



**GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI**

## **Provvedimento del 2 dicembre 2021 [9732497]**

[doc. web n. 9732497]

**Provvedimento del 2 dicembre 2021**

Registro dei provvedimenti  
n. 421 del 2 dicembre 2021

### **IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI**

NELLA riunione odierna, alla quale hanno preso parte il prof. Pasquale Stanzione, presidente, la prof.ssa Ginevra Cerrina Feroni, vicepresidente, il dott. Agostino Ghiglia e l'avv. Guido Scorza, componenti e il cons. Fabio Mattei, segretario generale;

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

VISTO il d.lgs. 30 giugno 2003, n. 196 recante "Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE (di seguito "Codice");

VISTO il Regolamento n. 1/2019 concernente le procedure interne aventi rilevanza esterna, finalizzate allo svolgimento dei compiti e all'esercizio dei poteri demandati al Garante per la protezione dei dati personali, approvato con deliberazione del n. 98 del 4/4/2019, pubblicato in G.U. n. 106 dell'8/5/2019 e in [www.gpdp.it](http://www.gpdp.it), doc. web n. 9107633 (di seguito "Regolamento del Garante n. 1/2019");

VISTE le Linee guida in materia di Dossier sanitario - 4 giugno 2015" (pubblicato in G.U. 164 del 17 luglio 2015, doc web n. 4084632);

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 Stanzione;

### **PREMESSO**

#### **1. La violazione dei dati personali.**

Nel mese di ottobre del 2020, l'Azienda Ospedaliero Universitaria Integrata di Verona (di seguito

Azienda) ha inviato all'Autorità una comunicazione relativa a una violazione di dati personali ai sensi dell'art. 33 del Regolamento, in relazione alla presenza -nel dossier sanitario aziendale di una interessata- di documentazione sanitaria riferita ad altro soggetto (comunicazione del 29.10.2020).

Nella predetta comunicazione, l'Azienda ha affermato che:

- “Il titolare del trattamento è venuto a conoscenza della violazione in seguito a lettera di diffida e richiesta danni da parte del legale della paziente A”, la quale, “accedendo al proprio dossier sanitario elettronico (DSE) per controllare l'esito del proprio tampone Covid-19, veniva a conoscenza di un verbale del Pronto Soccorso con i suoi dati anagrafici relativo ad un evento occorso in data 02/09/2020 attribuibile ad altra paziente”;
- “In data 02/09/2020 la paziente B, (...), accedeva al Pronto Soccorso (PS) dell'Ospedale di Borgo Roma e in fase di accettazione veniva registrata nell'applicativo First Aid come se fosse la paziente A, sua omonima presente in anagrafica, (...). Pertanto, il verbale di PS del 02/09/2020 riportava i dati anagrafici della paziente A (...), mai recatasi al PS, anziché quelli della paziente B (...), ma i dati anamnestici, gli esiti degli esami effettuati, il diario clinico, la diagnosi di gesto lesivo causata da XX erano relativi alla paziente B”;
- “Giovedì 03/09/2020 la XX, presso cui la paziente B era stata ricoverata dopo l'accesso al PS, si accorgeva dell'errata accettazione e verificava che nell'applicativo Opera risultavano due persone con lo stesso nome e cognome, con codice paziente simile (unica differenza l'ultima lettera, ...) e dati anagrafici diversi. In tale frangente, la Psichiatria verificava che il medesimo errore era avvenuto anche in occasione di un precedente ricovero della paziente B”;
- “Martedì 08/09/2020 (...) le attività di correzione erano terminate”;
- “In data 02/10/2020 il legale della paziente A mediante lettera di diffida e richiesta danni trasmessa via PEC rappresentava che in data 18/09/2020 la sua assistita aveva avuto accesso al proprio DSE, riscontrando la presenza di un verbale di PS datato 02/09/2020 a lei non riferibile”;
- ciò stante a seguito di verifiche “emergeva che sull'applicativo First Aid (che gestisce il PS), grazie agli interventi tecnici effettuati all'inizio di settembre, i verbali di PS risultavano attribuiti alla paziente corretta (paziente B) ma tali modifiche non erano state recepite sull'applicativo GeCOs (che gestisce il DSE) perché avrebbero richiesto un intervento manuale da parte degli operatori del Servizio Sistemi Informativi che per errore umano non è stato effettuato. Tale operazione manuale veniva effettuata in data 07/10/2020 e quindi da quel momento i verbali di PS della paziente B non erano più presenti sul DSE della paziente A”;
- “In data 14/10/2020 una dirigente della DMO, di propria iniziativa e senza condivisione con il titolare, il referente dell'ufficio privacy aziendale e l'RPD, comunicava via posta elettronica ordinaria al legale della paziente A di aver interessato della sua richiesta il Servizio Sistemi Informativi il quale aveva provveduto alla rimozione del verbale, precisando inutilmente che esso era stato erroneamente ricondotto alla sua assistita "per omonimia”;
- “In data 21/10/2020 il legale della paziente A inviava via pec nuova missiva informando che risultava presente nel DSE della sua assistita anche un referto relativo a un tampone Covid-19 effettuato il 02/09/2020 da un'altra persona (la paziente B), e chiedendo la somma di euro 2.500/00 a titolo di risarcimento danni”;
- “L'incidente e conseguente data breach si sono verificati per un errore umano imputabile

dapprima all'operatore addetto all'accettazione in PS, e poi all'operatore del Servizio Sistemi Informativi che non ha proceduto alla rimozione manuale dei documenti riferiti alla paziente B dal dossier della paziente A”;

- “a seguito della lettera del legale della paziente A si è provveduto a cancellare dal DSE di quest'ultima sia il verbale di PS segnalato dal legale sia quello di cui è stata riscontrata la presenza in fase istruttoria, nonché il referto relativo al tampone COVID-19 effettuato in PS dalla paziente B in data 02/09/2020, anch'esso erroneamente pubblicato sul DSE della paziente A, sicché ora non sono lì più visibili”;

- “È stata poi fatta un'ulteriore verifica da cui è emerso che i verbali di PS in questione, a seguito della loro cancellazione sul DSE della paziente A, non risultano più indicizzati nemmeno sul suo FSE. Ovviamente i due verbali di PS sono stati anche ripubblicati sul DSE della paziente B”;

- “In occasione di un precedente caso di errata identificazione del paziente, anch'esso fatto oggetto di notifica in data 14/09/2018 a codesta spett.le Autorità, la quale di recente ha comunicato l'archiviazione del procedimento sanzionatorio avviato nei confronti dell'Azienda (rif. Vs. nota prot. n. 0023190 del 24/06/2020), si faceva presente l'adozione delle seguenti misure organizzative, dirette appunto a scongiurare possibili casi di "scambio di persona": (...)sono state fornite istruzioni anche operative, affinché il trattamento dei dati di salute dei pazienti fosse ispirato al massimo rispetto della loro dignità e riservatezza; (...) sono state trasmesse due Istruzioni Aziendali Gestionali dedicate alla corretta identificazione del paziente, che, se rispettate (si fa riferimento, in part., al punto 3 della IAG 39 – Fase di accettazione del Paziente in Pronto Soccorso, che prevede il riconoscimento certo del paziente in fase di triage, ma anche alla IAG 38, che descrive la procedura da attivare a livello aziendale per porre rimedio a possibili errori di identificazione dei pazienti), avrebbero impedito il verificarsi dell'episodio in questione; (...) è stata nuovamente trasmessa a tutti i Direttori delle Unità Operative aziendali la citata nota del 2015, con le allegate istruzioni di cui sopra, con l'invito a sensibilizzare i propri collaboratori al massimo rispetto delle medesime anche al fine di ridurre il più possibile i casi di scambio di persona, "con conseguente impropria divulgazione di dati sensibili appartenenti a persona diversa" (come appunto nel caso che ci occupa)”;

- “Sarà poi integrata la procedura descritta nella sopra citata IAG 38 nel senso di meglio dettagliare le azioni da intraprendere per essere certi che le modifiche eseguite dal Servizio Sistemi Informativi su segnalazione della DMO siano andate a buon fine, attivando doppi controlli per verificare che dell'errata identificazione del paziente non resti traccia, nemmeno in ipotesi sul profilo del terzo, al fine di impedire che, per varie ragioni, non ultima una possibile omonimia, questi possa vedere pubblicati sul proprio dossier documenti a lui non riferiti. Sarà proposta all'UOC Miglioramento Qualità l'attivazione di audit sul rispetto della procedura IAG 39 sulla corretta identificazione dei pazienti da parte delle Unità Operative più coinvolte”;

## **2. L'attività istruttoria.**

In relazione alla predetta comunicazione di violazioni, l'Ufficio, con atto n. 46094 del 2 dicembre 2020, con riferimento alle specifiche situazioni di illiceità in esso richiamate, 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, paragrafo 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, nel predetto atto, ha ritenuto che la violazione di dati personali notificata al

Garante ai sensi dell'art. 33 del Regolamento, abbia rilevato la sussistenza di elementi idonei a configurare da parte dell'Azienda le violazioni di cui agli artt. 5. par. 2, lett. a) e f), 9 e 32 del Regolamento, rappresentando 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 e dalla perdita, dalla distruzione o dal danno accidentali (principio di “integrità e riservatezza”)” (art. 5, par. 1, lett. a) e f) del Regolamento);
- il Regolamento prevede 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” e che “nel valutare l’adeguato livello di sicurezza si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall’accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati” (art. 32 del Regolamento);
- la disciplina in materia di protezione dei dati personali prevede –in ambito sanitario che le informazioni sullo stato di salute possano essere comunicate solo all’interessato e possano essere comunicate a terzi solo sulla base di un idoneo presupposto giuridico o su indicazione dell’interessato stesso previa delega scritta di quest’ultimo (art. 9 Regolamento e art. 83 d.lgs. n. 196 del 30 giugno 2003 (Codice in materia di protezione dei dati personali – di seguito, il “Codice”) in combinato disposto con l’art. 22, comma 11, d.lgs. 10 agosto 2018, n. 101; cfr. anche provv. generale del 9 novembre 2005, consultabile in [www.gpdt.it](http://www.gpdt.it), doc. web n. 1191411, ritenuto compatibile con il suddetto Regolamento e con le disposizioni del decreto n. 101/2018; cfr. art. 22, comma 4, del citato d.lgs. n. 101/2018);
- con riferimento ai trattamenti oggetto di notificazione, 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), 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 ha evidenziato la necessità di garantire la certezza circa l’origine del dato trattato, la sua esattezza, integrità e non modificabilità, nonché la disponibilità dello stesso (punto 7, allegato A alle Linee guida);
- la predetta Azienda è stata già destinataria di un provvedimento correttivo sanzionatorio con riferimento all’illiceità del trattamento di dati personali effettuato attraverso il dossier sanitario per violazione dell’art. 5 par. 1, lett. f) del Regolamento (provv. del 23 gennaio 2020, n.18);
- con specifico riferimento ad altro caso di omonimia, l’Azienda, nell’ambito di un ulteriore procedimento istruttorio, aveva già fornito assicurazioni in merito all’adozione di idonee misure organizzative, dirette “a scongiurare possibili casi di "scambio di persona"”.

Con nota del 31 dicembre 2021 (prot. n. 71723), l’Azienda ha fatto pervenire le proprie memorie difensive, in cui, in sintesi, è stato rappresentato che:

“Nonostante la situazione emergenziale che AOUIVR si è trovata ad affrontare nel corso dell’anno e tenuto altresì conto della complessità organizzativa dell’Azienda, l’attenzione al

trattamento dei dati personali dei pazienti e del personale aziendale è stata sempre tenuta nella massima considerazione e sono state attuate azioni proattive volte a prevenire situazioni che potessero mettere a rischio i dati personali degli interessati”;

“Giova premettere che la violazione contestata è da ascrivere, come dimostrato nel prosieguo, non a mancanze di natura organizzativa del titolare, ma a una serie concatenata e del tutto eccezionale di errori umani non intenzionali degli operatori coinvolti, nonostante AOUIVR avesse da tempo adottato sia una procedura per la corretta identificazione del paziente, sia una istruzione operativa sul corretto caricamento dei dati del paziente nell'applicativo in uso al Pronto Soccorso, atte ad impedire il verificarsi di casi di scambi di persona”;

“le misure tecniche e organizzative adottate dall'Azienda sono risultate adeguate al tipo di rischio legato al trattamento in questione, e che il personale coinvolto ha disatteso le procedure e istruzioni ricevute anche se peraltro convenientemente formato e informato al riguardo”;

“neppure un altro caso di errata identificazione di un paziente notificato a codesta Autorità nel settembre del 2018 ha rilevanti punti di contatto con quello in esame, poiché nel caso del 2018 non vi fu alcuna erronea identificazione del paziente in sede di accettazione, ma unicamente la consegna di un promemoria cartaceo a un paziente diverso dall'interessato per errore umano non intenzionale dell'operatrice, obnubilata da una discussione occorsa poco prima con il paziente medesimo” “l'episodio notificato il 28 ottobre 2020 deve ritenersi unico e del tutto eccezionale”;

“In considerazione della sua condizione di paziente fragile e complessa, oltre che per l'assenza di rischio reputato elevato per i suoi diritti, si conferma che AOUIVR non ha ritenuto opportuno di procedere alla comunicazione dell'avvenuta violazione alla paziente per evitare il rischio di peggiorare il suo stato di salute psichico; per quanto concerne la durata della violazione, la stessa ha esaurito i propri effetti nel momento stesso in cui è stata rilevata dalla paziente che ha rinvenuto nel suo dossier documenti sanitari a lei non riferibili; in ogni caso, tale durata può essere calcolata nella misura di un mese circa, che è il periodo intercorso fra il giorno (18 settembre 2020) in cui la paziente ha fatto accesso al proprio dossier trovandovi il verbale di Pronto Soccorso a lei non riferito e il giorno (26 ottobre 2020) in cui è stato deprecato l'altro documento visionato dalla paziente medesima, e riferito al tampone per ricerca del virus Sars-Cov 2 che la paziente omonima ha eseguito nella giornata del 2 settembre 2020”;

“nella catena che ha contrassegnato questo sfortunato episodio:

a. il primo errore è stato commesso dalla infermiera del triage del Pronto Soccorso dell'Ospedale di Borgo Roma che, nel registrare la paziente in fase di accettazione, non ha osservato puntualmente la procedura aziendale per la corretta identificazione dei pazienti nella fase di accettazione in Pronto Soccorso (Procedura IAG 39, in part. punto 3, Allegato 2) (...).

b. il secondo errore è stato commesso dagli operatori dell'UOS Servizio Sistemi Informativi chiamati a rimediare all'errore commesso in sede di triage sulla scorta di quanto previsto dalla sopra citata procedura IAG 38. (...). Secondo procedura, il Servizio Sistemi Informativi, effettuate le correzioni di competenza, tra cui la cancellazione dei documenti indebitamente pubblicati sul dossier relativo al paziente non destinatario delle prestazioni cui tali documenti si riferiscono, e sentiti i servizi produttori dei documenti stessi per le necessarie variazioni e ripubblicazioni sul dossier "giusto", avrebbe dovuto dare evidenza alla DMO, e alla UOC segnalante (nel caso di

specie, quella di Psichiatria), dell'avvenuta risoluzione del problema per le verifiche finali del caso da parte della stessa DMO, cui spetta di coordinare le attività necessarie "al ripristino delle normali condizioni di lavoro". Purtroppo, per cause in via di accertamento, ciò non è avvenuto, e dunque la procedura, in relazione al caso che ci occupa, non si è chiusa, pur avendo evidenza di comunicazioni interne al Servizio Sistemi Informativi in cui si leggeva che "le attività di correzione sono tutte terminate" già nella giornata del 8 settembre 2020, ben prima dunque del giorno, 18 settembre 2020, in cui la paziente che ha segnalato la violazione, per il tramite del proprio avvocato, ha preso visione del verbale di Pronto Soccorso riferito alla propria omonima (...);

c. il terzo errore, infine, è stato commesso dalla dirigente amministrativa della Direzione Medica, la quale, come anche segnalato in sede di notifica, in data 14 ottobre 2020, di propria iniziativa e senza alcuna condivisione con il titolare, il referente dell'Ufficio privacy aziendale e la Responsabile della protezione dei dati, comunicava via posta elettronica al legale della paziente”;

“AOUIVR ha posto in essere alcune delle misure proposte per prevenire in futuro casi ulteriori di scambio di persona, o comunque per evitare che essi possano esitare in violazioni di dati personali, mentre per altre ha creato i presupposti per la loro attuazione”. Sono stati tra l’altro organizzati corsi di formazione e “l’UOS Servizio Sistemi Informativi ha predisposto delle linee guida per la bonifica di un evento di errata identificazione del paziente”.

Come richiesto nella predetta nota del 31 dicembre 2021, l’11 febbraio 2021 si è svolta da remoto l’audizione dell’Azienda, nel corso della quale la stessa ha rappresentato, in particolare, che:

“il contesto in cui sono avvenuti i fatti oggetto del presente procedimento è caratterizzato da un numero considerevole di prestazioni denotate da un elevato livello di complessità (pronto soccorso). All’epoca dei fatti la struttura aziendale era in corso di conversione in relazione all’emergenza pandemica in atto, nonché all’incremento di accessi dovuti anche alle patologie legate al Covid-19”;

“L’Azienda ha da tempo posto in essere specifiche procedure per l’identificazione del paziente e ha fornito al personale sanitario istruzioni operative specifiche, nonché impiegato lo stesso in numerosi momenti di formazione. L’attività formativa svolta prima dei fatti oggetto di esame ha riguardato anche la corretta identificazione del paziente. Ciò è confermato dal fatto che l’errore che ha dato origine ai fatti in esame è stato rilevato il giorno seguente dalla stessa Azienda nell’ambito dei controlli che effettua costantemente sulla correttezza della documentazione prodotta”;

“l’interessato di cui non è stata effettuata una corretta attribuzione del codice identificativo si era presentato al pronto soccorso per un episodio grave, in relazione al quale è stato necessario procedere con tempestività, ciò ha portato alla necessità di procedere all’identificazione del paziente con estrema rapidità. si specifica che l’interessato non era accompagnato da familiari, in quanto dimora in una comunità protetta ed era in evidente stato di confusione”;

“i codici identificativi dei due soggetti coinvolti nella vicenda differiscono di un solo carattere”;

“Purtroppo l’operatore, in considerazione del contesto in cui operava e della delicatezza dell’intervento sanitario da prestare all’interessato, ha erroneamente attribuito il codice identificativo di un altro paziente allo stesso. Si è trattato di un episodio isolato e dettato da un comportamento sicuramente non doloso dell’operatore, con riferimento al quale il contesto in cui sono avvenuti i fatti legati al Covid-19 e alla particolare condizione di salute

dell'interessato ha portato il predetto operatore a commettere l'errore per ragioni di forza maggiore. Proprio per questo è stato effettuato nei confronti di tale operatore solo un richiamo verbale e nessun atto disciplinare ulteriore proprio perché non può non essere tenuto in considerazione il contesto in cui sono avvenuti i fatti”;

“A seguito dei fatti sono stati implementati ulteriori audit per verificare l'accuratezza delle attività di identificazione del paziente. Il 21 dicembre e successivamente il 4 febbraio 2021 si sono tenuti due incontri con il personale operante nei dipartimenti di emergenza, al fine di sensibilizzare lo stesso al rispetto delle procedure organizzative per la corretta identificazione del paziente anche con particolare riferimento alle attività prestate in pronto soccorso. Attualmente si sta tenendo un ulteriore corso di formazione a distanza sulle novità dettate dalla disciplina europea che vedrà coinvolto tutto il personale operante nell'Azienda (circa 6.000 utenti) nell'arco di 3 anni (circa 1.200 utenti l'anno). Un modulo di tale corso è dedicato al trattamento dei dati personali effettuato nello specifico contesto sanitario ed è caratterizzato da strumenti formativi dedicati agli aspetti operativi del trattamento (es. casistica delle fattispecie esaminate dal Garante nel corso dell'ultimo anno)”;

“Si evidenzia che l'Azienda ha implementato le misure per la protezione dei dati personali previste dal provvedimento sanzionatorio del 23 gennaio 2020 nonostante il periodo emergenziale in corso. Il contesto emergenziale infatti caratterizza l'attività della struttura; ciò deve essere tenuto presente anche nell'analisi della fattibilità degli interventi organizzativi e procedurali in materia di protezione dei dati personali. Si rappresenta inoltre che l'operato dell'Azienda si inserisce all'interno di un regime autorizzatorio regionale delle spese anche di natura informatica”.

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

Preso atto di quanto rappresentato dall'Azienda nelle memorie difensive, si osserva che:

1. la comunicazione di violazione effettuata dall'Azienda ha permesso di evidenziare che le misure adottate dalla stessa non hanno permesso di evitare del tutto la possibilità che il personale sanitario identifichi con esattezza i pazienti, proceda con tempestività ad aggiornare i dati erroneamente rilevati in tutti gli applicativi aziendali (dossier sanitario) e gestisca tali procedure in conformità ai principi generali del trattamento di cui all'art. 5 del Regolamento;
2. l'Azienda ha adottato misure tecniche e organizzative che si sono rilevate non pienamente adeguate al fine di garantire un'adeguata sicurezza dei dati personali, compresa la protezione da trattamenti non autorizzati come stabilito dall'art. 5, par. 1, lett. f), del Regolamento;
3. l'Azienda ha ulteriormente implementato le misure volte a garantire la certezza circa l'origine del dato trattato, la sua esattezza, integrità, confidenzialità e non modificabilità, nonché la disponibilità dello stesso (punto 7, allegato A alle Linee guida) che erano state già oggetto di revisione dopo l'adozione da parte del Garante del provvedimento del 23 gennaio 2020 (n. 18) e ha anche rinnovato le indicazioni nei confronti del personale coinvolto nelle attività di trattamento dei dati dei pazienti in merito ai principi generali del trattamento e alla specifica disciplina del trattamento dei dati personali nel contesto sanitario;
4. i fatti si sono verificati in un momento di particolare complessità per l'Azienda e per le strutture deputate a gestire l'emergenza sanitaria in atto;
5. l'origine dei fatti rappresentati dall'Azienda nella comunicazione di violazione è da ascrivere a errori umani anche dovuti alla delicatezza delle condizioni cliniche di uno dei

pazienti coinvolti nella vicenda, al contesto emergenziale in atto e alla circostanza che i due codici fiscali dei pazienti differiscono solo di un carattere;

6. l'Azienda ha corretto i dati erroneamente attribuiti ai pazienti in un breve arco temporale.

### **3.1. 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 non consentono di superare i rilievi notificati dall'Ufficio con l'atto di avvio del procedimento, non ricorrendo, peraltro, alcuno dei casi previsti dall'art. 11 del Regolamento del Garante n. 1/2019.

Per tali ragioni si rileva l'illiceità del trattamento di dati personali effettuato dall'Azienda Ospedaliero Universitaria Integrata di Verona, nei termini di cui in motivazione, in particolare, per aver trattato dati personali in violazione dei principi di base del trattamento di cui agli artt. 5, par. 2, lett. a) e f), 9 e 32 del Regolamento.

Ciò premesso, tenuto conto quanto sopra richiamato e, in particolare, che:

l'Azienda ha ulteriormente implementato le misure volte a garantire la certezza circa l'origine del dato trattato, la sua esattezza, integrità, confidenzialità e non modificabilità, nonché la disponibilità dello stesso che erano state già oggetto di revisione dopo l'adozione da parte del Garante del provvedimento del 23 gennaio 2020 (n. 18) e che ha anche rinnovato le indicazioni nei confronti del personale coinvolto nelle attività di trattamento dei dati dei pazienti in merito ai principi generali del trattamento e alla specifica disciplina del trattamento dei dati personali nel contesto sanitario;

i fatti si sono verificati in un momento di particolare complessità per l'Azienda e per le strutture deputate a gestire l'emergenza sanitaria in atto;

l'origine dei fatti rappresentati dall'Azienda nella comunicazione di violazione è da ascrivere a errori umani anche dovuti anche alla delicatezza delle condizioni cliniche di uno dei pazienti coinvolti nella vicenda, al contesto emergenziale in atto e alla circostanza che i due codici fiscali dei pazienti differiscono solo di un carattere;

il titolare si è attivato al fine di correggere i dati erroneamente attribuiti ai pazienti in un breve arco temporale;

non sono pervenute segnalazioni o reclami da parte dei soggetti i cui dati sono stati oggetto della comunicazione di violazione;

le circostanze del caso concreto inducono a qualificare lo stesso come "violazione minore", ai sensi del considerando 148 del Regolamento e delle Linee guida WP 253, riguardanti l'applicazione e la previsione delle sanzioni amministrative pecuniarie ai fini del Regolamento (UE) n. 2016/679. Si ritiene, pertanto, relativamente al caso in esame, che sia sufficiente ammonire il titolare del trattamento ai sensi degli artt. 58, par. 2, lett. b), e 83, par. 2, del Regolamento, per avere violato previsioni del Regolamento contenute negli artt. 5, 9 e 32 del Regolamento e che, considerando, in ogni caso, che la condotta ha esaurito i suoi effetti, atteso che l'Azienda Ospedaliero Universitaria Integrata di Verona ha attuato misure volte a ripristinare una corretta attribuzione dei documenti sanitari degli interessati nei

sistemi informativi aziendali, nonché migliorato le misure tecniche e organizzative volte a scongiurare che episodi come quello in esame posano ripetersi, non vi sono i presupposti per l'adozione di ulteriori provvedimenti correttivi da parte dell'Autorità, ai sensi dell'art. 58, par. 2, del Regolamento.

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**

a) ai sensi dell'art. 57, par. 1, lett. a) del Regolamento, dichiara l'illiceità del trattamento dei dati personali effettuato dall'Azienda Ospedaliero Universitaria Integrata di Verona, con sede legale con sede legale in Verona (VR), Piazzale Aristide Stefani, 1 - C.F./P. IVA 0390142023 per la violazione dei principi di base del trattamento, di cui agli artt. 5, par. 1, lett. a), e f), 9 e 32 del Regolamento, nei termini di cui in motivazione;

b) ai sensi dell'art. 58, par. 2, lett. b) del Regolamento, ammonisce la citata Azienda, quale titolare del trattamento in questione, per aver violato gli artt. 5, lett. a), e f), 9 e 32 del Regolamento, come sopra descritto;

c) 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.

d) 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, 2 dicembre 2021*

IL PRESIDENTE  
Stanzione

IL RELATORE  
Stanzione

IL SEGRETARIO GENERALE  
Mattei