GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Provvedimento del 17 settembre 2020 [9479364]

[doc. web n. 9479364]

Provvedimento del 17 settembre 2020

Registro dei provvedimenti
n. 158 del 17 settembre 2020

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, vice presidente, il dott. Agostino Ghiglia, l'avv. Guido Scorza, componenti e il dott. Claudio Filippi, vice segretario generale;

VISTO il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, 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, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) 2016/679 (d.lgs. 30 giugno 2003, n. 196, come modificato dal d.lgs. 10 agosto 2018, n. 101, di seguito "Codice");

VISTO il d.lgs. 10 agosto 2018, n. 101, recante Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del 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);

VISTO il d.m. 15 luglio 1997 e ss.mm. recante "Recepimento delle linee guida dell'Unione europea di buona pratica clinica per la esecuzione delle sperimentazioni cliniche dei medicinali";

VISTE le Linee guida per i trattamenti di dati personali nell'ambito delle sperimentazioni cliniche di medicinali, adottate dal Garante il provvedimento del 24 luglio 2008, doc. web n. 1533155;

VISTO il Regolamento n. 1/2019 concernente le procedure interne aventi rilevanza esterna, finalizzate allo svolgimento dei compiti e all'esercizio dei poteri demandati al Garante per la protezione dei dati personali, approvato con deliberazione del n. 98 del 4/4/2019, pubblicato in G.U. n. 106 dell'8/5/2019 e in www.gpdp.it, doc. web n. 9107633 (di seguito "Regolamento del Garante n. 1/2019");

Vista la documentazione in atti;

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

Relatore il dott. Agostino Ghiglia;

PREMESSO

1. La violazione di dati personali

Con nota del 10 ottobre 2019, l'Ospedale Pediatrico Bambino Gesù di Roma (di seguito OPBG), in qualità titolare del trattamento (ai sensi degli artt. 4, par. 1, n. 7 e 24 del Regolamento) e centro di sperimentazione dello studio clinico PH108 "The safety and efficacy of Prohance at the dose of 0.10 mmol/Kg in magnetic resonance imaging of the central nervous system in pediatric patients who are younger than two years of age", (Studio) ha notificato, ai sensi dell'art. 33 del Regolamento, una violazione di dati personali, dichiarando che: "la clinical monitor (personale della CRO -Contract Research Organization-) ha ritirato le CRF (Case Report Form) di 10 pazienti ma non ha ritirato i report degli esami di laboratorio e degli esami di Risonanza Magnetica come invece previsto dalla CRF e dal "Monitoring Plan". La clinical monitor ha quindi richiesto i report ad una collaboratrice dello Sperimentatore del Centro la quale ha inviato via email alla clinical monitor la scansione dei report dei 10 pazienti in data 07.09.2019. La clinical monitor ha inoltrato le scansioni ricevute alla study manager di Bracco Imaging S.p.A., che a sua volta le ha inoltrate alla study manager di Bracco Diagnostics Inc. (BDI) in data 09.09.2019. I report ricevuti presentano nome e cognome dei pazienti mascherati con un pennarello nero ma ancora visibili se esaminati con attenzione, nonostante il protocollo preveda che il Centro prima dell'invio allo sponsor debba deidentificarli e identificarli tramite il solo codice identificativo assegnato al paziente all'inclusione nello studio. La study manager di BDI, durante la verifica dei dati contenuti nei report rispetto ai dati presenti nelle CRF, si è accorta che la deidentificazione non era stata eseguita in modo adeguato e pertanto ha avviato la segnalazione al Data Protection Officer di Bracco Imaging S.p.A. in data 4 ottobre 2019 alle ore 22:50 (ora italiana) (…)".

Nell'atto di notifica, l'OPBG ha precisato che la violazione è occorsa il 28 agosto 2019 e di esserne venuto a conoscenza, il 7 ottobre 2019, dalla società Bracco Imaging S.p.A., promotore dello studio che a sua volta ha notificato gli eventi descritti all'Autorità ai sensi dell'art. 33 del Regolamento.

2. L'attività istruttoria

Con riferimento alla predetta violazione, nell'ambito dell'istruttoria preliminare avviata dall'Ufficio del Garante, l'OPBG ha rappresentato, ai sensi dell'art 168 del Codice, che la richiamata violazione di dati personali si è verificata nel contesto dello studio clinico osservazionale retrospettivo PH108 "The safety and efficacy of Prohance at the dose of 0.10 mmol/Kg in magnetic resonance imaging of the central nervous system in pediatric patients who are younger than two years of age" di cui è centro di sperimentazione, mentre la Società Bracco Imaging S.p.A. ne è il promotore (di seguito Bracco).

Rispetto al trattamento dei dati personali dei soggetti arruolati nello studio, promotore e sperimentatore, in base ad uno specifico accordo, sottoscritto in data 6 maggio 2019, si sono qualificati autonomi titolari del trattamento, convenendo, nel medesimo atto, che fosse compito della Bracco individuare la CRO e nominarla responsabile del trattamento (ai sensi dell'art. 28 del Regolamento) e che spettasse, invece, all'OPBG l'onere di incaricare formalmente il proprio personale addetto allo studio e di comunicare al promotore e/o alla CRO, dallo stesso individuata, i dati necessari allo sviluppo dello studio, conformemente al protocollo e al rispetto degli obblighi di monitoraggio e controllo di cui alla normativa di settore applicabile (art. 16 del richiamato accordo).

È stato rappresentato, inoltre, che l'OPBG ha adottato uno specifico "regolamento per la conduzione degli studi clinici" e un'apposita "procedura conduzione di studi clinici" in base alla quale è, tra le altre cose, previsto che il personale coinvolto nei temi di ricerca riceva una formazione specifica inerente alle "good clinal practice" con periodico "retreaning", all'interno della quale vengono trattati anche i temi inerenti al trattamento dei dati personali nel contesto specifico degli studi.

Con specifico riferimento all'applicazione del principio di minimizzazione dei dati, l'OPBG ha evidenziato che i dati oggetto dello studio sono presenti su due sistemi software dell'Ospedale -OPB Clinico ed il sistema RIS/PAS- che sono stati appositamente predisposti per consentire l'accesso per finalità connesse allo studio al solo personale sanitario coinvolto nello studio stesso. Tali sistemi consentono la profilazione degli accessi, la disconnessione temporizzata, la produzione di supporti ottici per la consegna dati a scopo di studio/trial ed altre attività preliminarmente autorizzate, scambio di dati.

È stato poi precisato che sussiste uno software per la "anonimizzazione" dei dati necessari agli studi che vengono normalmente messi a disposizione della CRO secondo le specifiche dei protocolli attraverso supporto ottico o per posta elettronica.

Con specifico riferimento alla violazione occorsa, è stato precisato che la comunicazione alla CRO dei dati degli esami di laboratorio e degli esami di risonanza magnetica, relativi ai 10 pazienti minori di età arruolati nello Studio, sarebbe avvenuta, per un errore umano, previa effettuazione di un'operazione di "anonimizzazione" differente rispetto a quella concordata per lo Studio e utilizzata per la comunicazione dei CRF.

L’OPBG ha, infine, rappresentato come la violazione non abbia determinato conseguenze dannose per gli interessati, in quanto i dati violati sono stati oggetto di accesso solo da parte di operatori che, seppur in relazione ad altre fasi del trattamento, erano comunque autorizzati ad accedervi e soggetti a specifici obblighi di riservatezza. Tali dati, inoltre, sarebbero stati trasmessi comunque in forma “deidentificata” ancorché secondo una procedura differente da quella concordata con lo sponsor.

L’OPBG ha, infine, precisato che, in ragione della violazione di cui trattasi, è stata “avviata una verifica interna con la collaborazione del Principal Investigator (…) al fine di comprendere la motivazione dell’accaduto. Una volta appurata la straordinarietà dell’evento dovuto ad errore umano è stata avviata una procedura di revisione, attualmente in corso, del “Regolamento per conduzione degli studi clinici” e la realizzazione di un’apposita procedura da inserire nel sistema qualità dedicata nello specifico alle modalità di anonimizzazione dei dati personali alla quale seguirà apposita attività formativa specifica degli operatori coinvolti nella procedura medesima” (cfr. nota del 15 gennaio 2020, prot. n. 69).

Sulla base degli elementi acquisiti, attraverso la comunicazione della violazione di dati personali nonché nell’ambito dell’istruttoria preliminare, l’Ufficio con nota 9 giugno 2020 (prot. n. 0020896.6707), ha notificato, ai sensi dell’art. 166, comma 5, del Codice, all’OPBG, in qualità di titolare del trattamento, l’avvio del procedimento per l’adozione delle misure correttive di cui all’art. 58, par. 2, del Regolamento, invitando l’OPBG 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, dalla l. n. 689 del 24 novembre 1981).

In particolare l’Ufficio, nel predetto atto, che qui deve intendersi integralmente riprodotto, ha rilevato la sussistenza di elementi idonei a configurare da parte dell’OPBG le violazioni di cui agli artt. 5, par. 1, lett. c) e f), 9, par. 2, lett. j), 32 par. 1, lett. a) e 89 del Regolamento.

Nel produrre i propri scritti difensivi, l’OPBG ha ribadito tutto quanto già rappresentato all’Autorità in fase di istruttoria preliminare, fornendo taluni specifici ulteriori elementi volti a circostanziare la violazione occorsa e consentire a questa Autorità una ponderata valutazione della stessa ai sensi dell’art. 83 del Regolamento (nota del 7 luglio 2020, prot. n. 1431/PR).

In tale ambito, l’OPBG ha, in particolare, specificato nuovamente che le informazioni sono state rese note per mero errore materiale verificatosi in un’unica occasione e su un ristrettissimo campione di interessati, a soggetti che appartengono alla CRO, ossia soggetti che in alcune fasi dello Studio sarebbero comunque autorizzati ad accedervi per lo sviluppo dei propri compiti istituzionali. Il titolare del trattamento ha evidenziato che “l’evento occorso, alla luce di quanto illustrato, non ha determinato un ampliamento dei soggetti astrattamente autorizzati a visionare i dati dei pazienti sottoposti allo studio”.

L’OPBG ha, inoltre, precisato di avere posto in essere, a seguito dell’evento occorso, una modalità di valutazione dei rischi maggiormente stringente anche in applicazione di un modus operandi dell’Ospedale improntato al miglioramento continuo nella gestione dei dati personali, basato sui principi e sulle linee guida dello standard ISO 31000 Risk menagment - Principles e guidelines e dello standard ISO, per il trattamento del rischio relativo alla sicurezza delle informazioni.

È stato, infine, sottolineato l’elevato grado di cooperazione con l’Autorità comprovato, tra l’altro, dalla tempestività ed esaustività dei riscontri forniti (art. 83, par. 2, lett. b) e d) del Regolamento).

3. Esito dell’attività istruttoria

In base al Regolamento, i dati personali devono essere trattati in modo lecito, corretto e trasparente, devono essere adeguati, pertinenti, limitati rispetto a quanto necessario per le finalità per le quali sono trattati e devono essere adottate misure tecniche e organizzative adeguate a garantire l’integrità e la riservatezza degli stessi e a prevenire trattamenti non autorizzati o illeciti (art. 5, par. 1 lett. a), c) e f) del Regolamento).

In merito alla fattispecie in esame appare opportuno precisare, altresì, che alla luce del Regolamento si intende per “«dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale” (art. 4, par. 1, n. 1). La disciplina sulla protezione dei dati personali riguarda, quindi, anche i dati pseudonimizzati, ossia quei dati oggetto di uno specifico trattamento per cui essi non possono “più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a

garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile" (art. 4, par. 1, n. 5). Sono anonime e quindi estranee alla disciplina in esame, invece, solo quelle informazioni che non consentono l'identificazione, seppure indiretta, dell'interessato (cfr. cons. 26 del Regolamento).

Il titolare, competente al rispetto dei principi applicabili al trattamento, è tenuto altresì a mettere in atto "misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio", tenendo conto, tra l'altro, "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" (art. 32 del Regolamento).

L'articolo 89 del Regolamento dispone, infine, che "il trattamento a fini di (...)ricerca scientifica è soggetto a garanzie adeguate per i diritti e le libertà dell'interessato, in conformità del presente regolamento. Tali garanzie assicurano che siano state predisposte misure tecniche e organizzative, in particolare al fine di garantire il rispetto del principio della minimizzazione dei dati. Tali misure possono includere la pseudonimizzazione, purché le finalità in questione possano essere conseguite in tal modo. Qualora possano essere conseguite attraverso il trattamento ulteriore che non consenta o non consenta più di identificare l'interessato, tali finalità devono essere conseguite in tal modo".

Alla luce della ricostruzione che precede e premesso che, salvo che il fatto non costituisca più grave reato, chiunque, in un procedimento dinanzi al Garante, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi ne risponde ai sensi dell'art. 168 del Codice "Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante", all'esito dell'esame delle dichiarazioni rese all'Autorità nel corso del procedimento nonché della documentazione acquisita, si rileva che:

l'OPBG e la Bracco (centro di sperimentazione e promotore dello Studio) hanno notificato all'Autorità, quasi contestualmente, le violazioni sopra richiamate, evidenziando entrambi che presso l'OPBG di Roma un'operatrice sanitaria ha comunicato via mail alla CRO gli esami di laboratorio e gli esami di risonanza magnetica riferiti ai pazienti arruolati nello Studio, con l'indicazione del nome e cognome degli interessati manualmente mascherati con un pennarello nero e che la CRO ha inoltrato le scansioni ricevute alla study manager di Bracco Imaging S.p.A., che a sua volta le ha inoltrate alla study manager di Bracco Diagnostics Inc, stabilita a Monroe Township, NJ, USA;

gli eventi descritti e notificati al Garante riguardano, invero, due violazioni distinte derivanti dalle condotte dei due titolari del trattamento coinvolti nella sperimentazione. La prima, tenuta dall'OPBG, concerne la non scrupolosa osservanza delle tecniche di pseudonimizzazione previste dal protocollo di studio la comunicazione dei dati alla CRO; la seconda concerne la raccolta e il successivo trattamento da parte della CRO e della Study menager di Bracco di tali dati, con particolare riferimento alla comunicazione all'estero degli stessi;

il presente provvedimento tiene conto, quindi, esclusivamente delle condotte imputabili all'OPBG;

la procedura di cancellazione manuale con pennarello non può essere definita, come erroneamente ritenuto in taluni passaggi dall'OPBG, idonea a rendere anonime le informazioni personali, riferite ai 10 pazienti arruolati nello studio in esame, ciò in quanto, come anche rappresentato dall'OPBG stesso, tale procedura consentiva di fatto la visibilità dei nomi e cognomi dei pazienti "se esaminati con attenzione";

la predetta procedura, invero, non può neppure definirsi di "pseudonimizzazione" -giusta la definizione sopra richiamata di tale operazione di trattamenti di dati personali (art. 4, par. 1, n. 4 del Regolamento) – in quanto, anche laddove eseguita in modo efficace, può essere piuttosto considerata un semplice oscuramento manuale delle generalità degli interessati;

diversamente da quanto sostenuto dall'OPBG, la condotta ha esteso la platea dei soggetti che avrebbero dovuto venire a conoscenza dell'identità dei pazienti arruolati nello studio. Infatti, come anche richiamato nelle Linee guida per i trattamenti di dati personali nell´ambito delle sperimentazioni cliniche di medicinali, adottate dal Garante con provvedimento del 24 luglio 2008, (doc. web n. 1533155) "al fine di tutelare l´identità delle persone coinvolte nello studio la (...) normativa prevede che il centro partecipante alla sperimentazione debba assegnare un codice di identificazione a ciascun interessato, al momento del suo coinvolgimento, e utilizzarlo al posto del relativo nominativo in ciascuna comunicazione al promotore di dati collegati allo studio (cfr. anche d.m. 15 luglio 1997, all. 1/1B punto 1.58). Il centro di sperimentazione può consentire solo agli addetti al monitoraggio della sperimentazione, facenti parte dell'organizzazione del promotore, l'accesso ai dati

direttamente identificativi dei pazienti, laddove necessario ai fini della supervisione, infatti, dell'andamento dello studio e per garantire che esso venga effettuato in osservanza del protocollo.

Per tali ragioni, come emerso dalle risultanze istruttorie, il trattamento di dati personali in questione è stato effettuato in maniera non conforme ai principi di minimizzazione e sicurezza dei dati, in violazione degli artt. 5, par. 1, lett. c) e f) e 89, comma 1 del Regolamento, con misure tecniche e organizzative non idonee a garantire un livello adeguato di riservatezza ai dati sulla salute degli interessati, in violazione dell'articolo 32, par. 1, lett. a) del Regolamento

4. Conclusioni

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

Per tali ragioni, confermando le valutazioni preliminari dell'Ufficio, si rileva l'illiceità del trattamento di dati personali effettuato dall'OPBG in quanto, l'avvenuta comunicazione via e-mail dei degli esami di laboratorio e degli esami di risonanza magnetica, con l'indicazione del nome e cognome dei pazienti arruolati nello studio clinico in esame, seppure mascherati con un pennarello nero, ha costituito una violazione dei principi di minimizzazione e sicurezza dei dati in forza dell'applicazione di una misura tecnica e organizzativa non adeguata ad assicurare l'effettività di tali principi (artt. 5, par. 1, lett. c) ed f), 32, par. 1, lett. a) e 89, par. 1, del Regolamento).

Conseguentemente, a prescindere dalla notificazione della violazione di dati personali effettuata dal titolare del trattamento, in osservanza dell'obbligo di cui all'art. 33 del Regolamento, i profili di illiceità del trattamento rilevati nel caso di specie, quale conseguenza della mancata adozione di misure tecniche e organizzative adeguate, richiedono comunque l'intervento correttivo di questa Autorità al fine di salvaguardare i diritti e le libertà fondamentali degli interessati.

In tale quadro, considerando le circostanze dell'evento occorso e che la condotta ha esaurito i suoi effetti, si ritiene di qualificare il caso come "violazione minore", ai sensi dell'art. 83, par. 2, e del considerando 148 del Regolamento.

Infatti, va tenuto conto che, dalle risultanze degli atti, l'episodio risulta essere stato unico e isolato, determinato da un errore umano di un operatore in servizio presso il titolare del trattamento, che quindi consente di qualificare la violazione come colposa. La condotta, invero, seppur non rispettosa delle tecniche di pseudonimizzazione previste dal protocollo di studio e delle buone pratiche cliniche per la esecuzione delle sperimentazioni cliniche dei medicinali, manifesta l'intenzione di salvaguardare l'identità degli interessati, escludendo il disvelamento dei dati direttamente identificativi se non a seguito di attento esame. Va notato, altresì, che seppur la violazione ha riguardato dati relativi allo stato di salute di soggetti vulnerabili, in quanto minori di età, essa ha coinvolto un numero estremamente circoscritto di interessati. Occorre considerare, inoltre, che l'Autorità ha preso conoscenza della violazione a seguito della notifica effettuata, nei termini, dal titolare del trattamento il quale ha messo in atto - appena venuto a conoscenza dell'accaduto – misure tecniche e organizzative idonee per pervenire l'ulteriore verificarsi di violazioni simili e ha cooperato con l'Autorità in fase istruttoria fornendo riscontri esaurienti e tempestivi. Non risultano, altresì, precedenti violazioni pertinenti commesse dal titolare del trattamento né sono stati precedentemente disposti provvedimenti di cui all'art. 58 del Regolamento.

Si ritiene, tuttavia, relativamente al caso in esame, di ammonire il titolare del trattamento ai sensi degli artt. 58, par. 2, lett. b), e 83, par. 2, del Regolamento, per la violazione degli artt. artt. 5, par. 1, lett. c) e f), 32, par. 1, lett. a) e 89, par.1, del Regolamento, e che non vi siano i presupposti per l'adozione di ulteriori provvedimenti correttivi da parte dell'Autorità, ai sensi dell'art. 58, par. 2, del Regolamento. Si rileva, infine, che ricorrono i presupposti di cui all'art. 17 del Regolamento n. 1/2019, concernente le procedure interne aventi rilevanza esterna, finalizzate allo svolgimento dei compiti e all'esercizio dei poteri demandati al Garante.

TUTTO CIÒ PREMESSO IL GARANTE

a) ai sensi degli artt. 57, par. 1, lett. f) del Regolamento e 166 del Codice, dichiara illecita la condotta tenuta dall'Ospedale Pediatrico Bambino Gesù, con sede in sede legale in Piazza S. Onofrio n. 4 - 00165 Roma CF 80403930581, descritta nei termini di cui in motivazione, e ammonisce l'Ospedale medesimo per la violazione degli artt. artt. 5, par. 1, lett. c) e f), 32, par. 1, lett. a) e 89, par. 1, del Regolamento;

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

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

Roma, 17 settembre 2020

IL PRESIDENTE
Stanzione

IL RELATORE
Ghiglia

IL VICE SEGRETARIO GENERALE
Filippi