



**GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI**

Provvedimento del 22 febbraio 2024 [10001279]

VEDI ANCHE [Newsletter del 10 aprile 2024](#)

[doc. web n. 10001279]

Provvedimento del 22 febbraio 2024

Registro dei provvedimenti
n. 97 del 22 febbraio 2024

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, alla quale hanno preso parte il prof. Pasquale Stanzone, 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 il dott. Agostino Ghiglia;

PREMESSO

1. I reclami, le violazioni dei dati personali e l'attività istruttoria

L'Autorità ha ricevuto due reclami e due notifiche di violazione in merito al trattamento di dati personali effettuato dall'Azienda sanitaria dell'Alto Adige (di seguito Azienda o ASDAA) mediante il

dossier sanitario aziendale. In particolare, sono stati segnalati ripetuti accessi al dossier da parte di personale sanitario che, sebbene autorizzato al trattamento, non era coinvolto nel processo di cura dei soggetti a cui i dossier sanitari si riferivano.

Con riferimento al primo reclamo presentato dal Sig. XX, che lamentava ripetuti accessi al dossier sanitario aziendale che “non coincidono con le date in cui (lo stesso era) (..) ricoverato o trattato in ospedale”, l’Ufficio ha richiesto informazioni alla predetta Azienda (note del XX, XX e XX) a cui è stato fornito riscontro con le note del XX, del XX e del XX, in cui è stato rappresentato, in particolare, che:

“Dagli approfondimenti degli accessi è emerso che su 1309 (accessi), 780 sono stati fatti dall’interessato stesso, il quale nel caso di specie è un dipendente dell’Azienda sanitaria con profilo professionale sanitario abilitato ad accedere al DSE stesso”;

“Relativamente al complesso degli accessi summenzionati si evidenzia che parte di essi sono stati ripetuti in brevissimo tempo dallo stesso operatore per ragioni tecniche e pertanto sono da ricondurre ad unici accessi andando pertanto a ridurre il numero degli accessi stessi al DSE dell’interessato”. Dall’elenco degli accessi forniti dall’Azienda si evince che la stessa ha contrassegnato alcuni come “non giustificato” o limitato alla “sola lista delle prestazioni sanitarie svolte e non il relativo dettaglio” con riferimento ai quali ha dichiarato di avviare “i doverosi e conseguenti procedimenti disciplinari”;

“Allo stato attuale se nel sistema è presente un evento clinico-amministrativo (ricovero, accesso al PS, prestazione specialistica), all’operatore sanitario viene attivata la possibilità di accedere al DSE. Nelle situazioni in cui non è presente un evento clinico-amministrativo, tracciato a livello informatico (es. Paziente che chiama il professionista per delucidazioni post ricovero), l’operatore sanitario, ha la possibilità, di accedere al DSE, tramite scelta di apposita voce all’interno di una lista predefinita che si sostanzia come segue: In pericolo di vita/emergenza; Prevenzione/diagnosi/cura/riabilitazione su paziente in carico ma non registrato nei percorsi informatizzati previsti”;

“l’operatore sanitario può fornire una specificazione aggiuntiva onde motivare al meglio l’accesso al DSE. Nell’ipotesi di accesso tramite selezione voce da lista predefinita, l’operatore è chiamato a confermare la sua scelta con firma elettronica semplice”;

“L’Azienda sanitaria ha provveduto ad inviare agli operatori sanitari due circolari, rispettivamente nel mese di aprile e di agosto corrente anno, ribadendo che il DSE, è lo strumento che documenta la storia sanitaria dell’interessato/a e può essere consultato esclusivamente dal personale sanitario che prende in cura il/la paziente”;

“ci sarà un aggiornamento delle autorizzazioni del trattamento dei dati nonché un primo corso fissato per il XX con oggetto “Protezione dei dati personali e Sanità Digitale””;

“i professionisti sanitari che operano esclusivamente in ambito amministrativo per es. al CUP, non possono accedere al DSE, così come non possono accedere al DSE gli operatori sanitari, medici, infermieri e altri professionisti sanitari operativi nell’ambito del servizio della medicina legale, del servizio della medicina del lavoro, nelle direzioni mediche”;

“Allo stato attuale l’Azienda Sanitaria ha attivato un alert automatico volto a rilevare anomalie negli accessi al DSE ripetuti in numero rilevante”; è in fase di completamento l’attivazione di un secondo alert, il tutto proprio per impedire/identificare il prima possibile un eventuale abuso”;

“in merito al quesito se i dipendenti dell’Azienda possano ancora accedere al proprio dossier sanitario con il profilo di sanitario, “l’Azienda a seguito dell’invio di relativa circolare ad aprile

corrente anno, ha provveduto a chiudere l'accesso, a partire dal XX, dei propri dipendenti con profilo sanitario al proprio DSE.

Successivamente, con riferimento al secondo reclamo pervenuto dal Sig. XX e in merito al quale l'Azienda ha provveduto ad effettuare una notifica di violazione il XX, successivamente integrata il XX, la stessa ha dichiarato, in particolare, che:

tra l'XX e il XX "Risultano essere stati eseguiti complessivamente 5 accessi inappropriati al DSE (dossier sanitario) di un interessato";

"Al DSE di un interessato hanno avuto accesso nell'arco temporale sopra citato due medici e un'infermiera, rispettivamente: Medico (A) XX; XX; XX; Medico (B) XX; Infermiera XX. In tali occasioni risulta che l'interessato non sia stato preso in carico dai servizi in cui tali professionisti sono/erano in servizio. Nello specifico l'Azienda ha contattato il Medico (A) e l'infermiera onde acquisire l'informazione sul motivo dell'accesso e gli stessi hanno evidenziato quanto segue: Medico (A) ha riferito di essere stato coinvolto nel processo di cura in data XX da un medico del PS quando l'interessato ha avuto effettivamente accesso al PS. L'infermiera ha riferito di aver eseguito in data XX il Triage al PS ma di non ricordarsi dell'accesso del XX. L'Azienda non è ancora riuscita a contattare il Medico (B) poiché non più operativo in Azienda e a riguardo ha richiesto all'ufficio del personale i relativi dati di contatto per chiedere delucidazioni".

In merito ai fatti sopra descritti l'Azienda ha comunicato all'interessato la predetta violazione dei dati personali che lo ha riguardato ai sensi dell'art. 34 del Regolamento.

In relazione alle istruttorie sopra descritte, l'Ufficio, con nota del XX (prot. n. XX) ha disposto la riunione dei procedimenti e ha richiesto ulteriori informazioni in merito alle modalità di accesso al dossier all'epoca dei fatti oggetto dei reclami con riferimento alle quali l'Azienda ha rappresentato, in particolare, che:

"Tra XX e XX la lista delle motivazioni che consentivano l'accesso al dossier sanitario includeva ulteriori" fattispecie ovvero: "in pericolo di vita / emergenza; prevenzione/diagnosi/cura/riabilitazione su paziente in carico ma non registrato nei percorsi informatizzati previsti; critical review per analisi ed eventuale miglioramento percorsi di cura; processo di prelievi/trapianto; Direzione medica: adempimenti normativi/organizzativi; Registro tumori: consultazione. A seguito dell'avvio dei procedimenti di violazione dati e delle attività di attivazione di alert, si è provveduto a ridurre la lista a quanto segue: In pericolo di vita / emergenza; Prevenzione/diagnosi/cura/riabilitazione su paziente in carico ma non registrato nei percorsi informatizzati previsti. L'operatore, pertanto, allo stato attuale può scegliere solo fra le due voci di cui sopra e successivamente una volta scelto una delle stesse, ha la possibilità, nell'ambito di un campo libero, di annotare un'eventuale aggiunta ulteriore in chiave di motivazione dell'accesso";

"Da una verifica ulteriore in associazione agli "accessi illeciti" non risultano esserci eventi clinici amministrativi tracciati a livello informatico, a favore dei reclamanti",

"ha attivato un alert che si basa sulla quantità degli accessi al DSE del singolo interessato (numero 0 superiore 10) e per singolo operatore, creando i presupposti per determinare una verifica incrociata ed approfondita dell'attività dell'operatore coinvolto".

A seguito di tali elementi, l'Ufficio, con nota del XX (prot. n. XX), ha chiesto ulteriori informazioni all'Azienda, che, con nota del XX, ha rappresentato, in particolare, che:

"laddove non sia stato manifestato il consenso al trattamento dei dati attraverso il dossier, l'accesso a questi dati non è consentito";

“L’Azienda in considerazione della necessità di garantire e assicurare che solo il personale sanitario aziendale coinvolto nel percorso di cura dell’interessato possa accedere al DSE ha previsto allo stato attuale l’attivazione degli alert (automatici) di cui nella ns precedente nota. Nello specifico un l’alert che si basa sulla quantità degli accessi al DSE del singolo interessato (numero 0 superiore 10) (già descritto e)(...) un secondo alert che rileva in automatico gli accessi al DSE rispetto ai quali non risultano esserci degli eventi amministrativi clinici attivi (ricovero, prestazione ambulatoriale in essere/ prestazione sanitaria in generale es. esame diagnostico), in automatico risulta essere evidenziata anche la motivazione di cui alla lista sopra citata, scelta dall’operatore che accede al DSE nonché l’eventuale aggiunta ulteriore in chiave di motivazione dell’accesso che l’operatore potrebbe addurre”;

“l’Azienda ha previsto l’introduzione e l’utilizzo di un nuovo SW “NGH” che entro la metà del prossimo anno sarà operativo su tutta l’Azienda e che opererà alla luce delle indicazioni adottate dalla direzione sulla base di un attento monitoraggio che sarà svolto da parte di apposito Gruppo di lavoro sul DSE all’uopo costituito”;

in merito ai diversi profili di autorizzazione per l’accesso al dossier previsti all’interno dell’Azienda, la stessa ha prodotto una tabella in cui ha evidenziato il grado di profondità degli accessi al dossier consentito a ciascuna tipologia di operatore;

con riferimento alle misure adottate per limitare l’accesso al dossier al tempo in cui si articola il processo di cura ha rappresentato che “sono state inviate soltanto nel XX - 2 circolari a tutti i professionisti sanitari circa il corretto utilizzo del DSE; già l’anno scorso è stata prevista relativa formazione mirata che andrà in modalità FAD ad essere portata a regime nel corrente anno e sarà somministrata a tutti gli operatori autorizzati ad accedere al DSE. In considerazione dell’elevato numero e ruolo dei professionisti sanitari che hanno accesso al DSE (vedasi allegati relativi al punto 4), l’Azienda, come su riportato, ha attivato un gruppo di lavoro formato dalla Cabina di regia privacy, ripartizione informatica ed esponenti della direzione sanitaria e tecnico assistenziale al fine di rivedere i ruoli di accesso e il grado di profondità di accesso stesso, il tutto entro il XX. Allo stato attuale al fine di non creare un disservizio prima di andare a chiudere di default degli accessi si auspica poter nei tempi indicati nella presente, ultimare l’attività richiamata, ed integrare la presente Nota entro il XX onde poterla inoltrare all’Autorità”.

In relazione alle risultanze della predetta attività istruttoria, l’Ufficio, con atto n. XX del 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’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).

A seguito della predetta notifica, l’Azienda ha inviato le proprie memorie difensive con nota del XX (prot. n. XX), chiedendo di essere udita. Successivamente all’audizione svoltasi il XX, l’Azienda ha integrato la documentazione in atti con nota del XX.

In pari data (XX) l’Azienda ha anche inviato una nuova notifica di violazione ai sensi dell’art. 33 del Regolamento con riferimento ad una fattispecie analoga a quelle già oggetto di istruttoria. In particolare, in tale ultima notifica è stato comunicato l’avvenuto accesso da parte di una “dipendente (professionista sanitaria)” al dossier sanitario di un paziente, nonché suo coniuge, non in cura presso la stessa nel periodo intercorrente tra il XX al XX. Attraverso tali e ripetuti accessi la predetta professionista ha visionato esami di laboratorio del marito al di fuori del suo percorso di cura e a sua insaputa. Secondo quanto dichiarato nella predetta notifica, la suddetta professionista è stata sottoposta a procedimento disciplinare.

Nella citata notifica l'Azienda ha, inoltre, richiamato quanto già rappresentato nella comunicazione inviata in pari data all'Ufficio in merito alle analoghe istruttorie in corso relative al trattamento dei dati effettuato attraverso il dossier aziendale.

Ciò stante, in relazione alla suddetta notifica effettuata il XX su trattamenti analoghi a quelli già oggetto di istruttoria, l'Ufficio, con atto n. XX del XX, nel richiamare integralmente quanto già rappresentato nella citata notifica di violazione del XX (prot. XX), ha disposto la riunione dei procedimenti istruttori in atto con quello relativo alla notifica presentata dall'Azienda il XX rilevando -anche per tale fattispecie- ai sensi dell'art. 166, comma 5, del Codice, che la configurazione del dossier sanitario aziendale è stata effettuata in violazione dei principi di base del trattamento di cui agli artt. 5, par. 1, lett. a), c) e f), 9, 25 e 32 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).

A seguito della predetta notifica, l'Azienda ha inviato ulteriori memorie difensive con nota del XX (prot. n. XX), chiedendo di essere udita. L'audizione si è svolta da remoto il XX.

Nelle richiamate memorie difensive (note del XX, del XX e del XX) e durante le audizioni del XX e del XX l'Azienda ha rappresentato in particolare:

“il carattere colposo delle violazioni”;

con riferimento all'ultimo episodio notificato al Garante il procedimento disciplinare è stato sospeso poiché l'interessato/a ha informato la commissione disciplinare della presentazione a suo carico di formale denuncia/querela in relazione all'ipotesi di reato di cui all'art. 615 ter c.p.”;

“A seguito dell'avvio dell'istruttoria da parte del Garante sono state modificate le modalità di accesso al dossier sanitario aziendale. Prima delle modifiche le modalità di accesso erano due: paziente in carico al professionista sanitario; autodichiarazione del professionista. Tale ultima modalità verrà disattivata e sostituita con una documentata presa in carico del paziente. Attualmente è in corso una indagine per conoscere l'opinione dei clinici in merito a tali modifiche con riferimento all'eventuale impatto in termini di cura”;

“Con specifico riferimento alle autodichiarazioni, l'Azienda ha deciso di eliminarle in quanto gli accessi illeciti erano avvenuti proprio attraverso tale modalità. Contestualmente l'Azienda mira a definire dei percorsi di cura specifici al fine di evitare che possa essere escluso l'accesso al dossier a un clinico che ha preso in carico l'interessato”;

di aver provveduto a:” inviare ai professionisti sanitari nel corso del XX tre circolari sul DSE; a chiudere la possibilità di accesso ai professionisti sanitari al proprio DSE; ad attivare un apposito gruppo di lavoro sul DSE che coinvolge tutte le direzioni aziendali così come la ripartizione informatica e la cabina di regia privacy; ad inoltrare ai professionisti sanitari ulteriore comunicazione circa l'avvio delle nuove modalità di accesso al DSE (...); a rivalutare gli alert in essere; a rivedere ulteriormente la profondità di accesso dei professionisti sanitari; a predisporre quanto necessario per l'avvio, entro l'anno, di un primo corso base in materia di protezione dei dati per tutti i dipendenti ASDAA, il tutto in modalità bilingue e fad”;

che “la modalità di accesso al DSE tramite “Autocertificazione” sarà adeguata a partire dal XX nell'ottica di garantire un accesso al DSE da parte dei professionisti sanitari con modalità tali da tracciare, sempre, la presa in carico del paziente alla luce delle prestazioni erogate e dei percorsi clinici attivati, e relativamente ai soli professionisti effettivamente coinvolti nel percorso di cura del paziente, senza che ciò implichi necessariamente la presenza fisica del

paziente in struttura (ad es. per consulto specialistico, teleconsulto, televisita, valutazione di caso clinico e programmazione di prestazione sanitaria successiva)” (circolare del XX);

L'Azienda ha inoltre prodotto un documento redatto nel XX intitolato “Dossier sanitario ASDAA” in cui sono state descritte le modalità con cui è effettuato il trattamento dei dati personali nell'ambito del dossier sanitario aziendale successivamente alle modifiche apportate a seguito dell'avvio dell'attività istruttoria da parte del Garante, con riferimento alle quali è stato rappresentato che:

“le finalità perseguite attraverso la costituzione del DSE sono da ricondurre, per l'Azienda, esclusivamente a finalità di cura dell'assistito e cioè di prevenzione, diagnosi, cura e riabilitazione, con esclusione di ogni altra finalità, preme sottolineare che allo stato attuale il DSE dell'Azienda Sanitaria dell'Alto Adige oltre a non contenere i cosiddetti dati a maggior tutela (ovvero relativi ad atti di violenza sessuale o pedofilia, infezione da HIV, dipendenze patologiche, prestazioni erogate alle donne che si sottopongono ad interventi di interruzione volontaria della gravidanza o che decidono di partorire in anonimato)”;

è richiesto il consenso dell'interessato alla costituzione del dossier e al recupero nello stesso dei dati relativi agli eventi generati prima della manifestazione del consenso;

con riferimento all'accesso al dossier, “Il metodo di autorizzazione e controllo degli accessi ai dati e alle risorse basato sul ruolo e profilo, associa dei ruoli ad ogni attore che abbia bisogno di interagire con il sistema. Ogni ruolo definisce una determinata serie di diritti di base che l'attore di quel ruolo può esercitare, i ruoli vengono assegnati sulla base delle responsabilità inerenti alle attività svolte nell'organizzazione”;

“L'accesso avviene per ruoli (profili professionali). A ciascun ruolo viene consentito uno specifico ambito di visione coerente con le proprie necessità e competenze”;

“Per i professionisti sanitari il contesto operativo di accesso al DSE, è determinato dal ruolo agli stessi assegnato, nonché dallo stato dell'evento o caso “aperto” o “non aperto” (di seguito evento aperto e/o chiuso) e dalla struttura di appartenenza. Nello specifico per evento o caso aperto si intende una prestazione in corso (ricovero, prestazione ambulatoriale, etc.) o che la stessa sia programmata nei 30 giorni successivi o che sia avvenuta nei 30 giorni precedenti. Nell'ipotesi di evento aperto: UO che ha in carico l'assistito: è quella che esegue la prestazione o che ne cura la parte predominante (es. ricovero, PAC, ambulatorio integrato, etc.). In termini generali il professionista sanitario ha accesso a tutte le informazioni contenute nel DSE dell'assistito, finché il caso rimane aperto. Accede agli eventi prodotti dalla stessa UO senza formalità. Altra UO: in caso di necessità di cura (es. consulenza, cogestione del caso, e ulteriori casi di seguito elencati.) in termini generali il professionista sanitario accede a tutte le informazioni contenute nel DSE dell'assistito in carico ad altra UO per un periodo connesso all'erogazione della consulenza (periodo di apertura della consulenza gestita in modalità analoga al periodo di apertura dell'evento). Trattasi di evento tracciato da apposita richiesta informatizzata (es. tramite Order Entry)”;

“In vista dell'unificazione dei diversi sistemi informatici in uso in Azienda, prevista per la fine del XX è necessario distinguere fra contesti in cui l'order entry è a pieno regime e contesti in cui lo stesso non è ancora dappertutto operativo”, con riferimento ai quali sono stati previsti 6 casi: consulenza, colloquio con paziente, Teleconsulto Multidisciplinare, Emergenza, Richiesta Consulto da MMG/PLS, Pre ricovero;

sono stati attivati alert automatici rispetto ad un interessato (più di 10 accessi giornalieri al dossier) in grado anche di rilevare “gli accessi al DSE rispetto ai quali sono stati aperti degli eventi”.

Con nota del XX l'Ufficio ha richiesto ulteriori informazioni in merito al termine entro il quale "l'order entry" sarà a regime per tutti i contesti di riferimento, ai limiti di profondità temporale eventualmente previsti con riferimento all'accesso al dossier da parte dei ruoli professionali indicati nel predetto documento e alle motivazioni tecnico-scientifiche che renderebbero indispensabile ai ruoli di logopedista, assistente di oftalmologia, podologo, igienista dentale, massaggiatore e massofisioterapista e tecnico audiometrista accedere alle molteplici tipologie di informazioni indicate nella tabella 5 del documento "Dossier sanitario ASDAA", atteso che nel predetto documento non sono previsti limiti alla profondità temporale di accesso a tali informazioni.

Con nota del XX, l'Azienda ha risposto alla predetta richiesta di informazioni rappresentando, in particolare, che:

ci sono state "delle ulteriori modifiche rispetto a quanto comunicato in data XX, modifiche che continueranno ad essere apportate, sia in relazione alle risultanze del gruppo di lavoro stesso, sia alla luce dei progressi delle attività di uniformazione del sistema informatico aziendale";

"per evidenziare il termine entro il quale tale modulo sarà a regime per tutti i contesti di riferimento, bisogna riferirsi ai piani di diffusione dei moduli Accettazione Dimissione Trasferimento (ADT) e Pronto Soccorso (PS)" da cui "si evince che l'ultima attività ad essere conclusa secondo quanto previsto dal cronoprogramma sarà (...) negli ospedali di Brunico e San Candido. (XX)", con conclusione il XX ";

"si è deciso di non prevedere limiti temporali di accesso per i medici (incluso gli odontoiatri operativi nel contesto ospedaliero, fermo restando che entro fine gennaio XX saranno chiusi gli accessi al DSE per gli odontoiatri operativi nel solo contesto territoriale), viceversa sono stati previsti dei limiti temporali di due anni per le professioni sanitarie ulteriori di cui alla tabella sotto riportata, il tutto a partire dal XX";

"Nell'ambito delle azioni di miglioramento della gestione delle profondità di accesso effettuate, nel corso dell'estate è stata fatta un'ulteriore ricognizione per affinare la gestione della profondità di accesso al DSE effettuando interviste ai referenti delle professioni sanitarie interessate e analisi dei log di accesso al dossier sanitario. Dopo questa ricognizione la profondità di accesso riguardo la tipologia dei documenti accessibili è stata rivista e in gran parte dei casi limitata ulteriormente. Riguardo alle professioni sopra citate sono state effettuate le seguenti modifiche: • Podologo/a: tolto l'accesso al DSE; • Igienista dentale: tolto l'accesso al DSE; • Massofisioterapista e massaggiatore/rice: tolto l'accesso al DSE; Logopedista: tolto l'accesso al DSE; • Ortottista-assistente di oftalmologia: tolto l'accesso al DSE; • Tecnico/a audiometrista: tolto l'accesso al DSE"; L'attività di monitoraggio come su evidenziato continuerà e sicuramente potranno esserci delle modifiche sia in chiave di profondità temporale di accesso che di mera profondità di accesso ai diversi documenti di cui alla tabella" già trasmessa all'Autorità che è stata inviata nuovamente in modalità aggiornata.

2. Esito dell'attività istruttoria.

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).

I dati inoltre devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (principio di minimizzazione dei dati) (art. 5, par. 1, lett. c) 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).

Con riferimento ai trattamenti oggetto del presente provvedimento, 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](http://www.gpdp.it/docweb/n.4084632)), 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 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 al titolare 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.

L’accesso al dossier deve essere, pertanto, limitato al solo personale sanitario che interviene nel tempo nel processo di cura del paziente. Ciò significa che deve essere consentito l’accesso solo al personale che a vario titolo interviene nel processo di cura. L’accesso al dossier deve essere limitato, poi, al tempo in cui si articola il processo di cura, ferma restando la possibilità di accedere nuovamente al dossier qualora ciò si renda necessario in merito al tipo di trattamento medico da prestare all’interessato.

Come già rappresentato dall’Autorità nelle citate Linee guida e in altri provvedimenti, tenuto conto del diritto di oscuramento esercitabile dall’interessato ai dati accessibili mediante il dossier sanitario e quindi la possibile incompletezza di tale strumento informativo, il titolare deve individuare, in relazione alle diverse funzioni a cui è adibito il personale, soluzioni tecniche organizzative che consentano agli organi amministrativi della direzione sanitaria di accedere, nei limiti delle attribuzioni previste per legge, a una base informativa più completa rispetto a quella presente nel dossier sanitario aziendale.

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).

Con provvedimento del 3 luglio 2014 (doc. web n. 3325808) l'Autorità era già intervenuta in merito al trattamento dei dati effettuati attraverso il dossier sanitario aziendale dell'ASDAA. In tale provvedimento il Garante aveva ravvisato specifici profili di criticità relativi all'informativa e al consenso degli interessati, vietando all'Azienda ulteriori trattamenti di dati personali, acquisiti senza il consenso informato degli interessati e prescrivendo alla stessa le misure necessarie per rendere il trattamento lecito.

Con specifico riferimento agli aspetti del trattamento oggetto del presente provvedimento, ovvero alla necessità che l'accesso al dossier sia consentito solo al personale che ha effettivamente in cura l'interessato, nel predetto provvedimento il Garante aveva rilevato che i dossier sanitari potevano essere consultati, in ogni momento, da parte degli esercenti le professioni sanitarie operanti all'interno dell'ASDAA a prescindere dalla circostanza che avessero in cura l'interessato. Ciò stante il Garante aveva prescritto all'Azienda di completare -entro il XX la messa in atto di specifici accorgimenti che consentissero ai soli professionisti sanitari che avessero in quel momento in cura il paziente (che abbia già manifestato un consenso informato alla costituzione del dossier) di accedere al suo dossier sanitario e per il tempo in cui si sarebbe articolato il percorso di cura (cfr. provvedimento di differimento dell'11 settembre 2014, doc. web n. 3494478).

Ulteriori criticità erano state rilevate anche in merito al diritto di oscuramento, con riferimento al quale il Garante aveva prescritto alla predetta Azienda di mettere in atto specifici accorgimenti che consentissero all'interessato di poter esprimere la volontà di oscurare nel proprio dossier sanitario singoli eventi clinici anche relativi al pregresso.

Successivamente all'adozione del citato provvedimento del 2014, il Garante ha adottato le Linee guida in materia di dossier sanitario (2015) applicabili anche al dossier sanitario tenuto dall'Azienda. Con la piena applicazione del Regolamento l'Azienda era tenuta inoltre ad adeguare tale strumento informativo ai principi di protezione dei dati fin dalla progettazione e per impostazione predefinita di cui all'art. 25 del Regolamento.

Ciò premesso, preso atto di quanto rappresentato dall'Azienda nelle memorie difensive relative ai procedimenti indicati nei precedenti punti, si osserva che:

1. Profili di autorizzazione per l'accesso al dossier. La configurazione del dossier sanitario presente nel momento in cui si sono verificati i fatti oggetto di reclamo e di notifica di violazione consentiva al personale sanitario di accedere a tale strumento informativo relativo a qualunque paziente fosse stato assistito dalla stessa, dichiarando la sussistenza di una pluralità di casistiche preordinate. Sebbene l'Azienda avesse dichiarato di aver ottemperato al citato provvedimento del Garante del 3 luglio 2014, le misure messe in atto non risultavano pienamente idonee a garantire che potesse accedere al dossier sanitario di un paziente solo il personale sanitario che lo avesse in cura, come poi è stato più analiticamente indicato dal Garante nelle richiamate Linee guida del 2015. In particolare, come dimostrano i casi in esame, la configurazione originaria del dossier sanitario effettuata da codesta Azienda, anche successivamente al citato provvedimento del Garante del 3 luglio 2014, ha reso di fatto possibile che attraverso l'utenza di un professionista sanitario operante presso la stessa si potesse accedere al dossier sanitario di interessati che non solo non erano in cura presso il titolare dell'utenza ("non sia stato preso in carico dai servizi in cui tali professionisti sono/erano in servizio"), ma che non risultavano neanche associati a "eventi clinici amministrativi tracciati a livello informatico". Le modifiche che l'Azienda, a seguito della notifica della violazione di cui all'art. 166, comma 5 del Codice, ha dichiarato di voler realizzare per l'accesso al dossier superano le criticità rilevate nel corso dell'istruttoria in quanto: è stata chiusa "la possibilità di accesso ai professionisti sanitari al proprio DSE"

con il profilo di sanitario; “l’accesso avviene per ruoli (profili professionali). A ciascun ruolo viene consentito uno specifico ambito di visione coerente con le proprie necessità e competenze”; è stato precluso l’accesso al dossier da parte dei ruoli di logopedista, assistente di oftalmologia, podologo, igienista dentale, massaggiatore e massofisioterapista e tecnico audiometrista. Tali modifiche, secondo quanto dichiarato in atti, saranno a regime per tutti i contesti di riferimento, entro il XX;

2. Alert per accessi anomali al dossier sanitario. A seguito dell’avvio dell’istruttoria da parte del Garante l’Azienda ha attivato degli alert automatici in ordine al numero degli accessi e al controllo sull’esistenza di un evento amministrativo clinico attivo;

3. Finalità del dossier sanitario. Prima dell’avvio dell’istruttoria da parte del Garante l’Azienda aveva consentito l’accesso al dossier sanitario anche dal personale della Direzione medica per “adempimenti normativi/organizzativi” e per il “Registro tumori: consultazione”. Al riguardo, si evidenzia che, stante quanto rappresentato dall’Autorità nelle citate Linee guida, il titolare deve individuare, in relazione alle diverse funzioni a cui è adibito il personale, specifici profili per l’accesso al dossier anche con riferimento agli organi amministrativi della direzione sanitaria, affinché gli stessi possano accedere, nei limiti delle attribuzioni previste per legge, a una base informativa più completa rispetto a quella presente nel dossier sanitario aziendale. Stante il diritto di oscuramento esercitabile dall’interessato sui dati presenti all’interno del dossier sanitario, tale strumento informativo potrebbe infatti non essere completo. Con specifico riferimento al Registro tumori si osserva che le modalità di consultazione di tale Registro sono espressamente previste dalla disciplina di settore, su cui l’Autorità ha reso il proprio parere, che non prevedono l’uso del dossier sanitario (Parere su uno schema di decreto ai sensi dell’art. 12, comma 13 del d.l. 18 ottobre 2012, n. 179, convertito con modificazioni in legge 17 dicembre 2012, n. 221, per l’istituzione del Registro nazionale tumori - 7 aprile 2022, doc. web n. 9773977). Successivamente all’avvio del procedimento sanzionatorio da parte dell’Autorità, l’Azienda ha rappresentato di aver modificato le casistiche di accesso al dossier, perseguendo con lo stesso “esclusivamente” “finalità di cura dell’assistito e cioè di prevenzione, diagnosi, cura e riabilitazione, con esclusione di ogni altra finalità”. Sul punto si prende atto che tra i ruoli cui è consentito l’accesso non risultano più indicate la direzione medica e il Registro tumori.

4. pertanto, la configurazione del dossier risultante all’epoca dei fatti oggetto di istruttoria ha reso possibile che personale sanitario operante presso l’Azienda potesse accedere senza restrizioni al dossier sanitario di pazienti che non erano -all’atto dell’accesso- in cura presso gli stessi, in violazione dei principi di base del trattamento di cui agli artt. 5, par. 1, lett. a) e f) e 9 del Regolamento, nonché dei principi di protezione dei dati fin dalla progettazione (privacy by design) e per impostazione predefinita (privacy by default) contemplati all’art. 25 del Regolamento;

5. l’Autorità era già intervenuta sul trattamento dei dati in esame con il provvedimento del 3 luglio 2014 in cui era stato prescritto, tra l’altro, all’Azienda di mettere in atto specifici accorgimenti che consentissero ai soli professionisti sanitari che hanno in quel momento in cura il paziente di accedere al suo dossier sanitario per il tempo in cui si articola il percorso di cura. Tali accorgimenti dovevano essere adottati entro il 31 ottobre 2014 (cfr. provvedimento di differimento dell’11 settembre 2014, doc. web n. 3494478). L’Azienda, nell’ottemperare al provvedimento del Garante del 2014, ha individuato misure tecniche e organizzative che si sono rivelate inidonee in quanto, come dimostrato i fatti in esame, non hanno impedito che personale sanitario accedesse ai dossier sanitari di pazienti che non avevano in cura e non ha aggiornato tali misure alla luce delle Linee guida del Garante del 2015 né in occasione della piena applicazione del Regolamento;

6. la configurazione del dossier risultante all’epoca dei fatti oggetto di istruttoria non

prevedeva un sistema per il rilevamento di eventuali anomalie che potessero 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 (artt. 5, par. 1, lett. f) e 32 del Regolamento);

7. l'Azienda ha illustrato nelle note in atti il programma il processo di adeguamento dei sistemi informativi utilizzati da "tutti i contesti di riferimento" che si concluderà entro il XX.

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 con riferimento ai predetti procedimenti avviati a seguito delle comunicazioni di violazione e dei reclami, 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 è stato avviato un procedimento disciplinare e in un caso anche penale nei confronti dell'autore dell'accesso e che sono stati effettuati gli adeguamenti necessari a superare le criticità sopra descritte, non ricorrono 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, è soggetta all'applicazione della sanzione amministrativa pecuniaria ai sensi dell'art. 83, par.4 e 5, del Regolamento.

In considerazione del fatto che i predetti procedimenti riguardano il medesimo titolare, trattamenti di dati personali analoghi, verificatesi nello stesso arco temporale e che l'Azienda nelle memorie difensive relative ai predetti procedimenti ha fornito i medesimi elementi difensivi, si ritiene opportuno adottare le rispettive sanzioni amministrative in un unico provvedimento (artt. 10, comma 4, e 19 del Regolamento del Garante n. 1/2019).

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 due notifiche di violazione e di due reclami (art. 83, par. 2, lett. h) del Regolamento);
- con riferimento a tutti gli eventi oggetto di notificazione e di reclamo, gli accessi illeciti hanno riguardato il dossier sanitario di tre pazienti da parte di professionisti sanitari che non erano coinvolti nel processo di cura degli stessi e nei confronti dei quali è stato avviato un procedimento disciplinare e in un caso anche penale (art. 83, par. 2, lett. a), b) e g) del Regolamento);
- nel caso del primo e del secondo reclamo, che è stato anche oggetto di notifica di violazione, gli accessi non sono stati giustificati da motivi clinici (due nel primo caso e cinque nel secondo) e si sono verificati nel periodo XX, mentre nel caso oggetto dell'ultima notifica di violazione tra il XX e il XX (accesso da parte di un dipendente dell'Azienda al dossier sanitario del coniuge a sua insaputa) (art. 83, par. 2, lett. a) e b) del Regolamento);
- i predetti accessi sono stati possibili in quanto le misure in essere con riferimento ai trattamenti dati idonei a rilevare informazioni sulla salute effettuati attraverso il dossier sanitario aziendale non erano pienamente proporzionate al fine di garantire un'adeguata sicurezza e integrità dei dati personali e di scongiurare accessi non consentiti, sebbene l'Autorità fosse già intervenuta in merito con il citato provvedimento del 3 luglio 2014 e successivamente con le Linee guida del 2015 (art. 83, par. 2, lett. d) e e) del Regolamento);
- l'Azienda ha modificato le modalità e le fattispecie di accesso al dossier sanitario aziendale a seguito dell'avvio dell'istruttoria da parte dell'Autorità, nonché introdotto sistemi di alert, cooperando con l'Autorità a tal fine (art. 83, par. 2, lett. c) e f) 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), 9, 25 e 32 del Regolamento nella misura:

- di 25.000 (venticinquemila) per il procedimento avviato a seguito del reclamo presentato dal Sig. XX;
- di 25.000 (venticinquemila) per il procedimento avviato a seguito della notifica di violazione del XX, successivamente integrata il XX, e del reclamo presentato dal Sig. XX; e
- di 25.000 (venticinquemila) per il procedimento avviato a seguito della notifica di violazione del XX;

quali sanzioni amministrative pecuniarie ritenute, ai sensi dell'art. 83, par. 1, del Regolamento, effettive, proporzionate e dissuasive.

Si ritiene, altresì, che debba applicarsi con riferimento ad entrambi i procedimenti esaminati 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 sanitaria dell'Alto Adige, 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 sanitaria dell'Alto Adige, Codice fiscale/partita iva n. 00773750211, di pagare la somma complessiva di euro 75.000 (settantacinquemila) così definita:

la somma di euro 25.000 (venticinquemila) a titolo di sanzione amministrativa pecuniaria per le violazioni rilevate nell'ambito del procedimento avviato a seguito del reclamo presentato dal Sig. XX, indicate nel presente provvedimento;

la somma di euro 25.000 (venticinquemila) a titolo di sanzione amministrativa pecuniaria per le violazioni rilevate con la notifica di violazione del XX, successivamente integrata il XX, e del reclamo presentato dal Sig. XX, indicate nel presente provvedimento;

la somma di euro 25.000 (venticinquemila) a titolo di sanzione amministrativa pecuniaria per le violazioni rilevate con la notifica di violazione del XX, indicate nel presente provvedimento;

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 la somma complessiva di euro 75.000 (settantacinquemila) 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 dinanzi 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, 22 febbraio 2024

IL PRESIDENTE
Stanzione

IL RELATORE
Ghiglia

IL SEGRETARIO GENERALE
Mattei