Ordinanza ingiunzione nei confronti di Azienda sanitaria universitaria Friuli Centrale - 26 maggio 2022 [9790365]

VEDI ANCHE NEWSLETTER DEL 26 LUGLIO 2022

[doc. web n. 9790365]

Ordinanza ingiunzione nei confronti di Azienda sanitaria universitaria Friuli Centrale - 26 maggio 2022

Registro dei provvedimenti
n. 201 del 26 maggio 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 dott. Claudio Filippi, vice segretario generale;

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

VISTO il d.lgs. 30 giugno 2003, n. 196 recante "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 la prof.ssa Ginevra Cerrina Feroni;

PREMESSO

1. La violazione dei dati personali e l'attività istruttoria

L’Autorità ha ricevuto due notifiche di violazione e un reclamo in merito al trattamento di dati personali effettuato dall’Azienda sanitaria universitaria Friuli centrale (di seguito ASUFC) mediante il dossier sanitario aziendale (denominato “Visore referti”). 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.

1.1 Le notifiche di violazione in ordine all’accessi al dossier sanitario aziendale di un dipendente da parte di personale medico aziendale.

L’ASUFC con nota del XX (prot. n. XX), ha notificato una violazione di dati personali rappresentando che “in data XX, due dipendenti dell’Azienda hanno avuto accesso al visore referti – dossier sanitario di una paziente che è al tempo stesso una dipendente, in assenza di un valido presupposto giuridico, venendo a conoscenza di dati inerenti lo stato di salute della stessa”, nonché di essere “venuta a conoscenza della violazione a seguito della segnalazione dell’interessata” e che al riguardo “è stato avviato il procedimento disciplinare nei confronti dei dipendenti che hanno effettuato l’accesso improprio ed è stato presentato un esposto alla Procura della Repubblica presso il Tribunale di Udine”.

In relazione alla predetta notifica di violazione l’Ufficio ha chiesto informazioni con le note del XX (prot. n. XX), del XX (prot. n. XX) e del XX (prot. n. XX), con riferimento alle quali l’ASUFC ha risposto con le note del XX, del XX e del XX a firma del responsabile per la protezione dei dati personali, in cui è stato, in particolare, rappresentato che:

- "il DSE funziona con l’applicazione Visore Referti, fornita da INSIEL SPA. L’accesso al Visore è riservato al personale sanitario” e “consente al personale sanitario di accedere ai dati relativi alle prestazioni sanitarie dei pazienti che risultano in cura presso la struttura”;

l’accesso al dossier è ammesso alle seguenti condizioni: “a) se il paziente risulta in cura, ossia è ricoverato in un reparto, o si trova nel Pronto Soccorso, oppure è in corso una visita ambulatoriale prenotata, i suoi dati sono accessibili al personale sanitario; b) se il paziente non risulta in cura, l’accesso ai dati tramite Visore Referti è subordinato al rilascio di una dichiarazione di responsabilità dell’operatore sanitario, il quale deve effettuare una scelta tra le quattro condizioni alternative”;

“Qualora il paziente non sia ricoverato nella struttura da cui si effettua l’accesso al Visore Referti, l’accesso ai dati è subordinato al rilascio di una dichiarazione di responsabilità dell’operatore sanitario, il quale deve effettuare una scelta tra quattro condizioni alternative di autorizzazione all’accesso. La mancanza dell’opzione è “bloccante” e la sessione non può proseguire”;

la dichiarazione di responsabilità è la seguente: “«dichiaro sotto la mia responsabilità di aver diritto a proseguire nella visualizzazione dei dati per attività di:

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 prelievo/trapianto

Direzione sanitaria – supporto ai processi organizzativi e adempimenti normativi»”;

“Le dichiarazioni sono registrate, al pari di tutti gli accessi effettuati mediante Visore Referti, al fine di consentire la successiva verifica della legittimità di tali accessi, e ciò in caso di istanze di accesso dell’interessato ex art. 15 RGPD, oppure ove emergano dubbi in proposito”.

"il Visore Referti è accessibile unicamente da medici ed infermieri autorizzati alle condizioni seguenti:

a) se il paziente è presente in Azienda, ossia è ricoverato in un reparto, o si trova nel Pronto Soccorso, oppure è in corso una visita ambulatoriale prenotata;

b) se il paziente non risulta presente, la circostanza che il paziente intervenga nel processo di cura è oggetto di specifica dichiarazione del personale che intende accedere ai dati, da trasmettere tramite l'applicazione Visore Referti mediante selezione di una delle quattro condizioni alternative già menzionate nella precedente nota del XX.

Il caso di specie rientra nella fattispecie citata sopra sub b), poiché l'interessata non era presente al momento degli accessi ai dati esposti nella notifica di violazione del XX";

con riferimento al protocollo di comunicazione sicura, "si comunica che il nuovo Visore Referti, per il quale è già in essere l'avvio della relativa e graduale implementazione, supporterà il protocollo "https" con decorrenza XX, al termine delle necessarie attività di adeguamento della intera infrastruttura dedicata. Tale implementazione potrà comunque subire dei ritardi in relazione anche ad eventi oggi non prevedibili o ad una differente prioritarizzazione delle esigenze definite dalla competente Direzione Centrale Regionale" (nota di Insiel del XX, prot. XX).

In relazione alle risultanze della predetta attività istruttoria, l'Ufficio, con atto n. XX del XX, ha notificato all'ASUFC, 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, l'Ufficio, ha evidenziato che la configurazione del dossier sanitario effettuata da ASUFC individua un unico profilo di accesso, consentendo, quindi, a tutto il personale sanitario di accedere ai dossier sanitari di qualsiasi paziente sia in quel momento presente in Azienda a prescindere dalla circostanza che lo stesso sia effettivamente in cura presso il soggetto che effettua l'accesso, senza alcuna limitazione temporale.

L'Ufficio ha poi rilevato che la mancata individuazione di diversi profili di accesso rende evidente come non si sia tenuto conto, non solo della circostanza che può accedere al dossier solo il personale che ha in quel momento in cura il paziente, ma anche che non tutto il personale sanitario può essere abilitato a effettuare le stesse attività di trattamento di dati personali attraverso il dossier.

E' stato inoltre rilevato che non è stato adottato, come richiesto dalle citate Linee guida, 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.

Nel predetto atto è stato inoltre evidenziato che ASUFC utilizza per il trattamento in esame il protocollo di rete "http" (hypertext transfer protocol) che, oltre a non garantire la riservatezza e l'integrità dei dati scambiati tra il browser dell'utente e il server che ospita l'applicazione, non consente agli utenti di verificare l'autenticità del server con cui colloquiano.

Ciò stante, è stata contestata la violazione dei principi di base del trattamento di cui all'art. 5, par. 1, lett. a) e f), del Regolamento e dei successivi artt. 9, 25 e 32. 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 (prot. n. XX) l'ASUFC ha inviato scritti difensivi e ha chiesto di essere sentita, rappresentando, in particolare, che il fatto oggetto di notifica ha riguardato la "signora XX, già dipendente della stessa Azienda presso la UO Pronto Soccorso di Latisana, in conseguenza dell'accesso non autorizzato – attraverso l'applicazione Visore Referti – da parte di un medico, signor XX, e di un'infermiera, signora XX, entrambi servizio nello stesso reparto dell'interessata". gli accessi si sarebbero verificati "tutti in data 24/09/2020, rispettivamente dalle ore 2.30 alle 2.33 (accesso della signora XX), e dalle ore 3.22 alle ore 3.28 (signor XX). In ambedue i casi, poiché la signora XX non era presente nella struttura sanitaria al momento dell'accesso ai dati, sia l'infermiera che il medico – al fine di accedere ai dati medesimi – dichiaravano sotto la propria responsabilità di aver diritto a proseguire nella visualizzazione dei dati per l'attività di "Prevenzione/diagnosi/cura/riabilitazione su paziente incarico ma non registrato nei percorsi informatizzati previsti"". L'ASUFC in tale atto ha contestato quanto rappresentato dall'Ufficio nella nota del XX ritenendo che "le prestazioni sanitarie fornite dall'ASUFC sono quantitativamente e qualitativamente estremamente numerose, eterogenee ed interdisciplinari, sicché non appare possibile stabilire a priori rigide regole temporali sull'accessibilità ai dati per finalità di cura, proprio perché il processo di cura del paziente può essere caratterizzato dalla prestazione di servizi molto diversi, resi in tempi e luoghi diversi e da professionisti appartenenti a diverse discipline".

È stato inoltre precisato che "quanto poi all'accessibilità dei dati da parte del personale della Direzione Sanitaria dell'ASUFC, anch'essa oggetto di contestazione nella notifica della violazione del XX, occorre osservare che tale questione, oltre a non avere alcuna pertinenza con il caso di specie, rientra evidentemente nella nozione di trattamento per finalità di cura ai sensi del già citato art. 9.1.h) del RGPD".

In merito al protocollo di comunicazione usato dall'Azienda la stessa ha rappresentato che "Non si vede, infatti, in che modo l'adozione del protocollo "HTTPS" avrebbe potuto prevenire o evitare la violazione dei dati della signora A.R (…). Si è comunque indicato che, in un lasso di tempo che appare ragionevole, in nuovo visore referti supporterà il protocollo "HTTPS"".

Nel corso della predetta attività istruttoria l'ASUFC, con nota del XX (prot. n. XX), ha notificato una ulteriore violazione di dati personali relativamente ad una fattispecie analoga a quella precedentemente notificata descritta nel precedente paragrafo.

In particolare, nella predetta comunicazione l'AUFC ha dichiarato di aver verificato, a seguito di una segnalazione di un paziente, che "in un arco temporale compreso tra il 2018 ed il 2020, alcuni dipendenti dell'Azienda hanno avuto accesso al visore referti – dossier sanitario di una paziente che è al tempo stesso una dipendente, in assenza di un valido presupposto giuridico, venendo a conoscenza di dati inerenti lo stato di salute della stessa". Nel caso di specie, secondo quanto dichiarato in atti, "tutti gli operatori hanno dichiarato di aver diritto di proseguire nella consultazione della documentazione per "prevenzione / diagnosi/cura / riabilitazione su paziente in carico ma non registrato nei percorsi informatizzati previsti".

Nella predetta comunicazione l'ASUFC ha poi specificato "che è stato avviato il procedimento disciplinare nei confronti dei dipendenti che hanno effettuato l'accesso improprio e verrà presentato un esposto alla Procura della Repubblica presso il Tribunale di Udine" e che intende procedere ad una "maggior sensibilizzazione del personale sul corretto utilizzo degli strumenti informatici e sulle conseguenze derivanti dall'uso improprio degli stessi; controlli periodici e sistematici volti a verificare il corretto uso degli strumenti aziendali".

Ciò stante, l'Ufficio con nota del XX (prot. n. XX) ha riunito i procedimenti istruttori relativi alle notifiche di violazione del XX e del XX e ha notificato all'ASUFC, 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, ribadendo quanto già contestato con la nota del XX e 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).

Con nota del XX (prot. n. XX) l'ASUFC, nel chiedere di essere sentita, ha inviato scritti difensivi, ove ha ribadito quanto già rappresentato in atti, specificando che "la violazione dei dati della signora XX, dipendente della stessa Azienda presso il reparto di Pneumologia Riabilitativa dell'ospedale Gervasutta" è avvenuta "in conseguenza dell'accesso non autorizzato – attraverso l'applicazione Visore Referti – da parte di tre medici e di un'infermiera, tutti in servizio nello stesso reparto dell'interessata. (…) gli accessi non autorizzati sarebbero undici, verificatisi tra il 22/10/2018 ed il 04/12/2020. I quattro dipendenti, ai quali gli accessi risultano riconducibili, sono stati interpellati ed hanno tutti escluso di aver effettuato personalmente tali accessi, non avendo motivazioni di natura professionale o interessi personali che giustifichino tale condotta. Essi ipotizzano che gli accessi ai dati siano stati effettuati da ignoti che, avendo accesso a computer condivisi, si sarebbero inseriti in una sessione di lavoro lasciata aperta per ragioni di urgenza. L'ASUFC ha, quindi, avviato il procedimento disciplinare ed ha contestualmente presentato denuncia all'autorità giudiziaria per l'ipotesi di reato ex art. 615-ter c.p.".

Con successiva nota del XX (prot. n. XX) l'ASUFC ha rinunciato all'audizione che aveva precedente richiesto.

1.2. Il reclamo in ordine all'accessi al dossier sanitario aziendale di un dipendente da parte di personale medico aziendale

Nel mese di XX è pervenuto all'Autorità un reclamo da parte della Sig.ra XX che lamentava "plurimi accessi" al sistema informativo che gestisce il dossier sanitario dell'ASUFC "non attinenti a necessità terapeutiche e/o cliniche" da parte di professionisti operanti presso il reparto di Pneumologia riabilitativa dell'Ospedale Gervasutta afferente a codesta Azienda, ove, tra l'altro la reclamante presta servizio".

A seguito della richiesta di informazioni dell'Ufficio (nota del XX, prot. n. XX), l'ASUFC ha rappresentato che il suddetto reclamo si riferisce alla violazione di dati personali notificata dall'Azienda il XX, su cui l'Ufficio aveva già avviato il procedimento sanzionatorio (nota del XX, prot. n. XX).

1.3. Il coinvolgimento della Regione Friuli Venezia Giulia e successive fasi istruttorie

Nell'ambito dell'istruttoria avviata a seguito delle predette notifiche di violazione e di analoghe istruttorie avviate nei confronti di altre aziende sanitarie della Regione Friuli Venezia Giulia in merito ai trattamenti di dati personali effettuati attraverso il dossier sanitario è emerso che tutte le aziende sanitarie appartenenti al servizio sanitario regionale (SSR) hanno istituito il dossier sanitario aziendale mediante l'applicativo denominato "visore referti" messo a disposizione da Insiel S.p.A..

Secondo quanto dichiarato negli atti istruttori, la configurazione del dossier sanitario aziendale sarebbe stata effettuata secondo regole standard definite da Insiel sotto il coordinamento della predetta Regione, in un'ottica di uniformità e omogeneità a livello informativo del Servizio sanitario regionale. In particolare, la configurazione del dossier sanitario messa a disposizione da Insiel consentiva di fatto al personale sanitario di accedere al dossier relativo a qualunque paziente fosse in quel momento fisicamente presente nell'Azienda sanitaria e, dichiarando la sussistenza di una pluralità di casistiche preordinate, anche a quelli dei pazienti non presenti nell'Azienda sanitaria.

Ciò stante, l'Ufficio -con nota del XX (prot. n. XX)- ha evidenziato alla Regione Friuli Venezia Giulia e alle aziende sanitarie coinvolte gli aspetti di criticità ravvisati nell'attuale configurazione dei dossier sanitari, legati principalmente ai profili di autorizzazione previsti per l'accesso al dossier sanitari e ai sistemai di alert. In tale nota l'Ufficio ha proposto un incontro con i predetti Enti, al fine di approfondire le caratteristiche del sistema informativo messo a disposizione da Insiel alle aziende sanitarie regionale ("visore referti") attraverso il quale le stesse hanno realizzato il dossier sanitario aziendale, nonché il margine di autonomia riconosciuto alle aziende sanitarie nell'implementazione delle misure ritenute dalle stesse necessarie, in qualità di titolari del trattamento, al fine di rendere conforme il trattamento alla disciplina sulla protezione dei dati personali.

A seguito del predetto incontro, svoltosi da remoto il XX, la predetta Regione ha inviato una nota nella quale sono stati riassunti gli "interventi adeguativi del sistema "Visore Referti", al fine di eliminare o per lo meno minimizzare le criticità ravvisate" (nota del XX, prot. n. XX).

Nella suddetta nota è stata descritta la "situazione attuale", ovvero le "regole generali, valide per tutta la Regione:

- Visualizzazione dei documenti sulla base dei consensi prestati dall'interessato, con esclusione: o dei documenti oscurati su base normativa (HIV, genetica, interruzioni di gravidanza, etc.) o oppure dei documenti oscurati puntualmente su richiesta del cittadino (a cura del medico, durante il processo di diagnosi e cura, ovvero su richiesta anche successiva da parte dell'interessato);

- In mancanza di una presa in carico amministrativa (per ricovero, accesso in pronto soccorso, o per erogazione di una prestazione ambulatoriale o di consulenza), i dati sono accessibili solo su esplicita autodichiarazione con motivazione (ad esempio, in caso di paziente cronico che contatta telefonicamente la struttura e necessita di un parere per il proseguimento di cure domiciliari)."

La Regione ha inoltre precisato che "a carico di ciascun titolare, è possibile, per il tramite dei suoi amministratori di sistema, intervenire sulle configurazioni del sistema per:

- Abilitare gli operatori all'accesso al sistema, assegnando loro ruoli specifici, tra quelli concordati tra gli enti operanti nel sistema sanitario regionale;

- Individuare le unità operative per le quali escludere completamente i documenti generati dalla visibilità (ad esempio, i referti del medico competente);

- Definire, per ciascuna unità operativa, il tipo di documento da visualizzare (referto, lettera di dimissione, lettera di trasferimento, verbale di Pronto Soccorso, …) e il suo stato (definitivo, firmato digitalmente, …);

- Operare l'oscuramento su singoli documenti, a cura del medico redattore".

Con riferimento al sistema di accesso al "visore referti" la Regione ha precisato che "non sono previsti ruoli di tipo amministrativo, in quanto non pertinenti con le finalità del sistema".

Nella predetta nota sono stati inoltre sommariamente descritti gli "adeguamenti previsti". In particolare, con riferimento alla visibilità dei documenti accessibili attraverso il suddetto "visore referti" è stato dichiarato che:

- "L'accesso senza autodichiarazione può essere ristretta alle sole unità operative per le quali è stata aperta un'accettazione amministrativa. Per gli episodi ambulatoriali o le richieste di consulenza, l'apertura ha validità per il giorno solare di apertura; per il pronto

soccorso, fino alla dimissione; per i ricoveri, fino alla dimissione/trasferimento.

• Nel caso fosse necessario accedere al dossier di pazienti non presenti dal punto di vista amministrativo (ad esempio, per visualizzare referti pervenuti a seguito della dimissione ospedaliera), sarà necessario compilare l'autodichiarazione, motivando il motivo di accesso. In tutti i casi in cui il paziente non è presente amministrativamente nella struttura che accede al visore, è necessaria l'autodichiarazione".

In merito alla tempistica della realizzazione dei suddetti adeguamenti, è stato dichiarato che gli stessi possono essere effettuati "in due fasi distinte:

• Prima fase (più restrittiva): tutti gli operatori accedono con autodichiarazione, indipendentemente dal fatto che il paziente sia presente amministrativamente nella specifica unità operativa. La soluzione è implementabile nell'arco di 10 giorni lavorativi dalla richiesta;

• A regime: consente alla struttura che ha il paziente presente per accettazione amministrativa (reparto, ambulatorio, PS, RSA, …) di accedere ai documenti senza autodichiarazione. Per tutte le altre strutture, l'autodichiarazione è obbligatoria. Implementazione graduale sui vari sistemi chiamanti il nuovo visore nell'arco di 6 mesi".

In merito agli "Strumenti di alert" è stato rappresentato che "nell'arco di tre mesi, verranno rilasciate delle ulteriori funzioni di datawarehouse, consultabili e personalizzabili da ciascun titolare. Sarà possibile incrociare i dati degli accessi al sistema, delle autodichiarazioni compilate, dello status di dipendente dei pazienti. I cruscotti che saranno resi disponibili consentiranno di monitorare le casistiche di autodichiarazione, la frequenza di consultazione, etc. Oltre a un set di visualizzazioni e riepiloghi che verranno resi disponibili per tutte le aziende, ciascun titolare, per mezzo dei suoi amministratori di sistema, potrà definire autonomamente estrazioni e riepiloghi, per raffinare le azioni di monitoraggio e di rilevamento di eventuali anomalie".

Preso atto di quanto dichiarato nella predetta nota, l'Ufficio, al fine di definire i procedimenti istruttori avviati nei confronti delle aziende sanitarie regionali, tra cui l'ASUFC, con nota del XX (prot. n. XX), ha chiesto alla predetta Regione informazioni in merito all'attuale stato di implementazione degli "adeguamenti" sopra descritti; alle modalità di accesso al visore referti previste nell'ipotesi in cui l'interessato sia presente per accettazione amministrativa in una unità operativa diversa da quella che effettua l'accesso; al margine di autonomia riconosciuto alle aziende sanitarie nel chiedere, in qualità di titolari del trattamento, alla società Insiel, già designata dalle stesse aziende responsabile del trattamento, la modifica o la personalizzazione delle suddette misure di adeguamento, con particolare riguardo alle configurazioni relative all'acceso al dossier sanitario; alle fattispecie che possono essere oggetto della suddetta "autodichiarazione", con particolare riferimento a quelle, sino ad ora consentite, relative alla "direzione sanitaria (supporto a processi organizzativi e adempimenti normativi)" e al "critical review, per analisi ed eventuale miglioramento dei percorsi di cura", indicate nella documentazione in atti; alla tipologia di informazioni registrate nei file di log relative agli accessi e alle operazioni compiute; alle misure che si intendono adottare per assicurare che l'accesso al dossier sanitario mediante l'applicativo "visore referti", quando effettuato da ambulatori esterni alle aziende, possa essere effettuato soltanto con riferimento ai dossier degli interessati in cura presso i suddetti ambulatori.

In risposta alla predetta richiesta di informazioni, la Regione Friuli Venezia Giulia ha risposto con nota del XX (prot. n. XX) dichiarando, in particolare, che "verrà attivato un percorso di verifica e analisi sui sistemi già in dotazione alle aziende sanitarie, al fine di valutare la loro possibile applicazione nell'ambito delle carceri/ambulatori esterni, nel rispetto della normativa relativa al trattamento dei dati personali".

In allegato alla risposta la Regione ha fornito una nota di Insiel del XX (prot. n. XX) nella quale la

Società ha rappresentato che:

"L'adeguamento previsto nella prima fase è attivabile, a livello regionale e previa concertazione con i titolari del trattamento, entro 15 giorni dalla ricezione della richiesta":

• Completamento della "fase a regime" entro il mese di giugno 2022. L'implementazione della fase a regime prevede che la presa in carico amministrativa del paziente avvenga a livello di singola unità operativa. L'attività prevede:

• una fase di analisi e progettazione degli sviluppi e la valutazione dell'impatto organizzativo sugli operatori delle aziende (entro il mese di febbraio/marzo 2022);

• l'adeguamento dei sistemi gestionali clinico-sanitari che invocano il Visore Referti e che indicano la presa in carico amministrativa del paziente per la specifica unità operativa; gli adeguamenti dovranno consentire l'attuale operatività fino al completamento dei rilasci (entro il mese di maggio 2022);

• l'adeguamento del visore Referti che recepisce l'informazione sulla presa in carico a livello di unità operativa per cui sia aperta una specifica accettazione amministrativa del paziente interessato e consente solo in questo contesto l'accesso al dossier del paziente stesso senza esprimere una autodichiarazione (entro la prima metà del mese di giugno 2022);

• l'attivazione degli adeguamenti sulle Aziende sanitarie, con contestuale formazione degli operatori sulle nuove modalità di utilizzo (entro il mese di giugno 2022).

• Si conferma, entro il mese di marzo 2022, il rilascio dei cruscotti di monitoraggio indicati nella sezione "Strumenti di alert";

• In caso di unità operativa diversa da quella nella quale l'interessato è presente per accettazione amministrativa, l'accesso al Visore Referti potrà avvenire solo previa autodichiarazione dell'operatore, con indicazione della motivazione;

• Si riportano di seguito le attuali voci selezionabili nel form di autodichiarazione:

Prevenzione/diagnosi/cura/riabilitazione su paziente in carico ma non registrato nei percorsi informatizzati previsti (ad esempio attività di pre/post ricovero o pre/post prestazione ambulatoriale, consulenza tra colleghi della stessa azienda).

Critical review per analisi ed eventuale miglioramento dei percorsi di cura (ad esempio audit, RCA, eventi sentinella, ecc. come previsto dalla normativa).

Processo di prelievo/trapianto (ad esempio attività di prelievo d'organo in donatore cadavere a garanzia del migliore processo di cura).

Direzione sanitaria: supporto ai processi organizzativi e adempimenti normativi (ad esempio attività di polizia mortuaria riscontro diagnostico, accertamento causa di morte, assenza di reato o di malattia infettiva). È anche previsto un campo note ove l'operatore può inserire un testo libero. E' possibile modificare/estendere/eliminare le voci presenti in elenco in base alle specifiche esigenze o a diverse modalità organizzative che si potrebbero mettere in atto.

• particolari richieste di implementazione che modificano il funzionamento generale vengono valutate a livello regionale e proposte come evoluzione per tutte le Aziende

• Nelle tabelle di audit vengono registrati i dati dell'operatore che ha avuto accesso al Visore

Referti, la sua struttura di appartenenza e, in caso di autodichiarazione, verrà registrata anche la specifica motivazione indicata. Per ciascun paziente, inoltre, vengono registrati i suoi estremi e se la visualizzazione si è limitata all'elenco dei suoi documenti, ovvero se l'operatore ha visualizzato anche il dettaglio dello specifico documento".

2. Esito dell'attività istruttoria.

Con riferimento ai trattamenti oggetto delle predette notifiche di violazione e 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), 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.

Con provvedimento del 10 gennaio 2013 (doc. web n. 2284708) l'Autorità era già intervenuta in merito al trattamento dei dati effettuati attraverso il sistema informativo di archiviazione e refertazione delle prestazioni sanitarie erogate dalle strutture sanitarie della Regione Friuli Venezia Giulia, denominato "G2" riconducibile allo strumento del dossier sanitario. In tale provvedimento il Garante aveva ravvisato specifici profili di criticità relativi all'informativa e al consenso degli interessati, all'accesso al dossier sanitario e al diritto di oscuramento tali da rilevare l'illiceità del trattamento effettuato da un'azienda sanitaria regionale e prescrivendo alla stessa le misure necessarie per rendere il trattamento lecito.

In tale provvedimento, l'Autorità aveva inoltre prescritto alle aziende sanitarie e agli istituti di ricovero e cura a carattere scientifico della Regione che avevano in uso il medesimo sistema informativo di rendere conforme il trattamento dei dati personali effettuato attraverso i dossier sanitari aziendali alle prescrizioni dettate alla predetta azienda entro i medesimi termini.

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 ritenuto necessario prescrivere di mettere in atto specifici accorgimenti –anche eventualmente avvalendosi del supporto tecnico fornito da Insiel- che consentano ai soli professionisti sanitari che hanno in quel momento in cura il paziente (che abbia già manifestato un consenso informato alla costituzione del dossier) di

accedere al suo dossier sanitario per il tempo in cui si articola il percorso di cura.

Successivamente all'adozione del citato provvedimento del 2013, il Garante ha adottato le linee guida in materia di dossier sanitario (2015) applicabili anche al dossier sanitario tenuto dall'ASUFC. 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. La configurazione del dossier sanitario predisposta da Insiel e attualmente utilizzata dall'ASUFC consente al personale sanitario di accedere a tale strumento informativo relativo a qualunque paziente sia in quel momento fisicamente presente in Azienda a prescindere dall'effettivo coinvolgimento nel percorso di cura dello stesso e, dichiarando la sussistenza di una pluralità di casistiche preordinate, anche ai pazienti non presenti in Azienda. Secondo quanto dichiarato nella richiamata nota del XX, infatti, "l'accesso ai dati del paziente" è sempre consentito al personale sanitario operante presso codesta Azienda "allorché questo sia presente in azienda, ricoverato in un reparto o nel pronto soccorso o durante una visita ambulatoriale prenotata". Tale impostazione non assicura che al dossier aziendale possa accedere solo il personale sanitario che ha effettivamente in cura il paziente, stante il fatto che non tutti i professionisti sanitari intervengono nel processo di cura di tutti i pazienti ricoverati nei reparti dell'Azienda (compreso quello di emergenza e urgenza) o che usufruiscono di una prestazione sanitaria ambulatoriale. Come dimostrano i casi oggetto di violazione, infatti, l'attuale configurazione del dossier ha reso possibile che personale sanitario operante presso l'Azienda potesse accedere senza restrizioni al dossier sanitario di colleghi ovvero di interessati 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;

2. La configurazione del dossier sanitario predisposta da Insiel e attualmente utilizzata dall'ASUFC -anche alla luce degli adeguamenti prospettati dalla Regione Friuli Venezia Giulia- consente l'accesso al dossier sanitario anche dal personale della Direzione sanitaria per attività di "supporto ai processi organizzativi e adempimenti normativi", per "Critical review per analisi ed eventuale miglioramento dei percorsi di cura (ad esempio audit, RCA, eventi sentinella, ecc. come previsto dalla normativa)" e per "Processo di prelievo/trapianto (ad esempio attività di prelievo d'organo in donatore cadavere a garanzia del migliore processo di cura)". Al riguardo, si evidenzia che, stante quanto già rappresentato dall'Autorità nelle citate Linee guida e in altri provvedimenti (cfr. provvedimento del 21 aprile 2021, n- 155), secondo cui, 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;

3. La configurazione del dossier sanitario predisposta da Insiel e attualmente utilizzata dall'ASUFC non rispetta inoltre il principio secondo cui l'accesso al dossier deve essere limitato 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. Sul punto, nelle predette memorie difensive

l'Azienda ha rappresentato che "le prestazioni sanitarie fornite dall'ASUFC sono quantitativamente e qualitativamente estremamente numerose, eterogenee ed interdisciplinari, sicché non appare possibile stabilire a priori rigide regole temporali sull'accessibilità ai dati per finalità di cura, proprio perché il processo di cura del paziente può essere caratterizzato dalla prestazione di servizi molto diversi, resi in tempi e luoghi diversi e da professionisti appartenenti a diverse discipline". Tali elementi non appaiono sufficienti per derogare alla necessaria individuazione temporale del periodo di validità del profilo di accesso al dossier, atteso che quanto riferito non appare essere una condizione che esima il titolare dall'applicazione dei principi generali del trattamento o una caratteristica unica di codesta Azienda;

4. La configurazione del dossier sanitario predisposta da Insiel e attualmente utilizzata dall'ASUFC non prevede 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 (artt. 5, par. 1, lett. f) e 32 del Regolamento;

5. l'ASUFC utilizza per il trattamento in esame il protocollo di rete "http" (hypertext transfer protocol) che, oltre a non garantire la riservatezza e l'integrità dei dati scambiati tra il browser dell'utente e il server che ospita l'applicazione, non consente agli utenti di verificare l'autenticità del server con cui colloquiano. Tenuto conto della natura, dell'oggetto e della finalità del trattamento, nonché dei rischi che insistono sui dati e della possibile "clonazione" del sistema in questione per l'acquisizione dei dati trasmessi per fini illeciti, la soluzione adottata dall'Azienda non può essere considerata una misura tecnica idonea a garantire un livello di sicurezza adeguato ai rischi presentati dal trattamento, che prevede la trasmissione di dati, anche relativi alla salute, su una rete pubblica di comunicazioni. Il mancato utilizzo di tecniche crittografiche per il trasporto dei dati configura, quindi, una violazione dell'art. 5, par. 1, lett. f), e dell'art. 32 del Regolamento, che peraltro al par. 1, lett. a), individua espressamente la cifratura dei dati come una delle possibili misure di sicurezza idonee a garantire un livello di sicurezza adeguato al rischio (sul punto, cfr. anche il considerando n. 83 del Regolamento nella parte in cui prevede che "il titolare del trattamento […] dovrebbe valutare i rischi inerenti al trattamento e attuare misure per limitare tali rischi, quali la cifratura"). L'ASUFC avrebbe, infatti, dovuto mettere in atto, fin dalla progettazione del proprio servizio, misure tecniche e organizzative adeguate, volte ad attuare in modo efficace i principi di protezione dei dati, tra cui il principio di "integrità e riservatezza", provvedendo ad adottare un protocollo di rete sicuro, quale il protocollo "https" (hypertext transfer protocol over secure socket layer), nell'ambito del sistema in esame. Secondo quanto dichiarato in atti il sistema in esame utilizzerà il protocollo di comunicazione sicura https: "con decorrenza aprile 2022, al termine delle necessarie attività di adeguamento della intera infrastruttura dedicata. Tale implementazione potrà comunque subire dei ritardi in relazione anche ad eventi oggi non prevedibili o ad una differente prioritarizzazione delle esigenze definite dalla competente Direzione Centrale Regionale" (nota di Insiel del XX, prot. XX). Allo stato degli elementi non è stata fornita alcuna assicurazione in merito al rispetto di tale termine;

6. le predette notifiche di violazione e il reclamo hanno permesso di evidenziare che le misure attualmente adottate dall'Azienda, con riferimento ai trattamenti effettuati attraverso il dossier sanitario aziendale, non hanno permesso di evitare la possibilità che il personale sanitario abilitato accedesse alla documentazione clinica di pazienti non in cura presso gli stessi, determinando un trattamento illecito dei dati personali riguardanti gli interessati, in violazione degli artt. 5 par. 1, lett. a) e f) , 9 del Regolamento;

7. la Regione Friuli Venezia Giulia ha illustrato nelle note in atti il programma di un sommario

processo di adeguamento dei sistemi informativi utilizzati dalle aziende sanitarie regionali e alle predette Linnee guida in funzione dei rilievi formulati dall'Ufficio con riferimento ai procedimenti istruttori in essere che indica un termine di adeguamento certo solo per alcuni degli adempimenti necessari. in particolare secondo quanto dichiarato è previsto entro:

a. 10/15 gg dalla richiesta dell'Azienda in qualità di titolare: "Prima fase (più restrittiva): tutti gli operatori accedono con autodichiarazione, indipendentemente dal fatto che il paziente sia presente amministrativamente nella specifica unità operativa";

b .febbraio /marzo 2022: "una fase di analisi e progettazione degli sviluppi e la valutazione dell'impatto organizzativo sugli operatori delle aziende";

c. maggio 2022: "l'adeguamento dei sistemi gestionali clinico-sanitari che invocano il Visore Referti e che indicano la presa in carico amministrativa del paziente per la specifica unità operativa";

d. giugno 2022: "l'adeguamento del visore Referti che recepisce l'informazione sulla presa in carico a livello di unità operativa per cui sia aperta una specifica accettazione amministrativa del paziente interessato e consente solo in questo contesto l'accesso al dossier del paziente stesso senza esprimere una autodichiarazione";

e. giugno 2022: "l'attivazione degli adeguamenti sulle Aziende sanitarie, con contestuale formazione degli operatori sulle nuove modalità di utilizzo";

f. marzo 2022:"il rilascio dei cruscotti di monitoraggio indicati nella sezione "Strumenti di alert";

g. un termine non definito: "verrà attivato un percorso di verifica e analisi sui sistemi già in dotazione alle aziende sanitarie, al fine di valutare la loro possibile applicazione nell'ambito delle carceri/ambulatori esterni, nel rispetto della normativa relativa al trattamento dei dati personali".

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'ASUFC con riferimento ai predetti procedimenti avviati a seguito delle comunicazioni di violazione e 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, considerando, che in entrambi i procedimenti sopra descritti è stato avviato un procedimento penale nei confronti dell'autore dell'accesso e che gli adeguamenti necessari a superare le criticità sopra descritte, ad esclusione dell'utilizzo del protocollo di rete "http", si collocano all'interno di una più generale ripensamento delle caratteristiche del dossier sanitario utilizzato dalle aziende sanitarie della Regione Friuli Venezia Giulia ad opera della stessa e della società Insiel S.P.A. si ritiene di dover ingiungere all'ASUFC, ai sensi dell'art. 58, par. 2, lett. d),

del Regolamento, le seguenti misure correttive:

- adottare, entro il termine di giorni 15 dalla notifica del presente provvedimento, un protocollo di rete sicuro, quale il protocollo “https” (hypertext transfer protocol over secure socket layer), nell’ambito del sistema visore referti utilizzato per il dossier sanitario aziendale;

-adottare le misure indicate nel provvedimento approvato da questa Autorità in pari data anche nei confronti della Regione Friuli Venezia Giulia e di Insiel S.P.A. cui si rinvia integralmente.

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’ASUFC, 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, in relazione a 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 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 un reclamo (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 due pazienti che erano al contempo dipendenti dell’Azienda da parte di professionisti sanitari (2 nel caso della notifica del XX e 4 nel caso della notifica del XX e del reclamo ricevuto) che non erano coinvolti nel processo di cura delle stessa e nei confronti dei quali è stato avviato un procedimento disciplinare e presentata una denuncia alla Procura della repubblica di Udine (art. 83, par. 2, lett. a) e b) del Regolamento);

- nel caso di violazione del 20.1.2020 gli accessi si sono verificati in data 24.9.2020, mentre nel caso oggetto della notifica di violazione in data XX, su cui è stato presentato anche il reclamo, tra il 2018 e il 2020 (11 accessi) (art. 83, par. 2, lett. a) e b) del Regolamento);

- i predetti accessi sono stati possibili in quanto le misure attualmente 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 10 gennaio 2013 e successivamente con le linee guida del 2015 ((art. 83, par. 2, lett. d) del Regolamento);

- dagli elementi in atti emerge un limitato potere di intervento dell'Azienda in merito all'adozione di misure aggiuntive rispetto a quelle predefinite dalla Regione Friuli Venezia Giulia e dalla società Insiel S.P.A. sul sistema informativo adottato dall'ASUFC quale dossier sanitario (art. 83, par. 2, lett. g) del Regolamento);

- non è stata documentata in atti la richiesta da parte di ASUFC alla Regione Friuli Venezia Giulia e a Insiel s.p.a. di interventi correttivi al sistema informativo denominato visore referti al fine di rendere conforme lo stesso al Regolamento e alle misure indicate dal Garante nelle richiamate linee guida del 2015 (art. 83, par. 2, lett. g) 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 25.000 (venticinquemila) per il procedimento avviato a seguito della notifica di violazione del XX; e

- di 45.000 (quarantacinquemila) per il procedimento avviato a seguito della notifica di violazione del XX e del reclamo presentato dalla Sig.ra 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 universitaria Friuli Centrale, 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 universitaria Friuli Centrale, Codice fiscale/partita iva n. 02985660303, di pagare:

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;

la somma di euro 45.000 (quarantacinquemila) a titolo di sanzione amministrativa pecuniaria

per le violazioni rilevate con la notifica di violazione del XX e con il reclamo presentato dalla Sig.ra 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 le somme di euro 25.000 (venticinquemila) e di 45.000 (quarantacinquemila) 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;

• ai sensi dell'art. 58, par. 2, lett. d), del Regolamento, all'Azienda sanitaria universitaria Friuli Centrale entro il termine di giorni 30 dalla notifica del presente provvedimento, di adottare un protocollo di rete sicuro, quale il protocollo "https" (hypertext transfer protocol over secure socket layer), nell'ambito del sistema visore referti utilizzato per il dossier sanitario aziendale.

Al riguardo, si richiede all'Azienda di comunicare quali iniziative siano state intraprese al fine di dare attuazione a quanto sopra ingiunto nel presente provvedimento e di fornire comunque riscontro adeguatamente documentato, ai sensi dell'art. 157 del Codice, entro il termine di giorni 15 dalla scadenza del termine sopra indicato; l'eventuale mancato riscontro può comportare l'applicazione della sanzione amministrativa pecuniaria prevista dall'art. 83, paragrafo 5, del Regolamento

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, 26 maggio 2022

IL PRESIDENTE
Stanzione

IL RELATORE
Cerrina Feroni

IL VICE SEGRETARIO GENERALE
Filippi