

Il primo periodico digitale per approfondire le novità in materia di GDPR, Privacy e Cybersecurity. Realizzato in collaborazione con lo Studio Legale Floreani e rivolto ai professionisti del mondo Automotive.

L'ABC della privacy e della cybersecurity



Sharenting

Con il termine "sharenting" si intende il fenomeno della condivisione online costante da parte dei genitori di contenuti che riguardano i propri figli/e (foto, video, ecografie). Il neologismo, coniato negli Stati Uniti, deriva dalle parole inglesi "share" (condividere) e "parenting" (genitorialità).

Dark Pattern

Vengono indicate quelle interfacce e quei percorsi di navigazione progettati per influenzare l'utente affinché intraprenda azioni inconsapevoli o non desiderate ma favorevoli all'interesse della piattaforma o del gestore del servizio.

Domande & Risposte



Come proteggersi dal phishing?

Tenere aggiornato sul pc o sullo smartphone in uso il programma antivirus che protegga anche dal phishing;

- controllare che sia attivato e verificarne le impostazioni;
- non memorizzare dati personali e codici di accesso nei browser utilizzati per navigare online;
- impostare password alfanumeriche complesse, cambiandole spesso e scegliendo credenziali diverse per ogni servizio utilizzato;
- prestare attenzione al mittente e al contenuto dei messaggi; capita spesso che contengano anche grossolani errori grammaticali, di formattazione o di traduzione da altre lingue.

Come faccio per gestire in modo "compliant" gli adempimenti GDPR?

La raccomandazione è quella di avvalersi di sistemi informatici e software CLOUD che consentano di semplificare la gestione degli adempimenti privacy e di gestire in modo sicuro e semplice la raccolta e l'archiviazione dei dati dei clienti.

Le novità in pillole



AI ACT

In data 1° agosto 2024 è entrato in vigore il nuovo Regolamento (UE) 2024/1689 ("AI Act") che definisce una normativa ad hoc sull'intelligenza artificiale. La Commissione UE ha pubblicato dei chiarimenti sotto forma di Q&A disponibili sul [sito](#). Di seguito un estratto:

A chi si applica la legge sull'IA?

Il quadro giuridico si applicherà ai soggetti pubblici e privati, all'interno e all'esterno dell'UE, a condizione che il sistema di IA sia immesso sul mercato dell'Unione o che il suo utilizzo abbia effetti su persone situate nell'UE. Gli obblighi possono riguardare sia i fornitori (ad esempio, uno sviluppatore di uno strumento di screening dei CV) sia i deployer di sistemi di IA (ad esempio, una banca che acquista il suddetto strumento di screening).

Quali sono le categorie di rischio?

La legge sull'IA introduce un quadro uniforme in tutti gli Stati membri dell'UE, basato su una definizione di IA che guarda al futuro e su un approccio basato sul rischio:

- **rischio inaccettabile**: una serie molto limitata di usi dell'IA particolarmente dannosi, che contravvengono ai valori dell'UE perché violano i diritti fondamentali e che saranno pertanto vietati.
- **rischio alto**: è considerato ad alto rischio un numero limitato di sistemi di IA definiti nella proposta, che possono potenzialmente avere ripercussioni negative sulla sicurezza delle persone o sui loro diritti fondamentali.
- **rischio minimo**: la maggioranza dei sistemi di IA possono essere sviluppati e utilizzati nel rispetto della legislazione vigente senza ulteriori obblighi giuridici. I fornitori di tali sistemi possono scegliere di applicare, su base volontaria, i requisiti per un'IA affidabile e aderire a codici di condotta volontari.

Quando sarà pienamente applicabile la legge sull'IA?

La legge sull'IA si applicherà il 2 agosto 2026, due anni dopo l'entrata in vigore, ad eccezione che per le seguenti disposizioni specifiche:

- le norme in materia di governance e gli obblighi per l'IA per finalità generali diventano applicabili 12 mesi dopo l'entrata in vigore, il 2 agosto 2025;
- gli obblighi per i sistemi di IA ad alto rischio si applicano 36 mesi dopo l'entrata in vigore, il 2 agosto 2027.

Foto dei minori sui social: le indicazioni dell'Autorità

La pubblicazione sui social network di immagini che ritraggono minori di 14 anni richiede necessariamente il preventivo consenso di entrambi i genitori. Tale principio è stato ribadito dal Garante in una vicenda in cui una madre lamentava la pubblicazione di una foto del figlio, minore di quattordici anni, da parte del padre sul proprio profilo Facebook. L'Autorità ha ammonito il padre e ha disposto il divieto di pubblicazione dell'immagine del figlio senza il consenso di entrambi i genitori.

Garante privacy: caso Foodinho

Il Garante per la protezione dei dati personali ha ordinato a Foodinho srl, società del gruppo Glovo, il pagamento di una sanzione di 5 milioni di euro per aver trattato illecitamente i dati personali di oltre 35mila rider attraverso la piattaforma digitale. In particolare, è stato appurato che la società effettuava diversi trattamenti automatizzati dei dati dei rider senza aver adottato le misure previste dal GDPR nonché le misure di sicurezza degli interessati, inviava i dati personali dei rider, compresa la posizione geografica, a società terze.

SCOPRI TUTTI I SERVIZI
SERMETRA NET SERVICE