

11/04/2024

Cerca
RICERCA AV

Tra sanzioni in ambito sanitario e più tutele per i dati personali nella PA: le ultime del Garante Privacy

Di seguito gli ultimi interventi dell'Autorità, pubblicati nella NL del 10 aprile 2024, n. 521.

di La Redazione



SOMMARIO

Il Garante Privacy ha sanzionato la Regione Lazio per l'attacco informatico al sistema sanitario regionale

Il Garante Privacy ha sanzionato per 75mila euro una ASL

Trasparenza online: il sì del Garante ad ANAC su 14 schemi standard di pubblicazione che dettano le regole alla PA

Intercettazioni della Procura UE: via libera del Garante Privacy al data base nazionale

Il Garante Privacy ha sanzionato la Regione Lazio per l'attacco informatico al sistema sanitario regionale

LAZIOcrea (società che gestisce i sistemi informativi regionali), Regione Lazio e ASL Roma 3 sotto accusa. Il **data breach** - causato da un ransomware introdotto nel sistema attraverso un portatile in uso a un dipendente della Regione - ha bloccato l'accesso a molti **servizi sanitari** «impedendo, tra l'altro, la gestione delle prenotazioni, i pagamenti, il ritiro dei referti, la registrazione delle vaccinazioni».

Dagli accertamenti e dalle ispezioni effettuate dall'Autorità è emerso che LAZIOcrea e Regione Lazio sono incorse in numerose e **gravi violazioni della normativa privacy**, dovute all'adozione di sistemi non aggiornati e alla mancata adozione di misure di sicurezza adeguate a garantire la sicurezza delle reti informatiche.

Le strutture sanitarie in questione non hanno potuto accedere al sistema ed erogare alcuni servizi sanitari ai loro assistiti.

Il Garante Privacy ha sanzionato per 75mila euro una ASL

Il motivo? Non aver configurato correttamente le **modalità di accesso** al dossier sanitario elettronico (**Dse**). L'Autorità si è attivata a seguito di alcuni reclami e segnalazioni che lamentavano «il trattamento illecito di dati personali effettuato tramite il sistema di archiviazione e refertazione delle prestazioni erogate dall'azienda sanitaria». In particolare, una professionista dell'ASL in questione era infatti riuscita a visionare gli esami di laboratorio dell'ex marito a sua insaputa pur essendo quest'ultimo non in cura da lei.

E ciò è avvenuto in **violazione** di quanto stabilito dal Garante Privacy con le **“Linee guida in materia di Dossier sanitario”** del giugno 2015, con cui l'Autorità ha stabilito che «il titolare del trattamento deve porre particolare attenzione nell'individuazione dei profili di autorizzazione, adottando modalità tecniche di autenticazione al dossier che rispecchino le casistiche di accesso proprie di ciascuna struttura garantendo che l'accesso al dossier sia limitato al solo personale sanitario che interviene nel tempo nel processo di cura del paziente».

Oltre ad applicare la **sanzione amministrativa**, l'Autorità ha dunque ordinato all'ASL di mettere in atto tutte le misure tecniche e organizzative necessarie per garantire la sicurezza dei dati personali trattati e scongiurare nuovi accessi abusivi.

Trasparenza online: il sì del Garante ad ANAC su 14 schemi standard di pubblicazione che dettano le regole alla PA

Ma è necessario, comunque, **innalzare il livello di tutela** e valutare l'opportunità di prevedere un periodo transitorio per consentire alle pubbliche amministrazioni di uniformarsi progressivamente e gradualmente alle nuove modalità di pubblicazione sui siti web istituzionali.

Al fine di **garantire la riservatezza** degli interessati ed evitare il **rischio** di eventuali sanzioni per **violazione** della normativa **privacy**, le PA dovranno «limitarsi, fra l'altro, a pubblicare nella sezione “amministrazione trasparente” dei rispettivi siti web solo dati necessari, come ad es., il numero di telefono, l'indirizzo email e PEC dell'ufficio - e non i dati del dipendente - cui il cittadino può rivolgersi per richieste all'amministrazione. E negli esiti dei concorsi pubblici dovranno pubblicare il nome, il cognome, (la data di nascita, in caso di omonimia) e la posizione in graduatoria dei vincitori e degli idonei dichiarati vincitori a seguito dello scorrimento della graduatoria». Sarà inoltre necessario «oscurare i dati identificativi dei destinatari di benefici economici inferiori a mille euro nell'anno solare e in ogni caso se dalla pubblicazione è possibile ricavare informazioni relative allo stato di salute o alla situazione di disagio economico-sociale».

Intercettazioni della Procura UE: via libera del Garante Privacy al data base nazionale

Lo schema di decreto del Ministro della Giustizia, esaminato dal Garante, disciplina «le modalità di conservazione e di consultazione dei dati contenuti nell'archivio e i soggetti legittimati all'accesso mediante le postazioni istituite presso le sedi di servizio dei Procuratori europei delegati». Potranno dunque accedere all'**archivio nazionale** «il giudice che procede e i suoi ausiliari; il pubblico ministero e i suoi ausiliari, ivi compresi gli ufficiali di polizia giudiziaria delegati all'ascolto; i difensori delle parti assistiti, se necessario, da un interprete».

Nel rilasciare parere favorevole sullo schema di decreto, il Garante ha ritenuto che «lo stesso **non** presenti particolari **criticità** sotto il profilo della protezione dei dati, ma ha comunque richiesto – in analogia con i sistemi nazionali - che venga previsto, riguardo ai flussi informativi e la memorizzazione dei dati, il ricorso a tecniche crittografiche, utilizzando protocolli di rete sicuri e algoritmi di cifratura robusti, anche tenendo conto di eventuali raccomandazioni fornite dall'Agenzia per la **cybersicurezza nazionale**».

Infine, l'Autorità ha richiesto di «adottare procedure di **autenticazione informatica a più fattori**, con credenziali e dispositivi di autenticazione assegnati all'utente e auspicabilmente gestiti direttamente dal Ministero della giustizia».

Lo schema di decreto dovrà infine contenere misure volte a **garantire la continuità operativa e il disaster recovery** (ripristino dei sistemi), «nonché rilevare, tramite specifici alert, comportamenti anomali o a rischio, prevedendo il tracciamento delle operazioni compiute e audit con cadenza almeno annuale».