Provvedimento del 26 settembre 2024 [10079346]

[doc. web n. 10079346]

Provvedimento del 26 settembre 2024

Registro dei provvedimenti
n. 581 del 26 settembre 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 il prof. Pasquale Stazione;

PREMESSO

1. Il reclamo e l'attività istruttoria

In data XX la signora XX ha formulato un reclamo, corredato da specifica documentazione, con il quale ha lamentato che l'Azienda Sanitaria Territoriale di Ascoli Piceno, di seguito "Azienda", avrebbe fornito "all'utente che ne fa richiesta un attestato (da presentare al datore di lavoro come giustificazione dell'assenza) che riporta il reparto presso cui il paziente ha effettuato la prestazione (neurologia, ginecologia, ortopedia), vanificando in tal modo il diritto dell'utente di non voler far sapere al datore di lavoro e al relativo ufficio del personale in quale ambito si stanno facendo accertamenti, visite o trattamenti".

Nell'ambito dell'attività istruttoria si è reso necessario richiedere all'Azienda elementi di informazione utili alla valutazione del caso nonché le iniziative assunte per conformare il trattamento dei dati personali alla disciplina rilevante in materia. Tale richiesta è stata formalizzata nella nota del XX (prot. n. XX), formulata dall'Autorità, ai sensi dell'art. 157 del Codice e trasmessa, via PEC, all'indirizzo: ast.ascolipiceno@emarche.it e regolarmente consegnata. A tale richiesta di informazioni, tuttavia, non è risultato pervenuto alcun riscontro. Pertanto, l'Autorità, con nota del XX (prot. n. XX), non avendo l'Azienda ottemperato alla richiesta di fornire gli elementi richiesti nel termine indicato, ha notificato alla medesima Azienda la violazione dell'art. 157 del Codice, comunicando, 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. Unitamente alla citata nota del XX è stata trasmessa nuovamente la richiesta inviata con la precedente nota del XX.

Con nota del XX, trasmessa a seguito dell'accoglimento dell'istanza volta ad ottenere un "differimento" del termine previsto per il riscontro alla richiesta di informazioni, l'Azienda ha fornito riscontro alla richiesta di informazioni del XX, dichiarando, tra l'altro, che:

- "la L.R. n. 19/2022 "Organizzazione del Servizio Sanitario Regionale" ha disposto la soppressione dell'ASUR Marche, alla data del XX, cui sono subentrate dal XX senza soluzione di continuità, le costituite Aziende Sanitarie Territoriali (…), aventi autonoma personalità giuridica pubblica e autonomia imprenditoriale, organizzativa, amministrativa, patrimoniale, contabile, gestionale e tecnica";

- "l'AST di AP è stata commissariata per 7 mesi, nel corso dei quali sono stati nominati 3 Commissari Straordinari";

- "solo dal XX la Giunta Regionale ha nominato i Direttori Generali delle 5 Aziende Sanitarie Territoriali (…)";

- "fino al XX le funzioni di DPO anche per quanto di riferimento le Aree Vaste territoriali, tra le quali l'area Vasta n. 5 di Ascoli Piceno (a far data dal XX AST di Ascoli Piceno dotata di personalità giuridica) facevano capo alla ASUR Marche di Ancona";

- alla luce di un recesso, proroghe interne e individuazione tramite Mepa "in un arco temporale di 13 mesi l'AST di AP ha proceduto alla nomina di n. 2 DPO";

- "pur non costituendo una giustificazione in ordine al mancato adempimento di alcuni obblighi normativi in materia di privacy, il commissariamento di n. 7 mesi in capo all'AST di AP e la recente conclusione del periodo pandemico da SARS-COV-2 non hanno facilitato l'avvio delle procedure previste. Ad oggi l'acquisizione della personalità giuridica con decorrenza dal XX da parte delle Aziende Sanitarie Territoriali (ex Aree Vaste territoriali dipendenti dall'ASUR Marche) della Regione Marche contestuale alla soppressione della ex ASUR Marche e agli avvicendamenti nei commissariamenti e DPO non hanno consentito di poter attuare con immediatezza tutte le attività a tutela della protezione dei dati";

- "in raccordo e su indicazione del DPO (…), è stata predisposta una task-force con i

responsabili degli uffici aziendali, al fine di adottare/predisporre misure atte a conformare il trattamento dei dati personali (…) alla disciplina: - adozione di specifiche procedure per prevenire la conoscenza presente e futura, da parte di estranei, dello stato di salute di un paziente, attraverso la semplice correlazione tra la sua identità e l'indicazione della struttura o del reparto, in cui è stato visitato o ricoverato; - messa in atto di urgenti misure correttive, necessarie al fine di garantire che i certificati, rilasciati a fini amministrativi, in occasione di ricovero/prestazioni ambulatoriali, non contengano indicazioni che possano ricondurre il certificato alla disciplina di erogazione della prestazione e comunque allo stato di salute del paziente";

- "il dirigente della UOC Affari Generali della AST ha provveduto ad avviare una istruttoria interna e quindi ad acquisire informazioni presso la UOC Servizio informatico aziendale e la UOC Governo clinico e gestione del rischio al fine di operare gli opportuni controlli sulla modulistica attualmente in uso come quella richiamata nel reclamo in parola e, avviato l'immediata predisposizione e comunicazione – con nota (..) del XX - ai Direttori delle macro aree sanitarie interessate della nuova modulistica (certificazioni rilasciate ai pazienti o loro accompagnatori per attestare la presenza in ospedale e giustificare ad es., l'assenza dal lavoro) conforme alle disposizioni dettate dal Garante e, quindi, tale da garantire il rispetto della normativa di settore, nella quale non sono riportate indicazioni della struttura presso la quale è stata erogata la prestazione, timbri con la specializzazione dei sanitari, o, comunque informazioni che possono far risalire allo stato di salute. Detta nota è stata pubblicata sulla rete intranet aziendale";

- "il XX si è tenuto un incontro con i Direttori/Responsabili delle diverse articolazioni organizzative dell'AST, al fine di sensibilizzare gli stessi all'utilizzo della modulistica inviata";

- "con nota (…) del XX, il Direttore medico del P.O.U trasmetteva altresì a tutti i direttori delle unità operative complesse, strutture semplici (…) la predetta nota (…) del XX al fine di uniformare in tutte le UU.OO.CC. le modalità di rilascio dei certificati all'utenza/giustificativi per assenze in adesione alla normativa dettata dal Garante della privacy";

- "il Dirigente della U.O.C SIA ha verificato che le ditte fornitrici di software contenenti, tra l'altro le attestazioni amministrative inerenti alle visite mediche/prestazioni ambulatoriali hanno adeguato dette attestazioni alle disposizioni impartite dal Garante privacy";

- "con nota (…) del XX, il Direttore della UOC Affari generali chiedeva ai Direttori di Macro area interessate un riscontro urgente circa lo stato di applicazione della circolare di cui alla succitata nota (..) del XX" i quali confermavano la presa visione e l'applicazione della circolare;

- "nella ex Area Vasta 5 (oggi AST di Ascoli Piceno) l'attività di formazione dei dipendenti rispetto alla nuova normativa di cui al Regolamento UE 2016/679 in ambito sanitario ha visto l'avvio nel XX. Fatto salvo il periodo della pandemia COVID-19 la formazione obbligatoria privacy di base è proseguita nel XX e nel XX. (…) l'Area Vasta 5 prima e l'AST di Ascoli Piceno hanno accreditato -attraverso l'U.O. Formazione aziendale - un corso e-learning modalità FAD asincrona (…)". Nell'anno XX il suddetto corso è stato svolto da 623 dipendenti, nel XX da 99 dipendenti e "l'attuale Direzione AST di Ascoli Piceno ha previsto che le iniziative formative sul GDPR e la normativa privacy abbiano seguito anche per il XX al fine di effettuare con continuità detto aggiornamento, a garanzia della riservatezza, dell'integrità e della disponibilità dei dati personali trattati ogni giorno in tutta l'azienda".

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 all'Azienda, 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 novembre 1981).

In particolare, l'Ufficio, nel predetto atto, ha ritenuto che l'Azienda ha effettuato un trattamento di dati sulla salute della reclamante non conforme alle disposizioni di cui agli artt. 5, par. 1, lett. c) e f), 25 e 32 del Regolamento, in violazione dei principi di minimizzazione, di integrità e riservatezza, di protezione dei dati fin dalla progettazione (privacy by design) nonché degli obblighi in materia di sicurezza del trattamento, indicando, nei moduli di certificazione, richiesti dalla paziente per giustificare l'assenza dal lavoro, il reparto presso il quale l'interessata ha effettuato la prestazione sanitaria e il timbro con la specializzazione del sanitario.
Con nota trasmessa, via PEC, il XX, la medesima struttura sanitaria ha fatto pervenire le proprie memorie difensive, nelle quali, in particolare, oltre a ribadire quanto già indicato nella nota del XX, ha evidenziato che:

- "la comunicazione prot.n. XX del XX, acquisita al protocollo aziendale con prot.n. XX, per quanto di competenza dell'Azienda, era stata trasmessa a mezzo Paleo (sistema di gestione informatizzata di protocollo aziendale) al DPO interno della AST di Ascoli Piceno (…) che, in quanto tale, avrebbe dovuto gestire la pratica in oggetto e quindi ottemperare alla richiesta di informazioni nella tempistica indicata";

- "appresa solamente in data XX la notizia del mancato riscontro da parte del DPO in ordine al reclamo in oggetto, il Direttore della UOC Affari Generali e contenzioso si attivava prontamente per poter raccogliere - con ogni urgenza - tutte le informazioni del caso attraverso l'avvio di una istruttoria interna, anche in considerazione del fatto che, nel frattempo, il predetto DPO cessava dal servizio XX e che la U.O.C Acquisti e Logistica di questa azienda aveva concluso la procedura di appalto per affidamento diretto del servizio biennale di DPO (…)";

- "sin dal XX e di seguito con l'allegata nota prot.n. XX del XX (…), il Direttore medico del Presidio Ospedaliero di San Benedetto del Tronto aveva fornito specifiche raccomandazioni in merito al rispetto della privacy con specifico riferimento alle certificazioni richieste all'utenza fornendo all'uopo idonea modulistica, comunicata ai Direttori delle UU.OO.CC. ospedaliere afferenti al predetto nosocomio. Nell'ottica del processo di integrazione tra le articolazioni organizzative afferenti alla medesima Area Vasta, detta nota veniva trasmessa alla Direzione medica del Presidio ospedaliero di Ascoli Piceno e al Referente privacy unico di Area Vasta (…)";

- "dalla dinamica dei fatti si deduce che il personale medico interessato non aveva alcuna intenzione di cagionare alcun pregiudizio alla Sig.ra XX. L'entità della gravità è qualificabile nel suo complesso come lieve, in quanto ad esempio nel caso dell'attestato, datato XX non è riportata alcuna intestazione, ma soltanto un timbro sbiadito, quasi illeggibile, del medico di riferimento, che, per imprudenza, ha utilizzato il timbro de quo. Diversa l'attestazione di presenza del XX che riporta nell'intestazione del foglio la U.O.C. e il Direttore del reparto";

- "il Titolare del Trattamento e il Direttore dell'UOC Affari Generali e Contenzioso, in raccordo con lo scrivente nuovo DPO, nel mese di febbraio dell'anno corrente, e procedendo ad una riorganizzazione aziendale, in osservanza dei principi della privacy by design e della privacy by default, hanno messo in campo task force e interventi urgenti, per scongiurare ulteriori condotte similari; ribadendo che si è di fronte ad un primo e isolato evento, la condotta in oggetto è qualificabile come "violazione minore"";

- “(…) l’erronea condotta nel trattamento dei dati effettuato dall’Azienda è relativa ad un solo interessato, circostanza quest’ultima attenuante la gravità della condotta”;

- “si conclude che, ad ogni buon conto, l’intenzione dell’AST di AP, a seguito dell’accaduto, è quella di scusarsi con l’interessata per l’eventuale pregiudizio arrecato e adottare ulteriori iniziative e atti, volti a sensibilizzare il personale al rispetto della disciplina dei dati personali”.

Durante l’audizione, che si è tenuta in data XX, la parte ha inteso precisare che:

- “l’AST pone l’attenzione sul profondo cambiamento organizzativo subito a partire dal XX, che ha comportato la necessità di emanare gli atti costitutivi della stessa Azienda e rivedere tutti i documenti e le procedure nonché la compliance dell’Azienda, prima gestite a livello centrale da parte di ASUR Marche”;

- “non appena conosciuti i fatti alla base del reclamo, l’Azienda si è prontamente attivata al fine di fornire riscontro all’Autorità e dare nuovamente disposizioni formali affinché venissero messe in atto i comportamenti corretti previsti dalla norma”;

- “il complesso processo di riorganizzazione non ha consentito un propedeutico passaggio di consegne tra i tre DPO che si sono avvicendati nell’ultimo periodo”;

- “è stata predisposta una nuova formazione nei confronti dei dipendenti dell’Azienda, oltre a quella già svolta negli anni precedenti”.

3 Esito dell’attività istruttoria

Preso atto di quanto rappresentato dall’Azienda nella documentazione in atti e nelle memorie difensive, si osserva che:

1. Per “dato personale” si intende “qualsiasi informazione riguardante una persona fisica identificata o identificabile (“interessato”)” e, per “dati relativi alla salute” quelli “attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute” (art. 4, par. 1, nn. 1 e 15, del Regolamento). Il considerando n. 35 del Regolamento precisa poi che i dati relativi alla salute “comprendono informazioni sulla persona fisica raccolte nel corso della sua registrazione al fine di ricevere servizi di assistenza sanitaria”.

2. In base al Regolamento, i dati personali devono essere “adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («principio di minimizzazione dei dati»)” 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 («principio di integrità e riservatezza»)” (art. 5, par. 1, lett. c) e f) del Regolamento).

3. I dati personali, devono essere, altresì, essere 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).

4. Secondo il principio di responsabilizzazione, il titolare del trattamento deve conformarsi ed essere in grado di comprovare sia il rispetto dei principi che degli adempimenti previsti dal Regolamento (artt. 5, par. 2 e 24 del Regolamento). Il titolare è, pertanto, tenuto ad

effettuare una valutazione in ordine alla pertinenza e non eccedenza delle informazioni trattate, al fine di garantire l'effettiva applicazione del principio di minimizzazione (artt. 5, par. 2 e 25 del Regolamento; cfr. anche punti 49, 51 e par. 3.5 delle Linee guida 4/2019 sull'articolo 25, Protezione dei dati fin dalla progettazione e per impostazione predefinita, adottate il XX).

5. Il titolare del trattamento è, inoltre, tenuto ad adottare misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio, tenendo conto, in special modo, dei rischi che derivano dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati (art. 32 del Regolamento).

6. Con specifico riferimento alla fattispecie in esame, si evidenzia che gli organismi sanitari devono mettere in atto specifiche procedure dirette a prevenire nei confronti di estranei un'esplicita correlazione tra l'interessato e reparti o strutture, indicativa dell'esistenza di un particolare stato di salute (cfr. art. 83 del Codice e art. 22, comma 11, d.lgs. 10 agosto 2018, n. 101 nonché provvedimento generale del Garante del 9 novembre 2005, doc. web n. 1191411, nel quale il Garante aveva espressamente previsto che "tali cautele devono essere orientate anche alle eventuali certificazioni richieste per fini amministrativi non correlati a quelli di cura (ad es., per giustificare un'assenza dal lavoro o l'impossibilità di presentarsi ad una procedura concorsuale)" (par. 3, lett. g) del citato provvedimento; cfr. art. 22, comma 4, del citato d.lgs. n. 101/2018). Il predetto orientamento è stato, altresì, ribadito nella Newsletter n. 398 del 9 febbraio 2015, doc. web n. 3710265, nella quale il Garante ha precisato che "nelle certificazioni rilasciate ai pazienti o ai loro accompagnatori per attestare la presenza in ospedale e giustificare ad es. l'assenza dal lavoro, non devono essere riportate indicazioni della struttura presso la quale è stata erogata la prestazione, il timbro con la specializzazione del sanitario, o comunque informazioni che possano far risalire allo stato di salute (…) Tali cautele devono essere osservate anche nella stesura delle certificazioni richieste per fini amministrative (ad es. per giustificare un'assenza dal lavoro o l'impossibilità di partecipare ad un concorso)" (sul tema, cfr., altresì, il punto 8.2. delle "Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico" - 14 giugno 2007, doc. web n. 1417809, nel quale è stato precisato che, con specifico riguardo al trattamento di dati idonei a rivelare lo stato di salute dei lavoratori, la sussistenza di specifici obblighi normativi nei riguardi del lavoratore per consentire al datore di lavoro di verificare le sue reali condizioni di salute nelle forme di legge, giustifica che venga fornita all'amministrazione di appartenenza un'apposita documentazione a giustificazione dell'assenza, consistente in un certificato medico contenente la sola indicazione dell'inizio e della durata presunta dell'infermità: c.d. "prognosi". In assenza di speciali disposizioni di natura normativa, che dispongano diversamente per specifiche figure professionali, il datore di lavoro pubblico non è legittimato a raccogliere certificazioni mediche contenenti anche l'indicazione della diagnosi).

7. L'art. 157 del Codice, prevede che "Nell'ambito dei poteri di cui all'articolo 58 del Regolamento e per l'espletamento dei propri compiti, il Garante può richiedere al titolare, al responsabile, al rappresentante del titolare o del responsabile, all'interessato o anche a terzi di fornire informazioni e di esibire documenti anche con riferimento al contenuto di banche di dati".

4. Conclusioni

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 dall'Azienda, in qualità di titolare del trattamento, nelle memorie difensive sopra richiamate e nel corso dell'audizione 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.

Si rileva, infatti, che il quadro normativo e provvedimentale sopra delineato risale ad un periodo temporale di gran lunga precedente rispetto alla riorganizzazione della sanità regionale, avvenuta ad opera della Legge Regionale n. 19/2022 che ha disposto, a partire dal XX, la soppressione dell'ASUR Marche, e il subentro delle Aziende Sanitarie Territoriali. I principi sopra indicati e le diverse descritte occasioni nelle quali il Garante ha fornito un chiaro e specifico quadro di garanzie, hanno rappresentato, da molto tempo, un orientamento ben consolidato, che avrebbe dovuto essere conosciuto e tenuto in considerazione già prima delle modifiche del nuovo assetto sanitario regionale, con le conseguenti difficoltà organizzative, aggravate dall'emergenza pandemica. Inoltre, l'avvicendarsi, in poco tempo, di più Responsabili della protezione dei dati (la cui designazione deve avvenire, ai sensi dell'art. 37, par. 5, del Regolamento, in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'art. 39 del medesimo Regolamento), non esonera il titolare del trattamento dalla verifica del rispetto della normativa in materia di protezione dei dati, sia in relazione all'assolvimento dell'obbligo di fornire le informazioni richieste dal Garante, ai sensi dell'art. 157 del Codice, sia con riferimento alla predisposizione e all'adozione di misure volte a prevenire nei confronti di estranei (e, in particolare, del datore di lavoro) un'esplicita correlazione tra l'interessato e reparti o strutture, indicativa dell'esistenza di un particolare stato di salute. Inoltre, nell'evidenziare che spetta al titolare del trattamento la valutazione dell'analisi del possesso dei requisiti del Responsabile della protezione di dati necessari per lo svolgimento dei suoi compiti, si osserva, altresì, che "la prassi di instaurare contatti, solo saltuari, tra il soggetto pubblico e il proprio RPD (sia interno che esterno) vanifica il senso della presenza del RPD e, con esso, l'approccio di privacy by design e by default promosso dal Regolamento, con conseguenze dirette in capo agli enti stessi in termini di accountability e di inadempimento agli obblighi regolamentari (ad esempio, ai sensi degli art. 82 e 83 del Regolamento). (…), si è riscontrato che tale atteggiamento può essere imputabile a entrambe le parti: al RPD, in quanto spesso portato a non proporre adeguatamente al titolare le attività necessarie per conformare i trattamenti alla disciplina in materia di protezione dei dati personali; all'ente pubblico, per la tendenza a considerare la nomina del RPD solo come un adempimento formale, non riconoscendo e tantomeno valorizzando i compiti e le potenzialità di questa figura" (cfr. punti 5 e 8 del "Documento di indirizzo su designazione, posizione e compiti del Responsabile della protezione dei dati (RPD) in ambito pubblico", documento allegato al provvedimento del 29 aprile 2021 n. 186, doc. web n. 9589467).

Ciò premesso, si rileva che l'Azienda, omettendo di fornire riscontro alla richiesta di informazioni dell'Autorità, formulata, ai sensi dell'art. 157 del Codice, ha posto in essere una violazione dell'art. 157 medesimo e, indicando, nei moduli di certificazione, richiesti dalla paziente per giustificare l'assenza dal lavoro, il reparto presso il quale l'interessata ha effettuato la prestazione sanitaria e il timbro con la specializzazione del sanitario, ha effettuato un trattamento di dati sulla salute in violazione del principio di minimizzazione, di integrità e riservatezza dei dati (artt. 5, par. 1, lett. c) e f) del Regolamento) e, non avendo, fin dalla predisposizione dei predetti modelli di certificazione, adottato adeguate misure per garantire l'effettiva applicazione del richiamato principio di minimizzazione, non ha rispettato il principio di privacy by design e gli obblighi in materia di sicurezza del trattamento (artt. 25 e 32 del Regolamento).

Per tali ragioni si rileva l'illiceità del trattamento di dati sulla salute effettuato dall'Azienda, nei termini di cui in motivazione, per la violazione degli artt. 5, par. 1, lett. c) e f), 25, 32 del Regolamento nonché dell'art. 157 del Codice.

In tale quadro, considerato che la condotta ha esaurito i suoi effetti e rilevato che l'Azienda ha modificato le modalità di rilascio dei certificati all'utenza e dei giustificativi per assenze in linea con la normativa sopra richiamata, verificandone la corretta applicazione e ha effettuato una specifica formazione in materia di protezione dei dati personali, 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. c) e f), 25 e 32 del Regolamento nonché dell'art. 157 del Codice, causata dalla condotta dell'Azienda è soggetta all'applicazione della sanzione amministrativa pecuniaria ai sensi dell'art. 83, par. 4, lett. a) e par. 5, lett. a) del Regolamento (cfr. art. 166, comma 2, del Codice).

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

Alla luce di quanto sopra illustrato e, in particolare, della categoria di dati personali interessata dalla violazione, del numero di interessati (pazienti), anche potenzialmente coinvolti, della natura del trattamento, nonché dalla durata della violazione, 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).

Tenuto conto che la violazione degli artt. 5, par. 1, lett. c) e f), 25, 32 del Regolamento ha avuto luogo in conseguenza di un'unica condotta (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 (che, nel caso di specie, riguarda l'art. 5, par. 1, lett. c) e f) del Regolamento).

Ciò premesso, 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 trattamento dei dati effettuato dall'Azienda ha riguardato dati idonei a rilevare informazioni sulla salute di una interessata, ma potenzialmente, di altri soggetti che hanno richiesto una certificazione amministrativa per giustificare l'assenza dal lavoro (art. 83, par. 2, lett. a) e g) del Regolamento);

- sotto il profilo riguardante l'elemento soggettivo la violazione ha carattere colposo (art. 83, par. 2, lett. b) del Regolamento);

- il titolare, al fine di evitare la ripetizione dell'evento occorso, si è impegnato nell'introduzione di misure volte a ridurre la replicabilità dell'evento occorso (art. 83, par. 2, lett. c) del Regolamento);

si ritiene di determinare l'ammontare della sanzione pecuniaria prevista dall'art. 83, par. 5 del Regolamento, nella misura di euro 13.000,00 (tredicimila/00) per la violazione degli artt.

5, 25 e 32 del medesimo Regolamento, quale sanzione amministrativa pecuniaria ritenuta, ai sensi dell'art. 83, par. 1, del Regolamento, effettiva, proporzionata e dissuasiva.

Considerato che la distinta condotta relativa alla violazione dell'art. 157 del Codice è soggetta alla sanzione amministrativa pecuniaria di cui all'art. 83, par. 5, del Regolamento (art. 166, comma 2 del Codice), l'importo totale della sanzione è da quantificarsi tenendo presente il massimo edittale cd. "statico" stabilito da Regolamento, pari al limite massimo di 20.000.000 di euro.

In relazione a ciò, si ritiene che, in tale circostanza, il livello di gravità, sulla base degli elementi di cui all'art. 83, par. 2, lett. a), b) del Regolamento, è da considerarsi media, tenuto conto del fatto che non emerge alcun comportamento doloso da parte del titolare del trattamento.

In ragione dei suddetti elementi, valutati nel loro complesso, si ritiene di determinare l'ammontare della sanzione pecuniaria nella misura di euro 4.000,00 (quattromila/00) per la violazione dell'art. 157 del Codice.

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

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

TUTTO CIÒ PREMESSO IL GARANTE

dichiara l'illiceità del trattamento di dati personali effettuato dall'Azienda Sanitaria Territoriale di Ascoli Piceno, per la violazione dei principi di cui all'art. 5, par. 1, lett. c) e f), 25 e degli obblighi di cui all'art. 32 del Regolamento, nonché dell'art. 157 del Codice, nei termini di cui in motivazione;

ORDINA

all'Azienda Sanitaria Territoriale di Ascoli Piceno, con sede legale in Ascoli Piceno (AP), Via degli Iris – 63100, Codice Fiscale/Partita Iva 02500670449, di pagare la somma di euro 17.000,00 (diciassettemila/00) a titolo di sanzione amministrativa pecuniaria, ai sensi degli artt. 58, par. 2, lett. i) e 83 del Regolamento, per la violazione indicata nel presente provvedimento; si rappresenta che il contravventore, ai sensi dell'art. 166, comma 8, del Codice, ha facoltà di definire la controversia mediante pagamento, entro il termine di 30 giorni, di un importo pari alla metà della sanzione comminata;

INGIUNGE

alla predetta Azienda, in caso di mancata definizione della controversia ai sensi dell'art. 166, comma 8, del Codice, di pagare la somma di euro 17.000,00 (diciassettemila/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;

DISPONE

la pubblicazione per intero del presente provvedimento sul sito web del Garante, ai sensi dell'art. 166, comma 7, del Codice, e ritiene che ricorrano i presupposti per l'annotazione nel registro interno dell'Autorità 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, 26 settembre 2024

IL PRESIDENTE
Stanzione

IL RELATORE
Stanzione

IL SEGRETARIO GENERALE
Mattei