



**GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI**

## **Provvedimento del 12 ottobre 2023 [9954220]**

VEDI ANCHE [Newsletter del 27 novembre 2023](#)

[doc. web n. 9954220]

### **Provvedimento del 12 ottobre 2023**

Registro dei provvedimenti  
n. 473 del 12 ottobre 2023

#### **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](http://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](http://www.gpdp.it), doc. web n.1098801;

Relatore il prof. Pasquale Stanzone;

#### **PREMESSO**

##### **1. Il reclamo e l'attività istruttoria**

L'Autorità ha ricevuto il reclamo della Sig.ra XX in cui ha lamentato ripetuti accessi, da parte di alcuni colleghi tra il 2019 e il 2020, al proprio dossier sanitario dell'Azienda socio sanitaria

territoriale di Lodi (di seguito Azienda).

Dalla documentazione allegata al reclamo e acquisita in atti risulta che la dott.ssa XX e la dott.ssa XX hanno effettuato i predetti accessi, rispettivamente, per “sapere su quali risorse umane poter contare per svolgere il nostro lavoro e curare i pazienti nel migliore dei modi” in quanto “il metodo più rapido era conoscere l’esito del tampone naso faringeo per il Covid -19” presente nel dossier sanitario dei colleghi e quindi anche della reclamante (cfr. nota dell’Azienda del XX, prot. n. XX allegata al reclamo).

Con specifico riferimento all’accesso effettuato da parte della dott.ssa XX, dalla documentazione allegata al reclamo e acquisita in atti, risulta che la stessa abbia acceduto al dossier della reclamante nell’ambito del “programma Telecovid Zcare” “con l’obiettivo di verificare la qualità e l’efficacia del servizio erogato anche mediante rielaborazione statistica delle caratteristiche della popolazione assistita, del percorso assistenziale e degli esiti del monitoraggio” (cfr. nota dell’Azienda del XX, prot. n. XX allegata al reclamo). Secondo quanto dichiarato dall’Azienda in atti “i consensi per tale progetto, non esclusa l’eventuale rielaborazione al fine di eventuale pubblicazione, venivano raccolti contestualmente all’arruolamento in Zcare e i nominativi dei pazienti inseriti in un data base da cui aveva seguito l’arruolamento”.

In merito alle operazioni di tracciamento degli accessi al dossier sanitario effettuate dalla predetta Azienda, la stessa, con nota del XX (prot. n. XX) allegata al reclamo e acquisita in atti, ha evidenziato che “gli accessi” di “tutte quelle figure sanitarie che nel periodo indicato (2019/2020) erano abilitate ad accedere alle unità operative in cui (...) (la reclamante) è transitata” “non vengono tracciati”.

In relazione a quanto segnalato l’Ufficio ha richiesto informazioni alla predetta Azienda con nota del XX (prot. n. XX), con riferimento alla quale quest’ultima ha risposto con la nota del XX (prot. n. XX) in cui è stato rappresentato, in particolare, che:

- “non è stato possibile trovare materialmente alcun consenso in forma cartacea prestato dalla signora XX” e che, considerato il contesto pandemico, è stato evidenziato che si è verificata “una commistione tra rapporti umani, di lavoro e di gestione della pandemia”;
- gli accessi al dossier sanitario della reclamante sono stati dettati da “modalità comportamentali improntate a bilanciare il più possibile la necessità di garantire l’attenzione alle esigenze personali manifestate dalla segnalante e nello stesso tempo la completa, coincidente dedizione nella gestione di un’emergenza mondiale, mai vissuta prima”;
- che i predetti accessi sono stati realizzati per lo svolgimento di “compiti istituzionali di interesse pubblico nel settore della sanità pubblica” di cui all’art. 9 del Regolamento;
- “si può affermare che ci sia stato un consenso implicito”.

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).

In particolare, nella predetta nota l’Ufficio ha evidenziato che la disciplina adottata per fronteggiare la pandemia da Covid-19 e, in particolare, l’art. 17-bis del d.l. n. 18/2020, richiamato anche dalla predetta Azienda, non ha e non avrebbe potuto derogare alla disciplina sulla protezione dei dati che, come è noto, si fonda su un Regolamento europeo, bensì ha previsto alcune semplificazioni nel trattamento e nella comunicazione dei dati personali fra diversi titolari del trattamento solo

qualora le stesse operazioni risultino indispensabili ai fini dello svolgimento delle attività connesse alla gestione della predetta emergenza sanitaria e comunque nel rispetto dei principi di cui all'articolo 5 del Regolamento, adottando misure appropriate a tutela dei diritti e delle libertà degli interessati.

Al riguardo, l'Ufficio ha inoltre rappresentato come l'Autorità abbia più volte evidenziato la necessità di valutare l'applicabilità della disciplina di cui al citato art. 17-bis del d.l. n. 18 del 2020 caso per caso, richiamando l'attenzione dei titolari del trattamento, anche operanti in ambito sanitario, sulla circostanza che non tutti i trattamenti e le comunicazioni di dati sulla salute possono essere ricondotte a tale disposizione (cfr. tra molti, nota del 9 giugno 2020, doc. web n. 9429175).

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

Con nota del XX (prot. n XX), l'Azienda ha inviato scritti difensivi, ribadendo quanto già rappresentato in atti e evidenziando, in particolare, che:

- il trattamento di cui all' "accesso ai dati della Sig.ra R.C. da parte dei colleghi" "ha in parte natura obbligatoria (con base giuridica nell'art.9, c.2, lett. h e i, ossia con riferimento alla natura delle funzioni pubbliche svolte e al periodo emergenziale nel quale si sono svolti i fatti) in parte facoltativa (per ciò che attiene nello specifico al riscontro alle richieste di attenzione e "cura" dell'interessata)";

- "Si ritiene dirimente il contesto emergenziale, non soltanto — si spera - quale possibile "attenuante", ma a livello giuridico per caratterizzare il peculiare ruolo che questa ASST svolge, e a maggior ragione ha svolto in quel periodo: ossia quello di Azienda sanitaria pubblica, unico punto di riferimento per l'intera Provincia - anche nei confronti della Regione Lombardia e dell'Agenzia per la Tutela della Salute di Milano — per l'erogazione dei servizi di salute ai cittadini, sia a livello ospedaliero che territoriale";

- "i fatti sono avvenuti in un Hospice ospedaliero, nel "primissimo" periodo della "primissima" "zona rossa";

- "Dai primi esiti dei tamponi il 50% degli OSS e il 75% degli infermieri risultava positivo e quindi le indicazioni erano di sospendere immediatamente dal servizio il personale infetto e di collocarlo in isolamento domiciliare, comunicando al Medico competente l'avvenuto isolamento". "Quindi molto spesso chiedevano aiuto ai loro colleghi presenti in Reparto, per conoscere l'esito dei loro tamponi prima di ottenerne il risultato sui fascicolo sanitario o dal Medico Competente". "Questo comportamento — oltre che dettato dalla concreta paura di aver contratto un morbo quasi completamente incurabile - era assolutamente necessario, sia per conoscere un 'eventuale positività per sé e per la loro famiglia ma anche per il desiderio di rimanere in collegamento operativo con l'equipe di lavoro, sia domiciliare che in hospice, che doveva essere gestita giorno dopo giorno per poter mantenere il servizio". "Lo scambio di notizie sui tamponi tra colleghi, assolutamente volontario, e anzi - come predetto - richiesto dagli operatori stessi, garantiva quindi sia la conoscenza dell'esito all'interessato sia la concreta possibilità di mantenere aperti i due servizi dell'Unità operativa e proprio grazie a questi sforzi e a questa disponibilità siamo stati l'Unica unità operativa che è restata sempre aperta nel Presidio di Casalpusterlengo per tutto il periodo della pandemia";

- "L'organizzazione dei turni ospedalieri in quel periodo di emergenza Covid non può

assolutamente essere assimilata all'ordinaria organizzazione dei turni da parte di un qualsiasi datore di lavoro, in un periodo qualsiasi"; "Pertanto, "sapere su quali risorse umane poter contare per svolgere il nostro lavoro e curare i pazienti nel migliore dei modi" significava tutelare l'interesse vitale di migliaia di persone";

- "Il trattamento dei dati da parte dell'Azienda era pertanto, da parte del datore di lavoro, assolutamente "necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento (art. 6, parr. I, lett. e) 2 e 3, e art.9, par.2), lett. g) del Regolamento (UE) 2016/679)".

- "Si richiama inoltre il Decreto Legge 7 marzo, n. 18, all'art. 17-bis (Disposizioni sul trattamento dei dati personali nel contesto emergenziale) che ha dato agli Enti, quali questa ASST, la possibilità di "effettuare trattamenti [...] anche relativi agli articoli 9 e IO del regolamento (UE) 20 16/679, che risultino necessari all'espletamento delle funzioni ad essi attribuite nell'ambito dell'emergenza determinata dal diffondersi del Covid-19)";

- "il consenso (della reclamante) è stato raccolto sull'applicativo di CCE Galileo il giorno 8 aprile 2020 dal dr. Inzoli" e viene riportata copia, sulla relazione stessa, dello stato del consenso (attivo) visibile sul DSE". "Tuttavia, è doveroso precisare che, nonostante ulteriori ricerche, non sono purtroppo stati trovati documenti in forma cartacea a supporto della prestazione del consenso";

- per il TeleCovid "La procedura era ben definita e prevedeva la firma del consenso in cartaceo e l'archiviazione separata dello stesso con consegna anche di saturimetro da parte della nostra struttura se non a disposizione del paziente. La scheda informativa che usavamo è disponibile in procedura e veniva firmata regolarmente", tuttavia "non è stata trovata copia cartacea in archivio", che potrebbe "essere stata erroneamente consegnata alla Paziente";

- "Non sfugge tuttavia a questa ASST che i trattamenti citati dovessero essere svolti "adottando misure appropriate a tutela dei diritti e delle libertà degli interessati" — quali il consenso, ove richiesto dalla norma, come nel caso del DSE" "Infatti non si palesano, nelle procedure aziendali di quel periodo, possibilità di deroghe rispetto alla necessità di richiedere il consenso";

- "E' lo svolgimento dei fatti, così come descritto, che conduce alla conclusione che: nel primo caso (TeleCovid) il consenso sia stato prestato oralmente (come attestato dalle dichiarazioni in atti) nel periodo in parola; sia nell'uno che nell'altro caso, la volontà della ricorrente sia comunque riconducibile a sue azioni positive inequivocabili essendo stato perso purtroppo, nel secondo caso, il documento cartaceo che la attestava"; "La ricorrente ha svolto anzi azioni positive inequivocabili sul fatto che i dati personali che la riguardavano fossero oggetto di trattamento: azioni quindi che possono lecitamente suffragare la validità del consenso";

- a seguito dei fatti in esame "sono state adottate e diffuse le seguenti comunicazioni di sensibilizzazione ai Responsabili di servizio e ai dipendenti:

- nota in data XX, ad oggetto: "Obbligo di acquisizione consenso all'attivazione del DSE (Galileo) "allegato n. 1 0 alla nota prot. n. XX del XX; nota: "Rispetto delle Linee Guida in materia di Dossier sanitario e delle disposizioni in materia di Consenso Privacy", prot. n. XX del XX, (allegato n.2 alla presente comunicazione) che è stata: o diffusa a tutti gli operatori aziendali (c.d, "trasmissione everyone") o inviata personalmente ai Responsabili di servizio aziendali (Direttori di SC e Coordinatori), via email, con richiesta per ciascun destinatario di conferma di lettura

- Si è stabilito inoltre di potenziare la formazione sull'argomento, inserendo per ogni modulo del corso privacy aziendale continuativo, già in essere, un evento formativo pomeridiano, finalizzato a far partecipare un numero ancora maggiore di operatori sanitari agli incontri formativi, come peraltro dagli stessi richiesto;

- È prevista un'attività di monitoraggio sulle autocertificazioni di accesso mediante estrazione elenco accessi e verifica a campione della reale necessità. Il personale medico è stato avvisato del fatto che tutti gli accessi sono tracciati e che potrebbero essere sottoposti a controlli";

- nelle note sopra evidenziate l'Azienda ha ricordato la necessità di assicurare il rispetto delle linee guida del Garante sul dossier sanitario del 4 giugno 2015.

Agli scritti difensivi è stata allegata una nota del Direttore dei sistemi informativi aziendali in cui è rappresentato che:

“vengono tracciate nel database dell'applicativo le azioni più significative eseguite dagli operatori”;

“Per la registrazione degli accessi occorre distinguere tra gli accessi eseguiti dal personale di reparto che è in carico il paziente dagli accessi ai dati storici o relativi a pazienti “non in carico”. Nel primo caso vengono tracciate solo le azioni di modifica o inserimento e non i semplici accessi, nel secondo caso viene registrato un set di informazioni concernenti riferimenti all'utente la motivazione per l'accesso data e ora di richiesta”;

“Gli accessi in consultazione per i pazienti non in carico sono registrati nel database e vengono sottoposti a verifiche periodiche di controllo”;

“Per rendere più regolare immediata la verifica è stata attivata un meccanismo di estrazione automatica dei log di accesso ed invio tramite mail alla direzione medica del polo ospedaliero e al direttore del SCD PSS”;

Ad ogni tentativo di accesso ai pazienti “non in carico” si attiva un banner di avvertimento con l'indicazione della non accessibilità dossier. Il contenuto del banner verrà ulteriormente modificato inserendo una nota relativa al fatto che l'accesso è tracciato e sottoposto a verifiche e che gli accessi non conformi alla finalità previste sono punibili ai sensi di legge”.

## **2. Esito dell'attività istruttoria.**

### **2.1. Quadro giuridico di riferimento.**

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

I dati inoltre devono essere raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità e comunque, “adeguati, pertinenti e limitati a quanto necessario alle finalità per le quali sono trattati” (principi della limitazione della finalità e di minimizzazione dei dati - art. 5, par. 1, lett. b) e c) del Regolamento)

Con particolare riferimento alla questione in esame, si evidenzia che i dati personali devono essere “trattati in modo lecito corretto e trasparente” (principio di “liceità, correttezza e trasparenza” e “in maniera da garantire un'adeguata sicurezza (...), compresa la protezione,

mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti (principio di “integrità e riservatezza”)” (art. 5, par. 1, lett. a) e f) del Regolamento).

Il Regolamento prevede poi che il titolare del trattamento metta in atto “misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio”, tenendo conto, tra l’altro, “della natura, dell’oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche” (art. 32 del Regolamento).

Con riferimento ai trattamenti oggetto del citato reclamo, il Garante ha adottato le “Linee guida in materia di Dossier sanitario - 4 giugno 2015” (Provvedimento del 4.6.2015, pubblicato in G.U. 164 del 17 luglio 2015, consultabile su [www.gpdp.it](http://www.gpdp.it) doc web n. 4084632), nelle quali sono state individuate un primo quadro di cautele, al fine di delineare specifiche garanzie e responsabilità, nonché misure e accorgimenti necessari ed opportuni da porre a garanzia dei cittadini, in relazione ai trattamenti di dati sanitari che li riguardano.

Ai sensi del Regolamento, qualora il trattamento sia necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero, che sono state indicate dalla predetta Azienda, lo stesso deve essere effettuato sulla base del diritto dell’Unione o degli Stati membri che deve prevedere misure appropriate e specifiche per tutelare i diritti e le libertà dell’interessato, in particolare il segreto professionale (art. 9, par. 2, lett. i)).

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

In particolare, con specifico riferimento alla disciplina adottata nel nostro Paese, ai sensi del richiamato art. 9, par. 2, lett. i) del Regolamento, per fronteggiare la predetta emergenza sanitaria, si rappresenta che l’art. 17-bis del d.l. n. 18/2020 non ha e non avrebbe potuto derogare la disciplina sulla protezione dei dati che, si evidenzia, si fonda su un Regolamento europeo 2016/679; detta disposizione legislativa nazionale ha previsto alcune semplificazioni nel trattamento e nella comunicazione dei dati personali fra diversi titolari del trattamento solo qualora le stesse risultino indispensabili ai fini dello svolgimento delle attività connesse alla gestione dell'emergenza sanitaria in atto e comunque nel rispetto dei principi di cui all'articolo 5 del Regolamento, adottando misure appropriate a tutela dei diritti e delle libertà degli interessati.

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

Al riguardo, come già rappresentato all’Azienda con la nota del XX, l’Autorità ha più volte evidenziato la necessità di valutare l’applicabilità della disciplina di cui al citato art. 17-bis del d.l. n. 18 del 2020, caso per caso, richiamando l’attenzione dei titolari del trattamento operanti anche in ambito sanitario sulla circostanza che non tutti i trattamenti di dati sulla salute possono essere ricondotte a tale disposizione (cfr. tra molti, nota del 9 giugno 2020, doc. web n. 9429175)

Con specifico riferimento al caso in esame, si richiama il provvedimento adottato da questa Autorità il 10 novembre 2022 con il quale è stata sanzionata un'Azienda sanitaria che aveva modificato le regole di visibilità del dossier sanitario nel periodo emergenziale consentendo, quindi, a tutto il personale sanitario di consultare i dossier sanitari di qualsiasi paziente fosse stato in cura presso l'Azienda a prescindere dalla circostanza che il soggetto che effettua l'accesso sia coinvolto nel percorso di cura dell'interessato e che quest'ultimo abbia manifestato il proprio consenso al trattamento dei dati effettuato attraverso il dossier (doc. web n. 9819792).

## **2.2. Il consenso dell'interessato**

Nelle richiamate Linee guida del 2015 il Garante ha specificato che il dossier sanitario, costituendo l'insieme dei dati personali generati da eventi clinici presenti e trascorsi riguardanti l'interessato, costituisce un trattamento di dati personali specifico e ulteriore rispetto a quello effettuato dal professionista sanitario con le informazioni acquisite in occasione della cura del singolo evento clinico. Come tale, quindi, si configura come un trattamento facoltativo. All'interessato, infatti, deve essere consentito di scegliere, in piena libertà, che le informazioni cliniche che lo riguardano siano trattate o meno in un dossier sanitario, garantendogli anche la possibilità che i dati sanitari restino disponibili solo al professionista sanitario che li ha redatti, senza la loro necessaria inclusione in tale strumento.

Ciò significa che qualora l'interessato non manifesti il suo consenso al trattamento dei dati personali mediante il dossier sanitario il professionista che lo prende in cura avrà a disposizione solo le informazioni rese in quel momento dallo stesso interessato (es. raccolta dell'anamnesi, delle informazioni relative all'esame della documentazione diagnostica prodotta) e quelle relative alle precedenti prestazioni erogate dallo stesso professionista. Analogamente, in tale circostanza, il personale sanitario di reparto/ambulatorio avrà accesso solo alle informazioni relative all'episodio per il quale si è rivolto presso quella struttura l'interessato e alle altre informazioni relative alle eventuali prestazioni sanitarie erogate in passato a quel soggetto da quel reparto/ambulatorio (c.d. accesso agli applicativi verticali dipartimentali).

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

Gli interventi normativi succedutisi durante il periodo di emergenza sanitaria non hanno derogato alle predette disposizioni, che sono rimaste pertanto pienamente efficaci. A ciò si aggiunga che nel periodo pandemico il legislatore è espressamente intervenuto nel settore degli strumenti sanitari digitali, semplificando la disciplina del Fascicolo sanitario elettronico; nell'ambito di tale intervento non è stato previsto, neanche limitatamente al periodo emergenziale, l'eliminazione del consenso alla consultazione del Fascicolo per finalità di cura della salute (art. 11, d.l. n. 34 del 2020).

Si precisa poi che nel caso in cui la condizione di liceità sia rappresentata, come nel caso di specie, dal consenso dell'interessato, questo deve essere prestato attraverso un atto positivo con il quale l'interessato manifesta una volontà libera, specifica, informata e inequivocabile relativa al trattamento dei dati personali che lo riguardano (Considerando 32, 42 e 43, artt. 5, 6, par. 1, lett. a) e 7 del Regolamento e Linee guida 5/2020 sul consenso ai sensi del Regolamento (UE) 2016/679, adottate dal Comitato europeo per la protezione dei dati personali il 4 maggio 2020).

Il consenso dell'interessato infatti per essere validamente prestato deve essere esplicito e specifico (art. 9, par. 2 lett. a) del Regolamento e par. 4 Linee guida 5/2020 sul consenso ai sensi del Regolamento (UE) 2016/679, adottate dal Comitato europeo per la protezione dei dati

personali il 4 maggio 2020).

Nel caso di specie pertanto non può ritenersi che il consenso dell'interessata sia desumibile da comportamenti concludenti ("consenso implicito" e "azioni positive inequivocabili"), essendo invece richiesta una espressione positiva e specifica che- allo stato degli atti- non risulta essere stato raccolto.

Una specifica ed esplicita manifestazione di volontà avrebbe dovuto essere acquisita, come del resto indicato dalla stessa Azienda, anche con riferimento al trattamento dei dati personali della reclamante effettuato nell'ambito del c.d. "programma Telecovid Zcare" con riferimento alla quale l'Azienda non ha prove dell'avvenuta acquisizione.

### **2.3. Utilizzo del dossier sanitario per finalità di organizzazione dei turni ospedalieri e valutazione della qualità dei servizi erogati nell'emergenza pandemica**

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.

Nelle citate Linee guida il Garante ha evidenziato infatti che il dossier sanitario costituisce uno strumento di ausilio per il personale sanitario consultabile da parte dello stesso nel processo di cura del paziente. In quanto tale, l'accesso al dossier deve essere limitato al personale sanitario che interviene in tale processo di cura e deve essere posto in essere esclusivamente da parte dei soggetti operanti in ambito sanitario, con esclusione di periti, compagnie di assicurazione, datori di lavoro, associazioni o organizzazioni scientifiche, organismi amministrativi anche operanti in ambito sanitario, nonché del personale medico nell'esercizio di attività medico-legale (ad es., visite per l'accertamento dell'idoneità lavorativa o per il rilascio di certificazioni necessarie al conferimento di permessi o abilitazioni) (cfr., punto 6)

Il Garante ha infatti più volte evidenziato che, attesa la natura facoltativa del dossier e l'incompletezza informativa (cfr. diritto di oscuramento) di tale strumento, lo stesso non può essere utilizzato per finalità riconducibili alla gestione di esigenze organizzative e amministrative del titolare anche nell'ipotesi in cui, come nel caso di specie, lo stesso assuma sia la veste di datore di lavoro che di autorità sanitaria che ha in cura l'interessata (cfr. Provvedimento del 26.5.2022, doc. web n. 9791909).

Si rappresenta inoltre che, in via generale, il datore di lavoro può trattare i dati personali dei lavoratori (art. 4, n. 1, del Regolamento), anche relativi a "categorie particolari", nella gestione del rapporto di lavoro, se il trattamento è necessario "per adempiere un obbligo legale al quale è soggetto il titolare del trattamento" (artt. 6, par. 1, lett. c), 9, parr. 2, lett. b) e 4; 88 del Regolamento) oppure quando sia "necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento" (art. 6, parr. 1, lett. e), 2 e 3, e art. 9, par. 2, lett. g), del Regolamento; artt. 2-ter e 2- sexies del Codice, nel testo antecedente alle modifiche apportate dal d.l. 8 ottobre 2021, n. 139).

Più nello specifico, il trattamento dei dati relativi alla salute dei dipendenti può essere legittimamente effettuato solo quando sia "necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o



degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato" (art. 9, parr. 2, lett. b), e 4, del Regolamento; v. pure, art. 88, del Regolamento e cons. 51-53).

In tale quadro si evidenzia che, in linea di continuità con quanto chiarito fin dalle "Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico" (prov. 14 giugno 2007, n. 23, doc. web n. 1417809) i cui principi sono da considerarsi tuttora validi, il datore di lavoro può trattare, nel rispetto dei principi di protezione dei dati e delle disposizioni di settore applicabili, dati personali relativi alla salute dei dipendenti solo per le finalità e alle condizioni normativamente previste ovvero su specifica segnalazione del medico competente, unico soggetto legittimato per legge a svolgere compiti di sorveglianza sanitaria, nel rispetto degli specifici limiti e presupposti stabiliti dalla disciplina in materia di tutela della salute e della sicurezza nei luoghi di lavoro (d.lgs. 9 aprile 2008, n. 81). Tale separazione dei ruoli trova, peraltro, conferma nell'impianto del Regolamento, che considera in via autonoma i trattamenti necessari per le finalità di "medicina del lavoro" (art. 9, parr. 2, lett. h), e 3 del Regolamento), nel quale ambito è riconducibile la funzione del medico competente prevista dall'ordinamento nazionale, rispetto a quelli posti in essere dal datore di lavoro per assolvere i propri obblighi "in materia di diritto del lavoro", ivi compresi quelli stabiliti dalle norme in materia di "salute e sicurezza sul lavoro" (cfr. combinato disposto artt. 9, par. 2, lett. b), e 88 del Regolamento; sul ruolo del datore di lavoro e del medico competente, anche alla luce del quadro normativo emergenziale, documento di indirizzo del 14 maggio 2021, doc. web n. 9585367).

Anche nell'eccezionale situazione emergenziale, tenuto conto delle problematiche derivanti dalle pressanti esigenze di tutela della sicurezza dei luoghi di lavoro e dai connessi trattamenti di dati personali, i datori di lavoro devono operare, quindi, nell'ambito e nei limiti previsti dalla disciplina applicabile, che costituisce la base giuridica dei relativi trattamenti, evitando di porre in essere iniziative non previste dalla legge - incluse le specifiche disposizioni introdotte nel periodo emergenziale e nei protocolli per la sicurezza dei luoghi di lavoro - con possibili effetti lesivi per gli interessati nel contesto lavorativo e professionale. In tale quadro, in assenza di espresse previsioni normative, non è pertanto consentito al datore di lavoro raccogliere e trattare, direttamente dagli interessati o, come nel caso di specie, da altre fonti, dati personali anche relative allo stato di salute del lavoratore (cfr., tali principi sono stati ribaditi in numerosi provvedimenti adottati nel contesto pandemico, fin dalle FAQ in materia di "Trattamento dei dati nel contesto lavorativo pubblico e privato nell'ambito dell'emergenza sanitaria", doc. web n. 9337010 e più di recente con provvedimento 26 maggio 2022 n. 195 doc. web n. 9788986, ancorché in relazione a vicende diverse da quella oggetto del presente provvedimento).

Nessuna disposizione emergenziale ha invece previsto la possibilità di conoscere tali informazioni attraverso il dossier sanitario che, come già evidenziato, è uno strumento informativo facoltativo e per sua natura incompleto che può essere utilizzato esclusivamente per finalità di cura dell'interessato.

A ciò si aggiunga che, secondo quanto dichiarato in atti, la reclamante aveva comunque comunicato il suo stato di positività al coordinatore infermieristico proprio al fine di agevolare l'organizzazione del lavoro in reparto, circostanza che mette in luce la non pertinenza delle argomentazioni difensive volte a giustificare il predetto accesso al dossier, con le modalità sopra descritte, per le asserite finalità di gestione e organizzazione dei turni di lavoro. L'utilizzo del dossier sanitario effettuato dall'Azienda nel periodo pandemico ha, invece, consentito l'accesso al dossier della reclamante anche per finalità diverse da quelle di cura ovvero per "sapere su quali risorse umane poter contare per svolgere il nostro lavoro e curare i pazienti nel migliore dei modi". Tale scelta, secondo quanto rappresentato in atti, sarebbe stata effettuata considerando che l'accesso al dossier sanitario è stato "il metodo più rapido per conoscere l'esito del TNF" (tampone naso faringeo) per il Covid -19 presente nel dossier sanitario dei colleghi e quindi anche della reclamante (cfr. note citate).

Dalle dichiarazioni rese in atti da parte degli autori degli accessi al dossier della reclamante oggetto di contestazione, che sono state riportate dall'Azienda, risulta accertato che gli stessi non sono avvenuti per finalità di cura, bensì per finalità organizzative/amministrative di gestione dei turni ospedalieri e di valutazione dei servizi erogati ai pazienti affetti da Covid-19.

Sebbene l'Azienda abbia agito per l'esigenza di organizzare con celerità i turni ospedalieri del personale sanitario, anche in considerazione dell'eventuale tasso di assenza per malattia dei dipendenti e che tale attività è stata caratterizzata da una particolare complessità attesa la delicata situazione legata al contesto pandemico, tuttavia avrebbe dovuto trattare i dati della reclamante nel rispetto della richiamata normativa di settore che ne costituisce la base giuridica e ne stabilisce limiti e presupposti.

Ciò anche nel richiamato rispetto del principio di limitazione della finalità secondo cui il dossier sanitario può essere utilizzato solo dal personale sanitario che ha in cura l'interessato, essendo inteso come strumento per agevolare il percorso di cura di quest'ultimo, e non invece per le richiamate esigenze organizzative -illustrate in atti- perseguibili con i tipici strumenti che il datore di lavoro possiede per la gestione del personale e della relativa presenza in servizio. Emerge infatti dalle dichiarazioni della reclamante e dell'Azienda che la sig.ra XX non era stata presa in carico dalla struttura che ha effettuato gli accessi; ciò risulta del resto evidente in quanto gli autori degli accessi, non avendo in carico la reclamante come paziente, hanno dovuto effettuare una autodichiarazione per poter consultare il suo dossier.

Tra l'altro, la facoltatività del dossier sanitario e l'incompletezza informativa, dettata dalla possibilità che l'interessato possa esercitare il diritto di oscuramento su alcune delle informazioni raccolte attraverso il dossier (ivi compresi i referti Covid-19) e dalla circostanza che in tale strumento non sono presenti i referti emessi da altre strutture sanitarie, rendono il dossier un mezzo non adeguato per svolgere in modo efficace le attività organizzative e amministrative che l'Azienda può, invece, compiere nel rispetto dello specifico e diverso quadro normativo di settore.

Si rileva pertanto che nel caso di specie l'utilizzo del dossier sanitario per gestire l'organizzazione dei turni del personale sanitario non solo non rientra tra le finalità proprie del dossier sanitario, ma si rivela una modalità anche inefficace in quanto tale strumento non solo è vincolato, come detto, al consenso dell'interessato, ma è anche, per sua natura, incompleto, potendo l'interessato esercitare il diritto di oscuramento su dati e documenti ivi compresi gli esiti dei test Covid – 1, ovvero non contenendo informazioni sanitarie relative a prestazioni sanitarie erogate da altre strutture sanitarie.

A ciò si aggiunga che, come evidenziato più volte dal Garante anche nelle citate linee guida e in altri provvedimenti (cfr. provvedimento del 21 aprile 2021, n- 155), il titolare del trattamento deve individuare, in relazione alle diverse funzioni a cui è adibito il personale, soluzioni tecniche organizzative che consentano ai soggetti che svolgono compiti organizzativi e amministrativi, come quello della gestione dei turni ospedalieri o di valutazione dell'assistenza erogata, di accedere, nei limiti delle attribuzioni previste per legge, ad una base informativa più completa rispetto a quella presente nel dossier sanitario aziendale.

Si rileva inoltre che lo svolgimento di compiti di interesse pubblico nel settore della sanità pubblica, richiamato dall'Azienda, non può considerarsi legittimante i predetti trattamenti dei dati sulla salute della reclamante attraverso il dossier sanitario (costituito tra l'altro senza il previsto consenso), in quanto in contrasto con le disposizioni in materia di protezione dei dati personali che sono state adottate nel periodo pandemico e che prevedono che il trattamento debba avvenire nel rispetto dei principi generali del trattamento tra i quali si configurano quelli di liceità, trasparenza, correttezza, limitazione delle finalità e minimizzazione dei dati (art. 5, par. 1, lett. a), b) e c) del Regolamento).

### **2.3 Sistemi di tracciamento degli accessi e delle operazioni effettuate e sistemi di alert**

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)".

Nelle medesime Linee guida questa Autorità ha evidenziato espressamente che, nella realizzazione del dossier sanitario, il titolare deve adottare sistemi di controllo delle operazioni effettuate sul dossier, mediante procedure che prevedano la registrazione automatica in appositi file di log degli accessi e delle operazioni compiute. In particolare, i file di log devono registrare per ogni operazione di accesso al dossier effettuata, almeno le seguenti informazioni: il codice identificativo del soggetto autorizzato che ha posto in essere l'operazione di accesso; la data e l'ora di esecuzione; il codice della postazione di lavoro utilizzata; l'identificativo del paziente il cui dossier è interessato dall'operazione di accesso da parte dell'incaricato e la tipologia dell'operazione compiuta sui dati.

In ragione della particolare delicatezza del trattamento dei dati personali effettuato mediante il dossier è necessario che siano tracciate anche le operazioni di semplice consultazione (inquiry).

La configurazione del dossier sanitario effettuata dall'Azienda nel contesto emergenziale non ha invece previsto, per espresso riconoscimento della stessa nella documentazione in atti, che venissero tracciati gli accessi al dossier sanitario da parte di "tutte quelle figure sanitarie che nel periodo indicato (2019/2020) erano abilitate ad accedere alle unità operative in cui (...) (la reclamante) è transitata" (nota del XX - prot. n. XX).

Al riguardo, si rileva quindi che, contrariamente a quanto indicato nelle predette Linee guida, dalla documentazione allegata agli scritti difensivi, allo stato, non è prevista la registrazione di tutte le operazioni effettuate sul dossier sanitario, nonché un sistema di controllo per tutte le tipologie di accessi al dossier.

### **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.

L'utilizzo del dossier sanitario della reclamante ha comportato, come sopra evidenziato, un trattamento illecito di dati in quanto lo stesso è stato effettuato per finalità diverse da quelle di cura perseguibili attraverso il dossier sanitario, nonché da parte di soggetti che non erano coinvolti nel percorso di cura della reclamante e, quindi, in violazione dei principi di liceità e limitazione delle finalità (art. 5, par. 1, lett. a) e b) del Regolamento).

Oltre che in violazione del principio di liceità, tali trattamenti sono avvenuti anche in violazione dei principi di trasparenza, correttezza e di minimizzazione dei dati in quanto, ai sensi del quadro normativo di settore, i responsabili dell'organizzazione dei turni ospedalieri e delle attività di verifica sulla qualità delle cure erogate, seppur professionisti sanitari, non avrebbero dovuto

accedere alla documentazione sanitaria dei colleghi nel perseguimento di tali specifiche e distinte finalità, bensì alle sole informazioni relative all'assenza dal servizio dei colleghi strettamente necessarie all'assolvimento dei loro compiti, senza conoscere i dettagli clinici e diagnostici correlati (art. 5, par. 1, lett. a) e c) del Regolamento).

Si rileva inoltre che una specifica ed esplicita manifestazione di volontà avrebbe dovuto essere acquisita, come del resto indicato dalla predetta Azienda, anche con riferimento al trattamento dei dati personali della reclamante effettuato nell'ambito del c.d. "programma TeleCovid Zcare" che non risulta essere invece stato acquisito.

In considerazione di quanto dichiarato in atti, non risulta neanche che l'Azienda abbia previsto 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 (art. 5, par. 1, lett. f), del Regolamento).

Gli elementi sopra descritti hanno reso possibile che colleghi della reclamante accedessero al suo dossier sanitario per finalità diverse da quelle di cura e nello specifico correlate all'organizzazione dei turni ospedalieri e alla valutazione della qualità delle cure erogate con riferimento al Covid-19, in assenza del consenso esplicito e specifico dell'interessata, e, quindi, di alcun presupposto giuridico.

In tale quadro, considerando quanto sopra rilevato e in particolare, che non sono registrate tutte le operazioni eseguite sul dossier ma solo "le più significative" e che sono sottoposti a monitoraggio solo gli accessi ai pazienti c.d. "non in carico", si ritiene di dover ingiungere alla predetta Azienda, ai sensi dell'art. 58, par. 2, lett. d), del Regolamento, le seguenti misure correttive, da adottarsi entro 90 giorni dall'adozione del presente provvedimento, mediante la messa in opera per tutte le tipologie di accessi al dossier:

di sistemi per il controllo 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;

di sistemi di controllo delle operazioni effettuate sul dossier, mediante procedure che prevedano la registrazione automatica in appositi file di log di tutti gli accessi e delle operazioni compiute (ivi compresa anche la semplice consultazione (inquiry)), con almeno le seguenti informazioni: il codice identificativo del soggetto autorizzato che ha posto in essere l'operazione di accesso; la data e l'ora di esecuzione; il codice della postazione di lavoro utilizzata; l'identificativo del paziente il cui dossier è interessato dall'operazione di accesso da parte dell'incaricato e la tipologia dell'operazione compiuta sui dati.

#### **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. 1, lett. a) lett. a), b), c) e f), 9, e 32 del Regolamento, causata dalla condotta dell'Azienda sociosanitaria territoriale di Lodi, è soggetta all'applicazione della sanzione amministrativa pecuniaria ai sensi dell'art. 83, par.4 e 5, del Regolamento.

Si consideri che il Garante, ai sensi ai sensi degli artt. 58, par. 2, lett. i) e 83 del Regolamento, nonché dell'art. 166 del Codice, ha il potere di "infliggere una sanzione amministrativa pecuniaria ai sensi dell'articolo 83, in aggiunta alle [altre] misure [correttive] di cui al presente paragrafo, o in

luogo di tali misure, in funzione delle circostanze di ogni singolo caso” e, in tale quadro, “il Collegio [del Garante] adotta l’ordinanza ingiunzione, con la quale dispone altresì in ordine all’applicazione della sanzione amministrativa accessoria della sua pubblicazione, per intero o per estratto, sul sito web del Garante ai sensi dell’articolo 166, comma 7, del Codice” (art. 16, comma 1, del Regolamento del Garante n. 1/2019).

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

- l’Autorità ha preso conoscenza dell’evento a seguito di un reclamo (art. 83, par. 2, lett. h) del Regolamento);
- gli accessi illeciti hanno riguardato il dossier sanitario di una paziente che era al contempo dipendente dell’Azienda da parte di professionisti sanitari suoi colleghi che non erano coinvolti nel processo di cura delle stessa (art. 83, par. 2, lett. a) e b) del Regolamento);
- la configurazione del dossier sanitario effettuata dall’Azienda ha di fatto consentito ai predetti professionisti sanitari di accedere al dossier sanitario di una paziente loro collega senza esserne legittimati e senza che fossero previsti alert o sistemi di monitoraggio colti a segnalare tali condotte illecite (art. 83, par. 2, lett. d) del Regolamento);
- il trattamento è avvenuto nel periodo pandemico che ha visto eccezionalmente coinvolta la predetta Azienda (art. 83, par. 2, lett. a) del Regolamento);
- il titolare ha collaborato nel corso dell’istruttoria provvedendo ad adottare nuove procedure e misure organizzative da seguire rivolte ai propri dipendenti, nel rispetto del quadro normativo applicabile e in coerenza con le indicazioni del Garante per i trattamenti in ambito sanitario e in ambito lavorativo (art. 83, par. 2, lett. 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), b), c) e f), 9, e 32 del Regolamento nella misura di 40.000 (quarantamila) per il procedimento avviato a seguito del reclamo quale sanzione amministrativa pecuniaria ritenuta, ai sensi dell’art. 83, par. 1, del Regolamento, effettive, proporzionate e dissuasive.

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

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

### **TUTTO CIÒ PREMESSO IL GARANTE**

dichiara l’illiceità del trattamento di dati personali effettuato, in entrambi i procedimenti descritti, dall’Azienda sociosanitaria territoriale di Lodi, per la violazione degli art. 5, par. 1, lett. a), b), c) e f), 9, 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 socio sanitaria territoriale di Lodi CF 09322180960, di pagare la somma di euro 40.000 (quarantamila) a titolo di sanzione amministrativa pecuniaria per le predette violazioni secondo le modalità indicate in allegato, entro 30 giorni dalla notifica in motivazione; si rappresenta che il contravventore, ai sensi dell'art. 166, comma 8, del Codice, ha facoltà di definire la controversia mediante pagamento, entro il termine di 30 giorni, di un importo pari alla metà delle sanzioni comminate.

## **INGIUNGE**

alla predetta Azienda:

1. in caso di mancata definizione della controversia ai sensi dell'art. 166, comma 8, del Codice, di pagare le somme di euro 40.000 (quarantamila) secondo le modalità indicate in allegato, entro 30 giorni dalla notificazione del presente provvedimento, pena l'adozione dei conseguenti atti esecutivi a norma dall'art. 27 della legge n. 689/1981;

2. ai sensi dell'art. 58, par. 2, lett. d), del Regolamento, entro il termine di giorni 90 dalla notifica del presente provvedimento, di mettere in opera per tutte le tipologie di accessi al dossier:

a. sistemi per il controllo 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;

b. sistemi di controllo delle operazioni effettuate sul dossier, mediante procedure che prevedano la registrazione automatica in appositi file di log di tutti gli accessi e delle operazioni compiute (ivi compresa anche la semplice consultazione (inquiry)) , con almeno le seguenti informazioni: il codice identificativo del soggetto autorizzato che ha posto in essere l'operazione di accesso; la data e l'ora di esecuzione; il codice della postazione di lavoro utilizzata; l'identificativo del paziente il cui dossier è interessato dall'operazione di accesso da parte dell'incaricato e la tipologia dell'operazione compiuta sui dati.

In merito al precedente punto 2, si richiede alla predetta azienda di comunicare quali iniziative siano state intraprese al fine di dare attuazione a quanto sopra ingiunto con il presente provvedimento e di fornire comunque riscontro adeguatamente documentato, ai sensi dell'art. 157 del Codice, entro il termine di giorni 20 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 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, 12 ottobre 2023*

IL PRESIDENTE  
Stanziome

IL RELATORE  
Stanzione

IL SEGRETARIO GENERALE  
Mattei