

Ce riscuri ascunse au deținătorii de site-uri web din perspectiva GDPR? Doua situații des întâlnite în practica



Pastrarea anonimitații online este în zilele noastre un deziderat greu de îndeplinit în condițiile în care simpla vizita a unui site web presupune, în mod aproape sigur, o prelucrare de date cu caracter personal. Mai mult, din nevoia de eficientizare a costurilor și dorința de maximizare a profiturilor, mulți deținători de site-uri web, fie de prezentare sau e-commerce, recurg la tot felul de metode care servesc acestor scopuri, dar care, în cele din urmă îi expun unor riscuri de sancționare pentru lipsa de conformitate din punct de vedere GDPR.

Printre metodele folosite pentru eficientizarea costurilor se numara: folosirea unor șabloane în designul site-ului (i.e. template-uri) cu scopul de a reduce cheltuielile, încorporarea unor tehnologii de urmarire sau de analiza cu scopul de a crește încasarile sau realizarea unor audituri necorespunzatoare din perspectiva protecției datelor cu caracter personal, tot în scopul de reduce costurile.

În ciuda beneficiului temporar pe care îl poate aduce oricare dintre acțiunile menționate mai sus, acestea sunt inevitabil acompaniate de riscuri de sancționare pentru lipsa de conformitate, dar mai ales pentru încălcarea prevederilor legale aplicabile în domeniul protecției datelor cu caracter personal, precum Regulamentul (UE) 2016/679 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date (GDPR) sau Legea 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice (Legea E-Privacy). Și asta pentru ca toate acțiunile menționate mai sus implica sau au un efect direct asupra datelor cu caracter personal prelucrate prin intermediul site-ului web.

Vom analiza în continuare doua situații, mult prea des întâlnite în practica, care se pot transforma în adevarate probleme pentru deținătorii de site-uri web, având în vedere regimurile sancționatorii din GDPR și Legea E-Privacy, dar care pot fi evitate în urma unui audit corespunzator și a unui plan de (re)conformare adecvat.

● Prelucrari de date cu caracter personal contrar opțiunilor exprimate de vizitatori

Inevitabil, orice utilizator, este întâmpinat de interfața unei platforme de gestionare a consimțământului (Consent Management Platform sau CMP) privind tehnologiile de tip cookies sau alte tehnologii de urmarire în momentul în care accesează un site web pentru prima data sau după o perioada semnificativa de timp.

Prin intermediul unui CMP, ca regula generala, utilizatorul este informat în legatura cu: (i) faptul ca site-ul web pe care îl accesează folosește tehnologii de urmarire, precum cele de tip cookie sau pixeli de urmarire; (ii) care sunt aceste tehnologii folosite pe site-ul web pe care utilizatorul dorește sa-l acceseze; (iii) necesitatea consimțământului sau pentru plasarea acestor tehnologii folosite de site-ul web, cu excepția cookie-urilor strict

necesare.

În practica însă, un număr alarmant de mare de site-uri web procedează la plasarea unor cookie-uri de măsurare sau analiză, fie în absența consimțământului exprimat de către utilizator, fie și în cazul în care utilizatorul a optat doar pentru fișierele cookie strict necesare.

Cel mai des întâlnit caz este cel al lui Google, respectiv al cookie-urilor sale de măsurare și analiză (i.e. Google Analytics) aproape omniprezente pe majoritatea site-urilor web accesibile din Uniunea Europeană și nu numai. Aceste cookie-uri pot fi ușor identificate prin denumirea identificatorilor lor, respectiv `_ga` și `_gid`.

Deși exista o opinie anterioară privind inexistența datelor cu caracter personal în cadrul metadatelor colectate de acest tip de fișiere cookie, o hotărâre recentă a autorității de supraveghere din Austria a stabilit exact contrariul, schimbând astfel paradigma privind fișierele cookie de analiză și statuând ca metadatele cuprind date cu caracter personal. La scurt timp după hotărârea autorității din Austria, și autoritatea din Franța s-a aliniat la această opinie printr-o hotărâre de sancționare având concluzii similare.

În prezent, numeroase site-uri web din România se regăsesc în practica descrisă anterior, plasând fișiere cookie de analiză (mai ales din cele create de Google), fără a obține în prealabil consimțământul utilizatorilor care accesează site-ul web sau contrar opțiunilor exprimate de aceștia.

● Lipsa de transparență privind tehnologiile de urmărire folosite

În situațiile în care sunt achiziționate șabloane de design pentru site-uri web, există situații în care acestea au implementate, în mod implicit (by default) de către cel care a creat șablonul, și tehnologii de urmărire despre care viitorul deținător care folosește respectivul șablon nu poate avea cunoștința în absența unor cunoștințe de specialitate sau în lipsa unui audit corespunzător.

În mod corelativ, există și situații în care echipa IT din spatele unui site web nu realizează o informare corectă a deținătorului despre tehnologiile de urmărire prezente pe respectivul site web și modul de funcționare al acestora, inclusiv existența unor prelucrări de date cu caracter personal.

Ca urmare a unor situații precum cele de mai sus, apar prelucrări de date cu caracter personal ascunse, îndeosebi prin intermediul unor pixeli de urmărire, despre care utilizatorul nu este informat și pentru care acesta nu își exprima în prealabil consimțământul.

Trebuie reținut faptul că un „pixel de urmărire” este un program software menit să înregistreze o acțiune a unui utilizator (de exemplu, dacă utilizatorul a văzut o reclamă afișată pe site-ul web accesat), colectând totodată și alte metadate, în mod asemănător unui fișier cookie. De asemenea, trebuie avut în vedere că metadatele sunt definite în mod “crud” ca fiind date despre date, precum: momentul când au fost create, cine le-a creat, ce software / hardware a fost folosit pentru a le crea, etc.

În prezent, mai multe site-uri web din România plasează cookie-uri pe care nu le menționează în politica de cookies și în CMP, atunci când solicită consimțământul utilizatorilor, deși acestea nu intra sub categoria fișierelor cookie-urilor strict necesare. Dacă aceasta plasare are loc cu sau fără cunoștința deținătorului site-ului web nu reprezintă o cauză justificativă din perspectiva aplicării unor sancțiuni pentru încălcarea normelor legale aplicabile în domeniul protecției datelor cu caracter personal.

Mai mult decât atât, foarte mulți deținători de site-uri web folosesc pixeli de urmărire fără a solicita consimțământul prealabil al utilizatorilor și fără a le oferi informații despre existența acestora pe site-ul web. Dacă în cazul vulnerabilităților privind securitatea cibernetică, cauza lor este adesea exterioară, în cazul riscurilor prezentate mai sus, eventualele neconformități sau chiar sancțiuni pot fi evitate prin efectuarea unui audit corespunzător din perspectiva protecției datelor cu caracter personal și prin implementarea unui plan adecvat de

conformare cu prevederile din GDPR și din Legea E-Privacy.

Având în vedere faptul ca în prezent se afla în discuție un ghid redactat de catre Comitetul European pentru Protecția Datelor privind calcularea cuantumului amenzilor aplicabile în cazul încălcării prevederilor din GDPR, reiteram faptul ca amenzile aplicabile în cazul constatarii unor încălcări precum cele de mai sus se pot ridica de pâna la 20.000.000 euro sau, în cazul unei companii, de pâna la 4 % din cifra de afaceri totala anuala corespunzatoare exercițiului financiar anterior, luându-se în calcul cea mai mare valoare.