Newsletter
NOTIZIARIO
ANNO XXI
WWW.GARANTEPRIVACY.IT

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

NEWSLETTER N. 450 del 25 febbraio 2019

Lavoro: no a invio massivo di dati degli infermieri a Ordine professionale

Le strutture sanitarie non possono trasmettere in modo massivo i dati di tutto il loro personale infermieristico all'Ordine professionale di riferimento.

L'Ordine delle professioni infermieristiche, nello svolgimento degli specifici compiti istituzionali di vigilanza e disciplinari, può infatti trattare i dati di chi abbia richiesto l'iscrizione all'albo.

Deve essere il datore di lavoro ad accertare, all'atto dell'assunzione e nel corso del rapporto di lavoro, che un infermiere sia dotato dei requisiti necessari per prestare servizio e che sia iscritto all'apposito albo professionale.

Queste le indicazioni fornite dal Garante della privacy a un'azienda ospedaliera (/garante/doc.jsp?ID=9084551) che chiedeva di poter trasmettere, pur non avendo un'apposita base normativa, i dati di tutto il suo personale infermieristico al relativo ordine professionale, il quale intendeva effettuare controlli sulle iscrizioni.

Nel presentare l'istanza al Garante, sia l'Ospedale sia l'Ordine delle professioni infermieristiche avevano rappresentato che tale comunicazione di dati personali fosse utile per l'esecuzione di un compito di interesse pubblico, in quanto consentiva di verificare che tutti gli infermieri in servizio rispettassero i requisiti previsti dal decreto che, nel 2018, ha modificato la legge di Ricostituzione degli Ordini delle professioni sanitarie e per la disciplina dell'esercizio delle professioni stesse.

Nella sua risposta, però, il Garante ha evidenziato che l'attuale quadro normativo non attribuisce agli Ordini - pur dotati di specifici poteri disciplinari e di vigilanza - competenze per generalizzate attività di ricerca e raccolta di informazioni personali riferite al personale infermieristico. Spetta invece al datore di lavoro l'obbligo di effettuare le necessarie verifiche sul possesso dei particolari requisiti previsti per l'accesso a specifici impieghi, inclusa l'iscrizione del singolo professionista al relativo albo che, tra l'altro, è pubblico e reperibile anche on line.

L'Autorità ha quindi dichiarato che non sussistono i presupposti di liceità per la comunicazione generalizzata dei nominativi e della residenza degli infermieri impiegati dalle aziende sanitarie agli ordini territorialmente competenti. Tenendo conto del numero di quesiti pervenuti sul tema, ha inoltre trasmesso la decisione anche alla Federazione nazionale delle professioni infermieristiche al fine di darne ampia diffusione presso gli ordini provinciali e le altre istituzioni coinvolte.

Dati dei defunti: in Italia continuano a essere tutelati

La scelta del legislatore dopo il Regolamento Ue

Le persone decedute continuano a godere delle tutele previste dalla disciplina in materia di protezione dei dati personali anche dopo l'applicazione del Gdpr.

Il principio è stato affermato dal Garante privacy nel parere reso ad una Azienda sanitaria nell'ambito del riesame di un provvedimento di rigett (/garante/doc.jsp?ID=9084520)o, riguardante un accesso civico ai dati sanitari di un paziente deceduto. La richiesta, relativa ad un caso di presunta malasanità, era stata rivolta all'azienda sanitaria da una persona che attraverso il cosiddetto "Foia" intendeva avere accesso agli atti di audit clinico e agli approfondimenti condotti dal risk manager. Una documentazione contenente informazioni particolarmente riservate (ricovero, sintomi, anamnesi, diagnosi, esami effettuati, alcuni particolarmente invasivi, terapia, farmaci somministrati, credo professato).

Prima di entrare nel merito della vicenda, il Garante ha rilevato che il Regolamento europeo sulla protezione dati, pur escludendo l'applicazione della normativa ai dati delle persone decedute, stabilisce, con una "clausola di salvaguardia", la possibilità per gli Stati membri di prevedere norme che riguardano il trattamento dei dati personali delle persone decedute. Facoltà di cui si è avvalso il legislatore italiano con il d. lgs. n.101/2018, sancendo che i diritti relativi ai dati personali dei defunti possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato, in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione. Da tale riconoscimento deriva quindi la logica conseguenza che ai dati delle persone decedute continuano ad applicarsi le tutele previste dalla disciplina sulla protezione dei dati.

Per quanto riguarda invece la richiesta di accesso alla documentazione sanitaria il Garante ha affermato che questo tipo di informazioni non sono accessibili con il Foia. Il Codice sulla protezione dei dati prevede infatti un espresso "divieto di diffusione" di dati relativi alla salute per cui è impossibile darne "conoscenza a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione".

La vicenda esaminata rientra dunque in una delle ipotesi di esclusione dell'accesso civico previste dalla normativa sulla trasparenza, che prevede espressamente come l'accesso civico deve essere escluso nei "casi di divieto di accesso o divulgazione previsti dalla legge".

Il Garante ha quindi concluso che l'Azienda sanitaria, pur con una motivazione sintetica, ha correttamente respinto l'istanza di accesso.

Privacy: no all'accesso civico generalizzato su pratiche SCIA e CILA

Non è possibile accedere ai dati personali completi contenuti nei titoli abilitativi edilizi (SCIA e CILA) sulla base di una mera richiesta di accesso civico generalizzato. Lo ribadisce il Garante per la protezione dei dati personali nel parere fornito a un Comune dell'Emilia-Romagna (/garante/doc.jsp?ID=9080951) in merito alla decisione di respingere parzialmente una richiesta di accesso civico alle Segnalazioni Certificate di Inizio Attività (SCIA) e alle Comunicazioni Inizio Attività Asseverata (CILA), presentata da una impresa privata.

La richiesta di copia completa delle pratiche edilizie era stata presentata una prima volta al Comune, che aveva però risposto fornendo solamente una sintesi con dati aggregati, depurati di quelli personali, al fine di non arrecare un possibile pregiudizio alla privacy delle persone interessate. L'impresa, supportata dal Difensore civico regionale dell'Emilia-Romagna, aveva contestato la decisione e chiesto il riesame della pratica. Il Garante privacy aveva invece sostenuto la correttezza della scelta dell'amministrazione cittadina. L'impresa aveva poi ripresentato la domanda, ma il Garante è nuovamente intervenuto sulla vicenda, anche al fine di evitare pericolosi precedenti che incoraggino possibili trattamenti illeciti di dati personali.

Nel proprio parere (/garante/doc.jsp?ID=9080951), l'Autorità ha innanzitutto chiarito che, diversamente da quanto indicato per altre pratiche edilizie, come i permessi a costruire, la normativa non prevede lo stesso regime di conoscibilità per la CILA e la SCIA, come per quelle utilizzate nel caso di opere di manutenzione straordinaria, di restauro o di risanamento conservativo.
Il Garante ha quindi sottolineato che la generale conoscenza delle informazioni riportate nelle SCIA e nelle CILA, considerando la quantità e qualità dei dati personali contenuti - come data e luogo di nascita, codici fiscali, residenza, e-mail, pec, numeri di telefono fisso e cellulare, documentazione tecnica sugli interventi - avrebbe potuto determinare un'interferenza ingiustificata e sproporzionata nei diritti e libertà dei soggetti controinteressati. Tutto ciò, in violazione anche del principio di minimizzazione previsto dal Regolamento europeo sulla privacy (Gdpr), con possibili ripercussioni negative sul piano relazionale, professionale, personale e sociale.
Nel corso dell'istruttoria, il Garante ha inoltre rilevato che l'impresa richiedente - che ha tra le sue attività quella di conduzione di campagne di marketing e web marketing, nonché la fornitura di servizi di gestione dei programmi di fidelizzazione e affiliazione commerciale - aveva presentato la stessa domanda in maniera sistematica, per più periodi, a diversi enti locali. L'accoglimento della richiesta di accesso civico avrebbe tra l'altro potuto esporre al pericolo di duplicazione di banche dati di soggetti pubblici da parte di soggetti privati, in assenza del consenso dei soggetti interessati o degli altri presupposti di liceità del trattamento.
L'Autorità, ha così confermato, anche alla luce della normativa e delle stesse linee guida Anac, la correttezza dell'operato del Comune, nel valutare l'esistenza di un possibile pregiudizio concreto alla protezione dei dati delle persone interessate - ad esempio i proprietari, gli usufruttuari e tecnici incaricati - e fornendo di conseguenza solo una sintesi delle pratiche richieste. Ha comunque rimarcato che tale decisione sull' "accesso civico generalizzato" non impedisce di accedere ai documenti amministrativi completi a chi dimostri di avere un interesse qualificato.

Privacy: le regole sul trasferimento di dati UK-UE in caso di "Hard Brexit"

L'Edpb adotta anche le Linee-guida sui codici di condotta e un parere sulla vigilanza finanziaria

Il Comitato europeo per la protezione dei dati (Edpb), nel corso della settima sessione plenaria, ha adottato una nota informativa (https://edpb.europa.eu/our-work-tools/our-documents/other /information-note-data-transfers-under-gdpr-event-no-deal-brexit_en) destinata alle aziende e alle autorità pubbliche sui trasferimenti di dati personali a norma del Regolamento generale sulla protezione dei dati (Gdpr) in caso di Brexit senza accordo con l'Ue ("Hard Brexit").
Nel documento approvato, il board dei Garanti europei, di cui è componente anche l'Autorità italiana, ha chiarito che in caso di "Hard Brexit" il Regno Unito diventerà un paese terzo dal 30 marzo 2019. Di conseguenza, il trasferimento di dati personali dal SEE (Spazio economico europeo) verso il Regno Unito dovrà basarsi su uno dei seguenti strumenti: clausole-tipo di protezione dei dati o clausole di protezione dei dati ad hoc, norme vincolanti d'impresa, codici di condotta e meccanismi di certificazione e strumenti specifici di trasferimento a disposizione delle autorità pubbliche. In assenza di clausole-tipo di protezione dei dati o di altre garanzie adeguate, si possono utilizzare alcune deroghe a determinate condizioni.
Per quanto riguarda i trasferimenti di dati dal Regno Unito al SEE, secondo il governo britannico l'attuale situazione, che prevede la libera circolazione dei dati personali dal Regno Unito al SEE, continuerà anche in caso di Brexit senza accordo con l' Ue.
Un'apposita scheda informativa (/regolamentoue/brexit) sulle procedure da adottare in caso di "Hard Brexit" è stata resa disponibile sia sul sito del Garante italiano, sia su quello del Comitato europeo.
Nel corso della plenaria, l'Edpb ha anche adottato delle Linee-guida in materia di codici di condotta (/garante/doc.jsp?ID=9083571), al fine di chiarire le procedure e le norme relative alla presentazione, all'approvazione e alla pubblicazione dei codici di condotta sia in Italia, sia negli altri Paesi europei.
Il Comitato ha inoltre espresso il suo primo parere (https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64 /opinion-42019-draft-administrative-arrangement_en)su un accordo amministrativo per i trasferimenti di dati personali tra autorità di vigilanza finanziaria del SEE, tra cui l'Autorità europea degli strumenti finanziari e dei mercati (ESMA) e le loro controparti extra-Ue.

L´ATTIVITÁ DEL GARANTE - PER CHI VUOLE SAPERNE DI PIÚ

- Redditi on line dei dirigenti Pa: la sentenza della Consulta indica un percorso di bilanciamento tra protezione dei dati personali e interessi costituzionalmente rilevanti. Dichiarazione di Antonello - 22 febbraio 2019 (/garante /doc.jsp?ID=9084440)
- Linee-guida sui codici di condotta. Consultazione pubblica - 20 febbraio 2019 (/garante/doc.jsp?ID=9083571)
- Trasferimento di dati in caso di "Hard Brexit" - Pagina informativa - 18 febbraio 2019 (/regolamentoue/brexit)
- Memoria del Presidente del Garante per la protezione dei dati personali nell'ambito del ddl di conversione in legge del decreto-legge 28 gennaio 2019, n. 4 recante disposizioni urgenti in materia di reddito di cittadinanza e di pensioni (AS 1018) - 8 febbraio 2019 (/garante/doc.jsp?ID=9081679)

NEWSLETTER
del Garante per la protezione dei dati personali (Reg. al Trib. di Roma n. 654 del 28 novembre 2002).
Direttore responsabile: Baldo Meo.
Direzione e redazione: Garante per la protezione dei dati personali, Piazza Venezia, n. 11 - 00187 Roma.
Tel: 06.69677.2751 - Fax: 06.69677.3785
Newsletter è consultabile sul sito Internet *www.garanteprivacy.it (http://www.garanteprivacy.it/)*