

## **1. CE ESTE UN COOKIE?**

Un cookie este un fișier de mici dimensiuni, în general alcătuit din litere și cifre, care este descărcat în memoria unui calculator (sau altui echipament folosit pentru navigare online - telefon mobil, tabletă, etc), atunci când utilizatorul accesează un anumit site web.

Cookie-urile sunt create atunci când browserul folosit de către un utilizator afișează un anumit site web. Site-ul web transmite informații către browser, iar acesta creează un fișier text. De fiecare dată când utilizatorul accesează din nou respectivul site web, browserul accesează și transmite acest fișier către serverul site-ului web. Altfel spus, cookie-ul poate fi văzut ca un card de identificare a utilizatorului de Internet, care anunță site-ul web de fiecare dată când utilizatorul se întoarce pe respectivul site.

### **Exemplu:**

Pentru un utilizator de Windows XP și Mozilla Firefox, cookie-urile stocate în calculatorul său se găsesc la următoarea locație:

C: \Documente și Setări\[nume\_de\_utilizator]\Datele  
Aplicațiilor\Mozilla\Firefox\Profiluri\[nume\_profil].default\cookies.sqlite

Un cookie poate arăta așa:

SNID50=eR0azHquz-E3211B7uLIasD63\_ZWxrS9fkAc37Z4CQ=Q4levhdDnydqjJGNgoogle.ro/verify 9728  
2076339328 30210107 446809680 30173295 \*

## **2. SCOPUL COOKIE-URILOR**

Cookie-urile pot asigura o interacțiune mai rapidă și mai ușoară între utilizatori și site-urile web. Spre exemplu, în momentul autentificării unui utilizator pe un anumit site web, datele de autentificare sunt stocate într-un cookie; ulterior, utilizatorul poate accesa respectivul site fără să fie nevoie să se autentifice din nou.

În alte cazuri, cookie-urile pot fi utilizate pentru stocarea de informații referitoare la activitățile desfășurate de utilizator pe o anumită pagină web, astfel încât acesta să își poată relua ușor respectivele activități la o accesare ulterioară a site-ului. Cookie-urile spun serverului ce pagini trebuie să arate utilizatorului, astfel încât acesta să nu fie nevoit să își amintească acest lucru sau să navigheze întregul site de la început. Astfel, cookie-urile pot fi asimilate unor „semne de carte” care îi spun utilizatorului exact unde a rămas în cadrul unui site web.

În mod similar, cookie-urile pot stoca informații referitoare la produsele comandate de către utilizator pe un site de comerț electronic, făcând astfel posibil conceptul de „coș de cumpărături”.

De asemenea, cookie-urile pot oferi site-urilor web posibilitatea de a monitoriza activitățile online ale utilizatorilor și de a stabili profiluri de utilizatori, care pot fi apoi folosite în scopuri de marketing. Spre exemplu, pe baza cookie-urilor pot fi identificate produsele și serviciile agreate de către un utilizator, aceste informații servind ulterior la transmiterea de mesaje publicitare adecvate către respectivul utilizator.

Este important de menționat faptul că site-urile web din România au obligația de a specifica în mod public dacă folosesc cookie-uri și în ce scop (vezi pct.5 – Reglementarea utilizării cookie-urilor).

## **3. TIPURI DE COOKIE-URI**

### **3.1. COOKIE-URI SPECIFICE UNEI SESIUNI ONLINE**

Paginile web nu au memorie. Un utilizator care navighează de la o pagină web la alta va fi considerat de către site-ul web drept un nou utilizator. Cookie-urile specifice unei sesiuni stochează, de regulă, un identificator care permite utilizatorului să treacă de la o pagină web la alta fără să fie nevoie să introducă de fiecare dată informațiile de identificare (nume de utilizator, parolă, etc). Astfel de cookie-uri sunt utilizate la scară largă de către site-uri comerciale, spre exemplu, pentru a ține evidența produselor adăugate de către un utilizator în coșul de cumpărături. Atunci când utilizatorul vizitează o anumită pagină a unui catalog de produse și selectează

anumite produse, cookie-ul reține produsele selectate și le adaugă în coșul de cumpărături, care va conține toate produsele selectate în momentul în care utilizatorul dorește să părăsească pagina.

Cookie-urile specifice unei sesiuni sunt stocate în memoria calculatorului utilizatorului doar pe durata unei sesiuni de navigare pe Internet și sunt șterse în mod automat în momentul în care browser-ul este închis. Pot deveni inaccesibile și dacă sesiunea a fost inactivă pentru o anumită perioadă de timp (de regulă, 20 de minute).

### 3.2. COOKIE-URI PERMANENTE, PERSISTENTE SAU STOCATE

Cookie-urile persistente sunt stocate la nivelul calculatorului utilizatorului și nu sunt șterse atunci când sesiunea de navigare este închisă. Aceste cookie-uri pot reține preferințele utilizatorului pentru un anumit site web, astfel încât acestea să poată fi utilizate în cadrul altor sesiuni de navigare pe Internet.

Pe lângă informațiile de autentificare, cookie-urile persistente pot reține și detalii referitoare la limba și tema selectate pe un anumit site web, preferințe privind meniul unui site, pagini favorite în interiorul unui site, etc. Atunci când utilizatorul accesează un site pentru prima dată, acesta este prezentat în modul implicit. Ulterior, utilizatorul selectează o serie de preferințe, care sunt apoi reținute de către cookie-uri și folosite atunci când utilizatorul accesează din nou site-ul. Spre exemplu, un site web își oferă conținutul în mai multe limbi. La prima vizită, utilizatorul selectează limba engleză, iar site-ul reține această preferință într-un cookie. Atunci când utilizatorul vizitează din nou site-ul respectiv, conținutul va fi afișat automat în limba engleză.

Cookie-urile persistente pot fi folosite pentru identificarea utilizatorilor individuali și, astfel, pentru analizarea comportamentului online al utilizatorilor. Ele pot furniza informații referitoare la numărul de vizitatori ai unui site web, timpul (în medie) petrecut pe o anumită pagină, și, în general, performanțele unui site web. Aceste cookie-uri sunt configurate pentru a putea urmări activitățile utilizatorilor pentru o perioadă îndelungată de timp, în unele cazuri fiind vorba chiar despre ani.

### 3.3. COOKIE-URI FLASH

Dacă utilizatorul are Adobe Flash instalat pe calculator, mici fișiere pot fi stocate în memoria respectivului calculator de către site-uri web care conțin elemente Flash (cum ar fi clipuri video). Aceste fișiere sunt cunoscute sub numele de „local shared objects” sau „cookie-uri flash” și pot fi utilizate pentru aceleași scopuri ca și cookie-urile obișnuite.

Atunci când cookie-urile obișnuite sunt șterse prin intermediul funcțiilor unui browser, cookie-urile flash nu sunt afectate. Astfel, un site web care utilizează cookie-uri flash poate să recunoască un utilizator cu ocazia unei noi vizite, dacă datele specifice cookie-urilor șterse au fost reținute și într-un cookie flash.

Întrucât cookie-urile flash nu sunt stocate în calculatorul utilizatorului în aceeași manieră în care sunt stocate cele obișnuite, ele sunt mai dificil de identificat și de șters. Băncile și site-urile de natură financiară folosesc astfel de cookie-uri tocmai pentru acest motiv. Pentru că sunt dificil de identificat, aceste cookie-uri sunt stocate în calculatoarele utilizatorilor pentru a permite autentificarea utilizatorilor și a preveni fraudele, deoarece eventualii infractori pot deține numele de utilizator și parola pentru autentificare, dar nu au acces la calculatorul utilizatorului. Astfel, cookie-urile acționează ca un al doilea nivel de autentificare, pe lângă numele de utilizator și parolă.

### 3.4. COOKIE-URI FIRST PARTY VS COOKIE-URI THIRD PARTY

Fiecare cookie are un „proprietar” – site-ul web/domeniul Internet care plasează respectivul cookie.

Cookie-urile *first party* (*prima parte*) sunt plasate de către domeniul Internet /site-ul web accesat de către utilizator (a cărui adresă apare în bara de adrese a browserului). Spre exemplu, dacă utilizatorul vizitează **www.apti.ro**, iar domeniul cookie-ului plasat pe calculatorul său este **www.apti.ro**, atunci este vorba despre un cookie first party.

Un cookie *third party* (*terță parte*) este plasat de către un alt domeniu Internet/site web decât cel accesat de către utilizator; acest lucru înseamnă că site-ul web accesat conține și informații provenind de la un site web terț - spre exemplu, un banner publicitar care apare pe site-ul accesat. Astfel, dacă utilizatorul vizitează **www.apti.ro** dar cookie-ul plasat pe calculatorul său are ca domeniu **www.traffic.ro**, atunci este vorba despre un cookie third party.

Grupul de Lucru Articolul 29 (alcătuit din autoritățile naționale pentru protecția datelor din statele membre ale Uniunii Europene) consideră că, din punct de vedere juridic, și având în vedere legislația europeană, noțiunea de „cookie third party” se referă la un cookie plasat de către un operator<sup>[1]</sup> distinct față de cel care operează site-ul web vizitat de către utilizator. Cookie-urile third party nu sunt strict necesare utilizatorului care accesează un site web, întrucât ele sunt, de regulă, asociate unui serviciu distinct față de cel care a fost „solicitat” în mod explicit de către utilizator (prin accesarea site-ului web).

#### **4. COOKIE-URILE DIN PERSPECTIVA SECURITĂȚII INFORMATICE ȘI PROTECȚIEI VIEȚII PRIVATE**

Deși cookie-urile sunt stocate în memoria calculatorului utilizatorului de Internet, ele nu pot accesa/citi alte informații aflate în respectivul calculator. Cookie-urile nu sunt viruși. Ele sunt doar mici fișiere text; nu sunt compilate sub formă de cod și nu pot fi executate. Astfel, nu se pot auto-copia, nu se pot răspândi în alte rețele pentru a genera acțiuni și nu pot fi folosite pentru răspândirea de viruși.

Cookie-urile nu pot căuta informații în calculatorul utilizatorului, însă ele stochează informații de natură personală. Aceste informații nu sunt generate de către cookie-uri, ci de către utilizator, în momentul în care acesta completează formulare online, se înregistrează pe anumite site-uri web, utilizează sisteme de plăți electronice, etc. Deși, de regulă, informațiile sensibile sunt protejate pentru a nu putea fi accesate de persoane neautorizate, este însă posibil ca astfel de persoane să intercepteze informațiile transmise între browser și site-ul web. Chiar dacă sunt destul de rare, astfel de situații pot apărea atunci când browserul se conectează la server utilizând o rețea necriptată, cum ar fi un canal WiFi nesecurizat.

Pentru a reduce riscurile de interceptare a cookie-urilor, pot fi utilizate așa numitele „secure cookie” sau „HttpOnly cookie”. Cookie-urile de tip „secure” sunt menite să limiteze comunicarea informațiilor stocate în cookie-uri la transmiterea criptată, indicând browser-ului să folosească cookie-uri doar prin conexiuni sigure/criptate. Astfel, dacă site-ul web folosește HTTPS, cookie-urile aferente site-ului sunt marcate cu atributul „secure”, acest lucru împiedicând transmiterea lor către o pagină non-HTTPS, chiar dacă aceasta este localizată la același URL. Spre exemplu, dacă google.ro folosește un „secure cookie”, acel cookie poate fi obținut doar de către google.ro și doar de pe o conexiune https (care certifică faptul că cel care cere cookie-ul este Google Inc și nu altcineva). Atributul „HttpOnly” indică browserului să folosească cookie-uri doar prin intermediul protocolului HTTP (care include și HTTPS). Un cookie HttpOnly nu este accesibil prin metode non-HTTP, cum ar fi JavaScript, neputând fi ținta unor atacuri de tip cross-site scripting.<sup>[2]</sup>

O altă sursă de îngrijorare este reprezentată de utilizarea cookie-urilor în scopuri de publicitate direcționată comportamental. Astfel, cookie-urile pot fi utilizate de către companiile de publicitate online pentru monitorizarea comportamentului și preferințelor online ale utilizatorului, în scopul identificării și livrării către utilizator a celor mai relevante mesaje publicitare. Însă aceste preferințe nu sunt exprimate explicit sau conștient de către utilizator, ci sunt modelate în funcție de istoricul navigării online a utilizatorului, paginile vizualizate de către acesta, mesajele publicitare accesate. Spre exemplu, atunci când utilizatorul citește o pagină web despre mașini și se mută ulterior pe o altă pagină, mesaje publicitare referitoare la mașini vor fi afișate în noua pagină, chiar dacă aceasta nu are legătură cu mașini. Întrucât utilizatorul nu este informat despre faptul că acțiunile sale online sunt monitorizate, acest lucru generează îngrijorări referitoare la protecția vieții private.

Astfel, utilizarea cookie-urilor ridică îngrijorări referitoare la folosirea informațiilor reținute prin aceste cookie-uri în scopul monitorizării utilizatorilor și folosirii de tehnologii de tip spyware, mai ales în cazurile în care informațiile sunt stocate în calculatoarele utilizatorilor și folosite pentru recunoașterea lor, fără ca utilizatorii să aibă cunoștință despre acest lucru sau să-și fi dat acordul în acest sens.

## **5. REGLEMENTAREA UTILIZĂRII COOKIE-URILOR**

Utilizarea cookie-urilor și obligațiile furnizorilor sunt reglementate atât în legislația Uniunii Europene, cât și în legislația națională.

Astfel, Directiva 2002/58/CE (PDF) privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor electronice, modificată prin Directiva 2009/136/CE (PDF), prevede că :

“Art.5 - (3) Statele membre se asigură că stocarea de informații sau dobândirea accesului la informațiile deja stocate în echipamentul terminal al unui abonat sau utilizator este permisă doar cu condiția ca abonatul sau utilizatorul în cauză să își fi dat acordul, după ce a primit informații clare și complete, în conformitate cu Directiva 95/46/CE, inter alia, cu privire la scopurile prelucrării. Aceasta nu împiedică stocarea sau accesul tehnic cu unicul scop de a efectua transmisia comunicării printr-o rețea de comunicații electronice sau în cazul în care acest lucru este strict necesar în vederea furnizării de către furnizor a unui serviciu al societății informaționale cerut în mod expres de către abonat sau utilizator.”

Aceste prevederi au fost transpuse în legislația națională în Legea nr.506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice, cu modificările și completările ulterioare:

“Art.4 -

- (5) Stocarea de informații sau obținerea accesului la informația stocată în echipamentul terminal al unui abonat ori utilizator este permisă numai cu îndeplinirea în mod cumulativ a următoarelor condiții:
  1. abonatul sau utilizatorul în cauză și-a exprimat acordul;
  2. abonatului sau utilizatorului în cauză i s-au furnizat, anterior exprimării acordului, în conformitate cu prevederile art. 12 din Legea nr. 677/2001, cu modificările și completările ulterioare, informații clare și complete care:
    1. să fie expuse într-un limbaj ușor de înțeles și să fie ușor accesibile abonatului sau utilizatorului;
    2. să includă mențiuni cu privire la scopul procesării informațiilor stocate de abonat sau utilizator ori informațiilor la care acesta are acces.

În cazul în care furnizorul permite unor terți stocarea sau accesul la informații stocate în echipamentul terminal al abonatului ori utilizatorului, informarea în concordanță cu pct. (i) și (ii) va include scopul general al procesării acestor informații de către terți și modul în care abonatul sau utilizatorul poate folosi setările aplicației de navigare pe internet ori alte tehnologii similare pentru a șterge informațiile stocate sau pentru a refuza accesul terților la aceste informații.

- (51) Acordul prevăzut la alin. (5) lit. a) poate fi dat și prin utilizarea setărilor aplicației de navigare pe internet sau a altor tehnologii similare prin intermediul cărora se poate considera că abonatul ori utilizatorul și-a exprimat acordul.
- (6) Prevederile alin. (5) nu aduc atingere posibilității de a efectua stocarea sau accesul tehnic la informația stocată în următoarele cazuri:
  1. atunci când aceste operațiuni sunt realizate exclusiv în scopul efectuării transmisiei unei comunicări printr-o rețea de comunicații electronice;
  2. atunci când aceste operațiuni sunt strict necesare în vederea furnizării unui serviciu al societății informaționale, solicitat în mod expres de către abonat sau utilizator.”

Conform acestor prevederi, utilizarea cookie-urilor third party este permisă cu următoarele condiții:

- informarea utilizatorilor, într-o manieră clară, completă și ușor accesibilă, în legătură cu:
  - plasarea, de către un anumit site web, de cookie-uri în memoria calculatorului utilizatorului;

- scopul utilizării cookie-urilor (informațiile stocate în cookie-uri și scopul în care aceste informații sunt utilizate);
- modalitățile prin care utilizatorul poate șterge cookie-urile sau poate refuza accesul unor terți la informațiile stocate de respectivele cookie-uri;
- obținerea acordului utilizatorului pentru plasarea de cookie-uri și pentru utilizarea informațiilor conținute de către acestea.
- deși acordul utilizatorilor poate fi exprimat și prin utilizarea setărilor browser-ului folosit pentru navigarea pe Internet, este necesar ca și în acest caz să existe o informare prealabilă a utilizatorului în legătură cu plasarea de cookie-uri și cu scopul acestora.

Excepțiile prevăzute în legislația europeană și națională permit utilizarea de cookie-uri first party fără respectarea obligației obținerii acordului utilizatorului. În plus, în iunie 2012, Grupul de Lucru Articolul 29 a emis [un aviz \(PDF\)](#) prin care clarifică aceste excepții:

- unele cookie-uri pot fi exceptate de la obligația obținerii acordului informat al utilizatorului în anumite condiții și dacă nu sunt utilizate în scopuri suplimentare. Astfel de cookie-uri includ: cookie-urile utilizate pentru memorarea informațiilor introduse de către un utilizator atunci când completează un formular online, cookie-urile utilizate pentru stocarea datelor tehnice necesare rulării de conținut video și audio și cookie-urile utilizate pentru personalizarea paginilor web (spre exemplu, cele care rețin preferințele referitoare la limba în care este afișat conținutul unui site web).
- cookie-urile de tip first party nu generează riscuri pentru viața privată a utilizatorilor dacă site-ul web oferă utilizatorilor informații clare în ceea ce privește utilizarea de cookie-uri, precum și garanții privind protecția vieții private (spre exemplu, punerea la dispoziție a unui mecanism facil prin care utilizatorul să poată solicita ca datele sale să nu fie colectate) și dacă este asigurată anonimizarea informațiilor de autentificare.

## **6. MECANISMUL „DO NOT TRACK”**

Așa cum am arătat la [pct.5](#), la nivel european există reglementări referitoare la monitorizarea activităților online ale utilizatorilor în scopuri de marketing, fiind necesară, în general, obținerea acordului utilizatorilor pentru astfel de practici. Însă în alte părți ale lumii astfel de situații sunt mai puțin reglementate. În aceste condiții, în cadrul World Wide Web Consortium (W3C) se lucrează, în momentul de față, la un standard tehnic (și neutru din punct de vedere tehnologic) – „[Do Not Track](#)”. Acest standard va putea fi folosit de către utilizatori pentru a le spune browserelor să semnalizeze companiilor de publicitate faptul că nu doresc ca activitățile lor online să fie monitorizate.

W3C arată că „utilizatorii au dreptul să știe care date vor fi colectate și în ce scop vor fi utilizate. Având aceste informații, ei pot decide dacă să permită sau nu monitorizarea activităților desfășurate online și colectarea datelor cu caracter personal. Multe companii Internet folosesc datele colectate în legătură cu activitățile online ale utilizatorilor pentru a personaliza conținutul furnizat utilizatorilor și a direcționa către aceștia mesaje publicitare relevante, în funcție de interesele identificate pe baza informațiilor colectate. Deși unii utilizatori apreciază această personalizare a conținutului și a mesajelor publicitare în anumite contexte, alții sunt îngrijorați în legătură cu ceea ce percep a fi o intruziune în viața lor privată.

În aceste condiții, utilizatorii au nevoie de un mecanism care să le permită să-și exprime preferințele cu privire la monitorizarea activităților desfășurate online; acest mecanism trebuie să fie ușor de configurat și eficient. În plus, site-urile web care nu pot sau nu vor să furnizeze conținut fără să ofere în același timp și publicitate comportamentală sau fără să colecteze date despre utilizatori au nevoie de un mecanism prin care să indice aceste lucruri utilizatorilor și să le permită acestora să ia o decizie în cunoștință de cauză.”

Scopul standardului „Do Not Track” este „de a oferi utilizatorului posibilitatea de a-și exprima opțiunile personale cu privire la monitorizarea activităților desfășurate online și de a comunica aceste opțiuni fiecărui server sau aplicație web cu care interacționează, permițând astfel fiecărui serviciu accesat fie să-și ajusteze

practicile în funcție de opțiunile utilizatorului, fie să ajungă la un acord separat cu utilizatorul, care să fie convenabil ambelor părți. Principiul de bază este că exprimarea preferințelor privind monitorizarea este transmisă doar atunci când reflectă o opțiune deliberată a utilizatorului. În lipsa unei opțiuni a utilizatorului, se consideră că preferința privind monitorizarea activităților online nu este exprimată.”

### **Funcționalități Do Not Track pentru motoarele de căutare**

Opțiuni pentru împiedicarea monitorizării activității online a utilizatorului sunt implementate astăzi în diverse forme. De la Internet Explorer 8 care îți oferă posibilitatea să blochezi site-uri terțe care lasă conținut atunci când vizitezi un website, până la noile extensii, add-ons și opțiuni introduse chiar în preferințele motorului de căutare. În lipsa standardului amintit mai sus, la unele motoare de căutare e mai evident cum activezi această funcționalitate, la altele e mai ascuns. Instrucțiuni pentru a seta mecanismul Do Not Track pentru Safari, Internet Explorer 9, Firefox și Chrome găsești [aici](#)

Numărându-se printre ultimii care introduc această funcționalitate, versiunea numărul 23 Google Chrome oferă posibilitatea instalării extensiilor [Do Not Track Me](#), [AVG Do Not Track](#) sau [Keep My Opt-Outs](#) care blochează cookie-uri și împiedică (momentan) doar companiile de publicitate americane să personalizeze anunțurile în funcție de comportamentul online al utilizatorului de internet.

Firefox, pe lângă add-on-ul [Do Not Track Me](#), oferă și opțiunea „[Tell web sites I do not want to be tracked](#)” ce poate fi configurată în meniul privacy. Mai mult, Internet Explorer 10 vine cu Do Not Track ca opțiune default. Decizia Microsoft a stârnit o serie de reacții puternice, răspunsul unor companii precum Yahoo și Apache fiind că [vor ignora](#) semnalele Do Not Track ale Internet Explorer 10.

O altă unealtă pe care o poți instala pe majoritatea motoarelor de căutare (și chiar ca aplicație pe iOS) este [Ghostery](#). Ghostery scanează pagina pe care o vizitezi și te anunță de existența elementelor instalate de site-uri terțe pentru a îți urmări activitatea. Îți poți seta apoi preferințele în funcție de categoriile din meniu: advertising, analytics, beacons, privacy, widgets. Mai multe informații [aici](#).

De menționat este faptul că nu toate funcționalitățile Do Not Track blochează cookie-urile. Așadar e bine să verifici ce intră în componența fiecărei extensii Do Not Track și să o alegi pe cea care reprezintă cel mai bine limitările pe care vrei să le transmiți site-urilor care îți monitorizează activitatea pe internet.

Overview interesant [aici](#).

## **7. RECOMANDĂRILE IAB ROMÂNIA PENTRU ADMINISTRATORII DE SITE-URI WEB PRIVIND COOKIE-URILE**

În iunie 2012, IAB România a publicat o serie de [recomandări privind utilizarea cookie-urilor](#) de către site-urile web. Aceste recomandări au fost grupate în două categorii:

### **7.1. INFORMAREA UTILIZATORULUI**

În momentul în care un site web folosește cookie-uri, fie în interes propriu, fie din partea terților, acesta trebuie să pună la dispoziția utilizatorului, în mod vizibil și clar, cel puțin următoarele informații:

1. faptul că site-ul utilizează cookie-uri – în special menționat dacă sunt plasate de terți (în scopuri de publicitate țargetată, de exemplu) și menționarea clară a scopurilor pentru care site-ul respectiv folosește cookie-uri;
2. ce sunt cookie-urile;
3. care este rolul lor;
4. de ce sunt folosite de terți;
5. ce tip de informații sunt accesate cu ajutorul cookie-urilor;
6. cookie-urile, securitatea și confidențialitatea datelor personale;
7. managementul cookie-urilor prin intermediul setărilor browserului;
8. de ce sunt cookie-urile importante pentru Internet;

9. dezinstalarea cookie-urilor de la terți;
10. ce se întâmplă dacă utilizatorul refuză cookie-urile.

## 7.2. MODUL DE PREZENTARE A ACESTOR INFORMAȚII

1. informațiile referitoare la cookie-uri trebuie prezentate pe site într-un mod vizibil și accesibil utilizatorilor;
2. trebuie să existe un link separat de „termeni și condiții” sau „politica de confidențialitate”;
3. acest link trebuie să fie ușor de reperat sau utilizatorului trebuie să i se indice existența acestui link și a informațiilor referitoare la cookie-uri;
4. utilizatorului trebuie să îi fie recomandat în mod vizibil să citească aceste informații și instrucțiuni;
5. recomandări: fie printr-un banner plasat în primul ecran, fie printr-un sticky ribbon, fie printr-un widget plasat vizibil – utilizatorului trebuie să i se aducă la cunoștință că site-ul folosește cookie-uri și să i se recomande informarea suplimentară referitoare la acestea.

## 8. GESTIONAREA, DEZACTIVAREA ȘI ȘTERGEREA COOKIE-URILOR

Informații detaliate referitoare la modalitățile de gestionare, dezactivare și ștergere a cookie-urilor prin utilizarea setărilor browser-ului folosit pentru navigarea pe Internet sunt disponibile la următoarele adrese:

### 8.1. INTERNET EXPLORER

Ștergerea și gestionarea modulelor cookie (IE 8, 9 și 10):

- [Internet Explorer 8](#)
- [Internet Explorer 9](#)
- [Internet Explorer 10](#)

### 8.2. MOZILLA FIREFOX

Setările pentru cookie-uri și depanarea cookie-urilor (activare și dezactivare cookie-uri, eliminare cookie-uri, blocarea anumitor site-uri de la plasarea de cookie-uri, deblocarea plasării de cookie-uri, etc)

- [Șterge cookies pentru a elimina informațiile stocate în computerul tău de alte pagini web](#)

### 8.3. GOOGLE CHROME

Gestionarea cookie-urilor (ștergere, blocare, permitere, stabilirea de excepții, etc)

- [Gestionarea cookie-urilor și a datelor despre site-uri](#)

### 8.4. SAFARI

Manage cookies – Administrează cookie-uri (doar în limba engleză)

- [Safari 6 \(OS X Mountain Lion\): Manage cookies](#)

Remove cookies – Șterge cookie-uri (doar în limba engleză)

- Safari 6 (OS X Mountain Lion): Remove cookies and other data

## 8.5. OPERA

Gestionare și ștergere cookie-uri (doar în limba engleză)

- Gestionarea cookie-urilor și a datelor despre site-uri

## 9. SURSE ȘI INFORMAȚII SUPLIMENTARE:

Acest document a fost creat și este întreținut de ApTI. Informații actualizate la data de 15.02.2013.  
Pentru orice informații sau pentru corecturi vă rugăm să ne contactați.

- All About Cookies
- About Cookies
- UK Information Commissioner's Office – "Guidance on the rule of use of cookies and similar technologies", May 2012
- Directiva 2002/58/CE privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor electronice (PDF)
- Directiva 2009/136/CE de modificare a Directivei 2002/22/CE privind serviciul universal și drepturile utilizatorilor cu privire la rețelele și serviciile de comunicații electronice, a Directivei 2002/58/CE privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice și a Regulamentului (CE) nr. 2006/ 2004 privind cooperarea dintre autoritățile naționale însărcinate să asigure aplicarea legislației în materie de protecție a consumatorului (PDF)
- Legea nr.506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice, cu modificările și completările ulterioare
- Avizul nr.4/2012 al Grupului de Lucru Articolul 29 privind cookie-urile exceptate de la obtinerea acordului, iunie 2012 (PDF)
- Recomandări IAB România privind informarea utilizatorilor cu privire la utilizarea cookie-urilor pe un site web
- World Wide Web Consortium, Tracking Preferences Expression (DNT), W3C Working Draft, 2 Octombrie 2012
- Secure Cookies
- Wikipedia - HTTP Cookie

---

[1] - Conform Legii nr.677/2001 privind protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date, un operator este „orice persoană fizică sau juridică, de drept privat ori de drept public, inclusiv autoritățile publice, instituțiile și structurile teritoriale ale acestora, care stabilește scopul și mijloacele de prelucrare a datelor cu caracter personal [...]”

[2] - Dacă folosiți Firefox, puteți afla dacă site-ul accesat folosește cookie-uri „secure” urmând instrucțiunile de la <https://httpsnow.org/help/securecookies>