CTI Jelentés

Ezeket érdemes tudni a GDPR-ról és a webes sütikről

NEMZETBIZTONSÁGI SZAKSZOLGÁLAT
1996
Fortes fortuna adiuvat

NEMZETI
KIBERVÉDELMI INTÉZET

Bevezetés

A weboldalakon felugró adatvédelmi tájékoztatók már egy ideje elválaszthatatlan társai a webes böngészésnek. Hozzászoktunk ezekhez, de tudjuk-e azt, hogy voltaképp mik ezek, és a „bosszantáson" kívül mire szolgálnak?

Jelen tájékoztatónkban azt a célt tűztük ki magunk elé, hogy érthetővé tesszük a GDPR logikáját és célját, valamint, hogy ez hogyan függ össze például a webes sütikkel. Bár 2022-ben ezek a mindennapi életünk szerves részét képezik, nem biztos, hogy mindannyian tisztában vagyunk azzal, hogy tulajdonképp hogyan kapcsolódnak egymáshoz.

Felelősségvállalás és jognyilatkozat

A tájékoztató nem teljes körűen mutatja be a GDPR-t, elolvasásával nem lehet adatvédelmi szakértővé válni, a kiadvány emellett nem minősül szakmai vagy jogi tanácsadásnak, azonban elolvasásával meg lehet megérteni a GDPR célját, azt, hogy mik számítanak személyes adatnak, és ezáltal egy kicsit másképp tekinteni a felhasználókról keletkező adatokra. Ez olyan tudás, ami a mai digitális világban biztosan hasznunkra lesz.

Mi a GDPR lényege?

Az EU 2016-ban rendeletet alkotott az európai természetes személyek személyes adatainak védelme érdekében, ez az Általános Adatvédelmi Rendelet – General Data Protection Regulation, azaz röviden: GDPR. A rendelet legfontosabb megállapítása, kiindulópontja, hogy **a természetes személyek személyes adataik kezelésével összefüggő védelme egy alapvető jog.**

A GDPR előtt is léteztek adatvédelmi jogszabályok, mint például a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. Törvény, amelyet az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Infotv.) helyezett hatályon kívül. A GDPR hatályba lépéséig az Infotv. volt a személyes adatok védelmének legfőbb szabályozója, azonban ezt követően **a két jogszabály egymással együtt, egymás kiegészítéseként alkalmazandó**. Leegyszerűsítve ez azt jelenti, hogy általános éllel a GDPR-t kell irányadónak tekinteni kivéve, ahol az Infotv. szabályai az alkalmazandók (egyebek mellett a nemzetbiztonsági vagy honvédelmi adatkezelés esetében).

Hogyan véd a GDPR?

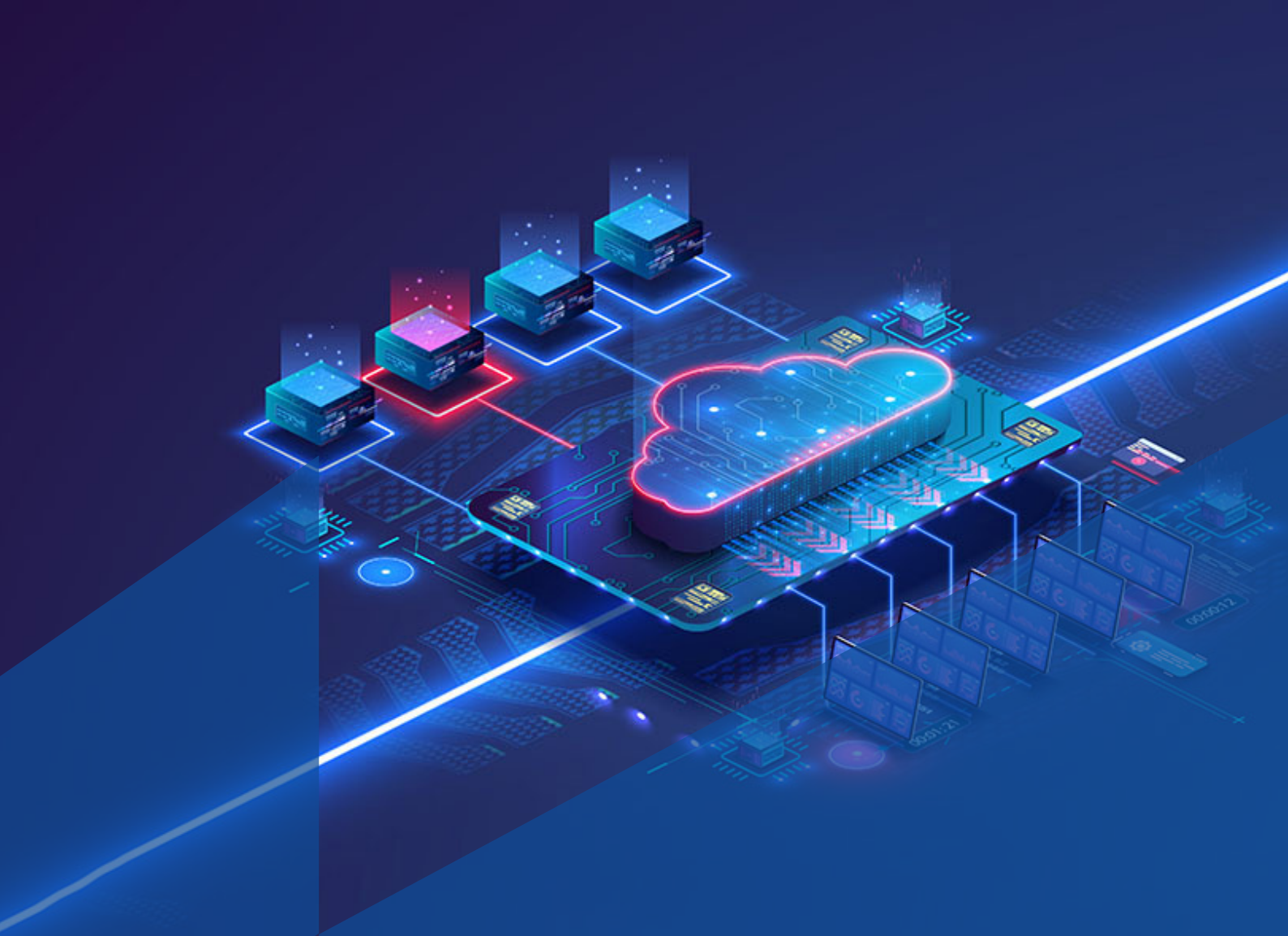
Személyes adataink védelme érdekében a GDPR a korábbiaknál szigorúbb követelményeket ír elő a személyes adatokat kezelők számára, akik egyszerűen szólva nem gyűjthetnek „hasraütés-szerűen" információt rólunk.

Személyes adatainkat csak a megfelelő jogalap megléte esetén, meghatározott célból, valamint a szükséges ideig kezelhetik, amiről közérthető módon tájékoztatniuk kell bennünket, és az adatkezeléshez egyértelmű hozzájárulást (a jogalap egy fajtája) kell kérniük tőlünk.

Fontos megjegyezni, hogy adatkezelés nem kizárólag a hozzájárulásunk alapján történhet, hanem az alábbi jogalap is eredményezheti személyes adataink kezelését:

- az adatkezelés szerződés teljesítéséhez szükséges (amelyben az érintett az egyik fél)
- az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges
- az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges
- az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásához szükséges
- az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges

Nekünk, magánszemélyeknek pedig lehetőséget biztosít az ezzel kapcsolatos jogaink érvényesítésére, ezek az ún. érintetti jogok).



Mi számít adatkezelésnek?

A személyes adatokkal végzett minden típusú tevékenység/művelet személyes adatkezelésnek minősül, például a

- gyűjtés,
- regisztráció,
- szervezés,
- strukturálás,
- tárolás,
- manipuláció,
- megváltoztatás,
- visszakeresés,
- olvasás,
- felhasználás,
- nyilvánosságra hozatal,
- terjesztés vagy más módon történő rendelkezésre bocsátás,
- módosítás,
- korlátozás,
- törlés (elektronikus adathordozó esetén) vagy
- megsemmisítés (pl. papír alapon rögzített adatoknál).

A GDPR minden fajta személyes adatkezelésre vonatkozik. Azonban egyebek mellett a statisztikai vagy oktatási célú, anonimizált adatkezelésre jóval enyhébb szabályok vonatkoznak, de ezek sem kerülnek ki a GDPR hatálya alól.

A GDPR minden tevékenységre és műveletre vonatkozik, függetlenül attól, hogy ki végzi a személyes adatok kezelését/feldolgozását. Így a szabályozás vonatkozik a vállalatokra, egyesületekre, szervezetekre, hatóságokra és magánszemélyekre.

A jogszabály „technológiasemleges" és egyaránt vonatkozik az automatizált és manuális kezelésre, feltéve, hogy az adatokat kritériumok szerint rendszerezik (pl. betűrendben). Nem számít az sem, hogy az adatokat milyen módon tárolják: IT-rendszerben, videokamerás megfigyelőrendszerben vagy papíron; ezen esetek mindegyikére vonatkoznak az általános adatvédelmi rendelet személyes adatok védelmére vonatkozó követelményei.

Röviden és tömören mindez azt jelenti, hogy a bennünket jellemző személyes információk értéket képviselnek, és elvárható, hogy a velünk kapcsolatba kerülő szervezetek ezt nem csak, hogy tiszteletben tartsák, hanem aktívan tegyenek is azért, hogy személyes adatainkat – ezáltal bennünket – védjenek a lehetséges visszaélésektől, ami nagyon sokféle formában megvalósulhat.

Mi a személyes adat?

Mi jut az eszünkbe először, ha meghalljuk azt, hogy személyes adat? Szinte biztos, hogy először mindenkinek a neve, a személyi azonosítója, és a lakcíme, hiszen ezek az adatok egyértelműen köthetőek a személyünkhöz, személyazonosságot igazoló okmányokon is szerepelnek.

Fontos tudni azonban, hogy a GDPR ennél jóval széleskörűbben értelmezi a személyes adatok körét:

- Személyes adat minden olyan információ, amely valamely azonosított vagy azonosítható személlyel kapcsolatos.
- Mindazon információk, amelyek összegyűjtése egy bizonyos személy azonosításához vezethet, ugyancsak személyes adatnak minősülnek.

Milyen személyes információkról van szó?

Ez lényegében lehet bármi:

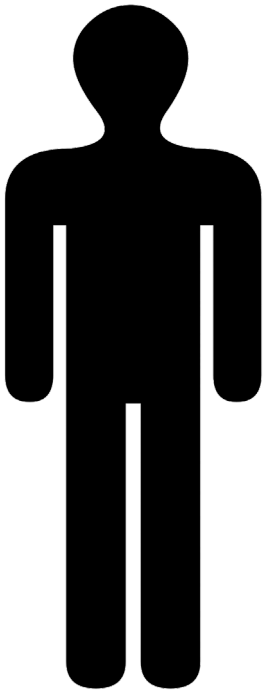
vallási és ideológiai nézetek

demográfiai jellemzők

etnikum

szexuális élet

végzettséggel és munkával kapcsolatos információk



fizikai jellemzők

viselkedés

egészségügyi állapot

vagyoni helyzet

preferenciák

családdal kapcsolatos információk

Azonban, ha az adatok utalnak valakinek az egészségügyi állapotára, politikai vagy vallási nézeteire, etnikai hovatartozására, nemi életére, vagy ezek személyazonosításra használt genetikai vagy biometrikus adatokra, azokat a GDPR különleges adatoknak nevezi, amelyek gyűjtése – főszabály szerint - tilos, mert mélyen a magánszférához tartoznak és jogosulatlan megismerésük lényeges érdeksérelmet okozhat az érintettnek.

Miért lehet gond az, ha valaki beazonosítható?

Azért, mert a beazonosítás során, vagy ezt követően az adott személyhez konkrét ismeretek társíthatók, ami sértheti az adott személy magánszféráját, és lehetőséget adhat arra, hogy ezekkel visszaélve számára kárt okozzanak.

Mi minden vezethet ahhoz, hogy valaki beazonosíthatóvá váljon?

A helyzet az, hogy a mai digitális korban elképesztően sokféle technikai adat vezethet ahhoz, hogy egy konkrét személy beazonosítható legyen, azaz válhat személyes adattá:

- azonosítók
- online fiókok
- az IP címünk,
- a mobiltelefonunk egyedi azonosítói,
- az online fiókjaink azonosítói, vagy épp a
- webes sütik.
- A digitális kép és hangfelvételek személyes adatnak minősülnek.
- A titkosított adatok és a különféle elektronikus azonosítók, például az IP-címek és a sütik akkor minősülnek személyes adatnak, ha természetes személyhez hozzákapcsolhatók.
- Személyes adatnak minősülnek az olyan információk is, amelyeket kódoltak, titkosítottak vagy álnévvel láttak el, de kiegészítő adatokkal a természetes személlyel kapcsolatba hozhatóak.

Ki és hogyan élhet vissza a személyes adatokkal?

Személyes adatokkal tulajdonképpen bárki követhet el visszaélést.

Elkövethet egy adatkezelő szervezet, ha nem tesz eleget a GDPR által meghatározott kötelezettségeknek, például egy szervezet konferenciát szervez, ahol fénykép készül az előadókról, azonban ehhez nem kéri a hozzájárulásukat.

De személyes adattal történő visszaélésnek számít az is, ha valaki egy másik személy nevével, és fényképével regisztrál egy Facebook fiókot.

- Személyes adataink biztonságára nézve jelentős kockázatot jelentenek az adatszivárgások, azok az események, amikor egy szervezet által kezelt adatok illetéktelenek számára elérhetővé válnak. A bűnözők számára a személyes adatok kifejezetten értékesek. Például, ha ismerik az e-mail címünket, azzal lehetőség adódik arra, hogy megtévesztő e-maileket küldjenek, ha pedig emellett további személyes információ is a rendelkezésükre áll rólunk, még inkább kifinomultabbá tehetnek egy internetes támadást. (ún. spearphishing) Arról nem is szólva, hogy amennyiben a bankkártya adataink rossz kezekbe kerülnek, oda lehet a megtakarításunk.

- De ne csak az internetes támadókra gondoljunk. Egy szervezet HR részlegén adott esetben jogszerűtlenül kezelt önéletrajzok – hogy egy tipikus rossz gyakorlatot említsünk – ugyanúgy személyes adatokat érintő, azaz adatvédelmi kockázatot, adott esetben konkrét incidenst jelentenek, hiszen ezekhez bármelyik, az adott cégnél dolgozó munkatárs hozzáférhet, és ezáltal ismeretet szerezhet születési

adatainkról, végzettségünkről, arról, hogy hol lakunk, hol dolgoztunk eddig. Ezekkel az adatokkal valaki visszaél, amennyiben pl. elmenti a telefonjában.

Ráadásul egy másféle kockázattal is számolnunk kell, ugyanis a szervezetek a tudtunkon kívül olyan megfigyeléseket is tehetnek rólunk, ami alapján képesek profilt alkotni vásárlási szokásainkról, érdeklődési körünkről, amit legtöbbször célzott marketing tevékenységre használnak fel.

Mik azok a sütik, és hogyan kapcsolódnak az adatvédelemhez?

A süti (angol szóhasználattal: cookie) olyan információ, amelyet egy weboldal helyez el a felhasználó számítógépén. A sütik olyan kisebb programok, amelyek a meglátogatott weboldal funkcionális működését segítik, adatokat gyűjtenek forgalomelemzési célból, esetleg marketing célokat szolgának. A sütik korlátozott mennyiségű információt tárolnak egy adott weboldalon egy webböngésző-munkamenetből, amelyek a jövőben visszakereshetők. Néha böngésző-, web- vagy internetes sütinek is nevezik őket.

A sütikhez hozzáférhet a böngésző felhasználója, az a webhely, amelyen a felhasználó tartózkodik, vagy egy harmadik fél, amely az információkat különböző célokra használhatja fel. A sütik általános felhasználási esetei közé tartozik a munkamenet-kezelés, a személyre szabás és a követés.

A sütik először 1994-ben jelentek meg a Netscape Navigator webböngésző részeként. Segítettek a böngészőnek megérteni, hogy a felhasználó felkeresett-e már egy adott webhelyet. A Netscape fejlesztője, Lou Montulli dolgozta ki a sütik kezdeti formáját. A találmány megkapta az 5 774 670A számú szabadalmat az Egyesült Államokban, a következő leírással: „Állandó kliens állapot a hipertext átviteli protokoll alapú kliens-szerver rendszerben”.

Mit tartalmaznak a sütik?

A sütiknek hat paraméterük van, amelyek jellemzik őket:

- a süti neve;
- a süti értéke;
- a süti lejárati dátuma – ez határozza meg, hogy a süti mennyi ideig marad aktív
- a böngészőjében;
- az elérési út, amelyre a süti érvényes – ez beállítja a süti URL elérési útját, amelyen belül érvényes, ezen az útvonalon kívüli weboldalakon nem használhatóak a sütik;
- az a domain, amelyen a cookie érvényes, ez a sütit használhatóvá teszi a szerver bármely oldalán, amennyiben az oldal több szerveren fut;
- Biztonságos kapcsolat szükségessége – ez azt jelzi, hogy a cookie csak biztonságos szerveren használható, úgymint egy SSL-t használó oldal.

A sütik típusai

Munkamenet sütik (Session cookies)

A munkamenet-sütik, más néven „ideiglenes sütik", segítenek a webhelyeknek felismerni a felhasználókat és a webhelyen való navigáció során szolgáltatott információkat. A munkamenet-sütik csak addig őriznek meg információkat a felhasználó tevékenységeiről, amíg azok a weboldalon vannak. A webböngésző bezárása után a sütik törlődnek. Ezeket általában vásárlási vagy e-kereskedelmi webhelyeken használják.

Állandó sütik (Permanent cookies)

Az állandó sütik a webböngésző bezárása után is működnek. Megjegyezhetik például a bejelentkezési adatokat és jelszavakat, így a webes felhasználóknak nem kell minden alkalommal újra megadniuk azokat, amikor egy weboldalt használnak. A törvény kimondja, hogy az állandó sütiket 12 hónap elteltével törölni kellene, valójában felhasználói interakció hiányában általában tovább is a gépen maradnak.

Első féltől származó sütik (First-party cookies)

Az első féltől származó sütiket közvetlenül a felhasználó által meglátogatott webhely (azaz a domain) telepíti (azaz a böngésző címsorában megjelenő URL). Ezek a sütik lehetővé teszik a webhelytulajdonosok számára, hogy elemzési adatokat gyűjtsenek, emlékezzenek a nyelvi beállításokra, és egyéb hasznos funkciókat hajtsanak végre, amelyek jó felhasználói élményt biztosítanak.

Harmadik féltől származó sütik (Third-party cookies)

A harmadik féltől származó sütiket harmadik felek telepítik azzal a céllal, hogy bizonyos információkat gyűjtsenek a webfelhasználóktól, hogy kutatásokat végezzenek például viselkedéssel, demográfiai adatokkal vagy költési szokásokkal kapcsolatban. Általában azok a hirdetők használják, akik biztosítani akarják, hogy a termékeket és szolgáltatásokat a megfelelő célközönség számára kínálhassák.

Flash sütik

A Flash sütik, más néven „szuper sütik", függetlenek a webböngészőtől. Úgy tervezték, hogy állandóan a felhasználó számítógépén tárolhatók legyenek. Az ilyen típusú sütik akkor is a felhasználó eszközén maradnak, ha az összes sütit törölték a böngészőből.

Zombi sütik

A zombi sütik a flash sütik egy fajtája, amely automatikusan újra létrejön, miután a felhasználó törölte őket. Ez azt jelenti, hogy nehéz észlelni őket, illetve megszabadulni tőlük. Gyakran használják online játékokban, hogy megakadályozzák a felhasználókat a csalásban, de arra is használhatják őket, hogy rosszindulatú szoftvereket telepítsenek a felhasználó eszközére.

Mit adunk át a honlapok üzemeltetőinek, amikor elfogadjuk a sütiket?

Minden honlap, minden szolgáltató a webhelyen Adatvádelmi tájékoztatót, szabályzatot köteles elhelyezni. Ezekben a szabályzatokban ki kell térni arra, hogy a honlap milyen sütiket, milyen célból használ, a megszerzett adatokat hogyan kezeli. Kötelező ezen kívül az Adatvédelmi tisztviselőjének (DPO, Data Protection Officer) az adatait, elérhetőségét megadni. A szabályzatok rendszerint felsorolják, hogy a fenti felsorolásból a honlap milyen típusú sütiket használ, az adatkezelés jogalapját és célját (ez a legtöbbször a személyre szabott szolgáltatás, valamint a marketing).

A sütik által összegyűjtött adatokat sok esetben profilalkotásra használják. Ehhez általában a következő adatok begyűjtése történhet: név, e-mail cím, születési idő, lakhely, nem, telefonszám, látogatás ideje-időtartama, megtekintett aloldalak (termékek), vásárlóerő (egyszeri költés, átlagos költés).

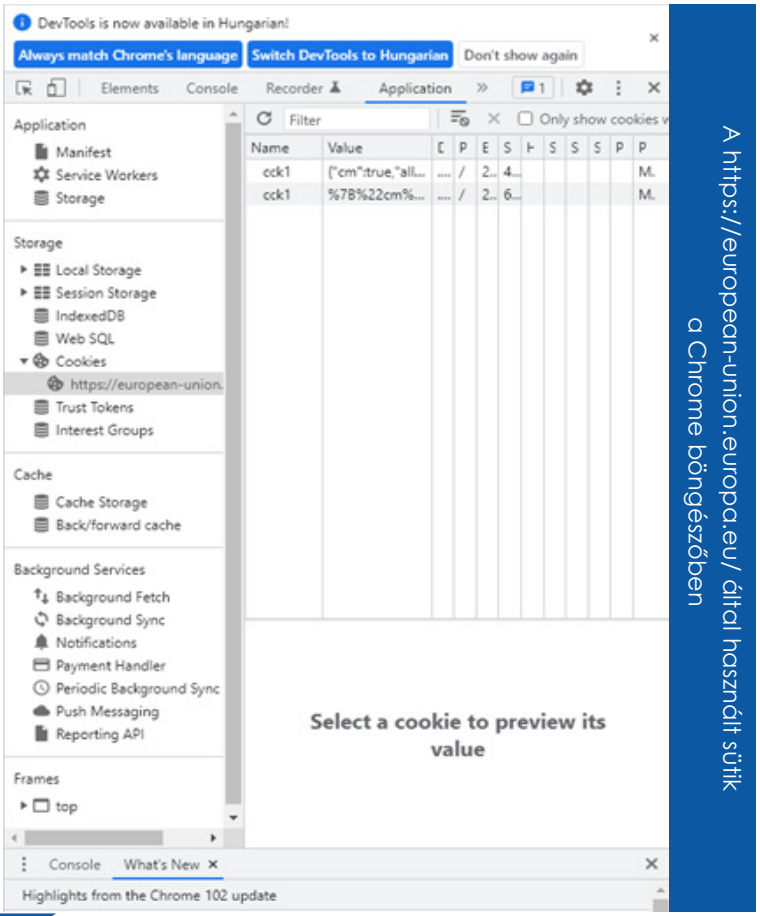
Mit tehetünk?

Fontos meghegyezni, hogy a sütikkel történő visszaélés, csalás jelenleg még ritka. A sütik nem vírusok, és nem hordoznak rosszindulatú programokat. Nem tartalmaznak végrehajtható, kihasználható kódsorokat. A sütikkel való csalás azonban világszerte egyre jobban teret hódít, főként azért, mert felhasználható a felhasználók személyazonosságának meghamisítására, munkamenetének ellopására vagy arra, hogy egy felhasználó személyazonosságát rosszindulatú műveletek végrehajtásánál felhasználja.

A legfontosabb lépések, amelyeket önmagunk védelmében megtehetünk, a következők:

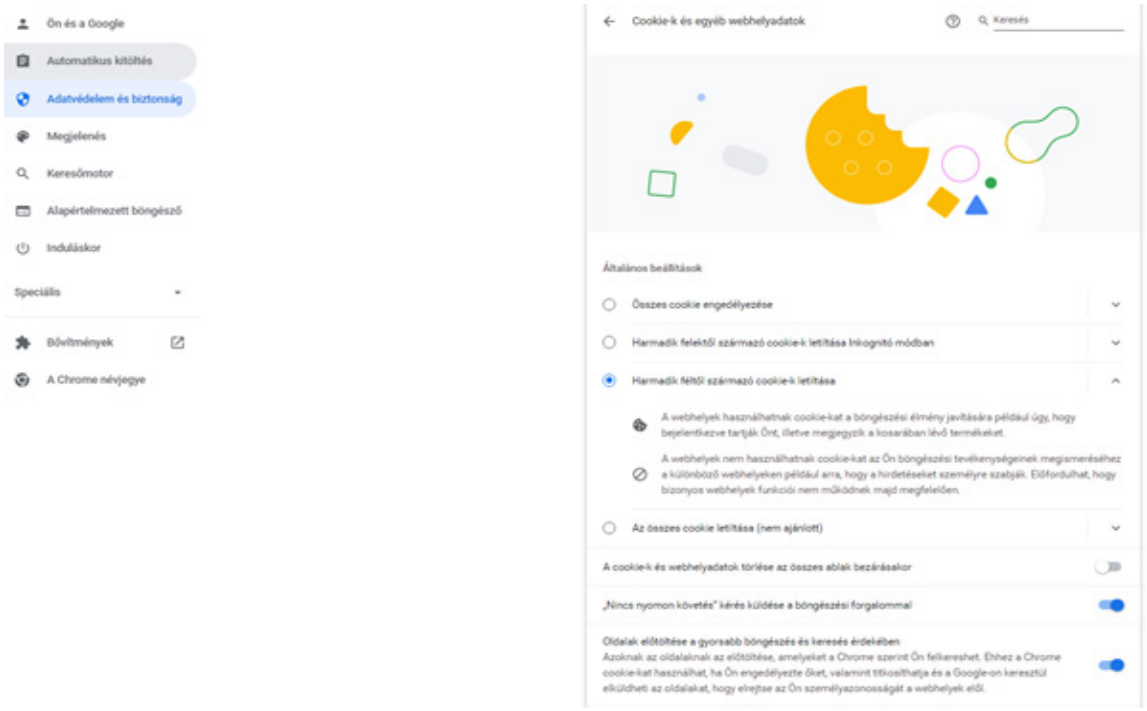
- tartsuk naprakészen a böngészőt és a beépülő modulokat;
- tiltsuk le a harmadik féltől származó sütiket;
- válasszuk ki, hogy webhelyenként engedélyezzük vagy blokkoljuk a sütiket (white list, black list);
- használjuk böngésző „inkognitó" módját;
- telepítsünk megbízható kémprogram-elhárító alkalmazásokat, és tartsuk azokat is naprakészen!

A böngészőnkkel ellenőrizhetjük, hogy a gépünkre milyen sütik települtek. Ezt pl. az egyik legnépszerűbb böngészőben a Google Chrome-ban az alábbiak szerint tehetjük meg. A honlapon jobb klikk > Vizsgálat > Sources > Application > Cookies



A https://european-union.europa.eu/ által használt sütik a Chrome böngészőben

A böngésző ad némi lehetőséget a sütik beállításait illetően. A jobb felső sarokban a legördülő menü Beállítások → Adatvédelem és biztonság → Sütik és egyéb webhelyadatok. Itt több lépésben lehet állítani a sütik engedélyezését, illetve tiltását.



A Chrome süti beállításai

Ugyanitt beállíthatjuk, hogy mely honalapoknak engedélyezzük, hogy sütiket használjanak (white list). Mely webhelyek bezárásakor törlődjenek mindenképpen a sütik és melyek azok a webhelyek, amelyek sosem használhatnak sütiket (black list).

Miért érdemes törölni a sütiket?

- **Titkosítatlan webhely.** Ha egy webhely nincs titkosítva, akkor nem védi a személyes adatainkat, amikor a sütikről és a személyes adatokról van szó. Ilyen oldalakon érdemes elutasítani, vagy elfogadás esetén az oldal használatának befejezését követően törölni a sütiket.

- **Harmadik féltől származó sütik.** A harmadik féltől származó sütik sebezhetővé tehetnek bennünket, és azokat javasolt visszautasítani vagy törölni, ha már tárolva vannak a böngészőben. Ellenkező esetben a webhely tulajdonosa eladhatja böngészési adatainkat harmadik félnek, például hirdetőknek. A harmadik féltől származó sütikkel az a probléma, hogy elveszítjük a kontrollt az adataink felett, nem tudhatjuk, hogy a harmadik fél mit tesz az adatokkal. A harmadik fél – vagy valaki, akinek tovább osztják az adatokat – felhasználhatják a személyes adatokat olyan online bűncselekmények elkövetésére, mint például a személyazonosság-lopás.

- **Lassabb számítógép-sebesség.** Bár kicsik, a sütik helyet foglalnak a számítógépen. Ha túl sokat tárolunk belőlük hosszú ideig, akár le is lassíthatják a számítógép és más eszközök sebességét.

- **Megjelölt, gyanús sütik.** Ha víruskereső szoftverünk gyanús sütiket jelez, töröljük azokat.

- **Személyazonosító adatok használatakor.** A sütik rögzíthetik a személyazonosításra alkalmas adatokat, hogy például automatikusan kitöltsék az űrlapokat a böngészőkben. Ezek az információk magukban foglalhatják a nevet, címet, bejelentkezési adatokat és egyéb személyes adatokat,

amelyeket károkozásra, például személyazonosság-lopásra és egyéb online csalásra használhatnak fel.

- **Elavult sütik.** Ha egy webhely oldalát frissítették, a sütikben tárolt adatok ütközhetnek az új oldallal. Ez gondot okozhat, például amikor legközelebb próbál meg kitölteni egy űrlapot az oldalon vagy betölteni az oldalt.

Mikor nem érdemes törölni a sütiket?

- **Weboldal elérése.** A sütik elfogadásának megtagadásával kapcsolatos egyik probléma az, hogy ha nem fogadjuk el a sütiket, előfordulhat, hogy egyes webhely-tulajdonosok nem engedélyezik a webhelyeik használatát. (Tegyük hozzá, hogy ez csupán a)
- **Jobb felhasználói élmény.** Előfordulhat, hogy bizonyos webhelyeken nem kapjuk meg a teljes felhasználói élményt, ha elutasítjuk a számítógépes sütiket. A sütik például megjegyezhetik és menthetik arólunk szóló hasznos adatokat, például érdeklődési körünket vagy a bevásárlókosárban megmaradt tételeinket.
- **Egyszerűbb, gyorsabb bejelentkezés.** A webböngészőbe mentett számítógépes sütik segítségével hatékonyabban használhatjuk kedvenc webhelyeinket. Rendkívül kényelmessé tehetik az online tranzakciókat, hiszen nem kell minden alkalommal megadnunk adatainkat, amikor felkeresünk egy webhelyet. Ehelyett gyorsan és egyszerűen bejelentkezhetünk kedvenc szolgáltatásainkba.

Milyen hatásai lehetnek annak, ha deaktiváljuk a sütiket?

A sütik elutasítása hatással lehet a felhasználói élményre a webhelyek használata során. Bizonyos sütik eleve szükségesek a webhely működéséhez. A sütik általában csak felhasználói interakcióra aktiválódnak, amelyek kérésként jelennek meg, mint például az adatvédelmi beállítások megadása, bejelentkezés vagy űrlapok kitöltése. Ha például úgy állítjuk be böngészőt, hogy blokkolja ezeket a sütiket, vagy figyelmeztessen rájuk, a webhely egyes részei nem fognak működni.

Ha elutasítjuk az összes lehetséges süti használatát, a belső és a harmadik féltől származó sütik deaktiválásra kerülnek. A belső sütik törlődnek, a harmadik féltől származó sütiket automatikusan nem lehet törölni, ezért a felhasználónak saját magának kell törölnie a harmadik féltől származó sütiket. Ezt megteheti böngészője beállításai között.

Ne feledjük! A GDPR alapján számtalan jog illet bennünket, amelyekkel az Adatvédelmi tájékoztatóban kötelezően megadott Adatvédelmi tisztviselőhöz (DPO) fordulhatunk. Ezen érintetti jogok a következők.

- **Tájékoztatás joga (GDPR 12. cikke):** Tájékoztatás kérhető az adatkezelőtől a személyes adatok körét, valamint az adatkezelés jogalapját, célját, forrását, idejét illetően. Tájékoztatás kérhető továbbá, hogy kinek, mikor, milyen jogszabály alapján, mely személyes adathoz biztosít vagy biztosított hozzáférést az adatkezelő, illetőleg történt-e adatvédelmi incidens az érintett adatait érintően.

- **Hozzáférés joga (GDPR 15. cikke):** Az érintett jogosult arra, hogy az adatkezelőtől tájékoztatást kapjon arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e, és ha ilyen adatkezelés folyamatban van, akkor jogosult arra, hogy az adatkezelés lényeges körülményeiről tájékoztatást kapjon.

- **Helyesbítés joga (GDPR 16. cikke):** Az érintett jogosult arra, hogy kérésére az adatkezelő helyesbítse a rá vonatkozó pontatlan adatokat, valamint kiegészítse a hiányos adatokat.

- **Törlés joga (GDPR 17. cikke):** Az érintett – általánosságban – jogosult arra, hogy kérésére az adatkezelő törölje a rá vonatkozó személyes adatokat.

- **Korlátozás joga (GDPR 18. cikke):** Az érintett jogosult arra, hogy kérésére az adatkezelő zárolja az adatait, ha:

  - az érintett vitatja a személyes adatok pontosságát;
  - az adatkezelés jogellenes, de az érintett a törlés helyett a zárolást kéri;
  - az adatkezelőnek nincs szüksége a személyes adatok kezelésére, de az érintett igényli azokat jogi igény előterjesztéséhez, érvényesítéséhez vagy védelméhez;
  - az érintett a GDPR 21. cikk (1) bekezdése szerint tiltakozik az adatkezelés ellen.

- **Tiltakozás joga (GDPR 21. cikke):** Az érintett jogosult tiltakozni személyes adatainak folyamatban lévő kezelése ellen és annak a továbbiakban történő megszüntetését kérheti, ha az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez, vagy közhatalmi jogosítvány gyakorlásához szükséges, vagy az adatkezelés közérdekű.

Ezen túl érdemes lehet a böngészőkhöz fejlesztett különböző, süti tematikájú beépülők használatát megfontolni.

Nemzetközi összehasonlítás

Érdemes megnézni, hogy az Európai Unió GDPR rendelkezéseihez képest az Egyesült Államok hogyan kezeli a személyes adatok védelmét.

Ma az Egyesült Államokban nincs egységes nemzeti adatvédelmi törvény. Ehelyett a vállalkozások megpróbálják értelmezni az egyes államok és iparági szabályozó testületek által hozott különféle szabályozások és törvények „vegyes salátáját". Széles körben elterjedt nézet, hogy országos adatvédelmi törvények megalkotására lenne szükség, mivel a technológia folyamatosan fejlődik, és életünk számos területére hatással van, személyes adataink tömkelegét kezelik a különböző digitális szolgáltatások. Tekintettel arra, hogy az elektronikus szolgáltatások, a kereskedelem ritkán áll meg az államhatároknál, ezért a különböző állami és iparági szabályozások csak zavart keltenek és hatékonysági problémákhoz vezetnek.

Különbség az Egyesült Államok és az EU adatvédelmi törvényei között:

Nem lehet tisztességes összehasonlítást végezni, mert jelenleg nincs a GDPR-nak megfelelő USA-beli szabályozás. Az EU alapvetően tiszteletben tartja a magánélet védelmét, mint a polgárok alapvető jogát.

A GDPR egy átfogó személyes adatvédelmi keretrendszer, amely ezen jogok védelmét szolgálja. Irányítja az EU-tagállamokban működő vállalatokat, valamint az EU-lakosokkal kapcsolatba kerülő nemzetközi szervezeteket.

Jónéhány törvényjavaslat létezik az USÁ-ban, pl. az amerikai adatterjesztési törvény (American Data Dissemination Act), a fogyasztói adatok védelméről szóló törvény (Consumer Data Protection Act) és az adatkezelési törvény (Data Care Act). Jelenleg azonban egyetlen javaslat sem kapott elegendő támogatást a Kongresszusban ahhoz, hogy új törvényként hatályba léphessen.

A jelenleg hatályban lévők közül a legközelebbi nemzeti törvény vitathatatlanul a HIPAA (Health Insurance Portability and Accountability Act – az egészségbiztosítási hordozhatóságról és elszámoltathatóságról szóló törvény) lenne, amelyet a betegek magánéletének és az egészségügyi információk védelmére terveztek. Ez azonban nem pótolja a fogyasztói adatvédelemre és adatbiztonságra vonatkozó szabályozásokat az összes többi iparágban.

NEMZETI
KIBERVÉDELMI INTÉZET

nki.gov.hu

titkarsag@nki.gov.hu

+36 (1) 325 7672

Nemzeti Kibervédelmi Intézet

@ nki.gov.hu

Kibertámadás!
podcast

2022