GDPR/PAPERS.

La prima newsletter dedicata al sempre più importante tema del GDPR. Realizzata con lo Studio Legale Floreani, l'informativa è divisa in 3 sessioni: l'ABC della privacy, le domande più frequenti e le ultime novità in arrivo.

L'ABC della privacy

Firewall

E' una tecnologia di protezione che ha la funzione di filtrare e controllare il traffico dei dati in entrata e in uscita dai dispositivi o attraverso la rete e che svolge la funzione di impedire a determinati elementi/connessioni dannose di accedere ai sistemi.

Assistenti digitali (smart assistant)

Si tratta di programmi software installati sui dispositivi (per esempio, negli smartphone) che tramite algoritmi di intelligenza artificiale dialogano con gli esseri umani al fine di rispondere a richieste di informazioni o compiere determinate azioni (ad esempio: regolare la temperatura o l'illuminazione di una casa, attivare elettrodomestici, etc.).
(fonte: https://www.garanteprivacy.it/temi/assistenti-digitali)

Domande & Risposte

Marketing

L'utilizzo degli indirizzi Pec pubblicati online per attività di marketing. Quali sono le regole da seguire?

Alcune utili precauzioni da adottare sono le seguenti:
a) senza il consenso preventivo dell'interessato non è possibile inviare comunicazioni promozionali mediante strumenti automatizzati neanche nel caso in cui i dati personali siano tratti da registri pubblici, elenchi, siti web, atti o documenti conosciuti o conoscibili da chiunque;
b) analogamente, senza il consenso preventivo degli interessati, non è lecito utilizzare per inviare e-mail promozionali gli indirizzi Pec contenuti nell'indice nazionale degli indirizzi Pec delle imprese e dei professionisti.

Videosorveglianza

L'utilizzo dei sistemi di videosorveglianza e l'informativa da fornire agli interessati: quali sono gli step operativi da osservare?

a) in ottemperanza al principio di trasparenza cui all'art. 5 del GDPR, "gli interessati devono essere sempre essere informati che stanno per accedere in una zona videosorvegliata"; a questo scopo quindi il titolare del trattamento deve apporre idonei cartelli informativi;
b) gli interessati devono essere informati sul trattamento dei propri dati con un duplice livello di informazioni;
c) l'informativa di primo livello (o "di sintesi") deve essere posizionata in modo da permettere all'interessato di riconoscere facilmente le circostanze della sorveglianza, prima di entrare nella zona sorvegliata e deve contenere le informazioni più importanti (ad esempio, l'identità del titolare del trattamento, le finalità del trattamento, i diritti dell'interessato, il luogo e le modalità di pubblicazione dell'informativa di secondo livello);
d) l'informativa di secondo livello (o "estesa") deve riportare gli ulteriori dettagli obbligatori sulle caratteristiche dei trattamenti previsti dall'art. 13 del GDPR e deve essere messa a disposizione degli interessati entro l e aree videosorvegliate tramite un codice QR inserito nell'informativa "sintetica" oppure indicando un sito web o altro luogo dove l'interessato possa consultare agevolmente l'informativa (anche in formato cartaceo).

Videosorveglianza e Cybersecurity
Come faccio per prevenire i furti dei video?

1) La prima raccomandazione è quella di individuare per iscritto i soggetti autorizzati al trattamento delle immagini delle telecamere;
2) è fondamentale poi scegliere esclusivamente fornitori esterni dei servizi di sicurezza che presentino garanzie adeguate (si pensi, soprattutto, all'ipotesi in cui sia stato stipulato un contratto con un terzo che accede alle immagini acquisite tramite i sistemi di videosorveglianza da remoto) e che siano in grado di costruire un impianto compliant con il GDPR;
3) da ultimo, è indispensabile ottenere dal fornitore la documentazione relativa alle misure di sicurezza adottate a protezione dei dati e alla durata di conservazione delle immagini.

Le novità in pillole

Dark Pattern, dati e legal design: in arrivo le "best practices" dei Garanti Europei

Il 14 marzo scorso sono state adottate dall'EDPB (Comitato europeo per la protezione dei dati) le "Guidelines 03/2022" in materia di dark pattern.
I cosiddetti "percorsi oscuri", in particolare, sono quell'insieme di tecniche adottate dagli sviluppatori di piattaforme e siti web che inducono gli utenti on line ad adottare azioni non intenzionali e a prendere decisioni dannose in relazione al trattamento dei dati personali.
Le linee guida europee forniscono alcuni esempi sulle varie categorie di dark pattern nonché consigli pratici ai titolari del trattamento su come implementare le prassi di interazione on line con gli utenti in conformità con il GDPR.

L'invio di sms per il recupero dei consensi a fini di marketing: il recente intervento della Cassazione.

La Suprema Corte con l'ordinanza n. 9926 depositata il 28 marzo u.s. ha affermato che l'invio di sms diretti ad acquisire il consenso per l'esecuzione di attività di marketing nei confronti degli utenti che non hanno prestato il proprio consenso al trattamento dei dati per offerte commerciali al momento di stipula del contratto, rappresenta un'attività non conforme al framework normativo in materia, siccome costituente trattamento per finalità di marketing nei riguardi di chi non ha rilasciato il proprio preventivo e specifico consenso.

SCOPRI TUTTI I SERVIZI DEL GRUPPO SERMETRA