GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Provvedimento del 23 settembre 2026 [10302112]

VEDI ANCHE Comunicato del 2 ottobre 2026

[doc. web n. 10302112]

Provvedimento del 23 settembre 2026

Registro dei provvedimenti
n. 710 del 23 settembre 2026

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, alla quale hanno preso parte il prof. Pasquale Stanzione, presidente, la prof.ssa Ginevra Cerrina Feroni, vicepresidente e il dott. Agostino Ghiglia componenti, e il dott. Luigi Montuori, segretario generale;

VISTO il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE-Regolamento generale sulla protezione dei dati (di seguito "Regolamento");

VISTO il Codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003, n. 196), (di seguito "Codice");

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

VISTA la documentazione in atti;

VISTE le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000 sull'organizzazione e il funzionamento dell'ufficio del Garante per la protezione dei dati personali, adottato con deliberazione del 28 giugno 2000 (doc. web n. 1098801);

RELATORE la prof.ssa Ginevra Cerrina Feroni;

1. FATTO E SVOLGIMENTO DELL'ISTRUTTORIA

1.1 Origine dell'istruttoria preliminare: l'attività ispettiva

1. L'istruttoria ha tratto origine da accertamenti ispettivi che si sono svolti in data XX e XX presso la società IQVIA Solutions Italy S.r.l. (di seguito anche solo "IQVIA" o "Società) sulla base dell'ordine di servizio del XX (prot. n. XX).

2. IQVIA è una società per azioni con sede legale in via Fabio Filzi 29, Milano. Essa appartiene al gruppo statunitense IQVIA (precedentemente QUINTILES e IMS HEALTH, INC.), presente in oltre cento Paesi nel mondo e che si presenta, sul proprio sito web, come "leader mondiale della ricerca clinica e dei dati sanitari" (1).

3. Gli accertamenti ispettivi hanno avuto ad oggetto la raccolta di dati da parte della Società per la realizzazione di studi osservazionali sponsorizzati dalle aziende farmaceutiche basati sui dati, raccolti dai pazienti di un panel di circa 800 Medici di medicina generale (MMG, di seguito anche il "Progetto"), aderenti alla Società Italiana dei Medici di medicina generale e delle cure primarie (di seguito "SIMG").

1.2 L'attività svolta

1.2.1 Accertamenti ispettivi del XX

4. In tale sede la Società ha in particolare rappresentato che:

- "a seguito dell'acquisizione di Cegedim (nel 2015), è subentrata nella collaborazione con la Società Italiana di Medicina Generale e delle cure primarie (SIMG), che è una società scientifica. La collaborazione prevede, […], la raccolta dei dati dei pazienti di un panel di circa 800 MMG (Medici di Medicina Generale) definiti ricercatori". Da XX, a seguito del provvedimento del Garante del 1° giugno del 2023 n. 226 e della sentenza del Tribunale di Milano, del 10 maggio 2024, sul caso che ha coinvolto la società THIN srl "il DB non è più alimentato con i dati dei pazienti dei MMG ma ancora utilizzato seppur in misura ridotta rispetto agli anni precedenti, sia per studi in essere che nuovi";

- "i dati raccolti presso i MMG confluiscono in una banca dati di IQVIA, denominata internamente LPD (Longitudinal Patient Data), dalla quale quest'ultima estrae semestralmente informazioni che vengono poi fornite alla SIMG o all'occorrenza elabora i predetti dati, per la realizzazione di specifici studi osservazionali retrospettivi richiesti dalle case farmaceutiche, fornendo loro report in forma aggregata";

- "la raccolta dei dati presso i MMG viene effettuata attraverso […] il gestionale del medico denominato "XX" sul quale, su commissione di IQVIA, viene installato un add-on per l'estrazione dei dati. […]";

- "[…] Il medico, a fronte dell'estrazione dei dati attraverso il cd add-on, riceve gratuitamente l'abbonamento del software gestionale "XX" e IQVIA, a sua volta, corrisponde a XX la cifra necessaria";

- il database LPD di proprietà della Società "è suddiviso in diverse tabelle e contiene le informazioni dei singoli pazienti dei MMG, identificati con un codice denominato "Pat ID". Le richiamate tabelle sono relative a: anagrafica, prescrizioni, diagnosi, esami, numero di visite. Ad esempio, la tabella delle prescrizioni contiene tutti i medicinali prescritti ai pazienti";

- "il paziente è censito sempre con lo stesso Pat ID nel tempo, in quanto è necessario "seguirlo" longitudinalmente. La tabella contiene un numero rilevante di record (nell'ordine dei milioni di record) e riguarda i dati di tutti i pazienti dei MMG arruolati nel progetto, per un totale di oltre circa un milione di pazienti per circa ottocento MMG";

- il Pat ID cambia nell'ipotesi in cui in paziente cambi il MMG ovvero qualora quest'ultimo sostituisca il proprio personal computer. "Nonostante tali accadimenti, il potenziale informativo, viste le esigenze informative delle case farmaceutiche, rimane adeguato. […]";

- "il DB è stato costruito sulla base di misure volte a ridurre il rischio di reidentificazione degli interessati. Il presupposto era quindi che il dato fosse anonimo, coerentemente agli standard del mercato anche sulla base di assessment […]" effettuati dalla società del gruppo IQVIA XX, di cui la Società si avvale "per la verifica dell'effettiva anonimizzazione dei dati";

- "il paziente riceve, nell'ambito dell'informativa privacy del MMG, alcune informazioni relative all'iniziativa descritta, che è presente all'interno del modello di contratto tra il MMG e IQVIA ma non è prevista la raccolta del loro consenso";

- "la DPIA è in corso di elaborazione […], allo stato, non risulta ancora formalizzata".

1.2.2 Gli accertamenti ispettivi del XX

5. Il secondo giorno di accertamenti ispettivi, la Società ha, in particolare, per quel che qui rileva, chiarito di essere autonomo titolare del trattamento dei dati presenti nel database LPD anche secondo quanto indicato nell'accordo con i MMG e di non aver accesso diretto al gestionale dei MMG.

6. Con specifico riferimento al flusso dei dati dal gestionale dei MMG al database di IQVIA, quest'ultima ha evidenziato che:

- "XX ha progettato il software affinché rimuova le informazioni direttamente identificative degli interessati (quali nome, cognome e indirizzo)";

- "viene regolarmente svolto un assessment sul rischio di reidentificazione, applicando specifiche misure quali ad esempio in Italia la generalizzazione dell'età attraverso l'indicazione del mese di nascita e la rimozione della città […]";

- "i dati trattati presentano un rischio molto basso di reidentificazione degli interessati e, per questo, non sono ritenuti identificativi; ciò nonostante, a maggior tutela, sono state interrotte le attività di raccolta. Di questa scelta sono stati informati tutti i MMG attraverso una nota informativa pubblicata sul sito internet di SIMG";

- "i dati più risalenti nel tempo contenuti nel DB sono relativi all'anno al XX";

- "non [è] a conoscenza di una policy di cancellazione dei dati e che generalmente non vengono trattati per gli studi dati che risalgono ad un periodo di oltre dieci anni" e che non è "a conoscenza di precedenti valutazioni in ordine alla necessità/opportunità di cancellare i dati più risalenti, neanche al fine di rendere le operazioni del DB più celeri";

7. La Società, a titolo esemplificativo, ha mostrato, esibendo una presentazione acquisita agli atti del procedimento, "un paziente che compare 34 volte nella tabella del DB relativa alle prescrizioni mediche, e che è possibile quindi tracciarne la storia clinica".

8. E' stato quindi effettuato un collegamento con i rappresentanti della Società del Gruppo IQVIA "XX" la quale effettua verifiche sul rischio reidentificazione degli interessati presenti nel database di IQVIA sulla base delle metodologie indicate dal Comitato europeo per la protezione dei dati (CEPD) e dal Gruppo art. 29. Tale Società ha illustrato le misure implementate con riferimento sia al rischio di singolarità che a quello di linkability, precisando di ritenere che il DB contenga dati anonimi "in quanto non è ragionevolmente probabile che un individuo possa essere identificato, ribadendo di lavorare per il pubblico interesse, prendendo molto seriamente i profili di protezione dei dati personali" e che "ha cercato di porre in essere ogni possibile misura per ridurre tale rischio anche attraverso nuove valutazioni e consulenze".

2. Ulteriore documentazione rilevante acquisita in sede ispettiva e a scioglimento delle riserve

2.1 Sul contratto di collaborazione tra IQVIA e la SIMG e sul set di dati fornito semestralmente alla SIMG

11. Dal contratto di collaborazione sottoscritto, in data XX, tra la Società e la SIMG, con specifico riferimento ai profili rilevanti in materia di protezione dei dati personali, risulta che:

- SIMG è un'associazione autonoma e indipendente nata per promuovere, valorizzare e sostenere il ruolo professionale dei MMG con particolare attenzione alle attività di formazione, ricerca e sviluppo professionale;

- SIMG è proprietaria di un centro di ricerca "Health Research" volto a valorizzare il ruolo e la funzione dei MMG attraverso la raccolta sistematica e l'elaborazione di informazioni desumibili, nel rispetto della normativa applicabile dalle cartelle dei pazienti e dalla loro gestione ambulatoriale;

- IQVIA è proprietaria del DB denominato LPD, progettato per raccogliere le informazioni e i dati anonimizzati provenienti dalla ordinaria attività assistenziale dei MMG al fine di condurre studi e indagini di interesse per enti pubblici e privati;

- tra gli obblighi di IQVIA vi è in particolare quello di garantire l'anonimizzazione dei dati raccolti dai MMG prima del loro inserimento nel DB LPD continuando a fornire apposite istruzioni a XX affinché i dati inseriti dai MMG attraverso il software "XX" siano resi anonimi prima del loro inserimento del DB LPD;

- i dati contenuti nel DB LPD sono utilizzati da SIMG per lo svolgimento di attività medico scientifiche e da IQVIA per lo svolgimento della propria attività d'impresa.

2.2 Sul contratto tra IQVIA e i MMG

12. Con riferimento a tale contratto, in esso è rappresentato, in particolare, che:

il Medico si impegna ad alimentare, in modo veritiero e continuativo, il "database", al fine di consentire a IQVIA la raccolta ed elaborazione di tali dati per condurre ricerche statistiche, epidemiologiche e di mercato d'interesse per enti pubblici ed aziende private;

il database grazie alle misure applicate consente di garantire il pieno rispetto della riservatezza e anonimato dei pazienti, non essendo in alcun modo identificabili né da IQVIA né da terzi ed essendo stata adottata ogni necessaria cautela tecnica ed organizzativa, in base alla costante evoluzione tecnologica, per garantire l'effettiva anonimizzazione dei dati portati a conoscenza di IQVIA";

pur essendo garantito l'assoluto anonimato dei pazienti assistiti dal Medico, fin dalla fase della raccolta ed elaborazione dei dati oggetto dell'attività descritta nel contratto, resta in capo a quest'ultimo l'obbligo di informare i pazienti, attraverso la loro informativa, in ordine alla circostanza che i dati personali saranno anonimizzati con tecniche che garantiscano la piena riservatezza delle informazioni, per poter essere utilizzati, sempre nel pieno anonimato del paziente, per lo svolgimento di analisi statistiche e ricerche da parte di soggetti operanti nel settore medico e farmaceutico.

2.3 Sulla generazione del Pat ID

13. Con specifico riferimento alle modalità di generazione del Pat ID, la Società, con nota del XX, ha dichiarato che "il processo prevedeva l'uso di un UUID (Universally Unique Identifier), un numero di 16 byte, da XX rappresentato con una stringa di 22 caratteri alfanumerici, generato dall'Add-on utilizzando un algoritmo proprietario di XX. Tale UUID, non conoscibile al MMG in quanto non visibile lato applicativo e in quanto il sottostante database XX era protetto con password, veniva associato ad un singolo paziente. Quale ulteriore misura di rafforzamento per la gestione del rischio di reidentificazione la data di nascita del paziente veniva modificata inserendo, di default, il primo giorno del mese. Questo campo non è riconducibile al paziente a meno di accesso diretto alle chiavi di ricongiunzione. A tutti gli effetti questo codice paziente, è chiave primaria della tabella dei Pazienti, ed è generato senza usare caratteristiche personali del paziente, ma semplicemente basandosi su algoritmi randomici che rispecchiano l'univocità dell'id nella tabella. Infatti, se il medico inserisse il Paziente A sull'applicativo e poi lo cancellasse, al successivo inserimento dello stesso Paziente A, il PAT ID sarebbe diverso".

2.4 Sugli assessment sul rischio di re-identificazioni dei pazienti

14. Relativamente al rischio di re-identificazione degli interessati e al parametro K (k-anonymity), la Società ha prodotto due "assessment effettuati da XX su incarico di IQVIA nel XX e XX", riguardo ai quali è possibile fin da ora formulare talune osservazioni meglio rappresentate nel prosieguo (par. 7.3).

15. La k-anonymity impone che ogni combinazione di taluni attributi di un individuo (ad esempio, località, età) sia condivisa da almeno k individui, generando così classi di equivalenza.

2.5 Sulla policy di conservazione dei dati

17. La Società ha inoltre trasmesso la "Policy di conservazione dei dati", dalla quale emerge, in via preliminare, un periodo di validità dal XX all'XX e che la stessa si riferisce alla conservazione dei documenti e delle registrazioni di IQVIA cosi definiti: "fax, posta elettronica, microfiche, memorandum, note, fotografie, informazioni registrate elettronicamente (inclusi documenti conservati su nastro magnetico,

cassette, dischi o altri strumenti per processare o conservare dati elettronici), periodici, articoli di stampa e presentazioni o progetti (inclusi previsioni, budgets e progetti a lungo termine).

18. Inoltre, nella sezione "Documenti in ambito Sicurezza delle informazioni e Privacy" (punto 5.17), è riportato in maniera del tutto generica che i dati personali "Devono essere conservati per un periodo di tempo non superiore a quello necessario agli scopi per i quali sono stati raccolti e trattati".

19. Al riguardo, la Società ha inoltre dichiarato che "provvederà a cancellare i dati dal database principale, conservandone temporaneamente una copia in un archivio ad uso esclusivamente ai fini del procedimento. Tale copia di archivio sarà cancellata al termine del procedimento e di ogni eventuale correlata pendenza".

3. La notifica di violazione di dati personali

20. A seguito dei predetti accertamenti ispettivi, la Società, in qualità di titolare del trattamento, il XX, ha trasmesso al Garante una notifica di violazione dei dati personali ai sensi dell'art. 33 del Regolamento (di seguito "data breach"), integrata con note del XX e XX.

21. Con nota del XX (prot. n. XX), l'Ufficio ha disposto la riunione dei procedimenti pendenti nei confronti della Società - quello relativo ai richiamati accertamenti ispettivi e quello concernente la notifica di violazione dei dati personali - comunicando contestualmente la sospensione dei termini procedimentali, in attesa della conclusione da parte della Società del procedimento di notifica della violazione di dati personali, intervenuta in data XX (art. 10, comma 4, 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 per la protezione dei dati personali, doc. web n. 9107633; Tabella B), del Regolamento 2/2019, - concernente l'individuazione dei termini e delle unità organizzative responsabili dei procedimenti amministrativi presso il Garante per la protezione dei dati personali, doc. web n. 9107640).

22. In particolare, la Società, ha rappresentato di aver scoperto in modo del tutto inaspettato che il database LPD ricevuto dai MMG, tramite il suddetto Add-on, conteneva informazioni personali su alcuni pazienti e medici all'interno di campi a testo libero. In particolare, diversi MMG hanno aggiunto informazioni "relative a persone fisiche (dati relativi a pazienti e a un numero limitato di medici)" e che nonostante dovessero essere anonimizzate "tramite l'Add-on prima di essere esportati per l'invio a IQVIA (si veda l'Allegato A del contratto XX-IQVIA e il Protocollo di qualità Sub A del contratto IQVIA-Medico che si allega qui). Tuttavia, tale processo non è stato applicato, con la conseguenza che i dati non sono stati rimossi dal file contenente l'estrazione. L'incidente è pertanto attribuibile ad una serie di fattori concomitanti, ciascuno dei quali (in caso di corretto funzionamento) avrebbe dovuto impedire o ridurre al minimo il rischio di una erronea comunicazione di dati personali".

23. Tale comunicazione, non autorizzata, avrebbe riguardato dati personali direttamente identificativi (quali nome e cognome, data di nascita, codice fiscale, indirizzo postale, indirizzo e-mail e numero di telefono) di n. 3.370 pazienti. La Società ha inoltre specificato che "sulla base delle analisi effettuate è risultato che la violazione ha interessato dati relativi allo stato di salute di 3.080 pazienti". Tali dati sono stati ricevuti da IQVIA quotidianamente (nei giorni feriali) nel periodo compreso tra il XX e il XX e poi inviati alla SIMG, la quale, su richiesta della Società, ha provveduto a rimuovere tutti i dati identificativi presenti nel file SIMG, dandone conferma alla Società.

4. AVVIO DEL PROCEDIMENTO PER L'ADOZIONE DEI PROVVEDIMENTI CORRETTIVI E SANZIONATORI E DIFESE DELLA PARTE

4.1. Avvio del procedimento (art. 166, comma 5, del Codice)

24. In base all'esame degli elementi acquisiti nel corso delle attività sopra descritte e all'accertamento delle presunte violazioni, con nota del XX (prot. n. XX), notificata ai sensi dell'art. 166, comma 5, del Codice, l'Ufficio ha avviato il procedimento per l'adozione dei provvedimenti di cui all'art. 58, par. 2, del Regolamento nei confronti della società IQVIA, invitando la stessa a produrre al Garante scritti difensivi o documenti ovvero a chiedere di essere sentito dall'Autorità (art. 166, commi 6 e 7, del Codice, nonché art. 18, comma 1, della l. 24 novembre 1981, n. 689).

25. Con il predetto atto l'Ufficio ha notificato le seguenti presunte violazioni. La società ha posto in essere trattamenti di dati personali:

in maniera non conforme ai principi di "liceità, correttezza e trasparenza", in assenza di un idoneo presupposto normativo e non adempiendo all'obbligo di fornire preventivamente le informazioni all'interessato, in violazione degli artt. 5, par. 1, lett. a), 9, 12 e 13 del Regolamento;

in maniera non conforme al principio di limitazione della conservazione dei dati (art. 5, par. 1, lett. e) del Regolamento);

in violazione del principio di integrità e riservatezza (art. 5, par. 1, lett. f) e 32 del Regolamento);

in violazione dell'art. 28 del Regolamento, non avendo effettuato la nomina di responsabili del trattamento dei MMG aderenti all'iniziativa della Società;

in violazione del principio di responsabilizzazione e di privacy by design, di cui all'art. 5, par. 2 del Regolamento;

in violazione dell'obbligo di effettuare la valutazione d'impatto ai sensi dell'art. 35 del Regolamento.

4.2 Difese della Parte (art. 166, comma 6, del Codice)

26. Con nota del XX, la Società ha fatto pervenire le proprie memorie difensive, con le argomentazioni che seguono, in parte difformi rispetto alle posizioni espresse in sede ispettiva, chiedendo altresì di essere sentita in audizione, ai sensi dell'art. 166, comma 6 del Codice (nota del XX).

4.2.1 Sul progetto Health Search

27. La Società ha rappresentato di essere subentrata nel 2017, a seguito di operazioni societarie straordinarie, alla società francese Cegedim nella gestione del database Health Search, mantenendo il ruolo di mero partner tecnologico - finanziario – operativo del progetto, denominato Health Search (il Progetto), la struttura, i ruoli, le istruzioni e le linee di indirizzo disegnate dalla SIMG nel corso degli anni, sulla base di accordi sostanzialmente identici al precedente modello di collaborazione tra la SIMG e la società Cegedim. Il predetto database trae le sue origini dalla scelta della SIMG di promuovere la costituzione di un progetto volto a "(i) "creare una scuola nella quale i Medici di Medicina Generale (MMG), su base volontaria (anche se con particolare attenzione alla distribuzione campionaria), ricevono la formazione per la descrizione e la registrazione codificata della loro attività professionale attraverso l'utilizzo di un software di gestione dei dati clinici appositamente personalizzato (XX)", (ii) "costituire un network di MMG ricercatori rappresentativi di ogni macroarea geografica in termini di numerosità della popolazione di riferimento", (iii) "costituire un database [di riferimento di un sistema strutturato di ricerca dei Medici Generali". La Società ha, inoltre, evidenziato:

- di non aver ha mai effettuato scelte relative a elementi essenziali del processo di estrazione dei dati tramite l'Add-on, limitandosi solo a garantire il corretto e sicuro funzionamento del processo di presa in carico ed elaborazione dei dati anonimi, trasmessi dai MMG;

- di non aver apportato alcuna variazione nella struttura dei record di estrazione dell'Add-on che sono rimasti nella stessa forma ideata da SIMG, come attestato anche da XX;

- che un elemento chiave del Progetto, come concepito da SIMG, è stato quello di garantire l'anonimato dei dati che confluivano nel database Health Search, in ragione dei processi di estrazione definiti da SIMG e implementati grazie alla collaborazione di XX e del relativo Add-on. In linea con la complessiva continuità operativa, IQVIA ha altresì preso atto e mantenuto questo aspetto nei propri rapporti contrattuali;

- che i dati trasmessi dai MMG tramite l'Add-on venivano archiviati in un database temporaneo di staging per essere destinati a due diversi processi, uno riguardante la creazione del file di estrazione dal database di staging per l'inoltro semestrale a SIMG per gli usi scientifici previsti, come da accordo di collaborazione con IQVIA ("Estrazione SIMG"), l'altro inerente all'invio dei dati per ulteriori

elaborazioni finalizzate a trasformare i dati nel formato standard interno IQVIA, applicando ulteriori misure di privacy enhancement, standardizzazione e assegnazione ai pazienti di un codice univoco interno, prima che confluissero nel Data Warehouse finale ("Data Warehouse LPD"), il quale costituiva il database di riferimento per le attività di produzione di IQVIA, in base agli accordi contrattuali con SIMG, prima dell'interruzione di qualsiasi attività nell'XX.

4.2.2 Sulla natura anonima dei dati

28. In relazione a tale profilo, la Società ha rappresentato che:

- in applicazione dei principi espressi nella sentenza della Corte di Giustizia C-413/23, i dati ricevuti da IQVIA sono anonimi, in quanto tutti i mezzi che potrebbero essere utilizzati per identificare i pazienti sono stati rimossi, sono vietati dalla legge o sarebbero praticamente impossibili da utilizzare per motivi di tempo, costi e manodopera. In particolare, la Società, in applicazione della predetta sentenza, afferma che per far si che un dato sia anonimo, non è necessario che sussistano tutti e tre i criteri indicati dal parere del 2014 del WP29 (singling out, linkability, inference), ma che in realtà occorre effettuare una valutazione del rischio di reidentificazione degli interessati, utilizzando i mezzi ragionevoli;

- IQVIA non ha accesso al computer del Medico che ha inviato i dati al fine di re-identificare l'interessato utilizzando l'ID paziente, in quanto IQVIA riceve semplicemente file crittografati mediante standard di sicurezza; inoltre IQVIA, in sede contrattuale, non ha alcun diritto di richiedere a XX (società fornitrice del software di estrazione) l'accesso al "segreto di pseudonimizzazione" e che il contratto tra il MMG e IQVIA vincola il MMG a fornire a IQVIA solo dati anonimi e IQVIA a trattare esclusivamente dati anonimi. A tal proposito, da quanto scritto nel predetto contratto, risulta che l'anonimizzazione avviene sulla base delle funzionalità automatiche dell'Add-on, in quanto al punto 2 si legge che "Il Programma (Add-on) sarà utilizzato dal Medico con la diligenza d'uso, essendo IQVIA tenuta comunque a garantirne la manutenzione e la continuità di funzionamento, senza alcun onere a carico del Medico";

- che IQVIA non può identificare un individuo selezionando le informazioni contenute nel database e incrociandole con altri dati (esterni) relativi a tale individuo, in quanto SIMG ha progettato l'Add-on al software di gestione dello studio medico dei MMG in modo che questi ultimi trasmettessero solo il mese e l'anno di nascita; la data di nascita è sempre impostata sul primo giorno di ogni mese. L'indirizzo del paziente, invero, non viene trasmesso dal MMG tramite l'Add-on; viene indicata solo la città del paziente. Nemmeno l'indirizzo del MMG viene tracciato dall'Add-on; viene trasmessa solo la provincia. IQVIA, dunque, non dispone di mezzi legali per identificare i pazienti presenti nel database confrontandoli con le cartelle cliniche conservate dai professionisti sanitari o da altri soggetti sotto la loro responsabilità;

- IQVIA nel XX aveva commissionato una relazione alla società XX, al fine di ridurre ulteriormente il rischio di re-identificazione su dati ritenuti da IQVIA già di per sé anonimi.

4.2.3. Sulla Liceità, correttezza e trasparenza

29. La Società ha rappresentato che non era tenuta al rispetto degli obblighi di trasparenza e di trattamento con una idonea base giuridica, in quanto i dati che IQVIA ha trattato per le attività di ricerca svolte a favore di terzi sono dati anonimi e di aver interrotto nel XX l'alimentazione del database LPD con i flussi dei dati da parte dei MMG.

30. I dati ricevuti da IQVIA sono già anonimi prima dei processi di aggregazione e trasformazione applicati al momento della ricezione dei dati e prima del trasferimento degli stessi nel Data Warehouse. Nel corso del tempo SIMG ha mantenuto il ruolo primario alla guida del progetto Health Search. Infatti era SIMG a definire i criteri di selezione dei MMG e successivamente provvedeva al loro reclutamento, verificava e controllava i contributi dei MMG al progetto e in alcune occasioni è anche intervenuta per sostituire i MMG che non rispettavano i criteri di partecipazione; inoltre, era SIMG, con il supporto e il coinvolgimento di XX, a definire l'uso di un Add-on per l'estrazione dei dati dei pazienti dal software gestionale XX e l'individuazione dei dati oggetto di estrazione e il loro formato e codifica, e ciò ben prima della

partecipazione di IQVIA e nulla è cambiato, dopo il coinvolgimento di quest'ultima, rispetto alla finalità della raccolta dei dati e ai suoi mezzi essenziali.

31. In conclusione, la Società non avrebbe mai determinato le finalità della raccolta dei dati dai MMG, né ha esercitato alcuna influenza sui mezzi essenziali del trattamento, non essendo pertanto qualificabile come titolare del trattamento rispondendo solamente delle operazioni di processamento di dati che rientrano nel proprio perimetro di competenza, e in cui - a quel punto – i dati sono anonimi.

4.2.4 Sui ruoli di protezione dei dati personali

32. Con specifico riferimento a tale aspetto, la Società ha ribadito di non essere titolare del trattamento dei dati effettuato dai MMG attraverso l'Add-on e, di conseguenza, i MMG non possono essere suoi responsabili del trattamento, e che la SIMG è titolare del trattamento, in quanto provvedeva in autonomia al reclutamento dei MMG, che a loro volta decidevano in autonomia se partecipare al Progetto Health Search, ed ha altresì definito l'utilizzo di un Add-on per l'estrazione dei dati dei pazienti dal software gestionale XX e l'individuazione dei dati oggetto di estrazione, il loro formato e la codifica, il tutto prima della partecipazione di IQVIA al progetto.

33. Pertanto, IQVIA non ha influito in alcun modo sulla scelta di utilizzare l'Add-on per l'anonimizzazione dunque non ha mai determinato né la finalità della raccolta dei dati dai MMG né i mezzi essenziali del trattamento;

4.2.5 Sui tempi di conservazione dei dati e sulla valutazione d'impatto

34. Il principio di limitazione della conservazione previsto dal Regolamento non può trovare applicazione vista la natura anonima dei dati estratti dal gestionale dei MMG. Ad ogni modo, anche laddove i dati raccolti dalla Società venissero considerati come dati personali, la predetta, a seguito dell'attività ispettiva svolta dall'Autorità, ha stabilito un tempo di conservazione di 10 anni, in linea con la normativa vigente.

35. In merito alla redazione della valutazione d'impatto ai sensi dell'art. 35 del Regolamento, che anche in tal caso trattando dati anonimi, è sottratta a tale obbligo. Pur volendo ammettere che i dati trattati siano dati personali, la Società ha altresì dichiarato che avendo iniziato il trattamento nel 2017 ed essendo il Regolamento entrato in vigore nel 2018, non era tenuta a conformarsi a tale obbligo. Tuttavia, la IQVIA ha iniziato a preparare una bozza di DPIA, al fine di rendersi più compliant alla materia della protezione dei dati personali.

4.2.6 Sulla violazione di dati personali e sul principio di integrità e riservatezza

36. La Società ha ribadito che i dati estratti dall'Add-on, prima di essere trasmessi, vengono sottoposti ad un processo di anonimizzazione. Una volta che la Società riceve i dati, applica ulteriori misure tecniche di de-identificazione. La Società ha altresì dichiarato di non aver sviluppato e installato l'Add-on, avendo agito nella convinzione che i dati che le sono stati trasmessi dai MMG fossero anonimi;

37. Per quanto concerne il data breach, causato da un erroneo inserimento da parte dei MMG di dati personali dei pazienti e di altri medici nei campi di testo libero, l'involontario trattamento di dati personali da parte di IQVIA è derivato da un uso non corretto da parte dei predetti medici dei campi di dati inseriti nel sistema di gestione dei pazienti. Inoltre, tali dati sono stati messi a disposizione esclusivamente di SIMG, che ha dichiarato di averli cancellati.

38. La Società ha infine dichiarato la non applicabilità ai trattamenti da essa svolta del principio di accountability, non essendo il titolare del trattamento e non trattando dati di natura personale.

4.2.7 L'audizione e la documentazione integrativa

39. In data XX 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:

> "IQVIA non gestisce l'applicativo di anonimizzazione dei dati e non definisce gli aspetti inerenti al relativo processo di anonimizzazione. La tecnologia viene fornita da altri, quello di IQVIA è un

supporto economico e ciò non implica che IQVIA possa essere considerata un titolare del trattamento";

C'è, dunque, uno scollegamento tra chi dà supporto economico e chi invece decide e incide su mezzi e finalità del trattamento. Su tale ultimo aspetto, il tutto è deciso da SIMG, MMG e partner tecnologico (XX).

C'è una differenza con il caso Thin, la quale aveva deciso il partner tecnologico con il quale ha sottoscritto specifici accordi e deciso le modalità di anonimizzazione. Inoltre, nel caso Thin non vi era un progetto sviluppato da una società scientifica. I dati arrivano a IQVIA già anonimizzati con una procedura già decisa sulla quale la Società non è intervenuta. Quest'ultima si limita ad effettuare una standardizzazione dei dati ricevuti

Con riferimento al data breach, una volta che la Società si è accorta che nei campi liberi dell'Add-on, i MMG avevano inserito dati direttamente identificativi di Medici e pazienti, la notifica effettuata da IQVIA va letta come atto di diligenza, ma ciò non può conferire a IQVIA il ruolo di titolare del trattamento

"Con riferimento all'anonimizzazione dei dati, non può non tenersi conto che medio tempore è intervenuta la sentenza cd Deloitte, che in qualche modo cambia la prospettiva nel senso che può rilevare un concetto di dati anonimi relativi. Dopo la sentenza Deloitte, occorre chiedersi se IQVIA, nella sua posizione di soggetto ricevente i dati, aveva gli strumenti per re-identificare i pazienti e se il livello di rischio di re-identificazione passa considerarsi alto o meno. Per fare ciò non possiamo esimerci dall'utilizzare i criteri della citata Sentenza […]".

40. Da ultimo, con email del XX, la Società ha trasmesso al Garante un ulteriore documento denominato "Valutazione dei rischi di re-identificazione sulla qualificazione dei dati contenuti nella banca dati LPD come dati anonimi dal punto di vista di IQVIA" volto a dimostrare che i dati contenuti nel database proprietario LPD devono essere qualificati come anonimi e non personali ciò in quanto IQVIA non dispone "ne direttamente, né indirettamente di alcun mezzo ragionevolmente utilizzabile per re-identificare gli interessati i cui dati sono presenti nel DB" ciò anche alla luce della la sentenza della Corte di Giustizia del 4 settembre 2025, causa C-413/23 P (cd "Sentenza SRB").

41. In particolare, nel predetto documento si legge che:

- "IQVIA non controlla, non gestisce né può modificare il processo di pseudonimizzazione" in quanto "[…] la pseudonimizzazione dei dati avviene interamente a monte della loro trasmissione a IQVIA, all'interno del software gestionale del MMG, attraverso un add-on sviluppato da XX. Il Patient ID (Pat ID), ossia il codice alfanumerico casuale che sostituisce i dati identificativi personali del paziente, è generato da un algoritmo proprietario direttamente sul sistema gestionale del MMG e non è mai visibile né accessibile a IQVIA. La chiave di ricongiunzione tra il Pat ID e l'identità del paziente è detenuta esclusivamente dal software gestionale del MMG, all'interno di un database protetto da password, nota soltanto al MMG, a cui IQVIA non ha accesso. IQVIA non controlla, non gestisce né può modificare il processo di pseudonimizzazione";

- IQVIA non può re-identificare gli interessati utilizzando altri mezzi, in quanto "i dati dei pazienti ricevuti da IQVIA non contengono identificatori diretti (nome, cognome, codice fiscale, ecc.). I quasi-identificatori presenti sono stati generalizzati (la data di nascita è stata ridotta al solo mese). Il Pat ID è un identificatore casuale non derivato dalle caratteristiche personali del paziente, e cambia se il paziente cambia MMG o se il MMG sostituisce il proprio computer: non consente pertanto alcuna correlazione con fonti esterne. Inoltre […] non esistono dataset disponibili pubblicamente né banche dati accessibili a IQVIA in forza di titoli giuridici esistenti - che permetterebbero un incrocio efficace tra i d ati LPD e l'effettiva identità dei pazienti";

- sulla base di tutti gli elementi analizzati e descritti nel citato documento, il rischio di re-identificazione degli interessati ha un valore finale pari a 3, corrispondente, dunque, a una soglia bassa e pertanto non significativo.

5. L'attività istruttoria svolta nei confronti di SIMG e della società XX

42. Alla luce delle memorie difensive presentate dalla Società, l'Ufficio, al fine di condurre una completa istruttoria in ordine ai trattamenti in esame che vedono coinvolte anche la SIMG e la società XX ha ritenuto necessario avviare specifiche istruttorie nei confronti di tali soggetti dai quali è emerso, per quel che qui rileva, quanto segue.

5.1. Sintesi dell'istruttoria nei confronti di SIMG

43. La SIMG ha rappresentato, in particolare, che il database LPD negli anni ha subito vari passaggi di proprietà, fino ad essere acquisito nel XX dalla società IMS (poi divenuta IQVIA).

44. Con specifico riferimento ai ruoli di protezione dei dati e al processo di anonimizzazione nell'ambito del progetto Health Search, la SIMG ha trasmesso il contratto di collaborazione stipulato con la società IQVIA, dal quale risulta che sebbene entrambe siano comproprietarie del database LPD, tuttavia è la società IQVIA che si impegna, in particolare, "a continuare a fornire apposite istruzioni a XX affinché i dati inizialmente sensibili inseriti dai MMG attraverso il software "XX" siano resi anonimi prima del loro inserimento nel database LPD" (cfr. art. 2.1. lett. a) del contratto sottoscritto tra le parti in data XX).

5.2. Sintesi istruttoria svolta nei confronti della Società XX

45. La Società XX ha innanzitutto rappresentato e altresì documentato, per quel che qui rileva, che a far data dal XX, è cessato l'invio dei dati tramite l'Add-on dai MMG ad IQVIA e ha dichiarato:

- di essere stata nominata da IQVIA quale responsabile del trattamento ai sensi dell'art. 28 del Regolamento, in relazione al progetto in esame, con specifico riferimento "all'attività di onboarding dei Medici Collaboranti dell'ambito del Progetto", avente ad oggetto non solo il trattamento dei dati dei MMG ma anche quello dei pazienti;

- che "il Software è stato realizzato da XX in base alle richieste di IQVIA";

46. A tale riguardo ha in particolare trasmesso il contratto stipulato con IQVIA in data 26 febbraio 2020, nel quale è previsto che: "2.6 XX garantisce che i dati contenuti nel database dei Medici Collaboranti, estratti mediante il Software, subiranno un processo di anonimizzazione, prima dell'invio all'infrastruttura di IQVIA, cosi come descritto nell'allegato A del presente contratto" proposto dalla stessa IQVIA.

6. VALUTAZIONI DELL'AUTORITA

47. All'esito dell'esame delle dichiarazioni rese dalla Società, nel corso del procedimento (della cui veridicità l'autore risponde ai sensi e per gli effetti di cui all'art. 168 del Codice "Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante"), nonché della documentazione acquisita agli atti, l'Autorità rileva quanto segue.

6.1 Il progetto Health Search e la sua evoluzione

48. In via preliminare, anche alla luce degli atti acquisiti dal Garante in occasione delle successive istruttorie avviate nei confronti della SIMG e della Società XX S.p.A. (di seguito "XX"), è necessario ricostruire cronologicamente il Progetto, al fine di meglio comprendere il ruolo svolto dalla Società nell'ambito del trattamento di anonimizzazione dei dati alimentanti il database denominato "LPD- Longitudinal Patient Database".

49. La SIMG e l'Associazione Health Search avevano concepito nel lontano XX e fino al XX un progetto volto a valorizzare il patrimonio informativo dei MMG poi successivamente ceduto, nella sua versione embrionale, ad una società del gruppo Cegedim (uno dei più grandi gruppi francesi di elaborazione dei dati in ambito sanitario che già aveva realizzato in Francia un progetto analogo a quello che la SIMG cercava di realizzare in Italia), non disponendo tuttavia delle necessarie strutture organizzative e dei relativi mezzi, essendo, "un'associazione autonoma e indipendente nata per promuovere, valorizzare e sostenere il ruolo professionale dei medici di medicina generale, sia nella sanità italiana che nelle organizzazioni sanitarie europee e extraeuropee" (cfr. https://www.simg.it/istituzione/presentazione/).

50. A seguito di tale cessione, la società XX del Gruppo Cegedim, ha acquisito la proprietà del database contenente i dati provenienti dall'ordinaria attività assistenziale dei pazienti dei MMG. Nel contratto di collaborazione con la SIMG era espressamente indicato che la stessa intendeva ulteriormente sviluppare il progetto, realizzando altresì sostanziali modifiche del database. Nel medesimo accordo di collaborazione è espressamente evidenziato che la predetta società avrebbe continuato a supportare l'attività scientifica della SIMG attraverso l'accesso al database, previa tempestiva comunicazione, in cui quest'ultima doveva illustrare il progetto di ricerca e ben potendo la società XX rifiutarne l'accesso qualora ad es. il progetto non avesse una rilevanza scientifica.

51. Come dichiarato dalla stessa IQVIA, tra il XX e il XX è intervenuto un trasferimento degli asset aziendali dal gruppo Cegedim al Gruppo IMS Health con il conseguente passaggio della proprietà del database dapprima alla società IMS Health Information Solutions Italy S.r.l. e poi a IMS Health S.r.l. (che a seguire ha assunto la denominazione di IQVIA Solutions Italy S.r.l., nuovo nome del gruppo IMS Health a partire dal XX, (cfr. il contratto di collaborazione tra IMS Health Srl e SIMG, del XX).

52. Dall'esame del modello di accordo di collaborazione proposto dalla società IMS Health Information Solutions Italy S.r.l ai MMG è chiarito che "IMS ha realizzato un progetto denominato IMS LPD, per cui dispone di un programma ed è titolare di un database e del know how necessari e funzionali a raccogliere ed elaborare dati provenienti dall'ordinaria attività assistenziale del MMG al fine di condurre attraverso tali informazioni utilizzate sempre in forma aggregata e sempre garantendo l'assoluto anonimato dei pazienti […], la prosecuzione seppure con diverse forme e modalità dell'attuazione del progetto a suo tempo elaborato dalla SIMG e dall'Associazione Health Search […]".

53. Inoltre, per quel che qui rileva, da tale documento contrattuale emerge che l'"alimentazione e la gestione del "DataBase" avverrà attraverso l'utilizzo dell'evoluzione del software XX, come progressivamente sviluppato ed aggiornato" e che "IMS ha potuto verificare con adeguato controllo tecnico informatico e legale come la garanzia dell'assoluto anonimato dei dati che vengono ad essa trasmessi escluda la necessità che il Dottore acquisisca un esplicito consenso dei propri pazienti alla comunicazione dei dati ad IMS LPD in quanto […] sono anonimi", fermo l'obbligo del medico di informare i propri pazienti in ordine al trattamento di anonimizzazione dei dati "per lo svolgimento di analisi statistiche e di ricerche da parte di soggetti operanti nel settore medico e farmaceutico".

54. Il modello di contratto in esame (tra la società IMS Health Information Solutions Italy e i MMG) prevedeva inoltre la concessione al medico a titolo gratuito del programma, comprensivo non solo del gestionale e dei relativi servizi offerti ai medici ma anche dell'Add-on estrattore dei dati asseritamente anonimizzati per la trasmissione alla società IMS, poi successivamente denominata IQVIA Solutions Italy S.r.l.

55. Già da quanto appena illustrato emerge che la SIMG nel progetto in esame non ha mai avuto un "ruolo primario nella guida del progetto", come affermato da IQVIA.

56. Ma vi è di più, nel contratto di collaborazione tra IMS Health Srl (IQVIA) e la SIMG, sottoscritto il XX, viene ribadito che "IQVIA è proprietaria del database denonimato LPD, che l'alimentazione del database avviene attraverso l'utilizzo dell'evoluzione del software di gestione di cartella clinica denominato XX, [sviluppato dalla società XX srl] […] secondo le istruzioni e specifiche fornite da IQVIA".

57. In particolare, all'art. 2 di tale contratto è espressamente scritto che IQVIA si impegna a "b) continuare a fornire apposite istruzioni a XX affinche i dati inizialmente sensibili inseriti da MMG attraverso il software XX siano resi anonimi prima del loro inserimento nel data base LPD […]".

58. Tale accordo, in continuità con i precedenti, prevede inoltre che IQVIA si impegna a sostenere l'attività scientifica di SIMG attraverso l'utilizzo delle informazioni contenute nel database, con aggiornamenti semestrali fino al XX, data in cui tale attività è cessata, anche a seguito della citata sentenza del Tribunale di Milano del 10 maggio 2024.

59. Nel successivo contratto stipulato da SIMG con IQVIA, del XX, è nuovamente ribadito il ruolo attivo di IQVIA nella fornitura di specifiche istruzioni dalla stessa fornite alla società XX affinché i dati inseriti dai MMG attraverso il software XX siano resi anonimi prima del loro inserimento nel DB proprietario LPD e ciò è del resto confermato anche dal contratto che IQVIA ha sottoscritto con la società XX in data XX, nel quale

è previsto all'art. 2.6 che "XX garantisce che i dati contenuti nel database dei Medici Collaboranti, estratti mediante il Software, subiranno un processo di anonimizzazione, prima dell'invio all'infrastruttura di IQVIA, cosi come descritto nell'allegato A del presente contratto" proposto dalla stessa IQVIA.

60. "IMS ha potuto verificare con adeguato controllo tecnico informatico e legale come la garanzia dell'assoluto anonimato dei dati che vengono ad essa trasmessi escluda la necessità che il Dottore acquisisca un esplicito consenso dei propri pazienti alla comunicazione dei dati ad IMS LPD in quanto […] sono anonimi".

61. Ciò è altresì ribadito nel modello contrattuale tra IQVIA e i MMG in cui viene evidenziato che: il Medico ha altresì valutato ed apprezzato la circostanza che il "database" e la metodologia di raccolta dei dati inserita nel Programma e sviluppata su indicazione di IQVIA […] consente, come per il passato, il pieno rispetto della riservatezza e anonimato dei pazienti, non essendo essi in alcun modo identificabili né da IQVIA né da terzi ed essendo stata adottata ogni necessaria cautela tecnica ed organizzativa, in base alla costante evoluzione tecnologica, per garantire l'effettiva anonimizzazione dei dati portati a conoscenza di IQVIA".

62. Le evidenze contrattuali dimostrano pertanto un ruolo attivo della Società nella realizzazione del Progetto volto alla costituzione e alla alimentazione di un database in cui confluiscono i dati personali dei pazienti estratti dal gestionale di un numero significativo e rappresentativo di MMG associati alla SIMG, di cui la Società è divenuta proprietaria, a seguito delle diverse operazioni societarie, sopra illustrate.

63. La Società, si è sempre impegnata da un punto di vista tecnologico - vista la disponibilità di mezzi e di una idonea struttura organizzativa- a garantire la raccolta di dati asseritamente anonimizzati necessari in primo luogo per lo svolgimento della propria attività d'impresa e in secondo luogo per consentire alla SIMG - nella convinzione da parte di quest'ultima di fare affidamento in buona fede su un database anonimizzato - di pubblicare report aggregati a carattere scientifico elaborati sulla base dei dati presente nel database LPD.

64. La SIMG infatti come contropartita economica derivante dalla condivisione del database si è impegnata, sulla base del rapporto associativo con i MMG, ad offrire ad IQVIA pieno sostegno e collaborazione nella gestione dei rapporti con i MMG in modo da consentire ad IQVIA di poter contare e di conseguenza contrattualizzare, un numero di MMG idoneo a garantire un database di pazienti effettivamente rappresentativo della popolazione italiana, per poterlo poi riutilizzare per il perseguimento della propria attività d'impresa ed in particolare per effettuare studi sulla valutazione e l'analisi delle pratiche di cura effettuate dai MMG.

65. Nella fattispecie in esame è inoltre IQVIA che offre ai MMG a titolo gratuito la licenza d'uso del software XX e l'Add-on estrattore dei dati a fronte dell'impegno di questi ultimi di alimentare attraverso il predetto Add-on, il database con i dati dei propri pazienti, unitamente ad altri servizi offerti dal gestionale per meglio razionalizzare e rendere maggiormente efficace la gestione dei propri pazienti. Tutto ciò assicurando ai MMG e alla SIMG, sempre per il tramite della società XX che attraverso il citato Add-on sia realizzata l'anonimizzazione dei dati.

66. La Società pertanto utilizza i dati personali dei pazienti per la costituzione di un database proprietario, a fronte dei quali offre ai MMG servizi di razionalizzazione nella gestione dei propri pazienti, oltre alla licenza d'uso gratuita del software, remunerato dalla Società direttamente a XX e condivide con la SIMG i dati raccolti dai MMG a fronte dei citati servizi di pieno sostegno e collaborazione nella gestione dei rapporti in essere con gli stessi MMG in modo che la Società possa fare affidamento sul mantenimento con tali medici di rapporti contrattuali certi fondati sul loro impegno alla trasmissione dei dati oltre ad una attività di controllo, informazione e pubblicità affinché i MMG non collaboranti (ovvero non alimentanti il database), siano sostituiti con altri medici disposti ad aderite al progetto e dunque ad installare l'Add-on estrattore dei dati sul proprio gestionale.

67. Ciò posto, emergono rilevanti profili di criticità in ordine alla disciplina in materia di protezione dei dati personali per i motivi di seguito illustrati. 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 rappresentate) di conseguire tale obiettivo. Cionondimeno la rilevanza della società IQVIA e le specifiche competenze tecniche che le misure di anonimizzazione di ingenti quantità di dati sulla salute richiedono, hanno giustificato il legittimo affidamento sia dei MMG che di SIMG sulle funzionalità dell'Add-on, ritenuto effettivamente in grado di anonimizzare i dati.

6.2 Sul ruolo di titolare del trattamento della Società

68. In base alla normativa in materia di protezione dei dati personali è essenziale 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.

69. 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, par. 1, 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, par. 1, n. 8).

70. 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.

71. 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. WP 169, Parere 1/2010 sui concetti di "responsabile e incaricato del trattamento" del 16 febbraio 2010).

72. Le linee guida 07/2020 relative ai concetti di titolare del trattamento e responsabile del trattamento nel RGPD, adottate il 7 luglio 2021 dal CEPD, precisano che "Determinare le finalità e i mezzi equivale a decidere, rispettivamente, il «perché» e il «come» del trattamento: data un'operazione di trattamento specifica, il titolare del trattamento è il soggetto che ha determinato il perché del trattamento (ovverosia «a quale fine» o «per che cosa» viene svolto) e come tale obiettivo è raggiunto (ovverosia quali mezzi sono impiegati per conseguirlo)" (punto 35).Tali linee guida precisano inoltre che "i concetti di titolare del trattamento e responsabile del trattamento sono concetti funzionali: mirano a ripartire le responsabilità in funzione dei ruoli reali delle parti. [...]" In altri termini, "la ripartizione dei ruoli dovrebbe di norma risultare da un'analisi degli elementi fattuali o delle circostanze del caso di specie e, in quanto tale, non è negoziabile" (punto 12). "Occorre prendere in considerazione tutte le circostanze di fatto pertinenti al fine di stabilire se uno specifico soggetto eserciti un'influenza determinante sul trattamento dei dati personali in questione" (punto 25 Linee guida cit.; cfr. anche i provv.ti del 14 gennaio 2021,doc. web n. 9542136, doc. web n. 9542113; del 1° dicembre 2022,doc. web n. 9871846; del 27 novembre 2024, doc. web n. 10095810).

73. Da quanto sin qui esposto (cfr. par. 6.1), risulta accertato che il ruolo di IQVIA, che tra l'altro, in tutti i documenti contrattuali si qualifica come titolare del trattamento dei dati, non può limitarsi a quello di mero partner tecnologico e finanziario, come sostenuto dalla Società nelle proprie memorie difensive. Le modalità di realizzazione dell'anonimizzazione nell'ambito del Progetto, (risultata in concreto inefficace) sono definite dalle società che nel tempo si sono succedute nella proprietà del database che a loro volta le hanno commissionate alla società XX, nominata responsabile del trattamento ai sensi dell'art. 28 del Regolamento, sulla base delle istruzioni ricevute, da ultimo da IQVIA.

74. Ciò è altresì confermato dal documento prodotto da IQVIA e acquisito agli atti unitamente alle memorie difensive, in cui la stessa società XX, a seguito di specifica domanda posta da IQVIA in data antecedente al deposito delle memorie stesse, dichiara che "il formato [del tracciato record] non è stato cambiato rispetto all'allegato tecnico del Contratto […]". Come sopra già evidenziato, la Società XX ha sottoscritto il contratto di licenza d'uso di software e prestazione dei servizi connessi, proposto da IQVIA, nella sua prima versione, il XX, il quale reca le indicazioni sul processo di anonimizzazione dei dati prima dell'invio all'infrastruttura di IQVIA (cfr. art. 2.6 e allegato A)), poi successivamente rinnovato alla sua naturale scadenza, il XX, in cui è nuovamente precisato che XX "si impegna […] ad inviare un set informativo inclusivo di tutte le informazioni attualmente inviate, arricchito da ulteriori tabelle come descritto nell'allegato A" che reca appunto le istruzioni fornite da IQVIA.

75. Pertanto, rispetto al trattamento in esame, l'insieme delle operazioni realizzate dai diversi attori chiamati a trattare materialmente i dati in questione (il medico, la SIMG e la società XX) partecipano ad un medesimo

trattamento, composto da più fasi, che non possono essere considerate separatamente (sul punto cfr. la sentenza della Corte di giustizia del 29 luglio 2019, FashionID Gmbh, C-40/17 la quale ha precisato che dalla definizione di "trattamento" di cui all'art. 4 (2) del Regolamento "ne deriva che il trattamento dei dati personali può consistere in una o più operazioni, ciascuna delle quali riguarda una delle diverse fasi che possono essere incluse nel trattamento dei dati personali").

76. Al riguardo, rileva infatti come sia stata IQVIA a determinare sia la finalità (vale a dire la costituzione di un flusso di dati riferiti ai pazienti dei MMG aderenti al Progetto che consenta di alimentare il proprio database LPD) sia i mezzi di tali operazioni (scegliendo di continuare ad avvalersi dell'Add-on, estrattore dei dati dei pazienti dai gestionali dei MMG, sviluppato nel tempo dalla società XX, contrattualizzata dalla stessa IQVIA a seguito delle operazioni societarie intervenute nel tempo e nominata da quest'ultima responsabile del trattamento, ai sensi dell'art. 28 del Regolamento (cfr. contratti del XX e del XX).

77. Pertanto, se la Società ha accettato di utilizzare il software messo a disposizione da XX senza ulteriori verifiche sulla robustezza delle tecniche di anonimizzazione, tenuto anche conto delle evoluzioni medio tempore intervenute sul tema della anonimizzazione in particolare nel periodo compreso fino al XX, data di cessazione dell'invio dei dati da parte dei MMG, e di non apportare alcuna variazione nella struttura dei record di estrazione dell'Add-on, ciò non fa venir meno il proprio ruolo di titolare del trattamento. Infatti, per i motivi appena illustrati, la Società non solo risulta essere la proprietaria del citato database, ma anche il soggetto che intrattiene i rapporti contrattuali con i MMG e con la stessa società XX, fornitrice del software di asserita anonimizzazione dei dati, finalità perseguita principalmente dalla Società, tenuto conto che il database LPD è poi ulteriormente utilizzato da quest'ultima impresa, in particolare, per realizzare studi, basati su report aggregati estratti dal predetto database LPD.

78. Tale ruolo si desume altresì dalla circostanza che la Società pur non avendo apportato sostanziali modifiche all'Add-on in uso presso i MMG ha commissionato due assessment effettuati dalla società del Gruppo IQVIA XX nel XX e XX, al fine di valutare il rischio di re-identificazione sui dati presenti nel database proprietario di IQVIA, e anche dal documento da ultimo trasmesso al Garante in data XX, nel quale l'analisi del rischio di re-identificazione è aggiornato alla luce della recente sentenza della Corte di Giustizia del 4 settembre 2025 (C-413/23). Del resto il ruolo della SIMG non può avere una rilevanza tecnologica. La stessa ha certamente avuto un ruolo determinante nel pubblicizzare l'iniziativa al fine di far aderire al progetto in esame il maggior numero di medici visto il rapporto associativo con questi ultimi.

79. A ciò si aggiunga che, l'operazione di (presunta) anonimizzazione dei dati non può certamente essere imputabile al Medico, il quale è e resta titolare del trattamento dei dati personali di propri pazienti per finalità assistenziali. Quest'ultimo è infatti deputato a svolgere esclusivamente trattamenti finalizzati alla cura del paziente. Tale operazione di "anonimizzazione" è infatti in concreto realizzata solo ed esclusivamente a beneficio di IQVIA. Nella fattispecie in esame non sono i MMG ad anonimizzare i dati dei loro pazienti bensì IQVIA, che con il Progetto interviene presso i medici per anonimizzare dati di cui tra l'altro non dispone in origine.

80. Da ultimo, merita rilevarsi che la Società, quale titolare del trattamento ha effettuato la notifica violazione di dati personali ai sensi dell'art. 33 del Regolamento causata da un erroneo inserimento da parte dei MMG di dati personali dei pazienti e di altri medici nei campi di testo libero presenti nel gestionale dei MMG. Né tale inserimento può essere ritenuto erroneo da parte dei MMG in quanto volto a raccogliere ulteriori informazioni nel proprio gestionale utilizzato per finalità assistenziali, certamente ritenute rilevanti nello svolgimento delle proprie attività assistenziali. Al riguardo, la responsabilità è da imputare ad IQVIA la quale non ha verificato, commissionando l'implementazione di adeguate misure di sicurezza alla società XX- che l'Add-on non estraesse anche le informazioni presenti nei campi liberi del gestionale dei pazienti, non rilevanti ai fini del Progetto.

81. Per tutto quanto sopra esposto, l'Autorità rileva che la società IQVIA debba essere considerata responsabile dell'insieme delle operazioni attuate nell'ambito della costituzione del database LPD e pertanto titolare del trattamento ai sensi dell'art. 4, par. 1 (7) e 24 del Regolamento, e ciò sin dalla raccolta dei dati in questione, nonostante l'eventuale responsabilità degli altri attori con i quali la Società ha stipulato i relativi contratti.

6.3 La natura personale dei dati trattati

82. 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).

83. 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” (cons. 26 e 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).

84. I dati pseudonimizzati sono quindi dati personali che devono essere trattati nel rispetto del Regolamento. A tale riguardo, il Gruppo 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 (WP216, 05/2014 sulle tecniche di anonimizzazione adottato il 10 aprile 2014)”.

85. Le recenti Linee guida “01/2025 on Pseudonymisation”, nella versione oggetto di consultazione pubblica che si è conclusa il 14 marzo u.s., hanno chiarito che i dati pseudonimizzati sono sempre dati personali e che essa rappresenta una misura che permette di non attribuire i dati personali a uno specifico interessato senza l'ausilio di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure di sicurezza tecniche e organizzative. Infatti, se i dati possono essere ricondotti a persone fisiche dal titolare del trattamento o da altri, rimangono dati personali e sono dunque soggetti agli obblighi dettati dal Regolamento. Le predette Linee guida inoltre, esaminano le misure tecniche e le salvaguardie, nell’utilizzo della pseudonimizzazione, per assicurare la confidenzialità delle informazioni ed evitare l’identificazione non autorizzata degli interessati.

86. Il dato anonimizzato è tale solo se non consente l’identificazione diretta o indiretta di una persona tenuto conto di tutti i mezzi (economici, informazioni, risorse tecnologiche, competenze, tempo) nella ragionevole disponibilità di chi (titolare o altro soggetto) provi a utilizzare tali strumenti per identificare un interessato.

87. Un compiuto processo di anonimizzazione deve impedire che chiunque utilizzi tali dati, in combinazione con i mezzi “ragionevolmente disponibili”, 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).

88. Tali criteri sono ribaditi anche nelle recenti linee guida 02/2026 sull’anonimizzazione, adottate dal CEPD il 7 luglio del 2026 (in consultazione pubblica), e devono essere utilizzati per valutare l’efficacia delle tecniche di re-identificazione degli interessati. In particolare, nel predetto documento viene chiarito che “In generale, la (re)identificazione ha maggiori probabilità di successo su dati a livello di record con elevata dimensionalità e alta risoluzione, ma anche altri fattori sono importanti” e che “Se tutti e tre i criteri vengono soddisfatti, sia con l'approccio contestuale che con quello semplificato, i dati forniti possono essere considerati anonimi in tutta sicurezza. Se un qualsiasi criterio non viene soddisfatto, è necessario effettuare ulteriori analisi per determinare se i dati possano comunque essere considerati anonimi. In particolare, occorre verificare se eventuali record isolati, eventualmente insieme a dati collegati, consentano di identificare singoli individui” (cfr. parr. 3.4 e 3.5).

89. Inoltre, le predette linee guida sottolineano che la valutazione sulla robustezza delle tecniche di anonimizzazione non è sempre assoluta, ma può variare da un’entità all’altra. Invero, lo stesso dataset può comprendere dati personali per un soggetto che dispone di informazioni aggiuntive necessarie a re-

identificare gli interessati, e dato anonimo per chi non ne dispone ne può ragionevolmente procurarsene. Pertanto, non si valuta più il dato in sé ma il dato nella disponibilità di un soggetto determinato, con i suoi mezzi, il suo contesto e le sue relazioni.

90. Sempre in riferimento all'anonimizzazione dei dati, sotto altro profilo, si sottolinea che il Comitato europeo per la protezione dei dati ha 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, Opinion del 2014 cit. e Linee guida 2/2026 cit., par. 2.5.2). Ciò è stato confermato anche dal Tribunale di Milano (Sentenza del 10 maggio 2024).

91. Anche la Corte di giustizia dell'Unione europea è stata chiamata, in più occasioni, a pronunciarsi sulla nozione di dato personale, da ultimo con la sentenza SRB del 4 settembre 2025, la Corte ha precisato che i "dati pseudonimizzati non devono essere considerati, in ogni ipotesi e per ogni persona, come dati personali ai fini dell'applicazione del regolamento 2018/1725, poiché la pseudonimizzazione può, a seconda delle circostanze del caso, effettivamente impedire a persone diverse dal titolare del trattamento di identificare l'interessato, cosicché, per esse, quest'ultimo non sia o non sia più identificabile" (punto 86). La Corte ritiene a tal riguardo che, se le misure tecniche e organizzative di pseudonimizzazione possono avere l'effetto di far perdere ai dati il loro "carattere personale" per un destinatario, ciò presuppone tuttavia che, da un lato, tale destinatario "non sia in grado di rimuovere tali misure in occasione di qualunque trattamento [di detti dati] effettuato sotto il suo controllo" e, dall'altro, che "dette misure [siano] effettivamente [...] idonee a impedire [al destinatario] di attribuire i medesimi [dati] all'interessato anche mediante il ricorso ad altri mezzi di identificazione quali l'incrocio con altri elementi, cosicché, per tale società, l'interessato non sia o non sia più identificabile" (punto 77 CGUE, prima sezione, 4 settembre 2025, C-413/23; cfr. anche sentenza Breyer, CGUE, 2a sezione, 19 ottobre 2016, C-582/14 e sentenza OC c/ Commissione europea, CGUE, 6a sezione, 7 marzo 2024, C-479/22).

92. A tale riguardo, si evidenzia che la CGUE non ha inteso segnare una rottura rispetto alle proprie precedenti decisioni, bensì al contrario collocarsi nella loro continuità. La Corte ha ricordato che "la prospettiva rilevante per valutare il carattere identificabile dell'interessato dipende essenzialmente dalle circostanze che caratterizzano il trattamento dei dati in ciascun caso particolare" (punto 100 della sentenza, corsivo aggiunto). Essa precisa che "la pseudonimizzazione può, a seconda delle circostanze del caso, effettivamente impedire a persone diverse dal titolare del trattamento di identificare l'interessato, cosicché, per esse, quest'ultimo non sia o non sia più identificabile" (punto 87 della sentenza).

93. In particolare, la Corte di Giustizia con la citata Sentenza del 4 settembre 2025 nella causa C-413/23 ha chiarito come dati pseudonimizzati possono perdere la natura di "personali" se i destinatari non dispongono dei mezzi necessari per risalire all'identità individuale. Tuttavia, ciò non è automatico, ma dipende da una valutazione che deve essere fatta "case by case" sulla base delle circostanze del caso concreto. In particolare, per il destinatario le informazioni possono perdere la natura di dati personali se sono soddisfatte le seguenti condizioni:

1. Il destinatario non deve poter incidere sulle misure attuate dal primo titolare e non deve poter essere messo nelle condizioni di alterare tali misure

2. Il soggetto che riceve il dato, non deve re-identificare l'interessato, anche ricorrendo ad altri mezzi di identificazione come il controllo incrociato con altri elementi, in modo tale che, per il destinatario, l'interessato non sia o non sia più identificabile

3. il destinatario non può trasferire il nuovo dato ricevuto ad un altro soggetto.

94. Sulla base di tale quadro giuridico di riferimento l'Autorità, relativamente al rischio di re-identificazione degli interessati e al parametro valore K (k-anonymity) e ai due due assessment effettuati da XX su incarico di IQVIA nel XX e XX rileva quanto segue.

95. La k-anonymity mitiga il rischio di re-identificazione imponendo che ogni combinazione di taluni attributi della persona (ad es. località, età) sia condivisa da almeno k individui indistinguibili e raggruppati in c.d. classi di equivalenza. Occorre precisare che questo vincolo agisce esclusivamente su un sottoinsieme

degli attributi, i c.d. quasi-identificatori e non sull'intero record. Ne deriva un potenziale rischio residuale di singolarità: anche se una classe di equivalenza rispetta formalmente il requisito di numerosità, i record che la compongono possono risultare di fatto unici quando si considerano informazioni presenti in altri attributi, come diagnosi, sequenze di ricoveri o pattern di assunzione di farmaci. Un attaccante che sia in grado di osservare o misurare indipendentemente tali parametri e di riferirli a un soggetto specifico potrebbe identificare tale soggetto, rendendo inefficace la protezione offerta dalla k-anonymity.

96. D'altro canto, il semplice hashing delle identità non mitiga questo rischio, poiché non rimuove singolarità (anzi, esso è costruito per mantenerle in modo da riferire la storia clinica a un soggetto determinato), protegge solo la parte del record direttamente collegata all'identità dell'interessato rendendola inintelligibile, mentre l'unicità e dunque la riferibilità dal dato alla persona deriva dalla combinazione di attributi diversi dai quasi-identificatori che se rimangono invarianti nel tempo risultano altamente distintive. Questo fenomeno evidenzia un limite strutturale della k-anonymity: concentrare lo sforzo di anonimizzazione solo sui quasi-identificatori non è sufficiente quando altre caratteristiche visibili del record possono fungere esse stesse da identificatori di fatto.

97. L'applicazione di tecniche crittografiche (hash) al PAT ID del paziente non consentono di rimuovere l'associazione univoca tra un individuo e il codice con cui questo è sempre rappresentato in modo univoco all'interno della base dati (singolarità). Né questo rischio è rimosso interamente dall'applicazione della tecnica di k-anonymity applicata ai soli attributi quasi-identificatori, in quanto alcuni elementi del payload (ad es. dati riferibili a patologie, assunzioni di farmaci o altre informazioni di carattere sensibile), in particolare quando questo è molto ricco di dettagli raccolti in un arco di osservazione della persona prolungato nel tempo, possono essi stessi costituire elemento identificativo forte di singoli interessati e vanificare il beneficio atteso dalla creazione di classi di equivalenza di pur cospicua ampiezza.

98. In relazione alle argomentazioni contenute nella memoria e nel documento acquisito agli atti del procedimento in data 1° maggio 2026, l'Autorità rileva altresì che per stabilire se i mezzi possono ragionevolmente essere utilizzati per identificare la persona fisica, si dovrebbe tenere conto di tutti i fattori oggettivi, quali i costi dell'identificazione e il tempo necessario per effettuarla, tenendo conto delle tecnologie disponibili al momento del trattamento e degli sviluppi tecnologici ciò anche alla luce dei criteri definiti non solo citato parere sulle tecniche di anonimizzazione del 2014 ma altresì ribadito nelle recenti linee guida 2/2026, cit.

99. Nel caso di specie si rileva che la società IQVIA si trova in una situazione ben diversa rispetto alla fattispecie analizzata dalla Corte nella richiamata sentenza del 4 settembre 2025 ciò in quanto essa non può essere considerata un semplice destinatario di dati pseudonimizzati, ma deve essere considerata responsabile dell'intero trattamento attuato, e ciò sin dalla fase di raccolta dei dati presso le i MMG. Dalla documentazione contrattuale acquisita emerge infatti un ruolo attivo della Società nella definizione delle asserite misure di anonimizzazione dei dati, tramite più processi e attraverso diverse parti che vi intervengono. Pertanto il ruolo della Società quale titolare del trattamento non consente di considerare i dati acquisiti da IQVIA come oggettivamente anonimi alla luce delle circostanze del caso di specie.

100. Inoltre, i dati trattati dalla società IQVIA recano un patrimonio informativo molto rilevante che, grazie al medesimo PAT ID attribuito a ciascun paziente del MMG consente un monitoraggio longitudinale di ciascun paziente il quale con mezzi ragionevoli potrebbe essere re-identificato a prescindere dalla effettiva intenzione di IQVIA di re-identificare tali pazienti. È infatti sufficiente che essa abbia la capacità di re-identificarle, mediante mezzi ragionevoli, affinché i dati in questione siano da qualificarsi come dati personali. (cfr. decisione vincolante 1/2021 relativa al contenzioso sul progetto di decisione dell'autorità di controllo irlandese riguardante WhatsApp Ireland ai sensi dell'articolo 65, paragrafo 1, lettera a), del RGPD, adottata il 28 luglio 2021 e il recente provvedimento della CNIL contro la società IQVIA Francia, del 26 maggio 2026).

101. Nel caso in esame, tenuto conto del patrimonio informativo del database LDP (anno di nascita del paziente, sesso, stato civile, il numero dei suoi figli, la sua categoria socio-professionale, la o le date delle visite dal medico, la diagnosi formulata, i suoi sintomi, le sue allergie, il suo peso, la sua altezza, le sue prescrizioni farmacologiche, i suoi vaccini, i suoi esami o ancora i suoi certificati di malattia), in cui ogni paziente dispone di un identificativo che gli è proprio per un determinato medico, cui si aggiungono dati di localizzazione, ciò consente alla Società di isolare ciascun individuo e che i trattamenti in questione non

resistono al rischio di individualizzazione, come in particolare menzionato nel parere del Gruppo Art.29 sopra citato e ribadito nelle Linee guida 2/2026 cit., ciò anche attraverso il ricorso a fonti esterne.

6.4. La base giuridica del trattamento e gli oneri informativi

102. 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).

103. 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).

104. 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).

105. Posto quanto rilevato nei precedenti paragrafi le operazioni di trattamento in questione (in particolare la raccolta e l'asserita anonimizzazione dei dati personali dei pazienti dei MMG) sono svolte da IQVIA, in qualità di titolare del trattamento in assenza di una idonea base giuridica.

106. A tale proposito, si evidenzia che anche l'anonimizzazione dei dati costituisce anch'essa un trattamento che, seppure compatibile con la finalità iniziale della raccolta, necessita di una idonea base giuridica per poter essere effettuata, come già rilevato al par. 90. Resta pertanto fermo che tale trattamento nell'ambito del Progetto in esame, è stato effettuato dalla Società in assenza di una idonea base giuridica, in violazione dell'art. 5, par. 1, lett. a) del Regolamento.

107. Tale base giuridica, non può infatti 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 al trattamento dei dati di cui all'art. 9, par. 2 del Regolamento che, allo stato non sembra sussistere.

108. In base al Regolamento il trattamento delle particolari categorie di dai 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).

109. Tale manifestazione di volontà deve essere libera, specifica, informata, inequivocabile, revocabile ed esplicita. Nella fattispecie in esame, nessun consenso è stato prestato nei confronti del titolare al fine di effettuare il trattamento di asserita anonimizzazione dei dati. Pertanto, 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).

110. La Società inoltre 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 i MMG. Nei paragrafi che precedono 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.

111. Nonostante il modello contrattuale con i MMG prevedeva l'obbligo di questi ultimi di informare i pazienti che i loro dati sarebbero stati oggetto di anonimizzazione non può certo ritenersi tale adempimento compiuto dalla Società, inoltre l'informativa fornita non reca tutti gli elementi di cui all'art. 13 del Regolamento

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

6.5 Sul principio di limitazione della conservazione

113. Il Regolamento enuclea tra i principi applicabili al trattamento anche quello di limitazione della conservazione dei dati, il quale impone che i dati siano "conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato" (art. 5, par. 1 lett. e).

114. Nel corso delle attività ispettive è stato accertato che i dati più risalenti contenuti del DB LPD sono relativi all'anno XX e la Società al riguardo ha dichiarato che seppur non vengono trattati per gli studi dati che risalgono ad oltre 10 anni non è a conoscenza di una procedura di cancellazione dei dati. La stessa Società infatti, nella nota del XX, a scioglimento di una specifica riserva ha dichiarato che provvederà "a cancellare i dati dal database principale".

115. È del tutto non pertinente la documentazione prodotta e acquisita agli atti e in particolare il documento denominato "Policy di conservazione dei dati". In via preliminare esso riporta un periodo di validità dal XX al XX, quindi successivo agli accertamenti ispettivi svolti e in ogni caso essa indica in particolare i tempi di conservazione riferiti a documentazione, amministrativa, fiscale e legale.

116. Tutto ciò premesso, nel prendersi favorevolmente atto delle misure prontamente assunte dalla Società, risulta comunque accertata la violazione del principio di limitazione della conservazione dei dati nella misura in cui la Società ha omesso di definire idonee procedure di cancellazione dei dati personali i quali sono stati pertanto trattati, oltre il periodo necessario al conseguimento delle finalità per le quali i dati sono stati raccolti, avendo la stessa dichiarato che per il conseguimento delle finalità di ricerca scientifica di terze parte è necessaria una longitudinalità dei dati non superiore a 10 anni (art. 5, par. 1, lett. e) del Regolamento).

6.6 Sul ruolo dei MMG

117. Posto quanto sopra evidenziato in ordine al ruolo della Società quale titolare dei trattamenti in esame risulta altresì accertata la violazione dell'art. 28 del Regolamento, non avendo la Società nominato i MMG quali responsabili del trattamento, in relazione all'invio dei dati dei propri pazienti per la realizzazione dell'iniziativa della Società stessa.

118. Dalla documentazione prodotta ed in particolare dal modello di accordo sottoscritto dalla Società con i MMG aderenti al Progetto risulta che gli stessi sono autonomi titolari del trattamento, infatti dal predetto accordo non risulta che gli stessi siano stati indicati quali responsabile del trattamento ai sensi dell'art. 28 del Regolamento.

119. A tale riguardo si evidenzia che i MMG aderenti al progetto non possono ritenersi titolari del trattamento seppure limitato alla presunta anonimizzazione dei dati- desumibile anche dalla circostanza che nel modello di accordo di collaborazione tra la Società e il MMG quest'ultimo è tenuto ad informare i pazienti circa il fatto che "i dati personali saranno resi anonimi con tecniche di anonimizzazione che garantiscano la piena riservatezza delle informazioni, per poter essere utilizzati, sempre nel pieno anonimato del paziente, per lo svolgimento di analisi statistiche e ricerche da parte di soggetti operanti nel settore medico e farmaceutico", ciò in quanto i MMG nei trattamenti in esame non effettuano alcuna scelta circa le finalità e i mezzi di realizzazione dello stesso (cfr. le "Linee guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR").

120. Sul punto si rileva infatti che l'autonomia decisionale che il medico dovrebbe poter operare in qualità di titolare del trattamento risulta del tutto carente nell'ambito dell'operazione di (presunta) anonimizzazione. Sotto altro profilo, si rileva come la Società si sia sostanzialmente inserita nel rapporto contrattuale tra MMG e la società XX (responsabile del trattamento dei medici che acquistano il gestionale) 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 c. d. add-on.

6.7 Sulla violazione dei dati personali e sul principio di integrità e riservatezza

121. L'art. 5, par. 1, lett. f), del Regolamento stabilisce che i dati personali devono essere "trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali".

122. In proposito, l'art. 32 del Regolamento, concernente la sicurezza del trattamento, stabilisce che "tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio […]" (par. 1) e che "nel valutare l'adeguato livello di sicurezza si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati" (par. 2).

123. Il citato art. 32 prevede in particolare che le misure tecniche e organizzative devono essere idonee a garantire un livello di sicurezza adeguato al rischio e, tra le altre cose, assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento e prevedere una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento (par. 1, lett. b) e d) del Regolamento).

124. Alla luce della notifica di violazione dei dati personali, trasmessa ai sensi dell'art. 33 del Regolamento, risulta accertato che la Società ha fatto installare sul gestionale del MMG (software XX) un add-on per l'estrazione dei dati asseritamente anonimizzati sul quale, solo a seguito degli accertamenti ispettivi del Garante, è stata rilevata la presenza di campi a testo libero che hanno comportato un trattamento di dati personali direttamente identificativi (di pazienti e di medici) da parte di IQVIA, presenti nel proprio data base LPD, non solo in violazione del richiamato principio di liceità, correttezza e trasparenza e dei conseguenti obblighi informativi nei confronti degli interessati ma altresì del principio di integrità e riservatezza dei dati, in quanto non risultano essere state implementate misure tecniche ed organizzative atte a garantire un livello di sicurezza adeguato al rischio, ciò tenuto anche conto che i predetti dati personali, direttamente identificativi, di circa 3.370 pazienti sono stati altresì comunicati, alla SIMG, di cui 3.080 hanno riguardato anche dati sulla salute dei pazienti.

125. La Società infatti non ha implementato misure atte ad assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento nonché a valutarne regolarmente l'efficacia (art. 32, par. 1, lett. b) e d) del Regolamento).

126. Risulta pertanto accertato che anche la comunicazione dei dati personali dei pazienti alla SIMG è stata effettuata in violazione degli artt. 5, par. 1, lett. a), 12, 13 del Regolamento e che la Società ha effettuato un trattamento di dati personali il violazione del principio di integrità e riservatezza e degli obblighi in materia di sicurezza del trattamento (art. 5, par. 1, lett. f) e 32, del Regolamento).

6.8 Sui principi di responsabilizzazione e di privacy by design

127. Il titolare del trattamento deve inoltre 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; cfr. considerando 75 e 78).

128. I titolari quindi devono assumere una condotta attiva nell'applicazione dei principi, ponendosi l'obiettivo di ottenere un reale effetto di tutela, implementando misure tecniche e organizzative adeguate ad attuare i principi di protezione dei dati, integrando nel trattamento le necessarie garanzie per adempiere ai requisiti e tutelare i diritti e le libertà degli interessati.

129. 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.

130. 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 adottate (cfr. Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, adottate il 13 novembre 2019 dal CEPD).

131. In relazione alla violazione dei dati personali, al fine di garantire il rispetto del citato principio di privacy by design, in particolare, il considerando 78 del Regolamento suggerisce una responsabilità dei titolari, ossia quella di valutare costantemente se stiano utilizzando, in qualunque momento, i mezzi appropriati di trattamento e se le misure implementate garantiscano l'integrità e la riservatezza dei dati personali. Inoltre, i titolari dovrebbero effettuare revisioni periodiche delle misure di sicurezza poste a presidio e tutela dei dati personali, nonché della procedura per la gestione delle violazioni dei dati. L'obbligo di mantenere, verificare e aggiornare, ove necessario, il trattamento si applica anche ai sistemi preesistenti. Ciò implica che anche i sistemi progettati prima dell'entrata in vigore del Regolamento devono essere sottoposti a verifiche e manutenzione per garantire l'applicazione di misure e garanzie che mettano in atto i principi e i diritti degli interessati in modo efficace (cfr. le Linee guida 4/2019, cit.).

132. Le condotte omissive sopra descritte in relazione alla liceità, correttezza e trasparenza dei trattamenti, alla puntuale definizione ed ex ante dei tempi di conservazione dei dati in base allo scopo della raccolta e alla loro successiva cancellazione, alla individuazione dei ruoli di protezione dei dati personali dei diversi soggetti coinvolti nelle operazioni di trattamento, all'assenza della valutazione d'impatto e da ultimo all'assenza di controlli ex ante sul software della Società XX utilizzato dai MMG per l'invio dei dati alla Società e di controlli anche automatizzati ex post sul data base LPD che avrebbero consentito alla Società stessa di rilevare la presenza di campi liberi e dunque di dati personali nel predetto data base, fanno rilevare un atteggiamento non sufficientemente responsabile da parte della Società in relazione ai dati trattati.

133. Medesime considerazioni devono svolgersi in particolare in relazione alla valutazione della natura anonima o meno dei dati raccolti presso i MMG, atteso che la Società, in qualità di titolare del trattamento si è basata esclusivamente sui generici assessment condotti dalla società Canadese, accettando in maniera passiva l'asserita natura anonima delle informazioni ricevute e fornendo inoltre informazioni non complete alla luce di quanto emerso a seguito della notifica di violazione dei dati personali ai sensi dell'art. 33 del Regolamento, ciò nonostante i precedenti provvedimenti di natura amministrativa a e giurisdizionale intervenuti sul tema, non solo a livello nazionale ma anche europeo, dove il gruppo IQVIA svolge analoghe attività (cfr. da ultimo provvedimento della CNIL del 26 maggio 2026)

134. Non risulta, nello specifico che la Società abbia, a seguito delle decisioni intervenute sul tema, svolto ulteriori analisi non solo sul rischio di re-identificazione degli interessati ma anche sulle caratteristiche del software della Società XX di raccolta dei dati dei pazienti dei MMG, sulla base di criteri oggettivi e di indicatori misurabili, se del caso anche attraverso l'impiego di strumenti automatizzati, affinché in via preliminare fosse verificata la presenza di campi liberi, che come noto presentano rischi elevati per i diritti e le libertà degli interessati e in subordine, con specifico riferimento al rischio di re-identificazione degli interessati, l'occorrenza percentuale di casi di single-out al fine di poterla stimare quantitativamente, anziché essere semplicemente esclusa sulla base di meri controlli inidonei a fornire sufficienti garanzie di efficacia in presenza, come nel caso in esame, di trattamenti su larga scala (elevati volumi di dati, significativa varietà degli attributi, ampia estensione geografica dei trattamenti).

135. Tutto quanto sopra determina una violazione il principio responsabilizzazione e di privacy by design, (artt. 5, par. 2 e 25 del Regolamento).

6.9 Sulla valutazione d'impatto

136. In base al Regolamento quando un tipo di trattamento, prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i

diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali (art. 35 del Regolamento e Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del regolamento 2016/679 - WP248rev.01 adottate il 4 aprile 2017 come modificate e adottate da ultimo il 4 ottobre 2017).

137. Il titolare, prima di procedere al trattamento, consulta l'autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati, a norma dell'articolo 35 del Regolamento, indichi che il trattamento presenta un rischio elevato in assenza di misure adottate dal titolare per attenuare il rischio (art. 36 del Regolamento).

138. Dall'istruttoria e dalle dichiarazioni rese dalla Società, risulta accertato che il trattamento svolto rientra tra quelli per i quali il titolare è tenuto ad effettuare, "prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali" (art. 35 del Regolamento). Ciò, in quanto, per tale trattamento, ricorrono certamente due dei criteri indicati dal Comitato Europeo per la protezione dei dati per individuare i casi in cui un trattamento debba formare oggetto di una valutazione di impatto.

139. In particolare, si fa riferimento ai seguenti criteri: "dati sensibili o aventi carattere altamente personale", "dati relativi ad interessati vulnerabili" tra i quali si annoverano i pazienti (cfr. Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679 adottate il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 -WP 248 rev.01, III, lett. B, punti 4 e 7). Con riferimento al caso di specie, possono essere, inoltre, potenzialmente soddisfatti anche i seguenti criteri: "trattamento di dati su larga scala" e "uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative" (cfr. richiamate Linee guida, III, lett. B, punti 5 e 8).

140. Tutto ciò premesso, la Società seppure si sia limitata ad avviare il processo di elaborazione della valutazione d'impatto, non avendo completato il predetto processo, ciò nonostante il trattamento sia iniziato a partire dal 2015 e non avendo prodotto tale documento nel corso dell'istruttoria ha violato quanto previsto dall'art. 35 del Regolamento in ordine all'obbligo la predetta valutazione d'impatto.

7. Conclusioni

141. 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 acquisiti e le difese addotte dal titolare del trattamento, non sono idonee a superare i rilievi formulati dall'Ufficio e, peraltro, non ricorre alcuno dei casi previsti dall'art. 11 del regolamento n. 1/2019.

142. Pertanto, l'Autorità rileva l'illiceità della condotta posta in essere IQVIA, in violazione degli articoli 5, par. 1 lett. a), e), f) e par. 2, 9, 13, 25, 28, 32 e 35 del Regolamento.

8. Misure correttive

143. L'art. 58, par. 2, del Regolamento attribuisce al Garante 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" (lett. d).

144. La Società nelle proprie memorie difensive ha dichiarato che il "Data Warehouse costituiva il database di riferimento per le attività di produzione di IQVIA Italia, […], prima dell'interruzione di qualunque attività dall'XX ("Data Warehouse LPD")" e tale circostanza è stata confermata dalla Società con nota del XX in riscontro alla richiesta di informazioni dell'Ufficio del XX (prot. n. XX). A tale riguardo, alla luce delle valutazioni sopra richiamate, si ritiene necessario, qualora la Società intenda proseguire l'attività svolta nei termini e secondo le modalità esaminate, di ingiungere a quest'ultima, ai sensi dell'art. 58, par. 2, lett. d) Regolamento, le seguenti misure correttive:

- individuare una idonea base giuridica per poter effettuare il trattamento dei dati personali dei pazienti dei MMG, ivi inclusa l'eventuale anonimizzazione dei dati;

- ottemperare agli obblighi informativi nei confronti dei pazienti dei MMG, ai sensi dell'art. 13 del Regolamento;

- svolgere la valutazione d'impatto, ai sensi dell'art. 35 del Regolamento;

- nominare i MMG responsabili del trattamento, ai sensi dell'art. 28 del Regolamento.

145. In alternativa, il processo di anonimizzazione dei dati dovrà essere svolto dai MMG conformemente al quadro normativo vigente (in particolare, in termini di base giuridica del trattamento e di adempimento da parte di questi ultimi agli obblighi informativi nei confronti dei loro pazienti) e alle indicazioni da ultimo fornite dal CEPD nelle citate linee guida 2 del 2026. Di talché, è necessario garantire quanto segue.

1. Determinazione indipendente delle misure di pseudonimizzazione.

146. IQVIA non dovrà determinare le modalità di pseudonimizzazione applicate ai dati oggetto di comunicazione. I soggetti mittenti (i medici) dovranno individuare autonomamente gli attributi dei dati personali dei propri pazienti da sottoporre a pseudonimizzazione (ad es. mediante hashing) e applicare meccanismi di codifica caratterizzati da un elemento casuale di adeguata complessità, debitamente documentato, tali da rendere il valore codificato, dal punto di vista di IQVIA, una sequenza priva di significato semantico e non riconducibile a schemi prevedibili o reversibili mediante mezzi ragionevolmente disponibili.

2. Individuazione dei quasi-identificatori e dimensionamento delle classi di equivalenza

147. IQVIA e i soggetti mittenti potranno definire preventivamente gli attributi da trattare quali quasi-identificatori e le relative tecniche di generalizzazione o trasformazione (k-anonimity). Gli attributi così individuati dovranno essere trattati in modo tale che le corrispondenti classi di equivalenza risultanti presentino, in ogni caso, una numerosità non inferiore a 10 unità.
3. Valutazione delle variabili residue rispetto alla capacità di osservazione e misura di IQVIA

148. Tutte le ulteriori variabili non sottoposte a pseudonimizzazione (hashing) (punto 1) e non considerate nella determinazione delle classi di equivalenza (punto 2) dovranno essere oggetto di una specifica valutazione rispetto alla loro osservabilità e misurabilità da parte di IQVIA, tenendo conto delle informazioni e dei mezzi ragionevolmente disponibili a quest'ultima. Qualora tali variabili risultino osservabili o misurabili da IQVIA e siano suscettibili di contribuire all'identificazione, esse dovranno alternativamente:

a) essere ricomprese tra i quasi-identificatori e concorrere alla determinazione delle classi di equivalenza, che dovranno comunque mantenere una cardinalità non inferiore a 10 unità; oppure,

b) essere trattate mediante tecniche di elaborazione distribuita che consentano a IQVIA una elaborazione del dato basata su porzioni del dato stesso (c.d. shares) e che impediscano a quest'ultima di acquisire il dato originario nella sua totalità e in chiaro, quali protocolli di secure multiparty computation o tecniche equivalenti; oppure

c) essere rimosse.

149. Qualora IQVIA decidesse di comunicare ulteriormente i dati ricevuti dai MMG a terzi soggetti, quest'ultima in qualità di mittente di tale nuova comunicazione di dati, è soggetta alle medesime prescrizioni ivi previste in capo ai MMG quali mittenti del primo flusso di comunicazione delle informazioni dei propri pazienti alla stessa IQVIA.

150. Ai sensi degli artt. 58, par. 1, lett. a), del Regolamento e 157 del Codice, la Società dovrà provvedere a comunicare all'Autorità, fornendo un riscontro adeguatamente documentato, entro 120 giorni dalla notifica del presente provvedimento, le iniziative intraprese al fine di dare attuazione a quanto sopra ingiunto ai sensi del citato art. 58, par. 2, lett. d), del Regolamento.

9. ORDINANZA INGIUNZIONE

151. La violazione degli artt. 5, par. 1 lett. a), e), f) e par. 2, 9, 13, 25, 28, 32 e 35 del Regolamento, causata dalla Società IQVIA Solutions Italy S.r.l. è soggetta all'applicazione della sanzione amministrativa pecuniaria, ai sensi dell'art. 83, par. 4, lett. a) e par. 5, lett. a) e b) del Regolamento.

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

153. Tenuto conto che la violazione delle predette disposizioni ha avuto luogo in conseguenza di un'unica condotta, ovvero in relazione allo stesso trattamento o trattamenti tra loro collegati, trova applicazione l'art. 83, par. 3, del Regolamento, ai sensi del quale l'importo totale della sanzione amministrativa pecuniaria non supera l'importo specificato per la violazione più grave. Considerato che, nel caso di specie, le violazioni più gravi sono soggette alla sanzione prevista dall'art. 83, par. 5, del Regolamento, l'importo della sanzione è da quantificarsi, nel massimo, in euro 20.000.000 ovvero, per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente se superiore.

9.1 Quantificazione della sanzione amministrativa

154. Per la determinazione del massimo edittale della sanzione pecuniaria occorre fare riferimento al fatturato dell'impresa, intesa ai sensi degli artt. 101 e 102 del TFUE come chiarito dal considerando 150 del Regolamento.

155. Poiché dalla documentazione in atti risulta che:

> IQVIA Solutions Italy S.r.l. è una società controllata al 100% dalla Società IQVIA Holdings INC. con sede legale negli Stati Uniti;
>
> il gruppo IQVIA si presenta, in particolare sul suo sito web www.iqvia.com, come un'entità unica, quale "leader mondiale nella ricerca clinica e nei dati sanitari", elaborando più di 120 miliardi di dati sanitari all'anno e conducendo più di 500 studi in più di 75 paesi". Ciò consente dunque di ritenere che le società IQVIA Holdings INC e IQVIA Solutions Italy S.r.l. costituiscano un'unica entità economica, ai sensi dell'articolo 101 TFUE;
>
> la documentazione tecnica prodotta dalla Società sul rischio di re-identificazione degli interessati nel corso dell'istruttoria, è stata elaborata dalla Società XX, società del Gruppo IQVIA Holdings INC;
>
> la Corte di Giustizia ha stabilito che quando una controllata è direttamente o indirettamente posseduta al 100% dalla sua società controllante, "da un lato, tale società controllante può esercitare un'influenza determinante sul comportamento [della] controllata [...] e dall'altro esiste una presunzione semplice secondo cui la detta società controllante esercita effettivamente un'influenza determinante sul comportamento della propria controllata" (sentenza del 10 settembre 2009, C-97/08, paragrafo 60).

Tanto premesso, in conformità con la giurisprudenza sopra menzionata della Corte di giustizia, si ritiene che vi sia la presunzione che IQVIA HOLDINGS INC. eserciti un'influenza decisiva sulle attività della sua controllata italiana, IQVIA Solutions Italy S.r.l. e pertanto si prenderà come riferimento il fatturato indicato nell'ultimo bilancio consolidato disponibile (XX) della società IQVIA Holding INC (cfr. CEPD, Linee guida 4/2022 sul calcolo delle sanzioni amministrative pecuniarie ai sensi del GDPR, 24 maggio 2023, §6.1.2), conseguentemente, si determina il massimo edittale, nel caso in argomento, fino al 4 % di tale fatturato in quanto superiore ad euro 20.000.000.

156. L'ammontare della sanzione amministrativa pecuniaria va determinata in funzione delle circostanze di ogni singolo caso, tenendo in debito conto i seguenti elementi previsti dall'art. 83, par. 2, del Regolamento:

- la gravità della violazione (art. 83, par. 2, lett. a) del Regolamento), in relazione alla natura (concernente l'inosservanza dei principi generali di liceità, correttezza e trasparenza, nonché di quelli di limitazione della conservazione di integrità e riservatezza, di privacy by design e di responsabilizzazione), alle modalità (pluralità di condotte illecite che si sono protratte nel tempo, numero elevato di interessati coinvolti nella violazione e categoria di dati personali trattati, che per loro natura sono con particolarmente sensibili sotto il profilo dei diritti e delle libertà fondamentali);

quale fattore aggravante, il carattere colposo della violazione (art. 83, par. 2, lett. a), b) e g) del Regolamento);

quale fattore attenuante, la circostanza che la Società ha svolto nel tempo delle verifiche sul rischio di re-identificazione degli interessati (cfr. assessment della società Privacy Analitycs e doc. da ultimo trasmesso il 25 maggio 2026) (art. 83, par. 2, lett. c) del Regolamento);

quale fattore attenuante, che i MMG a partire dal XX hanno sospeso qualsiasi trasmissione di dati dei pazienti al database proprietario LPD (art. 83, par. 2, lett. c) del Regolamento);

quale fattore attenuante, misure rafforzate di pseudonimizzaione dei dati (art. 83, par. 2, lett. c) del Regolamento)

quale fattore attenuante, il fatto che non risultano precedenti violazioni pertinenti commesse dal titolare del trattamento nel territorio nazionale né sono stati precedentemente disposti provvedimenti di cui all'art. 58 del Regolamento (art. 83, par. 2, lett. e) del Regolamento);

quale fattore attenuante, il fatto che in relazione ai trattamenti in esame, non sono pervenuti segnalazioni o reclami degli interessati (art. 83, par. 2, lett. k) del Regolamento).

quale fattore ulteriormente attenuante, la cooperazione dimostrata con l'Autorità nel corso del presente procedimento (art. 83, par. 2, lett. f), Regolamento);

157. In base al complesso degli elementi sopra indicati e ai principi di effettività, proporzionalità e dissuasività previsti dall'art. 83, par. 1, del Regolamento, e tenuto conto del necessario bilanciamento fra i diritti degli interessati e la circostanza il database LPD di IQVIA è stato creato quale risorsa di riferimento per l'informazione sanitaria in Italia e a livello internazionale - utilizzato per condurre studi, analisi di economia sanitaria, valutazioni farmacoepidemiologiche, anche al fine di limitare l'impatto economico della sanzione sulle esigenze organizzative e funzionali della Società, si ritiene debba applicarsi la sanzione amministrativa del pagamento di una somma di euro 7.000.000,00 (sette milioni/00) per la violazione degli artt. 5, par. 1 lett. a), e), f) e par. 2, 9, 13, 25, 28, 32 e 35 del Regolamento.

9.2 Sanzione accessoria

158. Nel caso in argomento si ritiene che debba applicarsi anche la sanzione accessoria della pubblicazione sul sito del Garante della presente ordinanza ingiunzione, prevista dall'art. 166, comma 7 del Codice e art. 16 del Regolamento del Garante n. 1/2019, tenuto conto della peculiare natura dei dati oggetto del trattamento dedotto in contestazione, in quanto inerenti ai dati sulla salute di un rilevante numero di interessati appartenenti alle particolari categorie, che nel Regolamento godono di una tutela rafforzata alla luce dei rischi che il trattamento di tali dati può comportare per i diritti e le libertà degli interessati, nonché della tipologia delle violazioni accertate che hanno interessato i principi generali del trattamento, in particolare il principio di liceità, correttezza e trasparenza, di limitazione della conservazione, di integrità e riservatezza di responsabilizzazione e di privacy by design.

TUTTO CIO' PREMESSO IL GARANTE

159. ai sensi degli artt. 57 e 83 del Regolamento, dichiara l'illiceità del trattamento posto in essere dalla società IQVIA Solutions Italy S.r.l., con sede legale in via Fabio Filzi 29, Milano, P.IVA: 00868270158 per la violazione degli artt. 5, par. 1 lett. a), e), f) e par. 2, 9, 13, 25, 28, 32 e 35 del Regolamento, nei termini di cui in motivazione, e:

a) ai sensi dell'art. 58, par. 2, lett. d) del Regolamento, ingiunge al titolare del trattamento di conformarsi, entro il termine di 120 giorni dalla data della notifica del presente provvedimento, alle prescrizioni formulate al paragrafo 8 del presente provvedimento;

b) ai sensi dell'art. 58, par. 1, lett. a) del Regolamento e dell'art. 157 del Codice, prescrive al titolare del trattamento di comunicare all'Autorità, entro il termine di 120 giorni dalla notifica del presente provvedimento, un riscontro adeguatamente documentato, ai sensi dell'art. 157 del Codice, recante le iniziative intraprese al fine di dare attuazione alle misure imposte al punto 8;

l'eventuale mancato riscontro può comportare l'applicazione della sanzione amministrativa pecuniaria prevista dall'art. 83, par. 5, lett. e) del Regolamento;

ORDINA

160. al predetto titolare, ai sensi degli artt. 58, par. 2, lett. i) e 83 del Regolamento, nonché dell'art. 166 del Codice, di pagare la somma di euro 7.000.000,00 (sette milioni/00) a titolo di sanzione amministrativa pecuniaria per le violazioni indicate nel presente provvedimento;

INGIUNGE

161. al predetto titolare del trattamento, in caso di mancata definizione della controversia ai sensi dell'art. 166, comma 8, del Codice, di pagare la somma di euro 7.000.000,00 (sette milioni/00) secondo le modalità indicate in allegato, entro 30 giorni dalla notificazione del presente provvedimento, pena l'adozione dei conseguenti atti esecutivi a norma dell'art. 27 della legge n. 689/1981.

162. Si rappresenta che, ai sensi dell'art. 166, comma 8, del Codice, resta salva la facoltà per il trasgressore di definire la controversia mediante il pagamento – sempre secondo le modalità indicate in allegato – di un importo pari alla metà della sanzione irrogata entro il termine di cui all'art. 10, comma 3, del d.lgs. 1° settembre 2011, n. 150 previsto per la proposizione del ricorso come di seguito indicato;

DISPONE

163. ai sensi dell'art. 166, comma 7, del Codice e dell'art. 16, comma 1, del Regolamento del Garante n. 1/2019, la pubblicazione dell'ordinanza ingiunzione sul sito internet del Garante;

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

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

166. Ai sensi dell'art. 78 del Regolamento, nonché degli artt. 152 del Codice e 10 del d.lgs. 1° settembre 2011, n. 150, avverso il presente provvedimento è possibile proporre opposizione all'autorità giudiziaria ordinaria, con ricorso depositato presso il tribunale ordinario del luogo individuato nel medesimo art. 10, a pena di inammissibilità, entro il termine di trenta giorni dalla data di comunicazione del provvedimento ovvero entra sessanta giorni se il ricorrente risiede all'estero.

Roma, 23 settembre 2026

IL PRESIDENTE
Stanzione

IL RELATORE
Cerrina Feroni

IL SEGRETARIO GENERALE
Montuori

---

(1) IQVIA è un fornitore leader a livello globale di analisi avanzate, soluzioni tecnologiche e servizi di ricerca clinica per il settore delle scienze della vita. Grazie alle sue capacità di analisi, alle tecnologie innovative, alle risorse di big data e alla vasta esperienza nel settore, IQVIA crea connessioni intelligenti in tutti gli aspetti dell'assistenza sanitari (https://www.iqvia.com/it-it/about-us).