MONITORAGGIO NORMATIVO PRIVACY

ULTIME NOTIZIE DAL MONDO PRIVACY

Gentilissimi,
vogliamo condividere con voi le ultime notizie più significative 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!

Italia:

Il Garante: no ai dati sulla salute per i certificati di assenza dal lavoro

"Il Garante, sanzionando un'Azienda Sanitaria Territoriale, ha ribadito che i certificati per assenza dal lavoro o di impossibilità di partecipare ad un concorso non devono riportare informazioni che possono far risalire allo stato di salute, come le indicazioni della struttura presso la quale è stata erogata la prestazione sanitaria e il timbro con la specializzazione del medico. L'Autorità, infatti, a seguito del reclamo di una paziente, ha appurato che il certificato per assenza dal lavoro indicava il reparto che aveva erogato la prestazione sanitaria, violando così il principio di minimizzazione dei dati personali e ha omesso di mettere in atto, fin dalla progettazione, misure tecniche ed organizzative adeguate volte a proteggere i dati e i diritti degli interessati violando così il principio di privacy by design."

Per ulteriori approfondimenti, si rimanda al relativo link.

Telemarketing e sanzione del Garante

"Illumia S.p.a, società operante nel mondo della fornitura dei servizi di luce e gas, è stata sanzionata dal Garante per la protezione dei dati personali per 678.897 euro. L'Autorità, al termine dell'istruttoria originata dai reclami degli utenti che lamentavano la ricezione di chiamate indesiderate, ha riscontrato molte criticità come: - l'assenza di un'idonea base giuridica; - la mancanza di controlli lungo tutta la filiera; - l'implementazione tardiva di alcune misure tecnico-organizzative rispetto all'entrata in vigore del Regolamento Ue."

Per ulteriori approfondimenti, si rimanda al relativo link.

Azienda ospedaliera sanzionata dal Garante

"Un'Azienda ospedaliero-universitaria, a dicembre del 2022, aveva subito un attacco hacker ai sistemi informativi. Il data breach è stato cagionato da un malware di tipo ransomware che si è introdotto nei sistemi attraverso l'accesso a un PC aziendale con VPN aperta, e ha comportato la perdita di riservatezza, integrità e disponibilità dei dati personali di dipendenti, consulenti e pazienti. A seguito della notifica dell'Azienda, il Garante ha appurato che sussistevano delle carenze relative agli obblighi di sicurezza dettati dal Regolamento europeo, in particolare: i sistemi adottati non erano aggiornati e le misure erano inadeguate a rilevare tempestivamente le violazioni di dati e a garantire la sicurezza delle reti informatiche. Infatti, venivano utilizzati dei software obsoleti, che non prevedevano aggiornamenti di sicurezza e alert a copertura h24, ciò ha favorito il verificarsi dell'attacco hacker. Per queste ragioni il Garante per la protezione dei dati personali ha inflitto una sanzione di 25 mila euro all'Azienda."

Per ulteriori approfondimenti, si rimanda al relativo link.

APP IO e IT -Wallet

"Dal 4 Dicembre 2024 tutti i cittadini italiani hanno la possibilità di utilizzare It-Wallet il "portafogli digitale" che consente di memorizzare sul telefono, attraverso l'app IO, alcuni documenti, come la patente, la tessera sanitaria e in futuro anche la carta d'identità. Un'innovazione che mira a semplificare la vita agli utenti. Per quanto riguarda il livello di sicurezza all'app IO si accede con lo SPID o CIE, una modalità di accesso che garantisce un buon livello di sicurezza soprattutto se si accede con SPID dallo smartphone, perché evita l'inserimento delle credenziali e riduce il rischio che username e password possano essere sottratti da attacchi phishing. I documenti inseriti nel "portafogli digitale" integrano un certificato di autenticità attraverso un QR Code temporaneo, generato dall'app IO, e che una volta inquadrato conduce al sito del Poligrafico e Zecca dello Stato che conferma la validità del documento. Problemi di protezione dei dati possono sorgere nei casi in cui ci sia una verifica dell'identità "a distanza" e si devono semplicemente inserire i dati del documento. I rischi per la sicurezza relativi a It-Wallet non derivano tanto dalle caratteristiche tecniche dell'applicazione, ma dall'attenzione che gli utenti impiegheranno nell'utilizzo dello strumento."

Per ulteriori approfondimenti si rimanda al relativo link.

Data breach di Infocert S.p.a

"Infocert S.p.a, provider italiano di servizi di identità digitale SPID, il 27 Dicembre 2024 ha subito un grave data breach. La violazione ha coinvolto un fornitore terzo che gestiva le richieste di assistenza clienti, tuttavia, l'attacco non ha compromesso i sistemi interni di InfoCert. L'hacker ha pubblicato su un forum del deep web un annuncio per la vendita di informazioni relative a 5,5 milioni di utenti InfoCert. Le informazioni riguardano nome e cognome degli utenti, gli indirizzi e-mail, i numeri di telefono. L'attacco è stato realizzato sfruttando la vulnerabilità del sistema di ticketing. InfoCert ha notificato l'incidente al Garante per la Protezione dei Dati Personali e avviato delle indagini interne per verificare con esattezza la portata del danno."

Per ulteriori approfondimenti si rimanda al relativo link.

Europa:

EDPB e i sistemi di intelligenza artificiale

"L'introduzione delle nuove tecnologie ha generato una serie di incertezze interpretative e il Comitato Europeo per la Protezione dei Dati (EDPB), con il parere 28/2024, affronta una questione cruciale per la tutela dei dati personali nell'era dell'intelligenza artificiale. In particolare, il documento affronta questioni chiave come: - l'anonimizzazione dei modelli IA; - l'uso legittimo dei dati attraverso il principio dell'interesse legittimo; - le conseguenze di un trattamento illecito dei dati. La possibilità che un modello di IA possa conservare tracce di dati personali o risultare suscettibile di re-identificazione, solleva interrogativi che si riflettono non solo sulla legalità del trattamento ma anche la sua moralità e la sua compatibilità con i principi costituzionali di dignità e libertà individuale. Un modello IA non può essere considerato anonimo se, seppur indirettamente, è possibile estrarre dati personali dai parametri del modello con delle tecniche avanzate di inferenza. L'EDPB ritiene che l'anonimizzazione debba essere valutata caso per caso, e che i titolari del trattamento hanno l'obbligo di dimostrare che il trattamento dei dati sia stato eseguito in modo tale da garantire che non si possa risalire agli individui a cui i dati appartengono. Viene, altresì, evidenziato che il concetto di "legittimo interesse" deve sempre essere valutato con estrema attenzione, soprattutto in contesti relativi all'uso di IA. Inoltre, il rispetto del principio di proporzionalità è di cruciale importanza, infatti il trattamento dei dati non deve essere solo legittimo, ma anche adeguato e necessario rispetto agli scopi perseguiti."

Per ulteriori approfondimenti, si rimanda al relativo link.

Netflix sanzionata

"Netflix raccoglie e memorizza vari tipi di dati degli utenti, come gli indirizzi email, i numeri di telefono, i dettagli di pagamento ma soprattutto memorizza tutto ciò che gli utenti guardano sulla piattaforma. Dell'utilizzo di questi dati e dell'eventuale condivisione degli stessi da parte del gigante dello streaming non sono stati correttamente informati gli utenti, ragion per cui Netflix è stato multato per 4,75 milioni di euro dal Garante della privacy olandese per non aver informato correttamente gli utenti sull'utilizzo dei loro dati tra il 2018 e il 2020."

Per ulteriori approfondimenti, si rimanda al relativo link.

Consiglio d'Europa: metodologia HUDERIA per la valutazione del rischio e dell'impatto dei sistemi di AI

"Il 28 Novembre 2024 il Committee on Artificial Intelligence (CAI) del Consiglio d'Europa ha adottato la metodologia HUDERIA che mira a delineare un approccio strutturato per la valutazione del rischio e dell'impatto dei sistemi di intelligenza artificiale (IA) dal punto di vista dei diritti umani (human rights – HU), della democrazia (democracy – DE) e dello Stato di diritto (rule of law – R) ("HUDERIA"). La metodologia, che può essere utilizzata sia da attori pubblici che privati, serve ad identificare e affrontare i rischi e gli impatti sui diritti umani, la democrazia e lo Stato di diritto durante l'intero ciclo di vita dei sistemi di IA. Nel 2025 saranno pubblicati dei "HUDERIA Model", ovvero delle risorse di supporto (come strumenti flessibili per implementare i diversi elementi del processo HUDERIA e raccomandazioni scalabili) che aiuteranno ad implementare la metodologia in contesti specifici. In particolare, queste risorse forniranno una biblioteca di conoscenze volte a facilitare la considerazione dei rischi e degli impatti legati ai diritti umani, alla democrazia e allo Stato di diritto."

Per ulteriori approfondimenti, si rimanda al relativo link.

Resto del mondo:

Thailandia: il PDPC chiarisce i requisiti per la notifica delle violazioni dei dati

"Il Comitato per la Protezione dei Dati Personali ha emesso dei chiarimenti rispetto agli obblighi di segnalazione delle violazioni dei dati. In particolare, si offre una guida per le organizzazioni che mirano a soddisfare i requisiti di notifica delle violazioni del PDPA. Il PDPC ha spiegato che i titolari del trattamento dei dati sono tenuti a notificare al PDPC una violazione dei dati personali senza indebito ritardo e, quando possibile, entro 72 ore dalla presa di coscienza della violazione, ma questo obbligo non si applica se la violazione non comporta rischi per i diritti e le libertà degli individui. In tali casi, i titolari del trattamento non sono tenuti a notificare il PDPC. Per essere esentati dalla notifica i titolari del trattamento devono, però, condurre una valutazione del rischio e se la valutazione determina che la violazione non ha il potenziale di influenzare i diritti o le libertà degli individui, l'obbligo di segnalare la violazione viene annullato. Le organizzazioni devono sempre documentare anche gli incidenti minori e conservare le relative valutazioni del rischio come prova di conformità in caso di future indagini o reclami."

Per ulteriori approfondimenti, si rimanda al relativo link.

Australia: Facebook paga una sanzione di circa 30 milioni di euro

"Per chiudere i procedimenti legali nati nell'ambito dello scandalo di Cambridge Analytica, Meta Platforms ha accettato di pagare la sanzione di 50 milioni di dollari australiani (pari a circa 30 milioni di euro), imposta dal Garante della Privacy australiano. In particolare, le violazioni contestate erano state segnalate per la prima volta all'inizio del 2018 dal Guardian, mentre l'Australia è stata coinvolta nella battaglia legale con Meta a partire dal 2020. I dati personali di 311.127 utenti australiani di Facebook erano stati "*esposti al rischio di essere divulgati*" a Cambridge Analytica, una società di consulenza, la quale li avrebbe poi utilizzati per scopi di profilazione."

Per ulteriori approfondimenti, si rimanda al relativo link.

India: Digital Personal Data Protection (Act) Rules

"Il Ministero indiano dell'Elettronica e delle Tecnologie dell'Informazione ha pubblicato la bozza delle Digital Personal Data Protection (Act) Rules, che integra il Personal Data Protection Act del 2023. La consultazione pubblica sarà aperta fino al 18 febbraio e costituisce un passo significativo nel campo della protezione dei dati personali. La bozza di tale regolamento si focalizza su numerosi aspetti, tra cui una maggiore trasparenza sulle attività di trattamento. Ciò significa che le aziende dovranno conformarsi a tali parametri privacy ed essere in grado di rilevare, valutare e coordinare gli incidenti di sicurezza. La bozza di regolamento rappresenta un significativo passo avanti per l'India che si allinea agli standard globali, ma al contempo si distingue, introducendo per le aziende nuove sfide di conformità, quali l'obbligo di notificare qualunque violazione dei dati personali a prescindere dalla gravità della violazione."

Per ulteriori approfondimenti, si rimanda al relativo link.