ATTACCO HACKER AI SISTEMI INFORMATICI DELLA REGIONE LAZIO

Inizio: 2021

Esito: 21 marzo 2024, doc. web n. 10002324, 10002533, 10002287

Principio GDPR violato: Integrità e Riservatezza (Articolo 5(1)(f) del GDPR)

Parole chiave: sicurezza, notifica, riservatezza, integrità.

Il **21 marzo 2024**, sono stati emessi tre provvedimenti da parte del Garante per la Protezione dei Dati Personali riguardanti la Regione Lazio, LAZIOcrea S.p.A., e l'Azienda Sanitaria Locale Roma 3, a seguito di violazioni nel trattamento dei dati personali.

1. **Regione Lazio**: È stata sanzionata con una multa di **120.000** euro per violazioni relative al trattamento illecito di dati personali, inclusa la **mancata adozione di misure adeguate a garantire la sicurezza e la protezione dei dati** contro trattamenti non autorizzati o illeciti e contro la perdita, distruzione o danneggiamento accidentali.
2. **LAZIOCrea S.p.A.**: Questa società, interamente partecipata dalla Regione Lazio e **responsabile per il trattamento dei dati** per conto della Regione e di diversi enti del servizio sanitario regionale, è stata sanzionata con una multa di **271.000** euro per trattamento illecito di dati personali, violando principi chiave del GDPR come l'integrità e la riservatezza, nonché per **non aver adottato misure tecniche e organizzative adeguate a garantire un livello di sicurezza appropriato al rischio.**
3. **ASL Roma 3**: È stata multata con **10.000** euro per non aver adottato misure tecniche e organizzative adeguate a garantire un livello di sicurezza appropriato al rischio, in particolare per la **violazione dell'art. 33, paragrafi 1 e 5, del GDPR.**

Questi provvedimenti sono stati presi in seguito a notifiche di violazione dei dati personali trasmesse dalla Regione Lazio e da LazioCrea, indicate come risultato di attacchi informatici. Il Garante ha richiesto informazioni e condotto ispezioni, stabilendo infine che le entità coinvolte non avevano adottato misure adeguate a proteggere i dati personali trattati.

Perchè LAZIOcrea è stata punita più delle altre?

LAZIOcrea S.p.A. è stata punita con una multa significativamente più alta rispetto alle altre entità per diverse ragioni, principalmente legate alla **natura** e alla **gravità** delle violazioni, al **numero di soggetti interessati**, e al **tipo di dati personali coinvolti**. Motivi chiave:

1. **Ruolo Centrale nella Gestione dei Dati**: LAZIOcrea S.p.A., agendo come responsabile del trattamento per conto della Regione Lazio, aveva un ruolo centrale nella gestione dei sistemi informativi e nel trattamento dei dati personali. Questo ruolo implicava una **responsabilità maggiore** nella protezione dei dati.

2. **Natura e Gravità delle Violazioni**: La società è stata ritenuta responsabile di violazioni che implicavano una **mancanza significativa di misure tecniche e organizzative** per garantire la sicurezza dei dati. Questo includeva la mancata protezione contro l'accesso non autorizzato e il rischio di perdita, distruzione o danneggiamento dei dati, soprattutto dati sensibili legati alla salute degli individui.
3. **Dati Sensibili Coinvolti**: I sistemi gestiti da LAZIOcrea contenevano dati personali estremamente sensibili, inclusi dati relativi alla salute dei cittadini. La violazione di dati così delicati è considerata particolarmente grave, dato l'alto rischio di danni significativi per gli individui coinvolti.
4. **Volume dei Dati e Numero di Interessati**: La violazione ha potenzialmente impattato un vasto numero di individui, data la portata dei servizi gestiti da LAZIOcrea per conto della Regione Lazio.
5. **Mancato Rispetto del GDPR**: LAZIOcrea è stata ritenuta non conforme a diversi principi fondamentali del GDPR, inclusa la mancanza di adeguate misure di sicurezza, che ha rappresentato un fattore chiave nella determinazione dell'entità della sanzione.

Questi fattori, combinati con le responsabilità dirette di LAZIOcrea nella gestione dei dati e nelle relative violazioni, hanno portato a una sanzione più elevata rispetto alle altre entità coinvolte, riflettendo la gravità delle violazioni e il ruolo centrale di LAZIOcrea nella loro occorrenza.

La regione Lazio cosa c'entra in tutto ciò?

La Regione Lazio è stata coinvolta in questa vicenda perché LAZIOcrea S.p.A., la società sanzionata con la multa più elevata, agiva come responsabile del trattamento per conto della Regione e di vari enti del servizio sanitario regionale. In altre parole, LAZIOcrea gestiva i sistemi informativi e trattava i dati personali per conto della Regione Lazio, tra gli altri, svolgendo quindi un ruolo centrale nella gestione dei dati e nei sistemi informatici regionali.

La Regione Lazio, in quanto ente pubblico che aveva delegato importanti funzioni di trattamento dei dati a LAZIOcrea, è stata considerata responsabile **per non aver verificato che LAZIOcrea adottasse tutte le misure necessarie per garantire la protezione dei dati personali trattati**. Questo includeva la **responsabilità di supervisionare** che fossero in atto misure tecniche e organizzative adeguate a prevenire accessi non autorizzati, perdite, distruzioni o danneggiamenti dei dati.

Quindi:

1. La Regione Lazio, in qualità di titolare del trattamento dei dati personali dei cittadini, **aveva la responsabilità ultima** di garantire la conformità al GDPR e la sicurezza dei dati personali.
2. L'attacco informatico e le violazioni dei dati hanno avuto **un impatto diretto sui servizi offerti dalla Regione Lazio** ai cittadini, inclusi servizi sanitari essenziali. Ciò ha

evidenziato la necessità di una gestione più stringente della sicurezza informatica e della protezione dei dati all'interno dell'amministrazione regionale.

In conclusione, la Regione Lazio è stata coinvolta in quanto entità che aveva affidato a LAZIOcrea compiti rilevanti per il trattamento dei dati personali, trovandosi quindi a dover rispondere delle mancate misure di sicurezza che hanno portato alle violazioni.

Cosa c'entra ASL Roma 3 nella vicenda?

L'Azienda Sanitaria Locale Roma 3 (ASL Roma 3) è coinvolta nella vicenda principalmente perché i suoi dati sono stati compromessi nell'attacco informatico che ha colpito i sistemi gestiti da LAZIOcrea S.p.A, **essendo uno degli enti del servizio sanitario regionale per i quali LAZIOcrea trattava i dati**, l'ASL Roma 3 è stata direttamente impattata dalla violazione di sicurezza.

Motivi specifici del coinvolgimento dell'ASL Roma 3 includono:

1. L'ASL Roma 3, **come ente sanitario, detiene e gestisce dati sanitari sensibili** per la popolazione che serve. **La gestione di questi dati era in parte affidata a LAZIOcrea, che fungeva da responsabile del trattamento per conto dell'ASL**.
2. L'attacco informatico a LAZIOcrea ha avuto **conseguenze dirette sull'operatività dell'ASL**, potenzialmente compromettendo la disponibilità e l'integrità dei dati sanitari dei pazienti. Questo ha implicazioni non solo per la sicurezza dei dati ma anche per la continuità dei servizi sanitari.
3. È emerso che ASL Roma 3 **non ha notificato tempestivamente il data breach all'Autorità Garante per la Protezione dei Dati Personali**, come richiesto dal GDPR. Questo ha portato a una sanzione pecuniaria perché la notifica di tali violazioni è obbligatoria quando il data breach può presentare un rischio per i diritti e le libertà delle persone fisiche.

In sintesi, l'ASL Roma 3 è stata implicata nella vicenda a causa delle sue connessioni dirette con i sistemi e i dati gestiti da LAZIOcrea e per le ripercussioni che l'attacco informatico ha avuto sui suoi servizi sanitari, nonché per la sua gestione della violazione dei dati personali.

Il principio GDPR più violato dai rispettivi attori.

Integrità e Riservatezza (Articolo 5(1)(f) del GDPR): Questo principio richiede che i dati personali siano trattati in modo da garantire un'adeguata sicurezza dei dati personali, inclusa la protezione contro il trattamento non autorizzato o illecito e contro la perdita, distruzione o danneggiamento accidentali, utilizzando misure tecniche o organizzative appropriate.

Violazioni specifiche includono:

1. **Mancanza di Misure di Sicurezza Adeguate**: LAZIOcrea e la Regione Lazio non avevano implementato misure tecniche e organizzative sufficienti per garantire un livello di sicurezza adeguato al rischio presentato dalla natura, dall'ambito di applicazione, dal

contesto e dalle finalità del trattamento, nonché dal rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.

2. **Risposta Inadeguata agli Incidenti**: La mancata risposta tempestiva e adeguata all'attacco informatico, nonché la mancata notifica della violazione dei dati all'Autorità Garante nei tempi previsti (come nel caso dell'ASL Roma 3), sono stati segni di non conformità con i requisiti di integrità e riservatezza del GDPR.
3. **Incapacità di Prevenire Accessi Non Autorizzati**: I dettagli dell'attacco informatico suggeriscono che non erano in atto controlli sufficienti per impedire l'accesso non autorizzato ai dati personali. Questo ha portato alla compromissione di dati sensibili e alla violazione della loro integrità e riservatezza.

Implicazioni: La violazione di questo principio è particolarmente grave, poiché mina direttamente la sicurezza dei dati personali degli individui coinvolti e può portare a conseguenze legali significative sotto forma di sanzioni pecuniarie, come visto nelle multe imposte da GDPR. Inoltre, danneggia la fiducia del pubblico nelle capacità dell'organizzazione di proteggere i dati sensibili, potenzialmente portando a una perdita di clientela o utenti e ad azioni legali da parte degli individui interessati.