

Le nuove Linee Guida del GPDP sui cookie



Il Garante per la Protezione dei Dati Personali (GPDP) ha recentemente emanato un provvedimento (pubblicato in G.U. lo scorso 09/07) denominato “Linee guida cookie e altri strumenti di tracciamento”, facendo seguito alla consultazione pubblica iniziata lo scorso dicembre.

Il presente articolo segue analogo articolo che commentava la versione posta in consultazione delle medesime Linee Guida e che ora sono state ufficialmente approvate, seppur con qualche modifica.

Tali Linee Guida di fatto aggiornano un provvedimento analogo (n. 229, dell’8 maggio 2014) adottato prima dell’entrata in vigore del Regolamento UE 679/2016.

I riferimenti normativi su cui si basa il provvedimento sono dunque i seguenti:

- Regolamento UE 679/2016 (GDPR)
- Codice Privacy (D.Lgs 196/2003) emendato dal D.Lgs 101/2018, in particolare l’art. 122 del Codice
- Direttiva 2002/58/CE del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (c.d. direttiva ePrivacy), come modificata dalla direttiva 2009/136/CE del 25 novembre 2009
- Parere dell’EDPB n. 05/2019 del 12 marzo 2019 sulle interrelazioni tra la direttiva e-Privacy ed il Regolamento
- Linee guida EDPB 05/2020 sul consenso ai sensi del regolamento (UE) 2016/679

Le Linee Guida dovranno essere recepite da tutti i proprietari di siti web entro sei mesi dalla pubblicazione, ovvero entro il 09/01/2022.

Si fa presente che le Linee Guida in oggetto rientrano in un ambito che verrà regolamentato da nuovo Regolamento e-Privacy – ormai di prossima emissione – che sostituirà la Direttiva e-Privacy sopra elencata.

Classificazione dei cookie ed altri strumenti di tracciamento

I GDPR distingue fra le seguenti tipologie di cookie:

1. i **cookie tecnici**, utilizzati al solo fine di “effettuare la trasmissione di una comunicazione su una rete di comunicazione elettronica, o nella misura strettamente necessaria al fornitore di un servizio della società dell’informazione esplicitamente richiesto dal contraente o dall’utente a erogare tale servizio” (cfr. art. 122, comma 1 del Codice);
2. i **cookie di profilazione**, utilizzati per ricondurre a soggetti determinati, identificati o identificabili, specifiche azioni o schemi comportamentali ricorrenti nell’uso delle funzionalità offerte (*pattern*) al fine del raggruppamento dei diversi profili all’interno di *cluster* omogenei di diversa ampiezza, in modo che sia possibile al titolare, tra l’altro, anche modulare la fornitura del servizio in modo sempre più personalizzato al di là di quanto strettamente necessario.

I cosiddetti “*cookie analytics*”, che normalmente servono ad elaborare statistiche sulle visite al sito web attraverso servizi di terze parti (ad es. Google Analytics) possono essere equiparati ai cookie tecnici solo se il gestore del sito, attraverso apposite tecniche di anonimizzazione (ad es. mascheramento delle ultime cifre dell’indirizzo IP) rende non identificabile l’utente da parte delle terze parti a cui vengono trasmessi i dati a fini statistici (il GDPR ritiene che siano possibili solo statistiche aggregate per ricadere in questa tipologia). Viceversa, i cookie analitici ricadono fra i cookie di profilazione.

Informativa e consenso

Il consenso dell’utente all’impiego dei cookie è ritenuto necessario solamente per i cookie di profilazione (compresi i cookie analitici di terze parti che presentano tali caratteristiche), mentre in ogni caso deve essere resa all’utente un’informativa sull’uso dei cookie.

In caso di utilizzo non solo di cookie tecnici il consenso all’installazione di cookie sul *device* dell’utente deve essere richiesto all’accesso al sito web, tramite apposito *banner* ben visibile. Tale *banner* deve avere le seguenti caratteristiche:

- riportare un’informativa breve sull’utilizzo dei cookie;
- richiamare tramite link un’informativa estesa – denominata **privacy policy** – che comprenda tutti i contenuti previsti dagli articoli 13 e 14 del GDPR;
- presentare all’utente un pulsante per poter rifiutare tutti i cookie;
- presentare all’utente un pulsante per accettare tutti i cookie e/o gestire diverse opzioni di scelta sui cookie, tramite link ad apposita area;

- riportare in alto a destra un pulsante a forma di X che permette la chiusura del banner; in tal caso la scelta di default sarà quella di rifiutare tutti i cookie;
- l'avvertenza che la chiusura del banner mediante selezione dell'apposito comando contraddistinto dalla X posta al suo interno comporta il permanere delle impostazioni di default e dunque la continuazione della navigazione in assenza di cookie o altri strumenti di tracciamento diversi da quelli tecnici.

Non sono ammesse forme di consenso tramite il semplice *scrolling* della pagina web.

Non è normalmente lecito implementare i c.d. *cookie wall* ovvero un banner che permette l'accesso al sito solo previa accettazione di tutti i cookie.

Il consenso raccolto deve essere documentabile e l'utente deve aver la possibilità di revocarlo successivamente, anche perché il sito deve mantenere traccia delle scelte effettuate dall'utente al primo accesso al sito (anche e soprattutto se ha rifiutato i cookie) e fornirgli la possibilità di aggiornare successivamente tali scelte (sempre che ciò sia possibile, salvo l'utente non sia identificabile, l'impiego dei cookie sia stato modificato, ecc.).

I consensi e le scelte relative all'utilizzo dei cookie devono essere mantenuti dal sito per sei mesi.

La privacy policy, che deve essere facilmente accessibile da tutte le pagine del sito, deve contenere, tra l'altro:

- l'indicazione circa gli eventuali altri soggetti destinatari dei dati personali raccolti tramite i cookie o tecnologie similari ed i tempi di conservazione delle informazioni acquisite;
- l'indicazione delle modalità previste dalle terze parti per esercitare i propri diritti in termini di modifica/revoca del consenso;
- l'elenco dei cookie – raggruppati in categorie omogenee – utilizzati dal sito.

Conclusioni

Premesso che il presente articolo rappresenta solo una sintesi del Provvedimento del GPDP in oggetto e che, pertanto, è necessario che siano letti attentamente sia le Linee Guida, sia l'allegata Scheda di Sintesi per provvedere all'aggiornamento dei siti web in conformità alle Linee Guida, si sottolinea il fatto che il documento del GPDP ha contenuti tecnici che dovrebbero essere esaminati dal gestore del sito o dal responsabile del suo sviluppo (in caso di nuovi siti).

Poiché i siti web sono pubblici e, quindi, facilmente ispezionabili dall'Autorità di Controllo, le eventuali non conformità rispetto alla normativa sono facilmente identificabili.

Ricordiamo che eventuali sanzioni sono sempre a carico del proprietario del sito web (facilmente individuabile – anche per siti “dimenticati” – dalle funzionalità *Whois* presenti sul web), mentre lo sviluppatore del sito o il suo gestore/manutentore è responsabile solo di adempiere al contratto fra le parti, nel quale il Titolare del trattamento dovrà prevedere appositi impegni di conformità alle Linee Guida in oggetto.

L’impatto su molti siti web i cui proprietari desidereranno adeguarsi alle nuove Linee Guida non sarà ininfluente, in quanto richiederà un intervento tecnico da parte di personale specializzato. Anche nel caso di siti realizzati con CMS (*Content Management System*) quali WordPress o Joomla, solo per citarne alcuni, si dovrà intervenire con appositi plugin o servizi specializzati, per lo più a pagamento, che permettono di gestire i cookie in modo guidato.

Prevedo già che alcuni fornitori se ne approfitteranno, richiedendo cifre esagerate per ottenere la conformità dei cookie.

In ogni caso ci sarà un aggravio di costi anche per siti di aziende senza particolari velleità di marketing digitale spinto e qualcuno accuserà la privacy di creare solo costi aggiuntivi per le imprese e questo non è bello.

Viceversa i siti che utilizzano pesantemente le tecnologie di tracciamento a fini di marketing ne subiranno le conseguenze più significative. Il Digital Marketing dovrà rivedere alcuni approcci, in quanto l’opzione di default, preimpostata come evidenziata, “Accetta tutti cookie” non potrà più essere contrapposta al classico pulsante “Personalizza” o “Gestisci le tue preferenze” che spesso ci porta in percorsi molto articolati nei quali è difficile districarsi (provate a gestire le preferenze sui cookie in Facebook per credere). Il default sarà “Rifiuta tutti i cookie non tecnici” e persino la chiusura del banner porterà automaticamente ad una scelta di rifiuto dei cookie.

Restano possibili, di default, le pure statistiche aggregate sulle visite al sito tramite Google Analytics, ma a condizione che l’indirizzo IP nel cookie sia mascherato, procedimento non certo immediato.

Francamente poco condivisibile è la necessità di conservare la scelta sul consenso o rifiuto dei cookie in sessioni successive, perché appesantisce la gestione dei cookie, soprattutto in siti molto trafficati, e di limitata utilità per l’utente che non si collega sempre con lo stesso dispositivo ad un certo sito web o che ha implementato procedure di cancellazione periodica dei cookie dal proprio terminale attraverso funzioni specifiche del browser o utility di pulizia del PC.

Permangono alcune perplessità sull’approccio non proprio omogeneo di diverse Autorità di Controllo sulla Protezione dei Dati a livello europeo (in ambito UE e di Paesi appena usciti dalla UE), vista l’internazionalità dei siti web: un sito deve seguire la normativa italiana se è di proprietà di un titolare del trattamento

italiano, se è un sito .it, se è un sito ospitato su server in Italia?

Anche se non citate esplicitamente nel provvedimento, le Linee Guida sui cookie comprendono anche altre tecnologie di tracciamento che dominano il mondo del *digital marketing*.

Molte imprese vorranno vedere prima Facebook, Amazon e Google mettere i pulsanti "Rifiuta tutti i cookie" in bell'evidenza prima di adeguare i loro siti.

Il divieto del c.d. *cookie wall* – da cui si può prescindere in casi non proprio chiarissimi – pone un interrogativo di fondo: perché non posso fornire un servizio informativo gratuito solo a chi è disposto a subire una profilazione ed un po' di pubblicità mirata? In fondo nel mondo analogico non è quello che avviene con le *fidelity card*?

Tutti i siti di informazione e notizie – quelli delle testate giornalistiche in primis – non potranno più contare su banner pubblicitari mirati, ma solo su pubblicità generica e questo porterà sicuramente a introiti inferiori. Vedremo però se tutto questo porterà vantaggi tangibili agli utenti di internet, soprattutto tramite smartphone e relative app, che dovrebbero vedere ridursi i banner/pop-up pubblicitari, per lo meno quelli derivanti da profilazione dell'utente stesso.