# Provvedimento del 12 dicembre 2024 [10102444]

[doc. web n. 10102444]

**Provvedimento del 12 dicembre 2024**

Registro dei provvedimenti
n. 770 del 12 dicembre 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 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 d.lgs. 30 giugno 2003, n. 196 recante il "Codice in materia di protezione dei dati personali", contenente 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 il "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 la prof.ssa Ginevra Cerrina Feroni;

**PREMESSO**

**1. La violazione dei dati personali**

Con nota del XX, successivamente integrata con comunicazione del XX, l'Azienda Sanitaria dell'Alto Adige, di seguito "Azienda" ha trasmesso all'Autorità, ai sensi dell'art. 33 del Regolamento, una notifica di violazione dei dati personali, nella quale è stato dichiarato che "un medico convenzionato che opera presso gli ambulatori dell'Azienda sanitaria, relativamente alla tematica "riduzione orario di servizio", ha scritto a diversi soggetti aziendali ed esterni (info@ordinemedici.bz.it) allegando alla Sua comunicazione la lista dei pazienti visitati in un determinato giorno. La comunicazione è stata inviata in chiaro e nella stessa erano riportati i seguenti dati: nome – cognome – data di nascita – residenza del paziente nonché sede di erogazione prestazione, prestazione erogata, indicazione su paziente pagante, esente (con indicazione del codice di esenzione), CF e numero di cellulare".

Nella medesima comunicazione è stato evidenziato che "l'autore della violazione ha inviato con una sola comunicazione mail l'allegato con i dati violati a 15 Strutture aziendali e Soggetti diversi tra cui anche l'ordine dei medici della Provincia" e che, come misure tecniche e organizzative adottate (o di cui si propone l'adozione) per porre rimedio alla violazione e ridurne gli effetti negativi per gli interessati e per prevenire simili violazioni future, sono stati indicati: "Coinvolgimento del DPO; Richiesta a tutte le strutture e soggetti che hanno ricevuto l'allegato di procedere a relativa cancellazione; Avviato iter procedimento disciplinare; Avviato iter per segnalazione dell'accaduto all'ordine dei medici"; "in Azienda sono state fornite indicazioni sulla modalità corretta di invio dei dati cosiddetti sensibili – tali indicazioni sono disponibili sulla pagina intranet sezione privacy dell'Azienda stessa".

La medesima Azienda ha trasmesso in allegato la documentazione contenente la citata mail, dalla quale si desume che la trasmissione dell'elenco dei pazienti (13) è stata effettuata al fine di fornire chiarimenti in merito all'orario di lavoro svolto ("con la presente per sottolineare che gli orari scritti nella delibera inerenti la giornata del martedì ambulatorio di Laives non sono quelli effettivi rispetto alla lista dei pazienti impostata dal CUP. Vedi esempio allegato").

**2. La notifica delle violazioni e le memorie difensive**

In ordine alla fattispecie descritta, l'Ufficio, sulla base di quanto rappresentato dal titolare del trattamento nell'atto di notifica di violazione nonché delle successive valutazioni, ha notificato all'Azienda, con atto n. XX del XX, ai sensi dell'art. 166, comma 5, del Codice, l'avvio di un procedimento per l'adozione dei provvedimenti di cui all'art. 58, par. 2, del Regolamento, invitando il predetto titolare 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 legge n. 689 del 24 novembre 1981). In particolare, l'Autorità ha ritenuto che l'invio, da parte del professionista sanitario che operava presso l'Azienda, a più soggetti, tra i quali l'Ordine dei medici, di una mail contenente in allegato dati sulla salute di 13 pazienti, ha comportato, in capo all'Azienda, un trattamento di dati in assenza di un idoneo presupposto giuridico. Pertanto, con il citato atto n. XX del XX, l'Autorità ha ritenuto che l'Azienda, in qualità di trattamento dei dati personali in questione, fosse incorsa nella violazione dei principi di cui agli artt. 5, par. 1, lett. c) e f) e 9 del Regolamento e degli obblighi in materia di sicurezza del trattamento, di cui all'art. 32 del medesimo Regolamento.

L'Azienda, ha fatto pervenire le proprie memorie difensive, ai sensi dell'art. 166, comma 6, del Codice. In particolare, con nota del XX, ha precisato quanto espresso nella notifica di violazione, dichiarando, tra l'altro, che:

- "l'episodio ha coinvolto 13 interessati";

- "la comunicazione è stata inviata nello specifico al servizio della medicina di base, al

coordinamento/servizio odontoiatrico, al coordinamento del distretto di riferimento, al servizio Cup, all'ufficio del personale competente per la gestione dell'orario di lavoro, alla Ripartizione prestazioni sanitarie ed assistenza territoriale nonché al Comitato Zonale di Bolzano, tutti soggetti facenti parte del Comprensorio sanitario di Bolzano, e infine all'ordine dei medici (indirizzo generale dell'ordine)";

- "la comunicazione pertanto è arrivata sia a professionisti sanitari che a personale amministrativo dell'Azienda sanitaria nonché anche a soggetti esterni (professionisti sanitari e personale amministrativo), tutti tenuti, a seconda del proprio ruolo professionale, al rispetto del segreto professionale e/o del segreto d'ufficio";

- "la Cabina di Regia Privacy ha provveduto a chiedere l'avvio del procedimento disciplinare. Il medico ha inviato al dirigente di riferimento una nota in cui evidenziava quanto segue: «In quel momento, ribadisco SBAGLIANDO, non ho riflettuto sul fatto che avrei dovuto cancellare i nominativi dei pazienti. Per il sottoscritto era la trasmissione della lista pazienti che non conteneva dati inerenti lo stato di salute a tutti i soggetti inclusi nella mail inviatomi che pensavo necessitassero di tale informazione per una pura questione organizzativa della attività lavorativa. Siccome la comunicazione telefonica non era risultata sufficiente, e mi è stato chiesto di spiegare meglio la variazione degli orari, commettendo un errore, ho allegato un esempio esplicativo che testimoniasse gli orari effettivi che poi sono stati corretti. Rammaricato per la mia "leggerezza" che ha innescato questo problema ho già provveduto alla cancellazione della mail come richiesto e porgo le mie più sentite scuse»";

- "l'Azienda non ravvede nell'agire del professionista un comportamento doloso";

- le misure adottate per attenuare gli effetti della violazione per gli interessati sono state: "richiesta a tutte le strutture e soggetti che hanno ricevuto l'allegato di procedere a relativa cancellazione";

- "l'Azienda già in data XX aveva provveduto all'invio ai propri dipendenti di apposita nota circa la corretta gestione di mail e allegati, nel merito con ulteriore comunicazione del XX l'Azienda ha provveduto a rendere ai propri dipendenti disponibili apposite indicazioni operative su come proteggere con password gli allegati. Tali disposizioni sono state poi rese disponili sulla pagina intranet aziendale";

- "in data XX l'Azienda ha inoltrato nota a tutti i dipendenti circa la Corretta identificazione degli interessati (utenti, pazienti dell'Azienda sanitaria). Obiettivo della nota è quello di ricordare a tutte le collaboratrici e tutti i collaboratori, che a prescindere dal proprio ruolo professionale è onere di ciascuno provvedere a verificare che ogni comunicazione inviata a livello cartaceo o con modalità elettronica avvenga previa corretta identificazione del/la destinatario/a";

- "l'Azienda sanitaria ha sempre provveduto a riscontrare puntualmente alle diverse richieste dell'Autorità Garante nell'ambito dei procedimenti che la coinvolgono davanti all'Autorità".

In data XX, si è tenuta l'audizione richiesta dalla parte, durante la quale, la stessa ha precisato che:

- "nonostante le indicazioni fornite agli operatori in ordine al rispetto della disciplina in materia di protezione dei dati personali, un medico dell'Azienda ha inviato una comunicazione a più destinatari contenente l'elenco dei pazienti che avrebbe visitato";

- "è stato avviato, subito dopo l'evento, un procedimento disciplinare nei confronti del medico sumaista, con successiva comunicazione all'ordine professionale di pertinenza e l'Azienda ha colto l'occasione per reiterare le indicazioni già fornite in passato";

- “nessuno degli interessati ha formalmente presentato un reclamo o una lamentela nei confronti dell’Azienda, la quale è venuta a conoscenza dell’evento a seguito di segnalazione da parte di collaboratori dell’Azienda stessa”;

- “l’Azienda ha chiesto ai destinatari della mail la cancellazione dei dati impropriamente ricevuti”;

- “l’Azienda ha attivato ad aprile una formazione massiva nei confronti di tutti i dipendenti attraverso modalità FAD; ad oggi risultano iscritti 4026 dipendenti, di cui 2426 hanno già sostenuto il corso; si intende attivare un’ulteriore edizione del medesimo corso nei prossimi 2 mesi che coinvolgerà altri 5000 dipendenti, con l’obiettivo, in ogni caso, di formare tutti i dipendenti, anche futuri, che prestano la propria attività professionale presso l’Azienda”;

- “il titolare sta pianificando una formazione più specifica che coinvolga solo i professionisti sanitari, avendo, altresì, come obiettivo anche i lavoratori non dipendenti, come era il medico coinvolto nel data breach”;

- “l’Azienda ha emanato diverse circolari in materia di protezione dei dati personali rivolte ai dipendenti e pubblicate sulla intranet della stessa”.

**3. L’esito dell’attività istruttoria**

Preso atto di quanto rappresentato dall’Azienda nel corso del procedimento, si osserva che:

per “dato personale” si intende “qualsiasi informazione riguardante una persona fisica identificata o identificabile (“interessato”)” e per “dati relativi alla salute” “i dati riguardanti lo stato di salute dell'interessato che rivelino informazioni connesse allo stato di salute fisica o mentale passata, presente o futura dello stesso. Questi comprendono informazioni sulla persona fisica raccolte nel corso della sua registrazione al fine di ricevere servizi di assistenza sanitaria o della relativa prestazione di cui alla direttiva 2011/24/UE del Parlamento europeo e del Consiglio; un numero, un simbolo o un elemento specifico attribuito a una persona fisica per identificarla in modo univoco a fini sanitari” (art. 4, par. 1, nn. 1 e 15 del Regolamento; Cons. n. 35);

la Corte di Cassazione ha reputato che “il fatto stesso di comunicare l’esigenza di un trattamento sanitario e, quindi, l’esistenza di una “malattia” in senso lato – intesa dunque come situazione che renda necessario un trattamento sanitario – attiene a dato sulla salute: non occorre cioè, a tal fine, che sia specificato di quale trattamento o di quale malattia si tratti” (Sent. n. 28417/2023; cfr., altresì, comunicato stampa della Corte di giustizia dell’Unione europea n. 159/24, in relazione alla sentenza 4 ottobre 2024, nella causa C-21/23);

per “comunicazione” si intende il “dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall’interessato, dal rappresentante del titolare nel territorio dell’Unione europea, dal responsabile o dal suo rappresentante nel territorio dell’Unione europea, dalle persone autorizzate, ai sensi dell’art. 2-quaterdecies, al trattamento dei dati personali sotto l’autorità diretta del titolare o del responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione” (art. 2-ter, comma 4, lett. a) del Codice);

le informazioni sullo stato di salute possano essere comunicate solo all’interessato e possano essere comunicate a terzi solo sulla base di un idoneo presupposto giuridico (art. 9 Regolamento);

il titolare del trattamento è tenuto a rispettare i principi in materia di protezione dei dati, fra i

quali quelli di «minimizzazione» e di «integrità e riservatezza», secondo il quale i dati personali devono essere “adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati” e “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. c) e f) del Regolamento).

L’adeguatezza di tali misure deve essere valutata da parte del titolare del trattamento rispetto alla natura dei dati, all’oggetto, alle finalità del trattamento e al rischio per i diritti e le libertà fondamentali degli interessati, tenendo conto dei rischi che derivano dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall’accesso a dati personali trasmessi, conservati o comunque trattati (art. 32, par. 1 e 2 del Regolamento).

**4. Conclusioni: dichiarazione di illiceità del trattamento. Provvedimenti correttivi ex art. 58, par. 2, Regolamento**

A fronte di quanto sopra rappresentato emerge che la condotta del medico era volta, come dallo stesso dichiarato, a fornire chiarimenti in merito all’orario di lavoro dallo stesso svolto. Tale finalità avrebbe potuto essere conseguita, nel rispetto del citato principio di minimizzazione, senza trasmettere la documentazione relativa ai pazienti, comprensiva di informazioni sulla tipologia e sede di erogazione della prestazione e sul codice di esenzione.

Inoltre, nel rispetto del principio di integrità e riservatezza dei dati e dell’obbligo di adottare misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio, in considerazione della particolare categoria dei dati trattati, l’Azienda avrebbe dovuto fornire specifiche istruzioni agli operatori sanitari che trattano dati sulla salute di pazienti dell’Azienda e richiamare l’attenzione sulla disciplina in materia di protezione dei dati personali e sulla maggiore protezione che meritano i dati sulla salute che, per loro natura, sono particolarmente sensibili sotto il profilo dei diritti e delle libertà fondamentali, considerato che il contesto del loro trattamento potrebbe creare rischi significativi per i diritti e le libertà fondamentali.

Alla luce delle valutazioni sopra richiamate, 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 dal titolare del trattamento nella memoria difensiva sopra richiamata e nel corso dell’audizione non consentono di superare i rilievi notificati dall’Ufficio con il richiamato atto di avvio del procedimento, non ricorrendo, peraltro, alcuno dei casi previsti dall’art. 11 del regolamento del Garante n. 1/2019.

A fronte di quanto sopra rappresentato, si rileva che la descritta condotta del professionista sanitario (invio a più soggetti, tra i quali anche l’Ordine dei medici, di una mail contenente in allegato dati sulla salute di 13 pazienti dell’Azienda) ha comportato in capo alla medesima Azienda una comunicazione di dati sulla salute in assenza di un idoneo presupposto giuridico; ciò, in violazione dei principi di cui agli artt. 5, par. 1, lett. c) e f) e 9 del Regolamento e degli obblighi in materia di sicurezza del trattamento, di cui all’art. 32 del medesimo Regolamento.

Si ritiene, infine, che ricorrano i presupposti di cui all’art. 17 del Regolamento del Garante n. 1/2019.

**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. c), f), 9 e 32 del Regolamento, causata dalla condotta posta in essere dall'Azienda, è soggetta all'applicazione della sanzione amministrativa pecuniaria ai sensi dell'art. 83, par. 4 e 5 del Regolamento.

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, legge 24 novembre 1981 n. 689), in relazione al trattamento dei dati personali posto in essere dall'Azienda, 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, si ritiene che il livello di gravità della violazione commessa dalla Azienda 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), nonostante il carattere non doloso della violazione.

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

- il Garante ha preso conoscenza dell'evento a seguito della notifica di violazione effettuata dall'Azienda, ai sensi dell'art. 33 del Regolamento e non sono pervenuti reclami o segnalazioni in ordine alla violazione oggetto del presente provvedimento (art. 83, par. 2, lett. h) e k) del Regolamento);

- il titolare, al fine di evitare la ripetizione dell'evento occorso, ha attivato una intensa attività di formazione nei confronti del personale, pianificandone una più specifica per i soli professionisti sanitari, e ha cooperato con l'Autorità in ogni fase dell'istruttoria, al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi, anche chiedendo ai destinatari della mail la cancellazione dei dati impropriamente ricevuti (art. 83, par. 2, lett. c) e f) del Regolamento);

- il titolare è stato già destinatario di un provvedimento sanzionatorio del Garante per precedenti violazioni pertinenti (provv. 22 febbraio 2024, n. 97, doc. web n. 10001279);

si ritiene di determinare l'ammontare della sanzione pecuniaria prevista dall'art. 83, par. 5 del Regolamento, nella misura di euro 5.000,00 (cinquemila) per la violazione degli artt. 5, 9 e 32 del medesimo Regolamento, quale sanzione amministrativa pecuniaria ritenuta, ai sensi dell'art. 83, par. 1, del Regolamento, effettiva, proporzionata e dissuasiva.

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 dell'operazione di trattamento sugli stessi effettuata.

**TUTTO CIÒ PREMESSO IL GARANTE**

ai sensi degli artt. 57, par. 1, lett. f) e 83, del Regolamento, rileva l'illiceità del trattamento

effettuato dall'Azienda Sanitaria dell'Alto Adige, con sede legale in Bolzano, via Thomas Alva Edison, 10 D, 39100, C.F. – P.I. n. 00773750211, per la violazione dei principi di base del trattamento di cui agli artt. 5, par. 1, lett. c), f), 9 del Regolamento e degli obblighi di cui all'art. 32 dello stesso Regolamento, nei termini di cui in motivazione;

**ORDINA**

ai sensi dell'art. 58, par. 2, lett. i) del Regolamento, all'Azienda Sanitaria dell'Alto Adige, di pagare la somma di euro 5.000,00 (cinquemila/00) a titolo di sanzione amministrativa pecuniaria, per la violazione indicata nel presente provvedimento;

**INGIUNGE**

alla predetta Azienda di pagare la somma di euro 5.000,00 (cinquemila/00) 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. n. 150 del 1° settembre 2011 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, 12 dicembre 2024*

IL PRESIDENTE
Stanzione

IL RELATORE
Cerrina Feroni

IL VICE SEGRETARIO GENERALE
Filippi