GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

GPDP newsletter

NOTIZIARIO DEL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

anno XXIII

NEWSLETTER N. 473 del 19 febbraio 2021

Data breach sanitari, il Garante privacy sanziona tre strutture

Avevano comunicato informazioni sulla salute alle persone sbagliate

Le strutture sanitarie devono adottare tutte le misure tecniche e organizzative necessarie per evitare che i dati dei loro pazienti siano comunicati per errore ad altre persone. Lo ha ricordato il Garante per la privacy nel sanzionare due ospedali e una Asl per le violazioni di dati personali causati non da attacchi informatici esterni, ma da procedure inadeguate e da semplici errori materiali del personale.

Un ospedale toscano ha ricevuto la sanzione di 10.000 euro per aver spedito via posta, al paziente sbagliato, una relazione medica contenente le informazioni sulla salute e la vita sessuale di un'altra coppia.

Anche un ospedale dell'Emilia-Romagna ha ricevuto la sanzione di 10.000 euro per aver consegnato a dei pazienti cartelle cliniche contenenti dati e referti riferibili ad altre persone, incluso un minore.

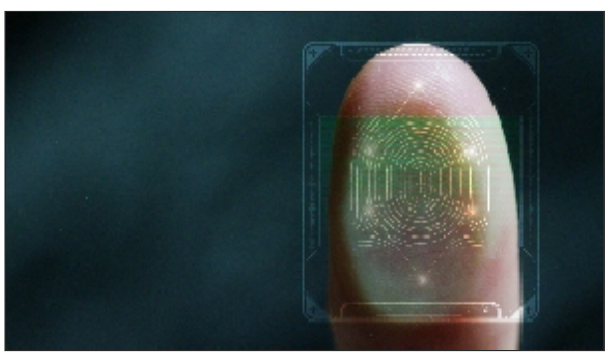
In entrambi i casi le sanzioni sono state calcolate tenendo conto che le strutture sanitarie hanno immediatamente dimostrato un elevato grado di cooperazione con il Garante e che gli episodi sono risultati isolati e non volontari. Le due strutture hanno anche pianificato ulteriori misure tecniche e organizzative per ridurre al minimo l'errore umano.

Un terzo caso riguarda invece una Asl dell'Emilia-Romagna, dove una paziente aveva esplicitamente richiesto – sottoscrivendo un apposito modulo – che nessun soggetto esterno, neppure i familiari, fosse informato sul suo stato di salute. Il modulo, però, era stato inserito all'interno della cartella clinica. Un'infermiera del reparto dove la donna stava seguendo delle terapie, non essendo a conoscenza della richiesta, invece che contattarla sul telefono cellulare privato, aveva chiamato il numero di casa registrato nell'anagrafe aziendale, parlando così con un familiare. Anche in questo caso, l'Azienda ha riconosciuto gli errori che hanno causato il data breach. Si è impegnata quindi ad implementare un sistema informatizzato di gestione dei numeri di telefono dei pazienti ricoverati, e a predisporre una modulistica unica con la quale i pazienti potranno esprimere la loro eventuale volontà di comunicare informazioni sul proprio stato di salute ai terzi, introducendo una specifica policy aziendale. La Asl, che ha subito anche una richiesta di risarcimento danni da parte della paziente, dovrà pagare una sanzione di 50.000 euro per la violazione del Gdpr.

Alla luce di questi episodi e di altri ancora in corso di valutazione, il Garante ha ricordato che le informazioni sullo stato di salute possono essere comunicate a terzi solo sulla base di un presupposto giuridico o su indicazione della persona interessata, previa delega scritta. E ha invitato tutte le strutture sanitarie al pieno rispetto dei principi di correttezza e trasparenza, adottando misure tecniche e organizzative utili non solo a proteggersi da attacchi informatici, ma anche a evitare violazioni di dati personali, in particolare quelli più delicati, come quelli sulla salute - troppo spesso causate da inadeguate procedure gestionali.

Lavoro: Garante, no all'uso delle impronte digitali dei dipendenti se manca base normativa

Sanzione di 30.000 euro ad una Asp



Il Garante ha sanzionato per 30.000 euro l'Azienda sanitaria provinciale (Asp) di Enna per l'utilizzo di un sistema di rilevazione delle presenze basato sul trattamento di dati biometrici dei dipendenti. A seguito del rafforzamento delle garanzie previste dal Regolamento e dal Codice privacy, per installare questo tipo di sistemi è necessaria infatti una base normativa che sia proporzionata all'obiettivo perseguito e che fissi misure appropriate e specifiche per tutelare i diritti degli interessati. Nel caso della Asp di Enna la base normativa invocata era carente, non essendo stato adottato il regolamento attuativo della legge 56/2019 (poi abrogata) che doveva stabilire garanzie per circoscrivere gli ambiti di applicazione e regolare le principali modalità del trattamento.

L'istruttoria dell'Autorità, avviata a seguito di alcuni articoli di stampa, ha consentito di accertare che il sistema di rilevazione presenze dell'Asp di Enna acquisiva le impronte digitali di oltre 2.000 dipendenti memorizzandole in forma crittografata sul badge di ciascun lavoratore. L'Azienda, poi, verificava l'identità del dipendente mediante il confronto tra il modello biometrico di riferimento, memorizzato all'interno del badge, e l'impronta digitale presentata all'atto del rilevamento della presenza e trasmetteva il numero di matricola del dipendente, la data e l'ora della timbratura, al sistema di gestione delle presenze.

L'Autorità ha ritenuto, contrariamente a quanto sostenuto dall'Azienda sanitaria, che in questo modo si effettuava un trattamento di dati biometrici dei dipendenti (sia all'atto dell'emissione del badge, sia all'atto della verifica dell'impronta in occasione di ogni "timbratura" di ciascun dipendente,) in assenza di una idonea base giuridica. Né il consenso dei dipendenti, invocato dall'Asp quale fondamento del trattamento, può essere considerato valido, nel contesto lavorativo, a maggior ragione pubblico, per effetto dello squilibrio del rapporto tra dipendente e datore di lavoro

Inoltre la struttura sanitaria, pur avendo informato il personale e i sindacati della scelta organizzativa compiuta, non aveva fornito tutte le informazioni sul trattamento, come richiesto dal Regolamento europeo in materia di privacy.

Considerati tutti gli aspetti della vicenda, il Garante ha dichiarato illecito il trattamento dei dati biometrici e ha applicato all'Asp 30.000 euro di sanzione. Ha inoltre disposto la cancellazione dei modelli biometrici memorizzati all'interno dei badge e chiesto all'Asp di far conoscere le iniziative che intende intraprendere per far cessare il trattamento dei dati biometrici dei dipendenti.

Dal Consiglio d’Europa le linee guida sul riconoscimento facciale

Preoccupazione per le tecnologie di “riconoscimento dell’affetto”

Il Consiglio d’Europa ha chiesto regole rigide per evitare i grandi rischi per la privacy e la protezione dei dati posti dall’utilizzo crescente delle tecnologie di riconoscimento facciale.

Il 28 gennaio 2021, nella Giornata europea per la protezione dei dati, il Comitato Consultivo della Convenzione 108, istituito presso il Consiglio d’Europa, ha adottato linee guida in materia.

Le linee guida, che si fondano sui principi della Convenzione 108 modernizzata, forniscono una serie di misure di riferimento che governi, sviluppatori di sistemi di riconoscimento facciale, produttori, aziende e pubbliche amministrazioni dovrebbero adottare per garantire che l’impiego di queste tecnologie non pregiudichi la dignità della persona, i diritti umani e le libertà fondamentali.

Il Comitato riconosce infatti i pericoli che possono derivare da tecniche particolarmente invasive e richiama la necessità di un dibattito pubblico e di un approccio precauzionale.

Il documento esprime particolare preoccupazione riguardo ai rischi derivanti dal riconoscimento facciale volto a rilevare i tratti della personalità, i sentimenti o le reazioni emotive dall'immagine del volto: le cosiddette tecnologie di “riconoscimento dell’affetto”. Tali tecnologie - afferma il Comitato - dovrebbero essere vietate e non dovrebbero essere impiegate, ad esempio, nelle procedure di assunzione di personale, nell'accesso ai servizi assicurativi e a all’istruzione. Allo stesso modo, non dovrebbe essere consentito l'uso del riconoscimento facciale al solo scopo di determinare il colore della pelle di una persona, le convinzioni religiose o di altro tipo, il sesso, l'origine etnica, l'età, le condizioni di salute o le condizioni sociali.

L’uso di sistemi di riconoscimento facciale da parte delle forze dell’ordine dovrebbe essere consentito solo quando è strettamente necessario per prevenire un rischio imminente e grave alla sicurezza pubblica.

Le Linee guida raccomandano agli sviluppatori di tecnologie di riconoscimento facciale di prestare specifica attenzione all’attendibilità degli algoritmi e all’accuratezza dei dati trattati, al fine di evitare disparità e possibili ricadute discriminatorie.

Le aziende e le pubbliche amministrazioni che intendano avvalersi di tecniche di riconoscimento facciale, da parte loro, hanno l’obbligo di garantire il rispetto dei principi di protezione dati, compresa la necessità di effettuare una valutazione dei rischi che il ricorso a tali tecniche può avere sui diritti delle persone, nonché dei profili etici che ne derivano, anche attraverso l’ausilio di comitati di esperti indipendenti.

Le persone devono, inoltre, poter esercitare i propri diritti, compreso quello di rettifica (ad esempio in presenza di false corrispondenze) o quello di non essere sottoposto a decisioni puramente automatizzate senza che la propria opinione sia adeguatamente considerata.

Infine, un ruolo importante a tutela dei diritti delle persone possono svolgerlo le Autorità di protezione dei dati che, in base all’art. 15 (3) della Convenzione 108+, devono essere consultate riguardo a proposte legislative e amministrative che comportino il trattamento dei dati personali mediante tecnologie di riconoscimento facciale. Le Autorità devono essere consultate prima di possibili sperimentazioni o utilizzi.

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

Gli interventi e i provvedimenti più importanti recentemente adottati dall´Autorità

- Vaccinazione dei dipendenti: le FAQ del Garante privacy. Principi generali e focus sugli operatori sanitari - Comunicato del 17 febbraio 2021
- EDPS - Opinions on the Digital Services Act and the Digital Markets Act -10 febbraio 2021
- "Se non ha l’età, i social possono attendere". Lo spot del Garante privacy e di Telefono Azzurro per sensibilizzare i genitori - Comunicato dell’8 febbraio 2021
- Tik Tok si adeguerà alle richieste del Garante privacy. Ma l’Autorità vigilerà sull’effettiva efficacia delle misure che verranno adottate – Comunicato del 3 febbraio 202
- La privacy e i nuovi scenari posti dalle neuroscienze nel convegno organizzato dal Garante in occasione della Giornata europea della protezione dati - 28 gennaio 2021

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*