MONITORAGGIO NORMATIVO PRIVACY

ULTIME NOTIZIE DAL MONDO PRIVACY

Gentilissimi,
vogliamo condividere con voi le ultime notizie e i provvedimenti più significativi che riguardano il mondo Privacy. In un'epoca in cui la protezione dei dati personali è di cruciale importanza, è fondamentale rimanere costantemente aggiornati sulle ultime tendenze per affrontare con successo le sfide legate alla protezione dei dati e al loro uso responsabile.
Di seguito un estratto delle notizie.

Buona lettura!

Data Breach

"**L'Ordine degli Psicologi della Regione Lombardia**, a novembre del 2023, è stato **vittima di un attacco ransomware** da parte dell'associazione criminale NoEscape che ha provocato: l'accesso abusivo alla rete informatica; la cifratura dei dati; e la cancellazione dei backup (successivamente recuperati).
I cyber criminali, a causa del mancato pagamento del riscatto **hanno pubblicato sul dark web i dati esfiltrati.**
L'Ordine ha notificato all'Autorità la violazione subita e ha precisato che: non c'è stata perdita di integrità e disponibilità dei dati; tutti gli archivi sono stati completamente ripristinati, grazie a dei salvataggi in cloud realizzati da un fornitore e grazie ai backup presenti su dischi esterni USB conservati in cassaforte.
Dalla documentazione prodotta è emerso che **la violazione ha coinvolto circa 15.000 registrazioni di dati personali**, e che l'attacco ha riguardato non solo **dati anagrafici** ma anche dati appartenenti a **categorie particolari**, come i dati relativi all'origine razziale o etnica, alle convinzioni religiose o filosofiche, all'appartenenza sindacale, alla vita o all'orientamento sessuale, allo stato di salute, nonché dati relativi a condanne penali e reati.
A causa di questo attacco gli interessati sono stati esposti a rischi di discriminazione, furto d'identità, frodi, rischi reputazionali e altri pregiudizi attinenti alla sfera economica e sociale.
Dall'istruttoria è emerso che **l'Ordine: non aveva adottato misure adeguate a rilevare tempestivamente le violazioni dei dati personali** sulla base di comportamenti anomali risultanti dagli accessi alla rete aziendale; **non aveva adottato misure adeguate a garantire la sicurezza dei sistemi** di trattamento. In particolare, non aveva adottato un sistema di autenticazione a più fattori (MFA), che avrebbe potuto impedire l'accesso non autorizzato ai sistemi anche a fronte della compromissione delle credenziali di autenticazione.
Alla luce di quanto rilevato, **il Garante ha sanzionato l'Ordine degli Psicologi della Regione Lombardia per 30 mila euro**."

Per ulteriori approfondimenti, si rimanda al relativo link.

News Italia:

Attacchi informatici alla sanità

"Negli ultimi anni sono aumentati in maniera esponenziale gli **attacchi informatici nell'ambito sanitario**. L'aumento di tali attacchi, secondo l'Agenzia per la Cybersicurezza Nazionale (ACN), è causato da una **scarsa formazione del personale** preposto all'attività di gestione dei sistemi informatici e da **inadeguate pratiche di sicurezza**. L'Agenzia europea ENISA ha evidenziato come il settore sanitario, a causa della sensibilità dei dati trattati, è tra i più vulnerabili. Infatti, dal 2023 al 2024 si è registrato **un incremento del 111% degli attacchi**, e le minacce più ricorrenti riguardano attacchi ransomware, malware e compromissioni di credenziali. L'ACN, per mitigare e contrastare le vulnerabilità, mette a disposizione delle **raccomandazioni che illustrano un approccio programmatico**, basato sulla gestione del rischio e sulla separazione dei ruoli. Inoltre, particolare attenzione è rivolta alla **formazione del personale** e all'adozione di **tecnologie avanzate**, a tal fine sono stati organizzati degli **incontri formativi**."

Per ulteriori approfondimenti, si rimanda al relativo link.

E-mail dei dipendenti: sanzione di 50 mila euro del Garante per la Regione Lombardia

"Il Garante per la Protezione dei Dati Personali ha sanzionato la Regione Lombardia, per 50 mila euro, a causa di numerose violazioni privacy afferenti **i log di navigazione in Internet e i metadati delle e-mail dei dipendenti**. In particolare, dall'istruttoria del Garante privacy è emerso che **la Regione**, senza previa stipula di un accordo collettivo con le rappresentanze sindacali e in assenza di adeguate garanzie a tutela dei lavoratori, **raccoglieva e conservava i log di navigazione in Internet dei dipendenti**, entrando in possesso di informazioni di carattere privato e non lavorativo. Peraltro, la Regione aveva iniziato un processo di adeguamento rispetto alle indicazioni fornite dal Garante sul tema, ma ciò non è stato sufficiente. Infatti, l'Autorità ha imposto non solo una **sanzione amministrativa** ma anche una serie di **misure correttive**, quali: **l'anonimizzazione dei log** relativi ai tentativi di accesso falliti ai siti web censiti nella black-list; **la cifratura del dato** concernente i nomi dei dipendenti assegnatari dei pc portatili; **la riduzione del termine di conservazione di tali dati**. Quindi, da tale provvedimento sanzionatorio, emerge che il datore di lavoro può raccogliere i log di navigazione in Internet e i metadati delle e-mail dei dipendenti a patto che vi siano specifiche condizioni e garanzie."

Per ulteriori approfondimenti, si rimanda al relativo link.

Cybersicurezza: sensibilizzazione dei cittadini

"L'Agenzia per la Cybersicurezza Nazionale (ACN) e il Dipartimento per la Trasformazione Digitale (DTD) hanno stipulato un **Protocollo d'intesa** volto a **rafforzare la consapevolezza e le competenze digitali dei cittadini** in tema di cybersicurezza. L'iniziativa si inserisce nel PNRR (Piano Nazionale di Ripresa e Resilienza) e coinvolge: oltre **3.300 "Punti Digitale Facile"; gli Operatori volontari del Servizio Civile Digitale; e oltre 280 Organizzazioni della Coalizione Nazionale** per le competenze digitali. Il primo passo dell'iniziativa prevede un percorso di formazione, per gli operatori dei **Punti di facilitazione digitale**, tramite l'erogazione da parte di ACN di **4 webinar** relativi alle seguenti tematiche: *1) introduzione alla cybersicurezza; 2) la minaccia del phishing e le modalità di prevenzione; 3) gli acquisti online; 4) i comportamenti virtuosi da attuare per la mitigazione dei rischi di profilazione degli utenti nella navigazione online*. Inoltre, ai Facilitatori, Operatori Volontari e Organizzazioni della Coalizione sarà fornito anche **materiale formativo di supporto.** Nello svolgimento della campagna di sensibilizzazione, al fine di promuovere le attività, **DTD e ACN utilizzeranno anche i propri canali social**."

Per ulteriori approfondimenti, si rimanda al relativo link.

News Europa:

Attenzione alla Privacy by design e by default

“In data 27 febbraio 2025, l'Autorità di controllo slovena ha emesso un rimprovero formale nei confronti di una scuola slovena e del suo dirigente, dopo aver rilevato **gravi carenze in materia di protezione dati**. In particolare, l'istituto **non aveva implementato le adeguate misure di sicurezza di cui all’art. 25 del GDPR** ("privacy by design" e "by default"). La scuola aveva affidato al **fornitore esterno** del servizio mensa l'accesso **all'intero database** degli studenti, contenente anche categorie particolari di dati come: informazioni sui sussidi e sui saldi dei conti. Tuttavia, **per svolgere il servizio, il fornitore necessitava solo dei dati anagrafici** degli studenti per il conteggio dei pasti e non anche degli ulteriori dati. L'Autorità, a seguito della notifica della violazione da parte della scuola, ha avviato l'istruttoria d'ufficio, dalla quale è emerso che **il fornitore ha utilizzato impropriamente e illegittimamente i dati.** La scuola, peraltro, anche in seguito alla violazione, non ha implementato misure di sicurezza efficaci a fronteggiare le cause dell'incidente e a prevenire il ripetersi dell'evento. Infatti, come rilevato dal tribunale locale, **la corretta applicazione dell'art. 25 del GDPR avrebbe potuto prevenire l’incidente.** Il caso dimostra l'importanza dell'adozione di protocolli per la protezione dei dati personali nelle istituzioni scolastiche, al fine di assicurare la sicurezza e l'integrità dei dati personali degli studenti.”

Per ulteriori approfondimenti, si rimanda al relativo link.

Le Guide della CNIL per riconoscere una violazione dei dati personali

“Negli ultimi cinque anni la CNIL ha ricevuto 30 segnalazioni di violazioni di dati personali. Tuttavia, secondo l’Autorità, tale dato non corrisponde a quanto accade realmente. Infatti, **per la CNIL, le violazioni spesso non sono segnalate**, talvolta **per la difficoltà di riconoscere una violazione di dati personali, e altre volte perché la procedura da seguire in caso di data breach è sconosciuta.** Così, la CNIL ha messo a disposizione delle **guide pratiche**, rivolte ai responsabili della protezione dei dati, ai dirigenti e al personale amministrativo degli istituti scolastici. Le guide, riportando **cinque situazioni tipiche**, aiutano a riconoscere una violazione di dati personali, le azioni da intraprendere in caso di incidenti e le misure tecniche e organizzative da adottare per evitare successive violazioni.”

Per ulteriori approfondimenti, si rimanda al relativo link.

Protezione per i dati biometrici

“Il 12 giugno 2025 l'Autorità per la Protezione dei Dati Personali Irlandese (Data Protection Commission - DPC) ha concluso l'indagine avviata nel luglio 2021 nei confronti del Dipartimento della Protezione Sociale (Department of Social Protection - DSP) per **l'uso di tecnologie di riconoscimento facciale** (SAFE 2 registration), utilizzate per il rilascio della Public Services Card (Carta dei Servizi Pubblici). In particolare, la registrazione SAFE 2 è obbligatoria per ottenere la Carta dei Servizi Pubblici e tale registrazione comporta la raccolta, la conservazione e il **trattamento, su larga scala, di dati personali** altamente sensibili, inclusi quelli **biometrici.** Infatti, dall'indagine è emerso che nel 2021 il **DSP conservava i dati biometrici del 70% della popolazione** dello Stato. Dall'indagine, inoltre, è emerso la violazione degli articoli 5, 6, 9, 13 e 35 del GDPR. Alla luce delle suddette violazioni l'Autorità ha: ammonito il DSP; inflitto una sanzione amministrativa di 550 mila euro; ordinato al DSP di interrompere, in caso di mancata identificazione della corretta base giuridica, il trattamento dei dati biometrici entro 9 mesi dalla decisione.”

Per ulteriori approfondimenti, si rimanda al relativo link.