



**GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI**

Provvedimento del 27 novembre 2024 [10095791]

VEDI ANCHE [Newsletter del 31 gennaio 2025](#)

[doc. web n. 10095791]

Provvedimento del 27 novembre 2024

Registro dei provvedimenti
n. 761 del 27 novembre 2024

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, alla quale hanno preso parte il prof. Pasquale Stazione, presidente, 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 Garante n. 98 del 4/4/2019, pubblicato in G.U. n. 106 dell'8/5/2019 e in www.gpdp.it, doc. web n. 9107633 (di seguito "Regolamento del Garante n. 1/2019");

VISTA la documentazione in atti;

VISTE le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del Regolamento del Garante n. 1/2000 sull'organizzazione e il funzionamento dell'ufficio del Garante per la protezione dei dati personali, in www.gpdp.it, doc. web n. 1098801;

RELATORE il prof. Pasquale Stazione;

PREMESSO

1. L'attività istruttoria.

Il 24 gennaio 2023 la Regione Molise (di seguito Regione) ha trasmesso al Garante, ai sensi dell'art. 33 del Regolamento, una notifica di violazione dei dati personali, riguardante il Portale

regionale del FSE (<https://fse.regione.molise.it>) che, a causa di una “vulnerabilità del sistema”, aveva consentito a un soggetto terzo “attraverso una manipolazione intenzionale della URL di effettuare una ricerca dei dati di altri cittadini presenti in Anagrafe Regionale del Molise”.

In particolare, nella predetta notifica, la Regione ha dichiarato che “sul Portale FSE della Regione Molise l’utente con ruolo “Assistito” è stato in grado, sfruttando una vulnerabilità del sistema attraverso una manipolazione intenzionale della URL, di effettuare una ricerca dei dati di altri cittadini presenti in Anagrafe Regionale del Molise. Nello specifico, manipolando la URL da <https://fse.regione.molise.it/fseui/dashboard> in <https://fse.regione.molise.it/fseui/list> l’utente è stato in grado di utilizzare la funzionalità di ricerca cittadino e successivamente selezionandolo accedere alla funzionalità di consultazione dei dati anagrafici e di consultazione del FSE del cittadino stesso” (v. notifica del 24 gennaio, sez. F, punto 7). Secondo quanto dichiarato in atti il numero di assistiti coinvolti è stato pari a 7.

In merito a quanto rappresentato dalla Regione, l’Ufficio ha effettuato due richieste di informazioni (note del 21 febbraio e del 17 aprile 2023) -a cui è stato fornito riscontro con le note del 3 marzo e del 5 maggio 2023- al fine di acquisire maggiori dettagli circa la violazione e gli interventi effettuati per rimuovere la vulnerabilità evidenziata, nonché elementi informativi sui ruoli dei diversi soggetti che sono intervenuti nei trattamenti oggetto di violazione, sulle misure tecniche e organizzative relative alle procedure di identificazione, autenticazione informatica (Identity Management) e di autorizzazione degli assistiti ai fini della consultazione dei propri documenti presenti nel FSE, sui soggetti responsabili della progettazione di tali procedure e sulle valutazioni effettuate in ordine ai rischi per i diritti e le libertà per gli interessati derivanti dalla violazione, anche al fine di verificare la sussistenza dei presupposti per la comunicazione della stessa agli interessati coinvolti.

In riscontro alle predette richieste di informazioni la Regione ha chiarito che “in data 17 gennaio 2023 il Sig. [...] segnalava a questo Ente, mediante posta elettronica certificata [...] un problema di sicurezza informatica riscontrato mentre visionava il suo fascicolo sanitario elettronico” e che “l’accesso è stato possibile alterando manualmente e forzatamente la URL (non visibile e accessibile agli utenti con il ruolo di Assistito); il segnalante, con il ruolo di assistito, ha forzato il sistema modificando la URL con il conseguente utilizzo della funzionalità di ricerca e consultazione dei dati. La funzionalità di ricerca era preclusa nella normale navigazione a sistema. Resta ignota la modalità con cui l’assistito si sia procurata l’esatta URL “<https://fse.regione.molise.it/fseui/list>” per poter fare la forzatura nel sistema” (v. nota del 3 marzo 2023, pag. 1 e allegato 1 e pag. 2 dell’allegato 2 alla medesima).

Per quanto riguarda le categorie dei dati che il soggetto terzo ha potuto consultare mediante il richiamo dell’URL <https://fse.regione.molise.it/fseui/list>, la Regione ha dichiarato che “sono riferite a: dati anagrafici (Nome, Cognome, Data di Nascita, Città di Nascita); dati di residenza e domicilio; dati relativi alla assistenza sanitaria (ASL appartenenza, Distretto di appartenenza, Medico di Base, Esenzioni); documenti e referti sanitari (ad es. referti di Laboratorio, referti specialistici, ecc.)” e che la “ricerca deve essere fatta in maniera puntuale con l’inserimento del Codice Fiscale completo e valido o tramite l’inserimento di Nome, Cognome e data di nascita (i tre dati sono obbligatori per finalizzare la ricerca)” (v. nota del 5 maggio 2023, pag. 3).

Con riferimento alle misure in essere al momento della violazione, la Regione ha richiamato il documento allegato alla notifica redatto dalla società Engineering Ingegneria Informatica S.P.A., designata responsabile del trattamento, con cui la medesima società ha comunicato la violazione dei dati alla Regione. Tra le misure tecniche ed organizzative adottate con riferimento ai trattamenti dei dati oggetto di violazione descritte nel predetto documento, sono indicate le attività di vulnerability assessment e penetration test svolti con cadenza periodica da un team preposto indipendente (v. notifica del 24 gennaio 2023).

Al riguardo, la Regione ha inoltre dichiarato che “le misure tecniche di autenticazione sono tutte

rimandate al proxy regionale (gestito dalla Molise Dati) di accesso SPID e CIE. La Web APP accede al proxy tramite un URL compreso di token di autenticazione. Il sistema riceve in risposta un body con i dati anagrafici che, a seconda del tipo di autenticazione, variano. Il middleware effettua i controlli in Anagrafe per controllare se effettivamente l'utenza è un assistito della regione Molise. In caso contrario viene rimandato alla pagina di autenticazione del sistema. In caso positivo al momento dell'accesso e alla selezione del ruolo viene generato il token dall'User Manager (modulo software per la gestione degli utenti) al fine di essere autorizzato all'utilizzo dei servizi API per la ricerca in anagrafe e alla documentale. [...] sono stati configurati i seguenti ruoli: 1. Medico/Dirigente Sanitario; 2. MMG/PLS; 3. Farmacista; 4. Operatore Amministrativo; 5. Assistito; 6. Tutore, Informal giver, Genitore. Per ognuno di questi ruoli sono state determinate le tipologie di interazioni che possono essere svolte" (v. nota del 3 marzo 2023, pagg. 2 e 3 dell'allegato 2 alla medesima).

In particolare, la Regione ha precisato che "a valle dell'analisi dei requisiti tecnici e funzionali del FSE alla quale hanno partecipato Regione Molise, Molise Dati, Tim S.p.A. ed Engineering S.p.A. (All. 6 denominato "FSE Regione Molise-Ruoli e permessi.pdf"), il sistema è stato progettato e realizzato dal punto di vista informatico da Engineering S.p.A, che, pertanto, rappresenta il soggetto responsabile della progettazione delle procedure di identificazione e autenticazione informatica (Identity Management) nonché di autorizzazione informatica degli assistiti ai fini della consultazione dei documenti presenti nel FSE e delle misure a garanzia della riservatezza dei medesimi documenti" (v. nota del 5 maggio 2023, pag. 2).

Con riferimento alle misure adottate a seguito della violazione, la Regione ha rappresentato che "è stata condotta un'analisi della possibile causa da cui è derivata la segnalazione, quindi, è stata fatta un'analisi dei log di tutti i moduli applicativi a tutti i livelli e successivamente è stata condotta un'analisi del codice per circoscrivere il bug e risolverlo definitivamente. La prima misura adottata è stata quella di inibire la possibilità di accedere alla pagina <https://fse.regione.molise.it/fseui/list> tramite chiamata diretta da browser. La seconda misura adottata è stata quella di implementare attraverso controlli inseriti nel codice sorgente un controllo che consenta di verificare che la pagina web <https://fse.regione.molise.it/fseui/list> non sia in alcun modo visibile ed utilizzabile da utenti autenticati con il ruolo "Assistito" (v. notifica del 24 gennaio 2023, sez. H, punto 1).

Per quanto attiene alle misure adottate per prevenire simili violazioni in futuro, è stato poi dichiarato di aver "richiesto a Molise Dati di dar luogo ad una analisi finalizzata a valutare eventuali presenze di simili errori nel software sviluppato dalla società Engineering SpA" (v. notifica del 24 gennaio 2023, sez. H, punto 2).

In merito alla comunicazione della violazione agli interessati, la Regione ha rappresentato che la gravità del potenziale impatto per gli interessati era "media" in quanto "la falla di sicurezza è stata segnalata dal medesimo soggetto che ha riscontrato la possibilità di accesso a dati non autorizzati. Non si ravvede nel medesimo la volontà di operare in maniera pregiudiziale nei confronti degli interessati", che la violazione "non è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche" e che "si è ritenuto di non dover procedere alla comunicazione agli interessati, non ravvisando un rischio elevato per i diritti e le libertà degli stessi. In particolare, tenuto conto che la falla di sicurezza veniva segnalata dallo stesso soggetto che aveva effettuato l'accesso non autorizzato, non si deduceva, da parte dello stesso, la volontà di operare in maniera pregiudizievole nei confronti degli interessati" (v. notifica del 24 gennaio 2023, sez. G, punto 3, e sez. L, punto 1 e nota del 3 marzo 2023 pag. 2 in riscontro alla richiesta di informazioni del 21 febbraio 2023).

Infine, la predetta Regione ha dichiarato che "in data 11 maggio 2021 [...] sottoscriveva, ex art. 26 del Regolamento UE 2016/679 (GDPR), con l'Azienda Sanitaria Regionale per il Molise -ASReM un accordo di contitolarità nel trattamento dei dati sanitari" e che "tale accordo di contitolarità, all'art. 2.3, prevedeva che ciascun contitolare potesse ricorrere a fornitori/subfornitori esterni per la

fornitura di qualsiasi servizio relativo alla gestione delle attività di cui al predetto accordo” (v. nota del 3 marzo 2023, pag. 2 e nota del 5 maggio 2023, allegato 2).

Sulla base di quanto sopra rappresentato, con nota del 28 settembre 2023 (prot. 133809), l'Ufficio ha effettuato una notifica di violazione di cui all'art. 166, comma 5, del Codice alla Regione Molise in quanto è stato rilevato che il trattamento di dati personali in esame è stato effettuato in maniera non conforme al principio di “integrità e riservatezza” (art. 5, par. 1, lett. f), del Regolamento), non adottando misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio (art. 32 del Regolamento) e adeguate, fin dalla progettazione dei trattamenti effettuati nell'ambito del FSE, ad attuare in modo efficace i principi di protezione dei dati e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del Regolamento e tutelare i diritti degli interessati, in violazione dell'art. 25 del Regolamento.

Con nota del 27 ottobre 2023, la Regione ha fatto pervenire le proprie memorie difensive nell'ambito delle quali ha rappresentato, in particolare, che:

“La Regione Molise demandava (...) l'attività di implementazione tecnica del FSE a Molise Dati S.p.A., organismo in house providing della Regione Molise”;

“Nell'esecuzione dell'incarico ricevuto, è rilevata la necessità di rivolgersi ad un partner tecnologico specializzato, Molise Dati S.p.A. aderiva al Contratto Quadro SPC Cloud Lotto 1 di Consip S.p.A., stipulando, in data 28 ottobre 2020, il contratto esecutivo n. 2000379980709001COE con un R.T.I. composto da TIM S.p.A., Enterprise Services Italia S.r.l., Poste Italiane S.p.A., Postecom S.p.A. e Postel S.p.A.” “Contestualmente alla stipulazione del contratto di servizio, Molise Dati S.p.A. e TIM S.p.A. sottoscrivevano l'atto di “nomina a responsabile del trattamento” ad esso allegato, nel quale, per quel che qui rileva, veniva delimitato l'ambito del trattamento e stabilito l'obbligo del fornitore di: (...) adottare tutte le misure tecniche ed organizzative che soddisfino i requisiti del Regolamento UE al fine di assicurare un adeguato livello di sicurezza dei trattamenti”;

“TIM S.p.A. individuava in Engineering Ingegneria Informatica S.p.A. l'ulteriore responsabile delle operazioni di trattamento svolte per finalità di implementazione del FSE, previa stipulazione, con l'operatore, di un accordo quadro per la fornitura dei servizi di cloud enabling in subappalto. L'accordo stipulato dalle parti prevedeva espressamente la designazione di Engineering Ingegneria Informatica S.p.A. quale (ulteriore) responsabile del trattamento “in relazione al Contratto Quadro sottoscritto in data 20/07/2016 tra Telecom e CONSIP...e /o ai Contratti Esecutivi sottoscritti tra Telecom e le varie Amministrazioni Beneficiarie”, con l'impegno del subappaltatore di “...osservare le condizioni/istruzioni riportate qui di seguito e nella citata lettera” (cfr. art. 21 del doc. E). Engineering Ingegneria Informatica S.p.A. rappresentava, quindi, il soggetto responsabile della progettazione e della realizzazione, dal punto di vista tecnico, del sistema informatico impiegato per la gestione del fascicolo sanitario elettronico, inclusa la progettazione delle procedure di identificazione e autenticazione informatica (Identity Management) nonché di autorizzazione informatica degli assistiti ai fini della consultazione dei documenti presenti nel FSE e delle misure a garanzia della riservatezza dei medesimi documenti”;

in merito ai fatti oggetto di violazione, “Molise Dati S.p.A. avviava immediatamente un'indagine volta a verificare l'effettiva sussistenza del problema di sicurezza informatica segnalata dal cittadino, chiedendo al subresponsabile Engineering Ingegneria Informatica S.p.A. di svolgere ogni più opportuno accertamento. All'esito delle verifiche effettuate, in data 21 gennaio 2023 Engineering Ingegneria Informatica S.p.A. trasmetteva a Molise Dati S.p.A. un documento, denominato “report”, nel quale veniva dato atto dell'effettiva presenza del bug rilevato dal segnalante”;

“sul Portale FSE della Regione Molise l’utente con ruolo “Assistito” è stato in grado, sfruttando una vulnerabilità del sistema attraverso una manipolazione intenzionale della URL, di effettuare una ricerca dei dati di altri cittadini presenti in Anagrafe Regionale del Molise. Nello specifico, manipolando la URL da <https://fse.regione.molise.it/fseui/dashboard> in <https://fse.regione.molise.it/fseui/list> l’utente è stato grado di utilizzare la funzionalità di ricerca cittadino e successivamente selezionandolo accedere alla funzionalità di consultazione dei dati anagrafici e di consultazione del FSE del cittadino stesso”;

“Engineering Ingegneria Informatica S.p.A. dava contestualmente atto di aver svolto un’indagine sulle cause della violazione e, una volta individuato il bug, di aver provveduto alla relativa risoluzione, effettuando gli interventi necessari ad evitare la possibile reiterazione dell’incidente di sicurezza”;

“Gli accertamenti svolti con maggior approfondimento in un momento successivo consentivano di ricostruire l’esatta dinamica della violazione e le vulnerabilità tecniche sottostanti. Secondo quanto appurato, infatti, il segnalante, autenticatosi univocamente in qualità di “assistito” mediante SPID, CIE o CNS , aveva manualmente manipolato l’URL della pagina web visualizzata all’atto dell’accesso, modificando l’indirizzo “<https://fse.regione.molise.it/fseui/dashboard>” in “<https://fse.regione.molise.it/fseui/list>” ed accedendo a quest’ultima senza che fosse necessario superare una procedura di autenticazione. Dalla seconda URL – il cui impiego era (ed è) riservato ad utenti autenticatisi come “Medico/Dirigente Sanitario” – risultava possibile utilizzare la funzionalità di ricerca dei singoli cittadini censiti e, successivamente, selezionando uno qualsiasi dei nominativi risultanti, accedere alla consultazione del fascicolo sanitario elettronico dell’assistito selezionato”;

“La vulnerabilità sottostante – la quale risultava sfruttabile soltanto da parte di quei soggetti autenticatisi (e quindi identificabili e rintracciabili) che, a conoscenza dell’URL di destinazione, avessero intenzionalmente effettuato tale manipolazione – è stata provocata da un errore di codifica del software riconducibile all’operato del sub responsabile del trattamento Engineering Ingegneria Informatica S.p.A”;

“A tutt’oggi, come già riferito, è ignoto come il segnalante possa aver avuto notizia dell’esatta URL “<https://fse.regione.molise.it/fseui/list>” e della possibilità di accedere, tramite lo stesso, alla banca dati sottostante il FSE”;

“la durata della violazione risulta contenuta nel periodo temporale che va dal 14 novembre al 30 dicembre 2022, poiché – come risulta dai file di log – è in tale arco che il segnalante ha effettuato accessi non autorizzati ai dati personali di altri assistiti”; “il numero di interessati coinvolti nella violazione è pari a 7”.

In relazione a quanto emerso dalle memorie della Regione, l’Ufficio ha avviato un procedimento sanzionatorio anche nei confronti delle società Molise dati s.p.a. e Engineering ingegneria informatica s.p.a. (note del 5 febbraio 2024) il cui esito è stato valutato con separati provvedimenti esaminati contestualmente al presente.

Il coinvolgimento della società Molise dati S.p.A., è stato effettuato in considerazione di quanto rappresentato dalla predetta Regione in merito all’aver demandato “l’attività di implementazione tecnica del FSE a Molise Dati S.p.A., organismo in house providing della Regione Molise” che con “atto allegato alla deliberazione di Giunta regionale n. 143 del 20 maggio 2021” veniva designata “quale responsabile del trattamento” e che tale nomina, in atti, prevede, tra l’altro, l’obbligo di mettere in atto misure di sicurezza adeguate alla protezione dei dati personali oggetto di trattamento, inclusa la “...definizione di appropriate soluzioni tecniche ed organizzative rivolte alla regolamentazione degli accessi logici...profili autorizzativi definiti in funzione del principio del

“Need to Know”” e della “...esecuzione di attività rivolte a individuare le vulnerabilità nelle applicazioni e nelle infrastrutture tecniche funzionali all'erogazione del servizio ed attivazione di opportuni piani di mitigazione”.

Per quanto riguarda la società Engineering Ingegneria Informatica S.p.A è stato avviato un procedimento sanzionatorio in considerazione di quanto rappresentato dalla predetta Regione in merito alla circostanza che “Engineering Ingegneria Informatica S.p.A. rappresentava, quindi, il soggetto responsabile della progettazione e della realizzazione, dal punto di vista tecnico, del sistema informatico impiegato per la gestione del fascicolo sanitario elettronico, inclusa la progettazione delle procedure di identificazione e autenticazione informatica (Identity Management) nonché di autorizzazione informatica degli assistiti ai fini della consultazione dei documenti presenti nel FSE e delle misure a garanzia della riservatezza dei medesimi documenti”; su richiesta di Molise Dati S.p.A. “Engineering Ingegneria Informatica S.p.A. ha dato atto di “aver svolto un’indagine sulle cause della violazione e, una volta individuato il bug, di aver provveduto alla relativa risoluzione, effettuando gli interventi necessari ad evitare la possibile reiterazione dell’incidente di sicurezza” e che secondo quanto dichiarato in atti “la vulnerabilità sottostante – la quale risultava sfruttabile soltanto da parte di quei soggetti autenticatisi (e quindi identificabili e rintracciabili) che, a conoscenza dell’URL di destinazione, avessero intenzionalmente effettuato tale manipolazione – è stata provocata da un errore di codifica del software riconducibile all’operato del subresponsabile del trattamento Engineering Ingegneria Informatica S.p.A”.

2. Esito dell’attività istruttoria.

Preso atto di quanto rappresentato nella documentazione in atti e nelle memorie difensive, si osserva che:

ai sensi del Regolamento si considerano “dati relativi alla salute” i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute (art. 4, par. 1, n. 15, del Regolamento). Il considerando n. 35 del Regolamento precisa poi che i dati relativi alla salute “comprendono informazioni sulla persona fisica raccolte nel corso della sua registrazione al fine di ricevere servizi di assistenza sanitaria”; “un numero, un simbolo o un elemento specifico attribuito a una persona fisica per identificarla in modo univoco a fini sanitari”;

il Regolamento prevede che i dati personali siano essere “trattati 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 («integrità e riservatezza»)” (art. 5, par. 1, lett. f) del Regolamento). In proposito, l’art. 32 del Regolamento, concernente la sicurezza del trattamento, stabilisce che “tenendo conto dello stato dell’arte e dei costi di attuazione, nonché 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, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio” (par. 1) 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” (par. 2);

tenendo altresì conto della finalità del FSE e della natura dei dati personali trattati, appartenenti anche a categorie particolari, i trattamenti effettuati nel contesto in esame richiedono l’adozione dei più elevati standard di sicurezza, al fine di non compromettere la riservatezza, l’integrità e la disponibilità dei dati personali di milioni di interessati. Su tale

base, gli obblighi di sicurezza imposti dal Regolamento richiedono l'adozione di rigorose misure tecniche e organizzative, includendo, oltre a quelle espressamente individuate dall'art. 32, par. 1, lett. da a) a d), anche tutte quelle necessarie ad attenuare i rischi che i trattamenti presentano.

l'art. 25, par. 1, del Regolamento prevede che “tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento [debba mettere] in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati” (cfr. anche cons. 75 e 78 del Regolamento).

in base al principio di “protezione dei dati fin dalla progettazione”, il titolare del trattamento è tenuto, pertanto, ad attuare i principi di protezione dei dati (art. 5 del Regolamento) adottando misure tecniche e organizzative adeguate e integrando nel trattamento le necessarie garanzie per soddisfare i requisiti del Regolamento e tutelare i diritti e le libertà degli interessati. Il considerando 78 del Regolamento suggerisce una responsabilità dei titolari, ossia quella di valutare costantemente se stiano utilizzando, in qualunque momento, i mezzi appropriati di trattamento e se le misure scelte contrastino effettivamente le vulnerabilità esistenti. Inoltre, i titolari dovrebbero effettuare revisioni periodiche delle misure di sicurezza poste a presidio e tutela dei dati personali, nonché della procedura per la gestione delle violazioni dei dati. L'obbligo di mantenere, verificare e aggiornare, ove necessario, il trattamento si applica anche ai sistemi preesistenti. Ciò implica che i sistemi progettati prima dell'entrata in vigore del Regolamento devono essere sottoposti a verifiche e manutenzione per garantire l'applicazione di misure e garanzie che mettano in atto i principi e i diritti degli interessati in modo efficace (cfr. le “Linee guida 4/2019 sull'articolo 25 - Protezione dei dati fin dalla progettazione e per impostazione predefinita” adottate dal Comitato europeo per la protezione dei dati il 20 ottobre 2020, spec. punti 7, 38, 39 e 84);

con particolare riferimento al principio di “integrità e riservatezza” (art. 5, par. 1, lett. f), del Regolamento), il titolare deve (cfr. le citate “Linee guida 4/2019 sull'articolo 25”, spec. punto 85) tenere conto non appena possibile dei requisiti di sicurezza nella progettazione e nello sviluppo del sistema, integrando e svolgendo costantemente test pertinenti;

la violazione dei dati personali oggetto della presente istruttoria è stata portata a conoscenza dell'Autorità da parte della predetta Regione, a cui è stata rappresentata dal responsabile del trattamento a seguito della segnalazione di un assistito;

spetta al titolare del trattamento “mettere in atto misure adeguate ed efficaci [e a ...] dimostrare la conformità delle attività di trattamento con il [...] Regolamento, compresa l'efficacia delle misure” adottate (cons. 74 del Regolamento), anche qualora si avvalga di un responsabile per lo svolgimento di alcune attività di trattamento, al quale deve impartire specifiche istruzioni, anche sotto il profilo della sicurezza (cons. 81 e art. 32, parr. 1, lett. d), e 4, del Regolamento). Infatti, il titolare deve porre in essere le misure tecniche e organizzative adeguate per garantire ed essere in grado di dimostrare che il trattamento è effettuato in conformità al Regolamento (artt. 5, par. 2, e 24 del Regolamento; cfr. le “Linee guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR”, adottate dal Comitato europeo per la protezione dei dati il 7 luglio 2021, spec. punto 41);

come indicato nelle richiamate Linee guida 07/2020 sui concetti di titolare del trattamento e

di responsabile del trattamento “Sebbene la catena possa essere alquanto lunga, il titolare del trattamento mantiene un ruolo centrale nella determinazione della finalità e dei mezzi dello stesso” (punto 152); infatti “anche se le decisioni sui mezzi non essenziali possono essere lasciate al responsabile del trattamento, il titolare del trattamento deve comunque stabilire determinati elementi nell'accordo sul trattamento dei dati quali, ad esempio, in relazione al requisito della sicurezza, l'istruzione di adottare tutte le misure richieste a norma dell'articolo 32 del GDPR”. Detto ciò le predette Linee guida aggiungono che “In ogni caso, il titolare del trattamento rimane responsabile dell'attuazione di misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al regolamento (punto 41 delle Linee guida e art 24 del Regolamento)”;

dall'esame delle informazioni e della documentazione fornita dalla Regione, emerge che il Portale FSE della Regione Molise, reso disponibile all'indirizzo <https://fse.regione.molise.it>, a causa di una “vulnerabilità” ha consentito a un utente autenticato con il ruolo di “assistito” “attraverso una manipolazione intenzionale della URL, di effettuare una ricerca dei dati di altri cittadini presenti in Anagrafe Regionale del Molise”, in assenza di una verifica dei permessi di autorizzazione attribuiti all'utente per l'accesso a tali dati;

il titolare del trattamento non aveva adottato misure e garanzie adeguate ad attuare efficacemente il principio di “integrità e riservatezza” (cfr. paragrafo 3.3), tenendo conto anche dei rischi per i diritti e le libertà degli interessati derivanti dai trattamenti in esame. Alla luce di quanto sopra esposto, si ravvisano gli estremi di una violazione del principio della “protezione dei dati fin dalla progettazione” di cui all'art. 25, par. 1, del Regolamento da parte di codesta Regione;

con specifico riferimento ai ruoli del trattamento effettuato attraverso il FSE, si richiama l'attenzione su quanto previsto dalla nuova disciplina di settore dettata dal decreto del Ministero della salute del 7 settembre 2023 che individua per ciascuna delle finalità perseguite attraverso il FSE i soggetti che assumono la veste di titolari del trattamento, a cui le regioni e le province autonome sono tenute ad adeguarsi (cfr. parere del Garante dell'8 giugno 2023, doc. web n. 9900433).

3. Conclusioni.

Alla luce delle valutazioni sopra richiamate, tenuto conto delle dichiarazioni rese dal titolare 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” 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 dalla Regione Molise nei termini di cui in motivazione, in violazione degli artt. artt. 5, par. 1, lett. f), 25 e 32 del Regolamento.

Si ritiene, infine, che ricorrano i presupposti di cui all'art. 17 del Regolamento del Garante n. 1/2019.

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. f), 25 e 32 del Regolamento comporta l'applicazione della sanzione amministrativa prevista dall'art. 83, parr. 4 e 5 del Regolamento.

Il Garante, ai sensi dell'art. 58, par. 2, lett. i) del Regolamento e dell'art. 166 del Codice, ha il potere di infliggere una sanzione amministrativa pecuniaria prevista dall'art. 83 del Regolamento, mediante l'adozione di una ordinanza ingiunzione (art. 18. L. 24 novembre 1981 n. 689), in relazione al trattamento dei dati personali posto in essere dalla Regione Molise, di cui è stata accertata l'illiceità, nei termini sopra esposti.

Ritenuto di dover applicare il paragrafo 3 dell'art. 83 del Regolamento laddove prevede che “se, in relazione allo stesso trattamento o a trattamenti collegati, un titolare del trattamento [...] viola, con dolo o colpa, varie disposizioni del presente Regolamento, l'importo totale della sanzione amministrativa pecuniaria non supera l'importo specificato per la violazione più grave”, l'importo totale della sanzione è calcolato in modo da non superare il massimo edittale previsto dal medesimo art. 83, par. 5.

Alla luce di quanto sopra illustrato, si ritiene che il livello di gravità della violazione commessa dalla Regione Molise sia basso (cfr. Comitato europeo per la protezione dei dati, “Guidelines 04/2022 on the calculation of administrative fines under the GDPR” del 23 maggio 2023, punto 60).

Con riferimento agli elementi elencati dall'art. 83, par. 2 del Regolamento ai fini dell'applicazione della sanzione amministrativa pecuniaria e della relativa quantificazione, tenuto conto che la sanzione deve essere “in ogni singolo caso effettiva, proporzionata e dissuasiva” (art. 83, par. 1 del Regolamento), si rappresenta che, nell'ipotesi in esame, sono state tenute in considerazione le circostanze sotto riportate:

l'Autorità ha preso conoscenza dell'evento a seguito della notifica di violazione dei dati personali effettuata dalla Regione Molise, che con riferimento ai trattamenti in esame, anche alla luce della specifica disciplina di settore, opera in qualità di titolare del trattamento;

il trattamento in esame riguarda dati idonei a rilevare informazioni sulla salute (dati anagrafici e di residenza, dati relativi all'assistenza sanitaria ricevuta (ASL di appartenenza, distretto di appartenenza, nominativo del medico di base, eventuale titolarità di esenzioni), dati sanitari desumibili dai documenti e dai referti sanitari eventualmente presenti nello specifico fascicolo sanitario elettronico (ad es. referti di laboratorio, referti specialistici, ecc.) di 7 soggetti che sono stati esposti a possibili accessi illeciti per circa 45 giorni (dal 14 novembre al 30 dicembre 2022);

il tipo di vulnerabilità riscontrato non era né di facile rilevazione, né di semplice sfruttamento, richiedendo la previa conoscenza della URL di destinazione <https://fse.regione.molise.it/fseui/list> e una manipolazione intenzionale della URL;

la Regione ha dimostrato un elevato grado di cooperazione adoperandosi al fine di introdurre nell'immediato misure idonee a superare le vulnerabilità sopra evidenziate;

la Regione Molise non è stata destinataria di altri provvedimenti sanzionatori e correttivi in merito alla fattispecie in esame.

Alla luce degli elementi sopra indicati e delle valutazioni effettuate, si ritiene, nel caso di specie, di applicare nei confronti della Regione Molise la sanzione amministrativa del pagamento di una somma pari ad euro 10.000,00 (diecimila/00).

In tale quadro si ritiene, altresì, che, ai sensi dell'art. 166, comma 7, del Codice e dell'art. 16, comma 1, del Regolamento del Garante n. 1/2019, si debba procedere alla pubblicazione del presente capo contenente l'ordinanza ingiunzione sul sito Internet del Garante.

TUTTO CIÒ PREMESSO IL GARANTE

a) ai sensi degli artt. 57, par. I, lett. a) e 83 del Regolamento, dichiara l'illiceità del trattamento dei dati personali effettuato dalla Regione Molise con sede in Via Insorti d'Ungheria, n. 81 – 86100 Campobasso (CB), C.F. / P. IVA 00169440708, per la violazione dei principi di integrità e riservatezza e di protezione dei dati fin dalla progettazione e per impostazione predefinita” (artt. 5, par. 1, lett. f), 25 e 32 del Regolamento), nei termini di cui in motivazione;

ORDINA

b) ai sensi dell'art. 58, par. 2, lett. i) del Regolamento, alla predetta Regione, quale titolare del trattamento in questione, di pagare la somma di euro 10.000,00 (diecimila/00) a titolo di sanzione amministrativa pecuniaria per aver violato gli artt. 5, par. 1, lett. f), 25 e 32 del Regolamento, come sopra descritto;

INGIUNGE

c) alla Regione Molise di pagare la predetta somma di euro 10.000,00 (diecimila/00), secondo le modalità indicate in allegato, entro trenta giorni dalla notifica del presente provvedimento, pena l'adozione dei conseguenti atti esecutivi a norma dall'art. 27 della legge n. 689/1981. Si rappresenta che ai sensi dell'art. 166, comma 8 del Codice, resta salva la facoltà per il trasgressore di definire la controversia mediante il pagamento -sempre secondo le modalità indicate in allegato- di un importo pari alla metà della sanzione irrogata entro il termine di cui all'art. 10, comma 3, del d. lgs. n. 150 del 1° settembre 2011 previsto per la proposizione del ricorso come sotto indicato.

DISPONE

d) ai sensi dell'art. 166, comma 7, del Codice e dell'art. 16, comma 1, del Regolamento del Garante n. 1/2019, la pubblicazione dell'ordinanza ingiunzione sul sito internet del Garante;

e) ai sensi dell'art. 154 bis, comma 3 del Codice dispone la pubblicazione del presente provvedimento sul sito del Garante;

f) ai sensi dell'art. 17 del Regolamento del Garante n. 1/2019, l'annotazione delle violazioni e delle misure adottate in conformità all'art. 58, par. 2 del Regolamento, nel registro interno dell'Autorità previsto dall'art. 57, par. 1, lett. u) del Regolamento.

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, 27 novembre 2024

IL PRESIDENTE
Stanzione

IL RELATORE
Stanzione

IL SEGRETARIO GENERALE
Mattei