Ordinanza ingiunzione nei confronti di Azienda Usl Valle d’Aosta - 10 novembre 2022 [9819792]

VEDI ANCHE Newsletter del 28 novembre 2022

[doc. web n. 9819792]

Ordinanza ingiunzione nei confronti di Azienda Usl Valle d’Aosta - 10 novembre 2022

Registro dei provvedimenti
n. 371 del 10 novembre 2022

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, alla quale hanno preso parte il prof. Pasquale Stanzione, presidente, la prof.ssa Ginevra Cerrina Feroni, vicepresidente, 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 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, in www.gpdp.it, doc. web n.1098801;

Relatore l’avv. Guido Scorza;

PREMESSO

1. Il reclamo e l’attività istruttoria

L’Autorità ha ricevuto il reclamo della Sig.ra XX in cui ha lamentato ripetuti accessi al proprio

dossier sanitario aziendale da parte di un operatore sanitario operante presso una struttura di riabilitazione dell'Azienda Usl della Valle d'Aosta, ove la stessa ha dichiarato di non aver mai ricevuto assistenza sanitaria. La reclamante inoltre ha rappresentato di aver negato il consenso al trattamento dei suoi dati personali attraverso il dossier sanitario aziendale.

In relazione a quanto segnalato, per i profili di competenza in materia di protezione dei dati personali, l'Ufficio ha richiesto informazioni alla predetta Azienda con nota del XX (prot. n. XX), con riferimento alla quale quest'ultima ha risposto con la nota del XX in cui è stato rappresentato, in particolare, che:

- "la reclamante XX risulta aver espresso consenso NO al dossier in data 30/01/2019 (…). Fino alla data del 17/03/2020 (quando si è ritenuto opportuno disattivare temporaneamente le regole del dossier per i motivi descritti al successivo par. SITUAZIONE DOSSIER SANITARIO IN EMERGENZA COVID, pag. 5) la volontà espressa dall'assistita è stata rispettata e pertanto gli operatori coinvolti nel processo di cura potevano consultare solo i dati/documenti clinici generati dalle rispettive strutture di appartenenza (in ottemperanza a quanto prescritto dalle Linee Guida in materia di dossier sanitario – 4 giugno 2015)";

- "a seguito di istruttoria interna è emersa la veridicità di quanto segnalato dalla reclamante. Nello specifico dai log degli accessi al dossier (…) è risultato che la signora XX (con rapporto di lavoro in somministrazione presso l'Azienda scrivente), appartenente al profilo "logopedista" (…), nel periodo dal 15/03/2021 al 06/12/2021 ha effettuato degli accessi dalla propria postazione di lavoro presso il Consultorio di Saint Pierre, (codificato nel sistema informativo sanitario aziendale come "Riab. Terr. ST. PIERRE"), afferente alla Struttura Complessa denominata "Distretti 1-2";

- "si può sicuramente affermare che l'operatrice non ha visualizzato documenti clinici relativi ai risultati delle visite sostenute avendo potuto solo prendere visione di una lista di episodi già effettuati o prenotati, da cui si evince esclusivamente la tipologia di prestazione";

- "Questo tipo di visualizzazione è stato reso possibile, pur non essendo la reclamante in cura presso il Consultorio di Saint Pierre nelle date oggetto di segnalazione, in quanto, a partire dal 17/03/2020, a causa dell'emergenza Covid, l'Azienda ha autorizzato un allentamento delle regole di visibilità del dossier";

- presso la predetta Azienda è in uso "TrakCare (un applicativo di tipo ERP - Enterprise Resource Planning- che ha come obiettivo la gestione di tutte le funzioni ospedaliere e ambulatoriali)" "su cui ruota e converge la quasi totalità dei dati. Nella soluzione in uso presso l'Azienda USL della Valle d'Aosta anche le attività territoriali sono gestite informaticamente da TrakCare. Oltre al predetto gestionale il sistema informativo clinico è costituito da ulteriori soluzioni verticali (cosiddetti sistemi producer) che generano documenti clinici che, dopo la firma digitale, sono inviati al Repository X1V1 (sistema di archiviazione intermedio tra i sistemi producer e il vero e proprio sistema di conservazione digitale), richiamabile anch'esso da TrakCare per la consultazione dei documenti". "Allo stato dell'arte si è convenuto che TrakCare potesse assumere il ruolo di dossier";

- con "nota prot. n. XX" la predetta Azienda ha chiesto "alla ditta Intersystems, proprietaria del prodotto TrakCare, di implementare le regole di visibilità delle informazioni come da indicazioni delle Linee Guida" del Garante del 2015. È stata pertanto realizzata la procedura di seguito descritta: a) il flusso operativo gestito prevede in prima istanza, al richiamo di una qualsiasi anagrafica assistito, la verifica della presenza o meno del consenso alla costituzione del dossier e, nel caso in cui l'assistito non l'abbia ancora espresso, la sua raccolta. b) sulla base della profilazione degli operatori ed in base al contesto (paziente in cura o meno, episodio con richiesta di oscuramento, etc…), il sistema applica i dovuti filtri

che definiscono la visualizzazione delle informazioni o meno. c) in TrakCare ogni operatore è assegnato ad un “gruppo/profilo”. Il “gruppo/profilo” di cui fa parte determina quello che può “fare” e quello che può “vedere”. Quando i filtri privacy sono attivi, in base ad una matrice di regole, TrakCare permette all’operatore di vedere ed eventualmente operare solo su episodi di competenza del profilo. Vengono tenute anche in considerazione l’espressione del consenso al dossier e se il paziente è “in cura” (cioè c’è un episodio “aperto/corrente”) per la specialità dell’operatore”. “Inoltre, per governare possibili emergenze o casistiche particolari, è stata implementata una funzione definita “Break The Glass” attivabile dai soli medici, che annulla tutti i filtri permettendo di visualizzare tutte le informazioni presenti nel sistema a condizione di aver registrato il motivo dell’utilizzo”;

- “Proprio questa visibilità parziale del profilo “logopedista” ha impedito che l’operatore che ha effettuato accessi impropri potesse consultare i referti delle prestazioni effettuate dalla reclamante anche in una situazione di disattivazione delle regole del dossier, consentendogli solo una vista su liste di episodi prenotati o effettuati, ma senza la possibilità di entrare dentro i singoli episodi e visionare la documentazione clinica prodotta”;

- “Tutte le azioni di visualizzazione dei dati (log accessi) vengono tracciate e possono essere estratte solo da alcuni operatori autorizzati”;

- “Da un punto di vista clinico, il contesto emergenziale ha costretto (ed ancora oggi obbliga) l’ospedale ad accorpare la quasi totalità dei reparti non COVID e a realizzare reparti COVID dedicati” “con tutte le conseguenze gestionali, cliniche ed organizzative derivanti” “era quindi necessario permettere di accedere, secondo le esigenze del momento, alle informazioni sanitarie di TrakCare. Infatti, secondo le rigide regole del dossier precedentemente vigenti, i sanitari di cui sopra, medici e altri operatori sanitari afferenti a Strutture e/o discipline specialistiche diverse, non avrebbero potuto, di fatto, accedere alla cartella clinica e ai dati sanitari di pazienti ricoverati in reparti COVID (formalmente assegnati al reparto di Pneumologia) o in reparti non COVID multi-specialistici e dunque non sarebbero stati in grado di assistere adeguatamente i pazienti”;

- “In relazione al personale medico nella fase iniziale si è consigliato di utilizzare il “Break the glass” (…) per sopperire all’impossibilità di visualizzare i dati completi della situazione corrente e storica dei pazienti per i quali non erano abilitati. L’utilizzo di tale funzione comportava però un notevole appesantimento nell’operatività (questa funzione va attivata per ogni singolo episodio e ricerca con indicazione del motivo), per cui al fine di permettere una fruibilità adeguata alla gestione della pandemia in corso, con nota Prot. n.XX del XX (v. All.XX), il Direttore Sanitario Aziendale ha autorizzato la disabilitazione del dossier Sanitario, fino alla fine dello stato di emergenza”;

- “In merito si ritiene di dover sottolineare come l’allentamento delle regole sul dossier trovava il proprio fondamento giuridico dapprima nell’art. 14 del D.L. 14/2020, e, successivamente nell’art. 17 bis (Disposizioni sul trattamento dei dati personali nel contesto emergenziale) del decreto legge 17 marzo 2020, n. 18 convertito nella legge 24 aprile 2020, n. 27, la cui efficacia è stata prorogata, in ultimo, fino al 31/03/2022 (data di cessazione dello stato di emergenza) dalla Tabella Allegato A (punto 3), richiamata dall'art. 16 comma 1 del decreto legge 24 dicembre 2021, n. 221, convertito con modificazioni nella legge 18 febbraio 2022, n. 11”;

- “Poiché, nella versione dell’applicativo TrakCare installata presso l’ospedale di Aosta (TrakCare T2014), il parametro che governa l’applicazione dei filtri del dossier è di sistema (questo significa che o è attivo o non lo è), nell’attuale versione non è possibile selezionare l’attivazione dei filtri rispetto a Reparti, Ambulatori/Servizi (non potendosi quindi operare una distinzione tra servizi ospedalieri e servizi territoriali). Nel momento in cui si disattivano i filtri,

il software TrakCare non è più nella possibilità di applicare le regole di visibilità indicate a livello di paziente, con la conseguente situazione che si visualizzano temporaneamente, ovvero limitatamente fino al perdurare dello stato di emergenza, anche le informazioni di coloro che hanno negato il consenso al dossier, cessato il quale si ripristineranno le limitazioni alla visibilità precedentemente impostate". "Tale limite tecnico verrà risolto nella nuova versione, che sarà installata nel corso dell'anno 2022 con il Consens manager che consentirà di gestire separatamente • consenso alla costituzione del DSE; • consenso collegato al singolo evento (oscuramento e deoscuramento dei DCE); • un gestore delle policy di accesso ai documenti (Privacy manager)" "Tale decisione si è concretizzata con la Determinazione dirigenziale n. 710 del 09/08/2021 avente ad oggetto "Aggiudicazione della "procedura telematica per l'affidamento dei servizi di progettazione, sviluppo e reingegnerizzazione, manutenzione applicativa e supporto, gestione dell'esercizio dei sistemi informativi sanitari in uso all'Azienda Usl della Valle d'Aosta mediante appalto specifico nell'ambito dell'Accordo Quadro per i servizi applicativi per le pubbliche amministrazioni stipulato da Consip – id 1881 - Lotto 1 CIG: 861432805" in favore del concorrente RTI Accenture S.p.a., Accenture Technology Solutions S.r.l., Gpi S.p.a., Pricewaterhousecoopers Public Sector s.r.l." e con la stipula del relativo contratto in data 18/01/2022, che ha preso formalmente avvio nel mese di febbraio c.a. e la cui realizzazione è prevista entro 8 mesi dalla presa in carico";

- "Il Direttore della SC Distretti 1-2 Dott.ssa XX (a cui afferisce il Consultorio di Saint Pierre che interessa il caso che ci occupa) con nota prot. XX del XX (v. XX) ha comunicato di aver raccolto, con il supporto della SC Sistemi Informativi e Telecomunicazioni, i dati relativi agli accessi effettuati dalla Sig.ra XX nelle date indicate e di aver richiesto alla stessa le motivazioni di tale comportamento (…). Con successiva nota prot. XX del XX (v…) comunicava di aver richiamato verbalmente la predetta XX al rispetto dell'osservanza del regolamento vigente in merito alla privacy e di aver contestualmente provveduto, con nota Prot. n. XX del XX (…), ad effettuare segnalazione alla SC Sviluppo delle Risorse Umane di quanto avvenuto, per gli eventuali provvedimenti disciplinari. Al fine di evitare il ripetersi di simili situazioni la Dott.ssa XX ha inoltre dichiarato di aver colto l'occasione per sensibilizzare tutto il personale afferente ai Distretti 1 e 2 sull'argomento";

Nell'allegato 7 alla nota di riscontro alla richiesta di informazioni, denominato "Motivazioni XX", su cui è apposta la firma autografa della sig.ra XX, è riportato che la stessa ha acceduto al dossier della reclamante, nonché sua collega, per "mera curiosità".

Nella richiamata nota del direttore sanitario della predetta Azienda del XX è stato indicato che "In relazione all'oggetto, si comunica che l'art. 14 del D.L. 14/2020, ha fornito, tra l'altro, indicazioni concernenti il trattamento dei dati particolari e giudiziari nell'attuale momento emergenziale. La disposizione, in sostanza, mira a bilanciare il diritto alla tutela dei dati personali con quello più generale alla tutela della sicurezza e della salute pubblica, introducendo un regime eccezionale che consente, a determinati soggetti, di effettuare il trattamento dei dati sanitari, compresa la loro comunicazione. In tale ambito, i soggetti operanti nel sistema di protezione civile (Stato, Ragioni, Province Autonome di Trento e Bolzano, Enti locali), i loro soggetti attuatori, le strutture pubbliche e private del Servizio sanitario nazionale possono, per motivi di interesse pubblico e per la diagnosi e l'assistenza dei contagiati, comunicare tra di loro i dati personali degli interessati. Nel contesto ospedaliero tale disposizione può tradursi nella possibilità, per tutti i medici e infermieri, di accedere all'applicativo Trackare per la consultazione e la comunicazione fra di loro dei dati personali dei pazienti degenti nei 3 presidi ospedalieri, sussistendo quei motivi di interesse pubblico e di assicurare la diagnosi e l'assistenza sanitaria dei contagiati nel contesto emergenziale conseguente al COVID 19, prevista dalla norma". La nota inoltre prosegue evidenziando che "In sostanza e operativamente: dalle 13:00 di oggi, 17/03/2020, siamo nelle condizioni di disabilitare le funzioni Privacy che gestiscono, per l'intero site TrakCare (quindi profili

utente Medici, Infermieri, Amministrativi ecc...), i concetti legati alla visibilità delle informazioni. Di fondo, la visibilità dei dati sarà quindi completa/generale e non più filtrata in base alla competenza".

Nella predetta nota di rimozione dei "filtri privacy", l'Azienda ha ricordato "la necessità di corretto e responsabile utilizzo della modalità di accesso libero, del quale andrà informato solamente il personale interessato" e ricordava "che dovranno comunque essere osservate le misure minime di sicurezza più volte oggetto di comunicazioni aziendali";

In relazione alle risultanze della predetta attività istruttoria, l'Ufficio, con atto n.XX del XX, ha notificato all'Azienda Usl della Valle d'Aosta (di seguito Azienda), ai sensi dell'art. 166, comma 5, del Codice, l'avvio del procedimento per l'adozione dei provvedimenti di cui all'articolo 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 24/11/1981).

In particolare, nella predetta nota l'Ufficio, ha evidenziato che la disciplina dettata dall'art. 17-bis del d.l. n. 18/2020, richiamata dall'Azienda nella documentazione trasmessa, non ha e non avrebbe potuto derogare alla disciplina sulla protezione dei dati che, come è noto, si fonda su un Regolamento europeo, bensì ha previsto alcune semplificazioni nel trattamento e nella comunicazione dei dati personali fra diversi titolari del trattamento solo qualora le stesse risultino indispensabili ai fini dello svolgimento delle attività connesse alla gestione dell'emergenza sanitaria in atto e comunque nel rispetto dei princìpi di cui all'articolo 5 del Regolamento, adottando misure appropriate a tutela dei diritti e delle libertà degli interessati.

Al riguardo, l'Ufficio ha inoltre rappresentato come l'Autorità abbia più volte evidenziato la necessità di valutare l'applicabilità della disciplina di cui al citato art. 17-bis del d.l. n. 18 del 2020 caso per caso, richiamando l'attenzione dei titolari del trattamento, anche operanti in ambito sanitario, sulla circostanza che non tutti i trattamenti e le comunicazioni di dati sulla salute possono essere ricondotte a tale disposizione (cfr. tra molti, nota del 9 giugno 2020, doc. web n. 9429175). L'Ufficio ha pertanto rilevato che l'art. 17-bis d.l. n. 18 del 2020, citato dall'Azienda quale disposizione legittimante la "possibilità, per tutti i medici e infermieri, di accedere all'applicativo Trackare per la consultazione e la comunicazione fra di loro dei dati personali dei pazienti degenti nei 3 presidi ospedalieri, sussistendo quei motivi di interesse pubblico e di assicurare la diagnosi e l'assistenza sanitaria dei contagiati nel contesto emergenziale conseguente al COVID 19, prevista dalla norma", non può essere considerata quale norma derogatoria al caso di specie dell'obbligo di acquisizione del consenso dell'interessato, né del rispetto dei principi di liceità, correttezza e trasparenza e di integrità e sicurezza.

È stato poi rilevato che con riferimento al trattamento dei dati personali oggetto d'esame lo stesso non riguarda prestazioni sanitarie erogate in emergenza, non afferisce ad un interessato che ha ricevuto prestazioni sanitarie legate al Covid-19 e non è stato effettuato da un operatore per assicurare interventi sanitari legati alla predetta pandemia, bensì per "mera curiosità".

Ciò stante, l'Ufficio ha contestato che la configurazione del dossier sanitario scelta dall'Azienda a seguito dell'emergenza sanitaria da Covid-19 è stata effettuata in violazione dei principi di base del trattamento di cui agli artt. 5, par. 1, lett. a) e f), e degli artt. 9, 25 e 32 del Regolamento. La violazione delle predette disposizioni rende applicabile la sanzione amministrativa prevista dall'art. 83, par. 4, lett. a) e par. 5, lett. a) del Regolamento.

Con nota del XX, l'Azienda ha inviato scritti difensivi e ha chiesto di essere sentita, ribadendo quanto già rappresentato in atti e evidenziando, in particolare, che:

- "la sospensione parziale dei filtri privacy è stata fin da subito bilanciata dal mantenimento di

due distinti profili (nurse/doctor) i quali consentivano una profondità di accesso ben differente l'uno dall'altro";

- "il Titolare si sia reso conto ben prima dell'evento oggetto del presente procedimento dei suddetti limiti tecnici e, quindi, avviando preventivamente un complesso processo di adeguamento tecnologico, si sia attivato per superare le criticità della versione TrakCare T2014 (parametro di sistema che governa l'applicazione dei filtri del Dossier) inserendo nell'appalto per i nuovi sistemi informativi sanitari specifiche tecniche volte a superare i limiti dell'attuale versione";

- "L'AUSL tiene a ribadire come la scelta di sospendere i filtri privacy si sia resa indispensabile per organizzare ed erogare - in tempi necessariamente ridottissimi - l'attività sia nei nuovi reparti Covid";

- "Il personale sanitario (medici ed infermieri) che si è trovato a turnare presso tutti i reparti COVID e non COVID (diventati reparti multi-specialistici e/o multichirurgici), dove erano ricoverati pazienti assegnati a Strutture specialistiche diverse (es. Chirurgia Vascolare + Pneumologia + Neurologia), non avrebbe più avuto la possibilità, alla luce del profilo di struttura assegnato (e, come detto, collegato al reparto di appartenenza), di accedere, secondo le esigenze del momento, alle informazioni sanitarie di TrakCare, né, d'altro canto, data l'elevatissima turnazione del personale nei reparti COVID, era ipotizzabile l'aggiornamento in tempo reale della profilazione in modo che fosse coerente con lo svolgimento dell'attività a favore dei ricoverati";

- "con riferimento all'interpretazione ed alla portata dell'art. 17-bis, l'AUSL ritiene che, se il Legislatore con la citata norma, nello spirito di "semplificazione" ha permesso a diversi titolari di essere facilitati nella comunicazione dei dati, non sembra errato dedurre come a maggior ragione lo stesso e unico Titolare (AUSL) poteva ritenersi legittimamente autorizzato a semplificare la "consultazione" dei dati di cui era, appunto, titolare da parte degli operatori AUSL coinvolti nella gestione dell'emergenza sanitaria";

- "inoltre, partendo dall'assunto che le deroghe introdotte dall'art. 17 bis valevano per lo svolgimento delle "attività connesse alla gestione dell'emergenza", l'AUSL ritiene doveroso interrogarsi su quale attività possa essere considerata più "connessa alla gestione dell'emergenza" se non quella specifica di cura dei pazienti COVID";

- l'"Azienda crede che la suddetta lista di prenotazioni, non possa essere considerata un dato relativo alla salute, quanto meno non in senso stretto";

- "l'accesso al Dossier ha avuto natura volontaria, ovvero l'operatrice - nonostante le precise istruzioni della Direzione che hanno accompagnato il temporaneo allentamento dei filtri - ha deliberatamente effettuato un accesso non giustificato";

- "A ben vedere, proprio l'unico fine che nel caso di specie ha mosso la scrivente AUSL (ovvero la tutela della salute pubblica), sembra ragionevolmente potersi ricondurre alle ipotesi di adempimento di un dovere, esercizio di una facoltà legittima e/o stato di necessità di cui all'artt. 4, L. n. 689/1981".

Il XX, mediante videoconferenza a distanza, si è svolta, ai sensi dell'art. 166, commi 6 e 7 del Codice, l'audizione dell'Azienda, durante la quale la stessa ha ribadito quanto già dichiarato in atti e ha rappresentato, in particolare, che:

- "Con la pandemia da Covid-19 l'impostazione relativa al trattamento dei dati personali prevista per il dossier sanitario aziendale costituiva un ostacolo allo svolgimento delle attività di cura, soprattutto con riferimento alla profilazione analitica dei ruoli degli operatori sanitari.

In particolare, nelle prime fasi dell'emergenza (marzo/aprile 2020) è stato necessario realizzare dei nuovi reparti dedicati alla cura del Covid-19 (quasi ¾ dei reparti ospedalieri), nonché convertire il personale sia di area medica, che chirurgica al servizio di tali reparti anche in considerazione dell'assenza del personale sanitario proprio a causa dello stesso Covid-19. Tale situazione ha portato le direzioni sanitarie e amministrative dell'Azienda a ritenere necessario eliminare i filtri di accesso al dossier sanitario, al fine di garantire le cure dei pazienti Covid-19. Tale gestione è stata mantenuta anche con le successive ondate. Tale scelta è stata effettuata nell'ottica del bilanciamento tra esigenze di cura e di tutela dei dati personali con riferimento allo stato di emergenza all'epoca in atto";

- "Durante tale periodo l'Azienda ha comunque fatto presente agli operatori la necessità di limitare l'accesso al dossier esclusivamente se coinvolti nel processo di cura degli interessati, facendo affidamento ai doveri di riservatezza e di servizio degli stessi";

- "Dal 22 aprile 2022 è stato avviato il processo di ripristino del sistema di gestione del dossier sanitario secondo le regole pre-pandemiche che si è concluso il 10 maggio 2022. Tale processo ha reso necessario verificare la corretta profilazione degli utenti";

- "I fatti oggetto del procedimento sono avvenuti in un ambulatorio afferente all'Azienda, cui è riconducibile la titolarità del trattamento. In tale ambulatorio erano prestate le cure anche dei pazienti che avevano avuto il Covid-19, sebbene il caso di specie si riferisca ad un paziente non Covid-19";

- "L'operatore che ha effettuato l'accesso era un operatore di una agenzia di somministrazione, cui sono stati segnalati i fatti oggetto del procedimento. In seguito non è stato rinnovato il contratto alla suddetta operatrice. Non risultano all'Azienda denunce alla Procura della Repubblica sui fatti oggetto del procedimento".

Nel corso della predetta audizione avvenuta in videocollegamento, l'Azienda ha condiviso lo schermo al fine di poter mostrare l'applicativo del dossier sanitario in uso presso la stessa illustrando le funzionalità presenti con le impostazioni previste nel periodo pre-pandemico e quelle vigenti all'epoca dei fatti in esame, accedendo con un profilo analogo a quello del predetto logopedista nei confronti di un dossier sanitario riferito ad un paziente inesistente (ambiente di test). Come riportato nel verbale di audizione in atti, tale presentazione ha evidenziato che con l'applicazione dei "filtri privacy" originari l'operatore (con profilo di logopedista) può accedere solo alle prestazioni sanitarie in cui è coinvolto, mentre con la rimozione dei predetti filtri poteva visualizzare l'elenco di tutte le prestazioni -con l'indicazione di alcuni dettagli (non referti) relativi alle stesse (tipologia di ambulatorio, ricovero, condizioni di salute) - ovvero anche quelle con riferimento alle quali non era coinvolto nel percorso di cura.

Con successiva nota del XX, l'Azienda ha trasmesso un video attestante le predette diverse modalità di accesso al dossier mostrate nel corso dell'audizione e una nota della società Synergie (Agenzia di somministrazione di personale) relativa alle azioni intraprese nei confronti della responsabile dell'accesso al dossier in esame (contestazione disciplinare e ammonizione disciplinare scritta).

2. Esito dell'attività istruttoria.

2.1. Quadro giuridico di riferimento.

In via preliminare, si rappresenta che il trattamento di dati personali deve avvenire nel rispetto della normativa applicabile in materia di protezione dei dati personali e, in particolare, delle disposizioni del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 (di seguito, il "Regolamento") e del d.lgs. n. 196 del 30 giugno 2003 (Codice in materia di

protezione dei dati personali – di seguito, il “Codice”).

Con particolare riferimento alla questione in esame, si evidenzia che i dati personali devono essere “trattati in modo lecito corretto e trasparente” (principio di “liceità, correttezza e trasparenza” e “in maniera da garantire un’adeguata sicurezza (…), compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti (principio di “integrità e riservatezza”)” (art. 5, par. 1, lett. a) e f) del Regolamento).

Il Regolamento prevede poi che il titolare del trattamento metta 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).

Tenendo conto tra l’altro della natura, dell’ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento deve poi mettere in atto misure tecniche e organizzative adeguate, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione e a garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento (art. 25 del Regolamento).

Con riferimento ai trattamenti oggetto del citato reclamo, il Garante ha adottato le “Linee guida in materia di Dossier sanitario - 4 giugno 2015” (Provvedimento del 4.6.2015, pubblicato in G.U. 164 del 17 luglio 2015, consultabile su www.gpdp.it doc web n. 4084632), nelle quali sono state individuate un primo quadro di cautele, al fine di delineare specifiche garanzie e responsabilità, nonché misure e accorgimenti necessari ed opportuni da porre a garanzia dei cittadini, in relazione ai trattamenti di dati sanitari che li riguardano, che, al pari degli altri provvedimenti dell’Autorità, continuano ad applicarsi anche dopo la piena applicazione del Regolamento, in quanto compatibili con lo stesso (art. 22, comma 4, d.lgs n. 101/2018).

Nelle richiamate linee guida del 2015 il Garante ha specificato che il dossier sanitario, costituendo l’insieme dei dati personali generati da eventi clinici presenti e trascorsi riguardanti l’interessato, costituisce un trattamento di dati personali specifico e ulteriore rispetto a quello effettuato dal professionista sanitario con le informazioni acquisite in occasione della cura del singolo evento clinico. Come tale, quindi, si configura come un trattamento facoltativo. All’interessato, infatti, deve essere consentito di scegliere, in piena libertà, che le informazioni cliniche che lo riguardano siano trattate o meno in un dossier sanitario, garantendogli anche la possibilità che i dati sanitari restino disponibili solo al professionista sanitario che li ha redatti, senza la loro necessaria inclusione in tale strumento. Ciò significa che qualora l’interessato non manifesti il suo consenso al trattamento dei dati personali mediante il dossier sanitario il professionista che lo prende in cura avrà a disposizioni solo le informazioni rese in quel momento dallo stesso interessato (es. raccolta dell’anamnesi, delle informazioni relative all’esame della documentazione diagnostica prodotta) e quelle relative alle precedenti prestazioni erogate dallo stesso professionista. Analogamente, in tale circostanza, il personale sanitario di reparto/ambulatorio avrà accesso solo alle informazioni relative all’episodio per il quale si è rivolto presso quella struttura l’interessato e alle altre informazioni relative alle eventuali prestazioni sanitarie erogate in passato a quel soggetto da quel reparto/ambulatorio (c.d. accesso agli applicativi verticali dipartimentali).

In seguito alla piena applicazione del Regolamento (maggio 2018), con il provvedimento del 7 marzo 2019, il Garante ha individuato- a titolo esemplificativo- alcuni trattamenti in ambito sanitario per i quali è ancora necessario richiedere il consenso esplicito dell’interessato (art. 9, par. 2, lett. a) del Regolamento), tra i quali sono stati annoverati anche quelli effettuati attraverso il dossier sanitario (doc. web n. 9091942).

Nelle predette Linee guida il Garante, al fine di scongiurare il rischio di un accesso alle informazioni trattate mediante il dossier sanitario da parte di soggetti non autorizzati o di comunicazione a terzi di dati sanitari da parte di soggetti a ciò abilitati, ha specificamente chiesto ai titolari del trattamento di porre particolare attenzione nell'individuazione dei profili di autorizzazione e nella formazione dei soggetti abilitati, dovendo essere limitato l'accesso al dossier al solo personale sanitario che interviene nel processo di cura del paziente ed essere adottate modalità tecniche di autenticazione al dossier che rispecchino le casistiche di accesso a tale strumento proprie di ciascuna struttura sanitaria. A tal fine, nelle predette Linee guida, il Garante ha indicato ai titolari del trattamento di effettuare un monitoraggio delle ipotesi in cui il relativo personale sanitario può avere necessità di consultare il dossier sanitario, per finalità di cura dell'interessato e, in base a tale ricognizione, individuare i diversi profili di autorizzazione all'accesso.

Si rappresenta inoltre che nelle predette Linee guida l'Autorità ha ritenuto che "il titolare del trattamento deve mettere in opera sistemi per il controllo degli accessi anche al database e per il rilevamento di eventuali anomalie che possano configurare trattamenti illeciti, attraverso l'utilizzo di indicatori di anomalie (c.d. alert) utili per orientare successivi interventi di audit. Il titolare deve prefigurare, quindi, l'attivazione di specifici alert che individuino comportamenti anomali o a rischio relativi alle operazioni eseguite dagli incaricati del trattamento (es. relativi al numero degli accessi eseguiti, alla tipologia o all'ambito temporale degli stessi)".

Sin dalla dichiarazione dello stato di emergenza deliberato dal Consiglio dei Ministri in data 31 gennaio 2020, sono state adottati molti atti normativi d'urgenza, che contengono disposizioni anche relative al trattamento dei dati sulla salute effettuato nell'ambito degli interventi relativi alla predetta emergenza sanitaria. Le disposizioni d'urgenza prevedono degli interventi emergenziali che implicano il trattamento dei dati e che sono frutto di un delicato bilanciamento tra le esigenze di sanità pubblica e quelle relative alla protezione dei dati personali, in conformità a quanto dettato dal Regolamento europeo per il perseguimento di motivi di interesse pubblico nel settore della sanità pubblica (cfr. art. 9, par. 2, lett. i), del Regolamento).

Con specifico riferimento alla disciplina dettata dall'art. 17-bis del d.l. n. 18/2020, richiamata dall'Azienda nelle memorie in atti, si ribadisce che tale disposizione, nei limiti consentiti dal quadro giuridico vigente, ha previsto alcune "semplificazioni" nel trattamento e nella comunicazione dei dati personali fra diversi titolari del trattamento solo qualora le stesse risultino indispensabili ai fini dello svolgimento delle attività connesse alla gestione dell'emergenza sanitaria in atto e comunque nel rispetto dei princìpi di cui all'art. 5 del Regolamento, adottando misure appropriate a tutela dei diritti e delle libertà degli interessati. Come più volte ribadito dal Garante, tale disposizione non ha e non avrebbe potuto derogare alle disposizioni previste nel Regolamento europeo a tutela di diritti fondamentali dell'interessato.

Pertanto, si ribadisce che il trattamento dei dati personali connesso alla gestione della predetta emergenza sanitaria deve svolgersi nel rispetto della disciplina vigente in materia di protezione dei dati personali e, in particolare, nel rispetto dei principi e dei limiti applicabili al trattamento, di cui all'art. 5 del Regolamento, secondo cui i dati devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»), "raccolti per finalità determinate, esplicite e legittime" («limitazione della finalità») e, comunque, "adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati" (principio di minimizzazione dei dati).

Il rispetto di tali principi nel trattamento dei dati personali effettuato nella richiamata emergenza sanitaria da Covid -19 è stato del resto più volte richiamato e valutato dall'Autorità nei numerosi parerei resi sugli atti normativi di regolamentazione dei sistemi informativi realizzati in urgenza per la rilevazione delle infezioni da Covid-19, per la prenotazione e la registrazione delle vaccinazioni, per il sistema di contact tracing nazionale (App Immuni) e per la generazione e il controllo delle

certificazioni verdi Covid-19.

Si rappresenta infine che, alla luce del Regolamento, si considerano “dati relativi alla salute”: i dati personali 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, n. 15 del Regolamento). Il Considerando n. 35 del Regolamento precisa infatti 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”; “un numero, un simbolo o un elemento specifico attribuito a una persona fisica per identificarla in modo univoco a fini sanitari”.

2.1 Ambito del trattamento e natura dei dati trattati.

In via preliminare si rileva che, secondo quanto indicato dalla stessa Azienda in atti, i trattamenti in esame, avvenuti in un ambulatorio aziendale, sono riconducibili alla titolarità della stessa.

Alla luce di quanto emerso negli atti istruttori, l’Azienda ha intenzionalmente scelto di adottare un atto amministrativo con il quale disporre la “rimozione dei filtri privacy” nel sistema informativo che gestisce il dossier sanitario aziendale, nella convinzione che tale misura avrebbe semplificato la gestione dei pazienti durante la pandemia.

La rimozione dei predetti filtri ha determinato:

- l’attivazione del dossier sanitario per tutti gli assistiti della Azienda, che coincidono con quelli della Regione, anche nel caso gli stessi abbiano espressamente negato il consenso all’uso del dossier o non lo abbiano mai prestato;

- la possibilità che il dossier fosse consultato, sebbene con diverse profondità di accesso, da parte di tutti gli operatori sanitari aziendali a prescindere dal loro coinvolgimento nel percorso di cura dell’interessato.

Si rileva inoltre che sebbene la predetta scelta aziendale sia stata effettuata in relazione all’emergenza da Covid-19, la rimozione dei predetti filtri non ha riguardato solo i pazienti affetti da tale patologia, ma tutti quelli afferenti all’Azienda e alle sue articolazioni (come la struttura ove è stato effettuato l’accesso in esame) e non è stata limitata alle sole prestazioni sanitarie rese in emergenza, bensì a tutte quelle erogate dall’Azienda dal marzo del 2020 al maggio del 2022.

Ciò stante si rileva che la scelta operata dall’Azienda ha consentito di fatto alla sig.ra XX di accedere alle informazioni relative alle prestazioni sanitarie erogate alla reclamante (collega della sig.ra XX) alle quali non avrebbe avuto accesso se non fosse stata disposta la rimozione dei predetti “filtri privacy”, ciò in quanto la reclamante non aveva acconsentito all’uso del dossier sanitario aziendale e la predetta operatrice non era coinvolta nel percorso di cura dell’interessata.

Alla luce di quanto sopra rappresentato, le informazioni relative alla reclamante a cui ha avuto accesso la sig.ra XX si qualificano come dati sulla salute. Sebbene infatti la presenza di alcuni filtri abbia consentito alla suddetta operatrice sanitaria di vedere solo la lista degli episodi già effettuati o prenotati dall’interessata con l’indicazione della tipologia di prestazione, e non anche di “consultare i referti”, tali informazioni sono comunque attinenti alla salute della reclamante e pertanto sono qualificabili come dati sulla salute della stessa.

Con il profilo della predetta operatrice era infatti possibile accedere a informazioni relative alla tipologia di prestazione erogata, all’ambulatorio erogante, all’eventuale ricovero e a elementi relativi alle condizioni di salute di qualunque assistito dell’Azienda a prescindere dalla volontà del soggetto cui si riferivano (negazione del consenso al dossier o assenza di consenso) e dall’effettivo coinvolgimento nel percorso di cura dell’operatore.

Pertanto, si rileva che la scelta effettuata dell'Azienda ha reso di fatto accessibili i dossier sanitari di tutti gli assistiti della stessa, che, come dichiarato in atti, coincidono con quelli della Regione (l'Azienda è l'unica presente in Valle d'Aosta), a prescindere dalla volontà degli stessi, dal coinvolgimento nel percorso di cura dell'operatore sanitario e dalla circostanza che la prestazione sanitaria fosse effettivamente resa ad un paziente Covid-19.

2.2 Il consenso dell'interessato e principi di liceità, correttezza e trasparenza e di protezione dei dati fin dalla progettazione e per impostazione predefinita.

Come sopra evidenziato, con il provvedimento del 7 marzo 2019 e nei successivi provvedimenti, anche di tipo sanzionatorio, adottati in materia, il Garante ha rilevato che la base giuridica dei trattamenti di dati personali effettuati attraverso il dossier sanitario è il consenso esplicito e informato dell'interessato (art. 9, par. 2, lett. a) del Regolamento).

Dall'esame dei documenti in atti emerge che la predetta "rimozione dei filtri privacy" sul dossier sanitario aziendale ha determinato, per ogni assistito aziendale/regionale, la realizzazione e l'accessibilità del dossier sanitario a prescindere dalla volontà espressa dagli interessati e anche contrariamente ad una esplicitata manifestazione di diniego degli stessi, come nel caso della reclamante.

Al riguardo, preme evidenziare che gli interventi legislativi adottati nel corso della pandemia per favorire la gestione della stessa hanno confermato la necessità del consenso dell'interessato anche con riferimento a peculiari trattamenti emergenziali come quello relativo alla refertazione on-line dei test per il Covid-19 (DM 2 novembre 2020 che richiama il dPCM 8 agosto del 2013) o alla consultazione per finalità di cura del Fascicolo sanitario elettronico, strumento che presenta finalità analoghe al dossier sanitario (cfr. art. 12 d.l. n. 179/2012 in relazione alle modifiche apportate dall'art. 11, d.l. n. 34 del 2020).

Ciò premesso, si ribadisce quanto già rilevato con la nota del XX, ovvero che l'art. 17-bis del d.l. n. 18 del 2020, citato dall'Azienda quale disposizione legittimante la "possibilità, per tutti i medici e infermieri, di accedere all'applicativo Trackare per la consultazione e la comunicazione fra di loro dei dati personali dei pazienti degenti nei 3 presidi ospedalieri, sussistendo quei motivi di interesse pubblico e di assicurare la diagnosi e l'assistenza sanitaria dei contagiati nel contesto emergenziale conseguente al COVID 19, prevista dalla norma", non può essere considerata quale norma derogatoria dell'obbligo di acquisizione del consenso dell'interessato.

La predetta disciplina emergenziale ha infatti previsto alcune semplificazioni (es. relativamente alle informazioni da rendere ai sensi dell'art. 13 del Regolamento o alle autorizzazioni di cui all'art. 2-quaterdecies del Codice) ribadendo la necessità di rispettare i princìpi di cui all'art. 5 del Regolamento (UE) 2016/679 , tra cui si colloca quello di liceità, ovvero di individuare la corretta base giuridica del trattamento, e di adottare misure appropriate a tutela dei diritti e delle libertà degli interessati.

La rimozione dei c.d. "filtri privacy" effettuata dall'Azienda ha determinato una violazione dei predetti principi e in particolare di quelli di liceità, correttezza e trasparenza, in quanto i dossier sanitari aziendali di tutta la popolazione regionale assistita sono stati:

- realizzati anche contrariamente alla volontà degli interessati o in assenza di un loro consenso esplicito;

- resi accessibili di default anche al personale sanitario non coinvolto nel percorso di cura dell'interessato, senza che gli stessi assistiti ne siano stati mai informati.

La violazione del principio di correttezza e del connesso principio di proporzionalità del trattamento si evince anche con riferimento alla circostanza che la rimozione dei c.d. "filtri privacy", non ha

riguardato solo le prestazioni sanitarie fornite in emergenza o i dossier degli interessati cui erogare prestazioni sanitarie legate al Covid-19, bensì a tutti i pazienti afferenti all'Azienda -anche attualmente non in cura- e con riferimento a qualsiasi percorso di cura dagli stessi intrapreso.

Da ciò si rileva che consapevolmente l'Azienda, in occasione della predetta emergenza sanitaria, ha rimosso le misure, richieste anche dalle richiamate Linee guida del Garante, che limitavano l'accesso al dossier al solo personale sanitario che ha in cura l'interessato. Tale scelta ha consentito di fatto alla sig.ra XX, non coinvolta nell'erogazione di prestazioni sanitarie emergenziali legate al predetto virus, di effettuare ripetuti accessi al dossier di un'assistita, nonché collega, senza un idoneo presupposto di liceità, ma solo per ragioni di "mera curiosità" (accessi avvenuti dal mese di marzo 2021 a quello di dicembre 2021).

Il caso in esame dimostra che le predette modifiche alla configurazione del dossier aziendale hanno reso possibile a un professionista sanitario operante presso l'Azienda di accedere al dossier sanitario anche di interessati che non erano in quel momento in cura presso l'Azienda o comunque presso il titolare dell'utenza e che non avevano mai prestato il consenso al dossier (ovvero, come nel caso di specie, il consenso al dossier era stato addirittura espressamente negato) in violazione dei principi di base del trattamento di cui agli artt. 5, par. 1, lett. a) e f) e 9 del Regolamento, nonché del principio di protezione dei dati fin dalla progettazione (privacy by design) e per impostazione predefinita (privacy by default) (art. 25 del Regolamento.

2.3 Profili di autorizzazione per l'accesso al dossier sanitario e sistemi di alert.

In via preliminare, si rappresenta che le regole circa l'accessibilità del dossier adottate dall'Azienda in epoca pre-pandemica, secondo cui "medici e altri operatori sanitari afferenti a Strutture e/o discipline specialistiche diverse, non avrebbero potuto, di fatto, accedere alla cartella clinica e ai dati sanitari di pazienti ricoverati in reparti COVID (formalmente assegnati al reparto di Pneumologia) o in reparti non COVID multi-specialistici e dunque non sarebbero stati in grado di assistere adeguatamente i pazienti" sono frutto di una scelta della stessa Azienda. Sul punto, l'Autorità ha infatti più volte ricordato la necessità di limitare l'accesso al dossier al solo personale sanitario che effettivamente interviene nel processo di cura del paziente indipendentemente dal reparto in cui lo stesso è assegnato, richiamando il titolare ad adottare modalità tecniche di autenticazione al dossier che rispecchino le casistiche di accesso a tale strumento proprie di ciascuna struttura sanitaria.

Si rappresenta inoltre che la problematica descritta dall'Azienda, secondo cui nel momento in sono stati disattivati i predetti filtri, "il software TrakCare non è più nella possibilità di applicare le regole di visibilità indicate a livello di paziente, con la conseguente situazione che si visualizzano temporaneamente, ovvero limitatamente fino al perdurare dello stato di emergenza, anche le informazioni di coloro che hanno negato il consenso al dossier", cessato il quale si ripristineranno le limitazioni alla visibilità precedentemente impostate", non dipende dalla "rigidità" della disciplina sulla protezione dei dati personali, bensì dalle caratteristiche del sistema scelto dalla stessa Azienda. L'aggiornamento del sistema ha infatti consentito all'Azienda di superare tale difficoltà.

La scelta operata dall'Azienda di "disabilitare le funzioni Privacy che gestiscono, per l'intero site TrakCare (quindi profili utente Medici, Infermieri, Amministrativi ecc…), i concetti legati alla visibilità delle informazioni. Di fondo, la visibilità dei dati sarà quindi completa/generale e non più filtrata in base alla competenza", non solo non trova fondamento, come già rappresentato, nel richiamato art. 17-bis del d.l.n. 18 del 2020, ma è stata operata in modo tale da consentire l'accesso al dossier sanitario anche da parte di operatori sanitari non coinvolti nell'emergenza sanitaria e con riferimento a tutte le prestazioni sanitarie e non solo a quelle emergenziali.

Come già evidenziato, la configurazione del dossier sanitario prevista dall'Azienda nel periodo emergenziale ha previsto di fatto un unico profilo di accesso (pur con differenti profondità di

accesso), consentendo, quindi, a tutto il personale sanitario di consultare i dossier sanitari di qualsiasi paziente fosse stato in cura presso l'Azienda a prescindere dalla circostanza che il soggetto che effettua l'accesso sia coinvolto nel percorso di cura dell'interessato e che quest'ultimo abbia manifestato il proprio consenso al trattamento dei dati effettuato attraverso il dossier.

Nel derogare alle limitazioni relative all'accesso al dossier sanitario dettate dall'applicazione della disciplina sulla protezione dei dati personali, l'Azienda, pur dichiarando che "la visibilità dei dati sarà quindi completa/generale e non più filtrata in base alla competenza", non ha neppure adottato un sistema per il rilevamento di eventuali anomalie che possano configurare trattamenti illeciti, ovvero l'utilizzo di indicatori di anomalie (c.d. alert) volti ad individuare comportamenti anomali o a rischio relativi alle operazioni eseguite dai soggetti autorizzati al trattamento (es. numero degli accessi eseguiti, tipologia o ambito temporale degli stessi), utili per orientare successivi interventi di audit, in violazione dei principi di integrità e riservatezza dei dati personali (art. 5, par. 1, lett. f), del Regolamento).

Secondo quanto dichiarato in atti, il sistema di ripristino nel dossier sanitario delle "regole pre-pandemiche" è stato avviato il 22 aprile 2022 e si è concluso il 10 maggio 2022; emerge, pertanto, che la rimozione dei c.d. "filtri privacy" è stata operativa per oltre due anni (50 mesi), essendo iniziata nel mese di marzo del 2021 e che tardivamente sono stati rilevati i richiamati "limiti tecnici" del sistema informativo utilizzato per il dossier sanitario. La scelta dell'Azienda "di sospendere i filtri privacy" in quanto "indispensabile per organizzare ed erogare - in tempi necessariamente ridottissimi - l'attività nei nuovi reparti Covid" si è dunque protratta oltre la prima fase emergenziale.

3. Conclusioni.

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" si rappresenta che gli elementi forniti dal titolare del trattamento nelle memorie difensive relative ai richiamati procedimenti non consentono di superare i rilievi notificati dall'Ufficio con gli atti di avvio dei procedimenti per l'adozione dei provvedimenti correttivi e sanzionatori, non ricorrendo, peraltro, alcuno dei casi previsti dall'art. 11 del Regolamento del Garante n. 1/2019.

Per tali ragioni si rileva l'illiceità del trattamento di dati personali effettuato dall'Azienda Usl della Valle d'Aosta con riferimento al procedimento avviato a seguito del reclamo, nei termini di cui in motivazione, in particolare, per aver trattato dati personali in violazione degli artt. 5, par. 1, lett. a) e f), 9, 25 e 32 del Regolamento.

In tale quadro, considerato che sono state adottate misure disciplinari nei confronti dell'autore dell'accesso e che dal mese di maggio 2022 sono state ripristinate le misure di accesso al dossier sanitario pre-pandemiche sopra descritte, non ricorrono allo stato i presupposti per l'adozione delle misure correttive di cui all'art. 58, par. 2, del Regolamento.

4. 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. 2, lett. a) e f), 9, 25 e 32 del Regolamento, causata dalla condotta dell'Azienda Usl della Valle d'Aosta, è soggetta all'applicazione della sanzione amministrativa pecuniaria ai sensi dell'art. 83, par.4 e 5, del Regolamento.

Si consideri che il Garante, ai sensi 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).

La predetta sanzione amministrativa pecuniaria inflitta, in funzione delle circostanze di ogni singolo caso, va determinata nell'ammontare tenuto conto dei principi di effettività, proporzionalità e dissuasività, indicati nell'art. 83, par. 1, del Regolamento, alla luce degli elementi previsti all'art. 85, par. 2, del Regolamento in relazione ai quali per entrambi i procedimenti si osserva che:

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

- gli accessi illeciti hanno riguardato il dossier sanitario di una paziente che era al contempo dipendente dell'Azienda da parte di una professionista sanitaria che non era coinvolta nel processo di cura delle stessa e nei confronti dei quali è stato avviato un procedimento disciplinare (art. 83, par. 2, lett. a) e b) del Regolamento);

- gli accessi al dossier sanitario della reclamante effettuati per ragioni di "mera curiosità" sono avvenuti nell'arco di 9 mesi dal 15/03/2021 al 06/12/2021 da parte di un'operatrice sanitaria che, oltre a non essere coinvolta nel percorso di cura dell'interessata, non era neanche impiegata nell'erogazione di prestazioni sanitarie emergenziali legate al predetto virus (art. 83, par. 2, lett. a) del Regolamento);

- i predetti accessi sono stati possibili in quanto la rimozione dei predetti "filtri privacy" ha consentito di fatto alla sig.ra XX, non coinvolta nel percorso di cura della reclamante e nell'erogazione di prestazioni sanitarie emergenziali legate al predetto virus, di effettuare ripetuti accessi al dossier di un'assistita, nonché collega, senza un idoneo presupposto di liceità, ma solo per ragioni di "mera curiosità" (art. 83, par. 2, lett. a) e d) del Regolamento);

- l'Azienda ha scelto consapevolmente di procedere alla rimozione dei c.d. "filtri privacy" per tutti i dossier sanitari aziendali di tutta la popolazione regionale assistita determinando l'attivazione del dossier sanitario per tutti gli assistiti della Azienda anche nel caso gli stessi abbiano espressamente negato il consenso all'uso del dossier o non lo abbiano mai prestato, nonché la possibilità che il dossier fosse consultato, sebbene con diverse profondità di accesso, da parte di tutti gli operatori sanitari aziendali a prescindere dal loro coinvolgimento nel percorso di cura dell'interessato (art. 83, par. 2, lett. b) e d) del Regolamento);

- la predetta scelta aziendale, sebbene sia stata effettuata in relazione all'emergenza da Covid-19, non ha riguardato solo i pazienti affetti da tale patologia, ma tutti quelli afferenti all'Azienda e alle sue articolazioni (oltre 120.000 interessati) e non è stata limitata alle sole prestazioni sanitarie rese in emergenza, bensì a tutte quelle erogate dall'Azienda dal marzo del 2020 al maggio del 2022 (art. 83, par. 2, lett. a), b), c) e d) del Regolamento);

- nel derogare alle limitazioni relative all'accesso al dossier sanitario dettate dall'applicazione della disciplina sulla protezione dei dati personali, l'Azienda non ha adottato un sistema per il rilevamento di eventuali anomalie che possano configurare trattamenti illeciti, ovvero l'utilizzo di indicatori di anomalie (c.d. alert) volti ad individuare comportamenti anomali o a rischio relativi alle operazioni eseguite dai soggetti autorizzati al trattamento (es. numero

degli accessi eseguiti, tipologia o ambito temporale degli stessi), utili per orientare successivi interventi di audit, in violazione dei principi di integrità e riservatezza dei dati personali (art. 83, par. 2, lett. d) del Regolamento);

- nel rimuovere i predetti "filtri privacy" l'Azienda aveva ricordato "la necessità di corretto e responsabile utilizzo della modalità di accesso libero, del quale andrà informato solamente il personale interessato" (art. 83, par. 2, lett. c) del Regolamento);

- il sistema di ripristino nella gestione del dossier sanitario delle "regole pre-pandemiche" è stato avviato il 22 aprile 2022 e si è concluso il 10 maggio 2022 (art. 83, par. 2, lett. a) e c) del Regolamento).

In ragione dei suddetti elementi, valutati nel loro complesso, si ritiene di determinare l'ammontare della sanzione pecuniaria prevista dall'art. 83, par. 5, lett. a) del Regolamento, per la violazione degli artt. 5, par. 1, lett. a) e f) e 9 del Regolamento nella misura di 40.000 (quarantamila) per il procedimento avviato a seguito del reclamo quale sanzione amministrativa pecuniaria ritenuta, ai sensi dell'art. 83, par. 1, del Regolamento, effettive, proporzionate e dissuasive.

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, in entrambi i procedimenti descritti, dall'Azienda Usl Valle d'Aosta, per la violazione degli art. 5, par. 1, lett. a) e f), 9, 25 e 32 del Regolamento nei termini di cui in motivazione.

ORDINA

ai sensi degli artt. 58, par. 2, lett. i) e 83 del Regolamento, nonché dell'art. 166 del Codice, all'Azienda Usl Valle d'Aosta, C.F. 91001750073, di pagare la somma di euro 40.000 (quarantamila) a titolo di sanzione amministrativa pecuniaria per le predette violazioni secondo le modalità indicate in allegato, entro 30 giorni dalla notifica in motivazione; 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 delle sanzioni comminate.

INGIUNGE

alla predetta Azienda, in caso di mancata definizione della controversia ai sensi dell'art. 166, comma 8, del Codice, di pagare le somme di euro 40.000 (quarantamila) 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

ai sensi dell'art. 166, comma 7, del Codice, la pubblicazione per intero del presente provvedimento sul sito web del Garante e 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, 10 novembre 2022

IL PRESIDENTE
Stanzione

IL RELATORE
Scorza

IL SEGRETARIO GENERALE
Mattei