proposte dalla Società descritte in premessa e in assenza di idonei accorgimenti per anonimizzare effettivamente i dati dei propri pazienti, può verosimilmente determinare una violazione da parte di questi ultimi delle disposizioni del Regolamento;

dichiara l'illiceità del trattamento di dati personali effettuato da THIN Srl., con sede legale in Piazza Vetra 17 20123 Milano CF e P.IVA 10780410964 per la violazione degli dell'art. 5, par. 1, lett. a), 9, 13 del Regolamento nei termini di cui in motivazione.

ORDINA

ai sensi degli artt. 58, par. 2, lett. i) e 83 del Regolamento, nonché dell'art. 166 del Codice, alla società Thin Srl, con sede legale in Piazza Vetra 17, 20123 Milano, P. IVA n. 10780410964, di pagare la somma di € 15.000 (quindicimila) a titolo di sanzione amministrativa pecuniaria per le violazioni indicate nel presente provvedimento. Si rappresenta che il contravventore, ai sensi dell'art. 166, comma 8, del Codice, ha facoltà di definire la controversia mediante pagamento, entro il termine di 30 giorni, di un importo pari alla metà della sanzione comminata.

INGIUNGE

alla Società THIN Srl:

1. di pagare la somma di euro € 15.000 (quindicimila) -in caso di mancata definizione della controversia ai sensi dell'art. 166, comma 8, del Codice-, secondo le modalità indicate in allegato, entro 30 giorni dalla notificazione del presente provvedimento, pena l'adozione dei conseguenti atti esecutivi a norma dall'art. 27 della legge n. 689/1981.

INGIUNGE altresì

alla Società THIN Srl:

1 ai sensi dell'art. 58, par. 2, lett. d) del Regolamento, di conformare i trattamenti a quanto indicato nei paragrafi 7.2, 7.3, 7.4 e 7.5 del presente provvedimento. L'inosservanza di un ordine formulato ai sensi dell'art. 58,

par. 2 del Regolamento, è punita con la sanzione amministrativa di cui all'art. 83, par. 6 del Regolamento.

DISPONE

1. ai sensi dell'art. 166, comma 7 del Codice, la pubblicazione per intero del presente provvedimento sul sito web del Garante e ritiene che ricorrano i presupposti di cui all'art. 17 del Regolamento n. 1/2019 concernente le procedure interne aventi rilevanza esterna, finalizzate allo svolgimento dei compiti e all'esercizio dei poteri demandati al Garante;
2. la trasmissione del presente provvedimento alla Federazione Nazionale degli Ordini dei Medici Chirurghi e degli Odontoiatri (FNOMCeO) e agli Ordini Provinciali dei Medici Chirurghi e degli Odontoiatri affiche' provvedano a segnalare il presente provvedimento ai propri iscritti.

Ai sensi dell'art. 78 del Regolamento, degli artt. 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, il 1°giugno 2023

IL PRESIDENTE

IL RELATORE

IL SEGRETARIO GENERALE