GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

GPDP newsletter

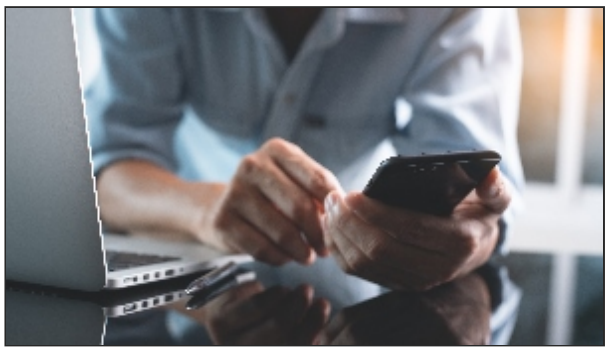
anno XXIII

NOTIZIARIO DEL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NEWSLETTER N. 472 del 25 gennaio 2021

Roma Capitale: sanzione del Garante privacy per "TuPassi"

Cittadini e dipendenti ignari su come venivano usati i loro dati



Il Garante per la protezione dei dati personali ha ordinato a Roma Capitale il pagamento di una sanzione di 500mila euro per illecito trattamento di dati personali di utenti e dipendenti, effettuato attraverso il sistema di prenotazione degli appuntamenti "TuPassi".

Il provvedimento di sanzione è stato adottato al termine di una complessa attività istruttoria avviata a seguito di controlli svolti dall'Autorità sulle app utilizzate dalla pubblica amministrazione per l'erogazione dei servizi, condotta anche in collaborazione con il Nucleo speciale tutela privacy e frodi tecnologiche della Guardia di finanza. Attività che aveva già portato all'adozione di un provvedimento nel marzo 2019 con il quale il Garante aveva dichiarato illeciti i trattamenti effettuati da Roma Capitale tramite "TuPassi e prescritto talune misure correttive.

Numerose le criticità rilevate sul sistema che consente agli utenti di prenotare servizi di sportello e appuntamenti, anche nel settore sanitario, utilizzando diversi canali: app mobile, sito internet, totem posizionati presso le Pa e i professionisti che erogano le prestazioni.

I trattamenti hanno infatti interessato un'ingente mole di dati personali, anche molto delicati perché relativi a prenotazioni di vari servizi e di prestazioni sanitarie. Il sistema consentiva, infatti, di acquisire e memorizzare sui server di Roma Capitale, per un lungo periodo di tempo, numerosi dati degli utenti relativi alle prenotazioni (tipo di prestazione, canale utilizzato, data e ora della prenotazione) e del personale impiegato nella gestione degli appuntamenti. In quest'ultimo caso, in particolare, il sistema registrava e generava report giornalieri contenenti anche informazioni di dettaglio sull'attività lavorativa (data, tipo di servizio, nominativo dell'addetto allo sportello, tempo di chiamata e tempo di attesa). Tutte le operazioni erano effettuate senza che né gli utenti né i dipendenti avessero ricevuto, come richiesto dal Regolamento Ue, un'informativa completa sui trattamenti resi possibili dall'applicativo.

Il Garante ha ritenuto, inoltre, inadeguate le misure tecniche e organizzative implementate dall'Ente, il quale non aveva altresì disciplinato il rapporto con la società fornitrice del sistema di prenotazione. Bocciata anche la funzione che consente di produrre report sull'attività degli addetti allo sportello, introdotta senza le necessarie garanzie previste dallo Statuto dei lavoratori sul controllo a distanza.

L'Autorità ha comminato, inoltre, con separato provvedimento una sanzione di 40mila euro alla società fornitrice del sistema per i trattamenti effettuati in qualità di autonomo titolare, in particolare, con riguardo alla prenotazione di servizi sanitari da parte degli utenti e alla manutenzione del sistema per conto dei clienti, nei casi in cui tale attività comportasse il trattamento di dati personali di utenti e dipendenti.

È stato inoltre adottato un provvedimento di avvertimento nei confronti della medesima società fornitrice e di tutti i soggetti pubblici e privati che utilizzano il sistema "TuPassi" in ordine alla possibilità che il suo utilizzo, con le modalità già censurate dal Garante, possa violare il Regolamento, ingiungendo alla società di avviare con loro i necessari aggiornamenti per rendere il sistema conforme alla disciplina in materia di protezione dati, secondo le indicazioni del Garante.

Si conclude così un procedimento complesso, aggravato dalle difficoltà operative derivanti dalle scelte organizzative dell'Ente, anche sotto il profilo della corretta individuazione della figura del Responsabile della protezione dei dati, soggetta ad avvicendamenti nel corso dell'istruttoria, circostanza che ha reso meno efficace la cooperazione con il Garante.

Telemarketing: Registro pubblico delle opposizioni, il regolamento si applica solo alle chiamate con operatore

I sistemi automatizzati di chiamata prevedono sempre il consenso dell'interessato

Il Garante privacy ha espresso parere favorevole al Ministero dello sviluppo economico su una versione aggiornata dello schema di regolamento del Registro pubblico delle opposizioni (Rpo), il servizio che permette di opporsi all'utilizzo per finalità pubblicitarie dei propri numeri di telefono. L'Autorità tuttavia ha chiesto di precisare che le nuove regole valgono solo per il telemarketing effettuato con chiamate tramite operatore. Le comunicazioni di marketing automatizzate, infatti, non possono in nessun caso effettuarsi senza il consenso esplicito dell'interessato.

Con il regolamento si dà attuazione alla riforma che prevede la possibilità per gli abbonati di iscrivere nel Registro tutte le numerazioni telefoniche nazionali fisse e mobili, che siano o meno riportate negli elenchi.

La nuova versione adegua il testo ai rilievi avanzati nei diversi pareri resi in materia dal Consiglio di Stato, dall'Agcom, dal Ministro per la Pa e da quello per l'innovazione tecnologica e la digitalizzazione, e recepisce, pressoché integralmente, le indicazioni rese dal Garante nel precedente parere sull'Rpo del 2019.

L'Autorità ha chiesto però di correggere il testo laddove individua tra gli ambiti di applicazione del regolamento i trattamenti di dati effettuati tramite "l'impiego del telefono". Occorre rispettare, precisa l'Autorità, la versione originaria dello schema, sulla quale il Garante ha reso il suo precedente parere, che si riferiva, per il telemarketing, solo ai trattamenti effettuati "mediante operatore umano con l'impiego del telefono".

L'articolo 130 del Codice, infatti, nel disciplinare tutte le comunicazioni indesiderate, distingue tra comunicazioni effettuate con modalità automatizzate e comunicazioni con l'intervento dell'operatore. Il decreto in esame, si inserisce solo ed esclusivamente in questa seconda categoria. Pertanto il Garante precisa come, allo stato attuale, non sia giuridicamente corretto estendere l'ambito dell'Rpo anche alle comunicazioni automatizzate, che prevedono sempre il consenso dell'interessato per il loro carattere invasivo.

Data breach: le istruzioni dei Garanti privacy Ue per gestire le violazioni di dati

Adottate le nuove linee guida, avviata una consultazione pubblica europea

Come procedere in caso di attacchi ransomware, di esfiltrazione di dati, di perdita o furto di dispositivi e documenti cartacei? A questa e ad altre domande rispondono le linee guida, adottate dall'Edpb (Comitato europeo per la protezione dei dati), per aiutare imprese e pubblica amministrazione ad affrontare correttamente le violazioni dei dati e definire i processi di gestione del rischio.

Le "Guidelines 01/2021 on Examples regarding Data Breach Notification", approvate nella riunione plenaria del 14 gennaio scorso, si basano sull'analisi dei casi più significativi di violazione dei dati - affrontati dai Garanti privacy nazionali, incluso quello italiano - subiti da banche, ospedali, medie imprese, municipalità, società che offrono servizi online di vario genere.

Sul documento l'Edpb ha avviato una consultazione pubblica per un periodo di sei settimane (fino al 2 marzo 2021).

Le linee guida presentano, per ciascuna casistica, esempi di buone o cattive pratiche, raccomandano modalità di identificazione e valutazione dei rischi (evidenziando i fattori che meritano particolare considerazione), indicano in quali casi chi tratta i dati deve notificare la violazione all'Autorità Garante e, se necessario, informare le persone coinvolte.

Tra le mancanze più frequenti ricordati dalle Linee guida vi è, ad esempio, l'omessa cifratura dei dati che consente a chi li acquisisce in maniera fraudolenta di consultare informazioni riservate. Potrebbe facilitare violazioni anche la non corretta gestione dell'autenticazione degli utenti a siti web, magari a causa dell'utilizzo di password deboli o conservate in chiaro. Nel settore bancario, potrebbe causare enormi danni l'impiego di identificativi di sessione all'interno degli indirizzi web degli utenti, informazioni che facilitano l'accesso illecito a contenuti che dovrebbero rimanere protetti. Drammatiche potrebbero essere le conseguenze di un attacco ransomware (un virus informatico che rende inservibili i dati fino al pagamento di un eventuale riscatto) ai referti e ad altri documenti dei pazienti di un ospedale, a meno che la struttura sanitaria non abbia provveduto a effettuare un backup separato dei dati. Non bisogna sottovalutare anche i problemi che può causare una semplice e-mail spedita ai destinatari sbagliati.

Il testo, che integra e aggiorna gli orientamenti già forniti negli anni passati dal Gruppo "Articolo 29", proprio per offrire un contributo concreto a imprese e Pa, analizza anche le misure adottate dai titolari del trattamento, prima di aver subito un data breach, per prevenire o attenuare i rischi di una potenziale violazione dei dati. E propone una lista di misure di prevenzione ai vari problemi rilevati.

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

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

- Tik Tok: dopo il caso della bimba di Palermo, il Garante privacy dispone il blocco del social - Comunicato del 22 gennaio 2021
- "I tuoi dati sono un tesoro": il video del Garante per raccontare cos'è la privacy - Comunicato del 21 gennaio 2021
- Fascicolo sanitario elettronico: nessuna scadenza per l'inserimento dei dati - Comunicato del 15 gennaio 2021
- Eddpb e Edps adottano pareri congiunti sulle nuove clausole contrattuali standard (Scc) proposte dalla Commissione - 15 gennaio 2021
- Whatsapp: Garante privacy, informativa agli utenti poco chiara. L'Autorità intenzionata ad intervenire anche in via d'urgenza - Comunicato del 14 gennaio 2021
- I neurodiritti al centro della Giornata europea della protezione dei dati. La privacy e i nuovi scenari posti dalle neuroscienze nel convegno organizzato dal Garante per la privacy il 28 gennaio - Comunicato del 12 gennaio 2021
- Call center Immuni: via libera del Garante privacy - Comunicato del 12 gennaio 2021
- Brexit: il punto sulle conseguenze della protezione dati - 7 gennaio 2021
- Covid: il Garante privacy scrive al Ministero dell'interno su controlli per Capodanno - Comunicato del 31 dicembre 2020
- Deepfake: dal Garante una scheda informativa sui rischi dell'uso malevolo di questa nuova tecnologia – 28 dicembre 2020
- Data breach: il Garante lancia un nuovo servizio online per semplificare gli adempimenti - 23 dicembre 2020

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*