Provvedimento del 17 ottobre 2024 [10074551]

[doc. web n. 10074551]

Provvedimento del 17 ottobre 2024

Registro dei provvedimenti
n. 620 del 17 ottobre 2024

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, alla quale hanno preso parte il prof. Pasquale Stazione, presidente, la prof.ssa Ginevra Cerrina Feroni, vicepresidente, il dott. Agostino Ghiglia e l'avv. Guido Scorza, componenti, e il Cons. Fabio Mattei, segretario generale;

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

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

VISTO il 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";

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

VISTA la documentazione in atti;

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

Relatore l'avv. Guido Scorza;

PREMESSO

1. Il reclamo e l'attività istruttoria

In data XX la signora XX ha formulato un reclamo lamentando una violazione della disciplina in materia di protezione dei dati personali derivante dalle modalità di consegna dei referti online da parte della Società Bios s.p.a. (di seguito la "Società"). In particolare, è stato rappresentato che la medesima Società "inserendo un indirizzo di posta errato, ha diffuso il referto di esami diagnostici relativi alla (figlia) minore … (di anni 2), che conteneva oltre ai dati sanitari di quest'ultima, anche tutti i dati anagrafici della stessa (luogo, data di nascita, residenza)", evidenziando che i referti erano "meramente allegati all'e-mail senza richiedere per la loro visione una password di accesso".

Nell'ambito dell'attività istruttoria si è reso necessario chiedere elementi di informazione utili alla valutazione del caso alla Società (note del XX e XX), la quale ha fornito riscontro (note del XX e XX), dichiarando che:

- "il giorno XX, arrivava all'operatore di Bios, una telefonata da parte della reclamante nella quale faceva presente di aver ricevuto via mail un solo referto riferibile alla prima figlia e non quello della seconda figlia";

- "l'operatore verificava nel corso della chiamata quanto avvenuto e resosi conto che il referto effettivamente non era stato allegato, faceva un secondo invio. Poco dopo la sig.ra richiama facendo nuovamente presente di non aver ricevuto il referto, allora l'operatore controllando in tempo reale si rendeva conto di aver sbagliato manualmente l'invio del referto indirizzandolo ad una e-mail diversa, e subito lo faceva presente all'interessata";

- "il soggetto inviante, come da istruzioni, contattava immediatamente l'erroneo destinatario tramite telefono significando l'erroneo invio e chiedendo l'immediata cancellazione del messaggio";

- "l'erronea destinataria riferiva di non aver aperto il messaggio (in quanto aveva compreso di non essere la destinataria, non avendo svolto di recente nessuna prestazione presso il titolare del trattamento), parimenti rassicurava l'autorizzato al trattamento di aver cancellato il messaggio contenente il prefato referto";

- "tutto questo avveniva in un tempo di una decina di minuti. Appare plausibile che nessun terzo ha avuto modo di visualizzare i dati particolari oggetto del reclamo. A riprova della buona fede dell'azienda, si rappresenta che le circostanze appena esposte sono state comunicate alla Signora (reclamante) immediatamente dall'operatore che ha provveduto poi al corretto invio";

- quali azioni di mitigazioni successive sono stati posti in essere: "nello specifico la settimana del 7 ottobre, formazione ed istruzione specifica con richiamo ad una maggiore attenzione da parte degli autorizzati"; "l'azienda nel rispetto del principio di accountability ed in ossequio all'art. 32 ha implementato con riferimento alla refertazione online con password ed al fine di ridurre il rischio residuo, una nuova procedura che prevedrà nel più breve tempo possibile (…) l'adozione delle password per l'invio dei referti online";

- "in ossequio alle citate linee guida del 2009 con riferimento alle misure di sicurezza è in uso quanto previsto dallo scenario 2 [la parte ha firmato esplicito consenso all'invio del referto in allegato alla e-mail, in formato pdf, ma senza password]";

- "nel programma informatico di "accettazione dei pazienti" appare un pop-up che richiama l'attenzione dell'operatore sull'indirizzo e-mail comunicato dall'utente, al fine di permettere un ulteriore controllo verbale sulla correttezza dell'indirizzo fornito";

- “in fattura consegnata sempre al termine dell’accettazione è riportato l’indirizzo e-mail al quale il cliente ha chiesto l’invio del referto, sempre al fine di permettere un ulteriore controllo”.

Alla predetta nota sono stati allegati alcuni documenti recanti “Procedura refertazione telematica”, “consenso al trattamento dei dati personali”, “espressione di consenso”, “acquisizione del consenso”, “autorizzazione al trattamento dei dati-accettazione”.

In particolare, nel documento “Procedura refertazione telematica” è espressamente stabilito che: “nel caso in cui l’interessato abbia deciso di aderire al servizio, l’operatore dovrà acquisire lo specifico consenso, dove dovrà essere esplicitato che il referto non sarà accompagnato da password. L’ipotesi in cui non sarà possibile fornire le credenziali per l’apertura del file da inviare via posta elettronica, si potrà verificare solo quando l’interessato stesso abbia fatto espressa e consapevole richiesta di inviargli il file privo di una chiave che ne consenta l’apertura. E’ necessario inoltre prima di terminare un’accettazione verificare sempre un’ulteriore volta la correttezza della mail inserita e chiedere al cliente di leggerla anche in fattura dove appare” (punto 5) e che “l’organizzazione assume anche le seguenti misure di sicurezza per garantire la tutela dei dati contenuti nel referto: 1. La spedizione del referto in forma di allegato a un messaggio e-mail e non come testo compreso nel body part del messaggio; 2. Convalida degli indirizzi e-mail tramite apposito pop-up che ricorda all’operatore di verificare la correttezza dell’indirizzo, in modo da evitare la spedizione di documenti elettronici, verso soggetti diversi dall’utente richiedente il servizio”.

Inoltre, nel documento recante “Consenso al trattamento dei dati”, al punto 10 (“Informativa specifica invio referto per e-mail”), viene indicato che “Si informa che il Gruppo Bios S.P.A è in grado di fornire copia del referto delle prestazioni eseguite tramite e-mail, in formato pfd senza l’utilizzo di password, alla casella di posta elettronica fornita dall’interessato. Tale servizio, facoltativo, è erogabile su consenso dell’interessato sia in modo permanente oppure riferito alla singola accettazione”.

2. Valutazioni del Dipartimento sul trattamento effettuato e notifica della violazione di cui all’art. 166, comma 5 del Codice

In relazione ai fatti descritti nel reclamo, l’Ufficio, con nota del XX (prot. n. XX), ha notificato alla Società, ai sensi dell’art. 166, comma 5, del Codice, l’avvio del procedimento per l’adozione dei provvedimenti di cui all’art. 58, par. 2, del Regolamento, invitandola a produrre al Garante scritti difensivi o documenti ovvero a chiedere di essere sentita dall’Autorità (art. 166, commi 6 e 7, del Codice; nonché art. 18, comma 1, dalla legge n. 689 del 24/11/1981).
In particolare, l’Ufficio, nel predetto atto, ha ritenuto che la Società, al momento del reclamo, non aveva ottemperato agli obblighi di cui all’art. 32 del Regolamento, in quanto non erano state adottate misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato ai rischi presentati dal trattamento e, quindi, in violazione dei principi di base del trattamento di cui agli artt. 5, par. 2, lett. f), 25, par. 1, e 32 del Regolamento.

La Società ha chiesto di essere sentita in audizione, che si è tenuta in data XX, durante la quale è stato evidenziato che:

- “Bios s.p.a. sta adeguando tutti i sistemi informativi con un codice criptato da fornire ai clienti per l’accesso al referto, allegato all’email del destinatario; in poche settimane tale attività di adeguamento sarà conclusa; verrà comunicata all’Autorità la data di avvenuto adeguamento”;

- “la Bios s.p.a. effettua attività di service di laboratorio a favore di strutture pubbliche e private sul territorio laziale e non solo e nell’ambito di tale attività, già da tempo, provvede a

inviare i referti protetti da password poiché l'invio avviene da un programma informatico più recente e snello, diverso da quello utilizzato per i pazienti della struttura";

- "la Bios s.p.a. si impegna costantemente ad implementare i propri sistemi informativi per garantire l'efficienza dei servizi offerti ai clienti, anche sotto il profilo della sicurezza e della protezione dei dati";

- "nel caso di specie un operatore inseriva manualmente l'e-mail del paziente per un nuovo invio del referto e, resosi conto di un errore materiale, comunicava alla paziente l'errore stesso. Contestualmente veniva contattato telefonicamente il destinatario errato, per richiedere l'immediata cancellazione della mail ricevuta";

- "nei casi di accettazione del paziente, l'operatore visualizza un pop-up automatico che lo allerta di controllare ulteriormente la correttezza e l'attualità dell'indirizzo mail e, nel caso di specie, l'operatore non visualizzava il pop-up poiché provvedeva manualmente all'invio a seguito di una chiamata della cliente e non in fase di accettazione".

3. Esito dell'attività istruttoria

Preso atto di quanto rappresentato dalla Società nella documentazione in atti e nelle memorie difensive, si osserva che:

1. il titolare del trattamento è, in particolare, tenuto a rispettare i principi in materia di protezione dei dati, fra i quali quello di «integrità e riservatezza», secondo il quale i dati personali devono essere "trattati in maniera da garantire un'adeguata sicurezza (…), compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali" (art. 5, par. 1, lett. f) del Regolamento). Gli stessi dati devono essere, altresì, trattati nel rispetto del principio di protezione dei dati fin dalla progettazione (privacy by design) secondo il quale, "sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso, il titolare del trattamento deve mettere in atto misure tecniche e organizzative adeguate, volte ad attuare in modo efficace i principi di protezione dei dati e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del Regolamento e tutelare i diritti degli interessati" (art. 25 del Regolamento);

2. in materia di sicurezza del trattamento, l'art. 32 del Regolamento 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);

3 l'attività di refertazione online è disciplinata da un provvedimento del Garante del 19 novembre 2009 (pubblicato in G.U. n. 288 dell´11 dicembre 2009, consultabile su www.gpdp.it, doc. web n. 1679033; cfr. art. 22, comma 4, del d.lgs. n. 101/2018), recante "Linee guida in tema di referti on-line", applicabile anche alle strutture sanitarie private. In particolare, nel predetto provvedimento, è stato precisato che "Qualora il titolare del trattamento intenda inviare copia del referto alla casella di posta elettronica dell'interessato, a seguito di sua richiesta, per il referto prodotto in formato digitale devono essere osservate le seguenti cautele: 1. spedizione del referto in forma di allegato a un messaggio e-mail e

non come testo compreso nella body part del messaggio; 2. il file contenente il referto dovrà essere protetto con modalità idonee a impedire l'illecita o fortuita acquisizione delle informazioni trasmesse da parte di soggetti diversi da quello cui sono destinati, che potranno consistere in una password per l'apertura del file o in una chiave crittografica rese note agli interessati tramite canali di comunicazione differenti da quelli utilizzati per la spedizione dei referti. Tale cautela può non essere osservata qualora l'interessato ne faccia espressa e consapevole richiesta, in quanto l'invio del referto alla casella di posta elettronica indicata dall'interessato non configura un trasferimento di dati sanitari tra diversi titolari del trattamento, bensì una comunicazione di dati tra la struttura sanitaria e l'interessato effettuata su specifica richiesta di quest'ultimo; 3. convalida degli indirizzi e-mail tramite apposita procedura di verifica on-line, in modo da evitare la spedizione di documenti elettronici, pur protetti con tecniche di cifratura, verso soggetti diversi dall'utente richiedente il servizio" (punto 6, Scenario 2). In tale materia è stato, altresì, adottato il d.P.C.M. 8 agosto 2013, recante "Modalità di consegna, da parte delle Aziende sanitarie, dei referti medici tramite web, posta elettronica certificata e altre modalità digitali, nonché di effettuazione del pagamento online delle prestazioni erogate", su cui il Garante ha espresso parere favorevole (cfr. provvedimento 6 dicembre 2012, doc. web 2223206).

4. Conclusioni: dichiarazione di illiceità del trattamento.

Alla luce delle valutazioni sopra esposte, tenuto conto delle dichiarazioni rese dal titolare del trattamento nel corso dell'istruttoria e considerato 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"), gli elementi forniti dalla Società, in qualità di titolare del trattamento, nell'audizione sopra richiamata non sono idonei ad accogliere le richieste di archiviazione, non consentendo di superare i rilievi notificati dall'Ufficio con il citato atto di avvio del procedimento.

Infatti, si rileva che la Società, al momento del reclamo, non aveva messo in atto alcuna modalità volta a impedire l'illecita o fortuita acquisizione delle informazioni trasmesse da parte di soggetti diversi da quello cui sono destinati, come, ad esempio, una password per l'apertura del file o una chiave crittografica. Tale misura, come, peraltro indicato nel citato provvedimento del 19 novembre 2009, avrebbe dovuto essere prevista, per impostazione predefinita, dal titolare del trattamento, il quale è sempre obbligato ad effettuare una valutazione, in concreto, sull'appropriatezza delle misure adottate per garantire la sicurezza del trattamento, tenendo conto del contesto in cui si opera. In particolare, l'acquisizione di un consenso degli interessati alla trasmissione via mail dei referti "in formato pfd senza l'utilizzo di password" (che, a ben vedere, in ogni caso, non può essere assimilata ad una espressa e consapevole richiesta degli stessi) non solleva il titolare dall'obbligo di valutare, continuamente nel corso del tempo, un adeguato livello di sicurezza che tenga anche conto dello sviluppo tecnologico e dei nuovi rischi connessi al trattamento per i diritti e le libertà degli interessati.

La Società ha, pertanto, mancato di ottemperare agli obblighi di sicurezza del trattamento, non avendo adottato misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato ai rischi presentati dal trattamento, in violazione dei principi di base del trattamento di cui agli artt. 5, par. 2, lett. f), 25, par. 1, e 32 del Regolamento.
Per tali ragioni si rileva l'illiceità del trattamento di dati personali effettuato dalla Società, nei termini di cui in motivazione, per la violazione degli artt. 5, par. 1, lett. f), 25 e 32 del Regolamento.

In tale quadro, considerato che la condotta ha esaurito i suoi effetti (la Società ha, infatti, chiesto, alla destinataria cui era stato erroneamente trasmesso il referto di eliminare lo stesso ed ha ottenuto rassicurazioni in tal senso) e tenuto conto che il titolare ha dichiarato di prevedere che sia fornito ai clienti un codice criptato per l'accesso al referto, allegato all'email del destinatario, non

ricorrono allo stato i presupposti per l'adozione delle misure correttive di cui all'art. 58, par. 2, del Regolamento.

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

La violazione degli artt. 5, par. 1, lett. f), 25 e 32 del Regolamento causata dalla condotta della Società è soggetta all'applicazione della sanzione amministrativa pecuniaria ai sensi dell'art. 83, par. 4, lett. a) e par. 5, lett. a) del Regolamento.

Il Garante, ai sensi degli artt. 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, di cui è stata accertata l'illiceità, nei termini sopra esposti.

Ritenuto di dover applicare il par. 3 dell'art. 83 del Regolamento laddove prevede che "se, in relazione allo stesso trattamento o a trattamenti collegati, un titolare del trattamento […] viola, con dolo o colpa, varie disposizioni del presente Regolamento, l'importo totale della sanzione amministrativa pecuniaria non supera l'importo specificato per la violazione più grave", l'importo totale della sanzione è calcolato in modo da non superare il massimo edittale previsto dal medesimo art. 83, par. 5.

Alla luce di quanto sopra illustrato e, in particolare, della categoria di dati personali interessata dalla violazione che, per loro natura, sono particolarmente sensibili sotto il profilo dei diritti e delle libertà fondamentali, nonché del numero dei soggetti potenzialmente interessati, si ritiene che il livello di gravità della violazione commessa dalla Società sia alto (cfr. Comitato europeo per la protezione dei dati, "Guidelines 04/2022 on the calculation of administrative fines under the GDPR" del 23 maggio 2023, punto 60).

Ciò premesso, sono valutati nel loro complesso taluni elementi e, in particolare, che:

- l'Autorità ha preso conoscenza dell'evento a seguito di reclamo da parte di una interessata (art. 83, par. 2, lett. h) del Regolamento);

- il titolare, al fine di evitare la ripetizione dell'evento occorso, si è impegnato nell'introduzione di misure volte a aumentare il livello di sicurezza del trattamento in esame e a ridurre la replicabilità dell'evento occorso e ha adottato misure, al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi (art. 83, par. 2, lett. c) e f) del Regolamento);

- il titolare ha collaborato con l'Autorità e non è stato destinatario di precedenti provvedimenti del Garante per violazioni pertinenti (art. 83, par. 2, lett. f) e e) del Regolamento).

Si ritiene inoltre che assumano rilevanza, nell'ipotesi di specie, le condizioni economiche del contravventore, determinate in base al volume d'affari della Società, di cui al bilancio d'esercizio per l'anno 2023.

Alla luce degli elementi sopra indicati e delle valutazioni effettuate, si ritiene, nel caso di specie, di determinare l'ammontare della sanzione pecuniaria nella misura di euro 7.000,00 (settemila/00) per la violazione degli artt. 5, 25 e 32 del medesimo Regolamento, in ragione dei principi di effettività, proporzionalità e dissuasività ai quali l'Autorità deve attenersi, ai sensi dell'art. 83, par. 1, del Regolamento.

In tale quadro si ritiene, altresì, che, ai sensi dell'art. 166, comma 7, del Codice e dell'art. 16,

comma 1, del Regolamento del Garante n. 1/2019, si debba procedere alla pubblicazione del presente capo contenente l'ordinanza ingiunzione sul sito Internet del Garante. Ciò, in considerazione della tipologia di dati personali oggetto di illecito trattamento e della circostanza che la disciplina relativa all'attività di refertazione online risale agli anni 2009 e 2013.

TUTTO CIÒ PREMESSO IL GARANTE

ai sensi degli artt. 57, par. 1, lett. f) e 83 del Regolamento, rileva l'illiceità del trattamento effettuato dalla Società Bios s.p.a., con sede in Via Domenico Chiellini, 39, 00197 Roma, C.F. 01014021008, nei termini di cui in motivazione, per la violazione degli artt. 5, 25 e 32 del Regolamento;

ORDINA

ai sensi dell'art. 58, par. 2, lett. i) del Regolamento, alla medesima Società, in persona del legale rappresentante pro-tempore, di pagare la somma di euro 7.000,00 (settemila) a titolo di sanzione amministrativa pecuniaria per la violazione indicata nel presente provvedimento.

INGIUNGE

alla predetta Società di pagare la somma di euro 7.000,00 (settemila) secondo le modalità indicate in allegato, entro 30 giorni dalla notificazione del presente provvedimento, pena l'adozione dei conseguenti atti esecutivi a norma dall'art. 27 della legge n. 689/1981. 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 sotto indicato.

DISPONE

a) 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;

b) 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;

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

Ai sensi dell'art. 78 del Regolamento, 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 ottobre 2024

IL PRESIDENTE
Stanzione

IL RELATORE
Scorza

IL SEGRETARIO GENERALE
Mattei