

FRUMKVÆÐISSKOÐUN FJARSKIPTASTOFU

NOTKUN Á VEFKÖKUM HJÁ VÖLDUM VEFÞJÓNUSTUADILUM



Efnisyfirlit

Efnisyfirlit	1
1. Inngangur	2
1.1. Almenn	2
1.2. Aðferðafræði við framkvæmd skönnunar	2
1.3. Afmörkun úttektarandlags	3
2. Vefkökunotkun í framkvæmd	4
2.1. Flokkun á vefkökum	4
2.2. Mikilvægi trausts í viðskiptum á netinu	5
2.3. Kröfur til notkunar á vefkökum eru ólíkar eftir tegund þeirra	6
3. Lög og reglur sem við eiga	7
3.1. Lög nr. 70/2022 um fjarskipti	7
3.2. Lög nr. 90/2018 um persónuvernd og vinnslu persónuupplýsinga	8
4. Frumniðurstöður	10

Um framkvæmd úttektarinnar



Framkvæðisúttekt þessi byggir á greiningu átta vefsvæða sem skönnuð voru með opnum hugbúnaði hins Evrópska persónuverndarráðs (e. European Data Protection Board) í þeim tilgangi að kanna hvort notkun á vefkökum samrýmist ákvæðum fjarskiptalaga. Hugbúnaðurinn sem notast var við var útbúinn til að eftirlitsstofnanir og aðrir aðilar gætu athugað hvort vefsvæði samrýmist viðeigandi lögum og reglum um notkun vefkaka. Hugbúnaðinum er hægt að hlaða niður á <https://code.europa.eu>. Skönnun vefsvæðanna fór fram frá júlí til desember 2024. Fjarskiptastofa naut ráðgjafar Deloitte við framkvæmd úttektarinnar.

1. Inngangur

Fjarskiptalög, nr. 70/2022, (hér eftir „fjarskiptalög“) setja fram grundvallarreglu um fjarskiptaleynd sem felur í sér að öll vinnsla fjarskipta, þ.m.t. geymsla, hlustun, upptaka eða hlerun, er óheimil nema með upplýstu samþykki notanda eða á grundvelli lagaheimildar. Fjarskiptalög innleiða ákvæði tilskipunar 2002/58/EB um persónuvernd í fjarskiptum sem er ætlað að tryggja fjarskiptaleynd og leynd fjarskiptaumferðarupplýsinga. Fjarskiptalög innihalda jafnframt reglur um hvenær og hvernig sé heimilt að nota kerfi og búnað, þ.m.t. vefkökur, til að safna og/eða geyma upplýsingar um athafnir eða samskipti notanda í endabúnaði hans, fylgjast með athöfnum notanda eða veita aðgang að slíkum upplýsingum. Meginreglan er sú að notkun á vefkökum í framangreindum tilgangi er óheimil nema samkvæmt upplýstu samþykki notanda eða samkvæmt heimild í lögum, sbr. 2. mgr. 88. gr. laganna.

1.1. Almenn

Fjarskiptalög gilda um fjarskipti, fjarskiptaþjónustu og fjarskiptanet, sbr. 1. mgr. 1. gr. laganna, og er markmið þeirra m.a. að auka vernd og valmöguleika neytenda, sbr. 2. gr. laganna. Í 1. mgr. 88. gr. fjarskiptalaga er lögð fram sú grundvallarregla um fjarskiptaleynd, að öll vinnsla fjarskipta, þ.m.t. geymsla, hlustun, upptaka eða hlerun, sé óheimil nema með upplýstu samþykki notanda eða á grundvelli lagaheimildar.

Fjarskiptastofu er heimilt að gera úttektir og prófanir á því hvort fjarskiptafyrirtæki uppfylli kröfur fjarskiptalaga. Þegar vefkökur eru notaðar á ölögmætan hátt skerða þær friðhelgi einkalífs notenda þar sem athafnir þeirra, virkni og hegðun eru kortlögð eftir atvikum yfir langan tíma án vitundar og/eða vilja þeirra. Í ljósi þess að fáar kvartanir hafa borist Fjarskiptastofu í tengslum við notkun á vefkökum eða annars konar búnaði samkvæmt framangreindu hefur stofnunin ákveðið að hefja frumkvæðisskoðun á því hvort valdir vefþjónustuaðilar fylgi framangreindu ákvæði um leynd fjarskipta í framkvæmd.

Beinist frumkvæðisúttektin að því hvort valdir vefþjónustuaðilar noti vefkökur á vefsvæðum sínum, sem ætlaðar eru í öðrum tilgangi en lögmætum, og komi þeim þar með fyrir í endabúnaði notanda, sem skoðar umrætt vefsvæði eða undirsíður þess í netvafr¹, sem og hvort upplýsts samþykkis notanda sé aflað á grundvelli fullnægjandi fræðslu, áður en slíkum vefkökum er komið fyrir. Þá tekur frumkvæðisúttekt þessi einungis til notkunar á vefkökum sem vefþjónustuaðilar koma fyrir í endabúnaði notaði við heimsókn á þau vefsvæði sem skoðun Fjarskiptastofu beinist að. Ekki er litið til notkunar á vefkökum sem umræddir vefþjónustuaðilar koma hugsanlega fyrir á öðrum vefsvæðum en þeim sem þeir sjálfir reka, t.d. á vefsíðum þriðju aðila eða viðskiptavina sinna.

1.2. Aðferðafræði við framkvæmd skönnunar

Skönnun var framkvæmd með opnum hugbúnaði hins Evrópska persónuverndarráðs (e. The European Data Protection Board website auditing tool). Hugbúnaðurinn er byggður ofan á chromium netvafra, chrome útgáfa 106.0.5249.103, og greinir og skráir allar upplýsingar og

¹ Í þessari frumkvæðisskoðun er jöfnum höndum vísað til vefsvæðis (sem nær yfir tiltekna forsiðu vefsvæðis og viðeigandi undir-síðna) og vefsíðu (einstök vefsíða s.s. forsiða eða undirsíða vefsvæðis).

hegðun sem innbyggður chrome og chromium vafri notar á tilteknu vefsvæði sem er til skoðunar. Í hugbúnaðinum eru upplýsingasamskipti vafrans tengd við lotur² sem skilgreindar eru af notanda tólsins, t.d. skoðun vefsvæðis þar sem notandi er auðkenndur eða ekki, eða skoðun þar sem að notandi hefur annað hvort veitt leyfi fyrir vefkökum umfram þær sem eru nauðsynlegar fyrir lotu eða ekki.

Hugbúnaðurinn útbýr yfirlitsskýrslur fyrir þær vefsíður og/eða undirsíður sem tilheyra því vefsvæði sem skoðað var með hugbúnaðinum. Í þessum yfirlitsskýrslum birtist tafla yfir allar vefkökur sem hugbúnaðurinn greinir ásamt nánari lýsingu á vefkökum út frá léni, hýsingu, uppruna og líftíma vefköku. Flokkun á vefkökum eftir tilgangi er byggð á mati sérfræðinga og opinberum upplýsingum um vefkökur.³ Jafnframt birtast í yfirlitsskýrslunum annars konar upplýsingar sem ekki eru teknar til skoðunar í frumkvæðisathugun þessari s.s. hvort vefsvæði sé öruggt fyrir tilstilli HTTPS og SSL svo dæmi séu tekin. Þær upplýsingar úr yfirlitsskýrslum hugbúnaðarins sem unnið var með í þágu frumkvæðisskoðunar þessarar eru upplýsingar um vefkökur og gildi þeirra sem vistuð voru í staðbundnu minni netvafra þegar skoðun vefsvæða fór fram.

1.3. Afmörkun úttektarandlags

Eins og fyrr greinir beinist úttektin að vefþjónustuaðilum. Í úttekt þessari er hugtakið vefþjónustuaðili skilgreint svo:

Aðili sem rekur vefsíðu í ágóðaskyni sem er almennt opin neytendum og býður þeim upp á milligöngu um kaup eða kynningu á vörum og þjónustu í boði annarra fyrirtækja. Vörur og þjónusta aðilans skulu alfarið eða nær eingöngu vera í boði á internetinu. Um er að ræða þjónustu sem er þess eðlis að hægt er að vinna upplýsingar um kauphegðun notenda vefsíðunnar, t.d. ekki þjónustusíður fyrir atvinnumiðlun, skoðanakannanir og þess háttar.

Fjarskiptastofa ákvað að velja þessa tegund fyrirtækja í úttektina í ljósi þess hvað markaðssetning og viðskipti yfir internetið er veigamikill og ráðandi þáttur í starfsemi þeirra. Má í raun segja að vefsíður þessara aðila sé rafrænt markaðstorg fyrir fyrirtæki með verslun á vörum og þjónustum.

Við val á tilteknum vefþjónustuaðilum var horft til niðurstöðu Meðmælinga Maskínu um vefþjónustur fyrir árið 2023.⁴ Hafa ber í huga að skilgreining Fjarskiptaþjónustu á vefþjónustuaðila er þó aðeins þrengri en sem leiðir af könnun Maskínu.

² Lota (e. session) er hugtak yfir þann tíma sem notandi er virkur á tilteknu vefsvæði eða forriti. Lota hefst þegar notandi byrjar að eiga samskipti eða nota vefsvæði t.d. með því að opna vefsíðu og lýkur þegar notandi fer af síðunni eða lokar netvafra. Á meðan á lotu stendur geta vefkökur fylgst með aðgerðum, virkni og hegðun notanda á vefsvæði m.a. vegna tæknilegrar geymslu í lögmætum tilgangi og/eða til að hægt sé að birta notendum sérsniðnar auglýsingar.

³ Flokkun og tilgangur vefkaka eins og þau eru sett fram í skýrslu þessari byggja á almennri skilgreiningu og opinberum upplýsingum út frá nöfnum og innihaldi þeirra. Ekki er útilokað að tilgangur og notkun vefkaka hjá einstaka vefþjónustuaðilum viki frá þeirri almennu skilgreiningu.

⁴ Nýliðar áberandi meðal 12 fyrirtækja sem hljóta Meðmælingu Maskínu 2023 | maskina.is

2. Vefkökunotkun í framkvæmd

Notkun á vefkökum getur þjónað margvíslegum tilgangi. Vefþjónustuaðilar og aðrir aðilar sem eiga og/eða reka vefsvæði geta sem dæmi notað vefkökur til að tryggja virkni vefsvæðis, til að fylgjast með því hvernig notendur nota vefsíðu og til að bera kennsl á notendur í því skyni að bjóða þeim sérsniðnar auglýsingar. Ólíkar lagakröfur hvíla á framangreindum aðilum eftir því í hvaða tilgangi vefkökur eru notaðar hverju sinni. Gildandi íslensk fjarskiptalöggjöf byggir á evrópsku regluverki einkum tilskipun 2002/58/EB um persónuvernd í fjarskiptum. Stofnanir Evrópusambandsins hafa unnið að endurnýjun tilskipunarinnar og fyrir liggur tillaga að reglugerð um sama efni en hún hefur ekki verið samþykkt.

2.1. Flokkun á vefkökum

Í framkvæmd og út frá gildandi Evrópuregluverki um persónuvernd í fjarskiptum⁵ hafa vefkökur almennt verið flokkaðar eftir þeim *tilgangi* sem þær eru notaðar í. Flokkun á vefkökum er mikilvæg þar sem ekki er nauðsynlegt að afla samþykkis þegar vefkökur eru notaðar til að fá aðgang að upplýsingum og/eða til tæknilegrar geymslu í lögmætum tilgangi⁶ og með vitund hlutaðeigandi notanda. Vefkökur eru almennt flokkaðar eftir tilgangi sínum í eftirfarandi flokka:

- 1. Nauðsynlegar vefkökur** (e. strictly necessary cookies): Þessar vefkökur eru m.a. nauðsynlegar í þeim tilgangi að veita umbeðna þjónustu, auðkenna endabúnað fjarskipta og uppgötva sendingarvillur.
- 2. Frammistöðu/tölfræði vefkökur** (e. performance/analytics cookies): Þessar vefkökur safna upplýsingum um hvernig notendur nota vefsvæði, s.s. um fjölda heimsókna á vefsvæði og birtingarhraða vefsvæðis (e. page load speed).
- 3. Virkni vefkökur** (e. functionality cookies): Þessar vefkökur gera vefsvæði kleift að muna val notenda á tilteknu vefsvæði, s.s. notendanafn og tungumál og veita af þeim sökum bættu og sérsniðna þjónustu.
- 4. Markaðssetningar vefkökur** (e. targeting/advertising cookies): Þessar vefkökur eru notaðar til þess að birta notendum sérsniðnar auglýsingar þar sem þær eru byggðar á efni sem viðkomandi hefur áhuga á að skoða t.d. út frá því efni sem notandi skoðaði á tilteknu vefsvæði. Slíkum vefkökum kann að vera komið fyrir jafnvel þó vefsvæðið sjálft birti ekki auglýsingar. Þessar vefkökur stafa oft frá öðrum en þeim sem heldur úti vefsvæði, þ.e. þriðju aðilum.

Vefkökur eru einnig flokkaðar eftir *líftíma* þeirra og teljast þær annað hvort setukökur (e. session cookies) eða viðvarandi kökur (e. local og/eða persistant cookies). Setukökur eru tímabundnar vefkökur sem eru geymdar í endabúnaði notanda á meðan vefsíða er skoðuð og eyðast sjálfkrafa þegar vafra er lokað. Þær halda utan um tímabundnar upplýsingar eins og innskráningu, innihald í innkaupakörfu og val notenda á vefsíðu á meðan á heimsókn stendur. Viðvarandi vefkökur vistast hins vegar á tölvu notanda og eru geymdar lengur í endabúnaði og hafa tiltekinn líftíma. Þær eru notaðar til að muna valkosti og stillingar milli heimasókna á

⁵ Tilskipun 2002/58/EB um persónuvernd í fjarskiptum eins og henni var síðast breytt, sbr. tilskipun 2009/136/EB.

⁶ Hér eftir er vísað til vefkaka sem ekki eru notaðar í lögmætum tilgangi sem valkvæðra vefkaka enda þarf notandi að veita upplýst samþykki fyrir notkun slíkra vefkaka í samræmi við ákvæði fjarskiptalaga.

vefsíðu, m.a. innskráningarupplýsingar og til að fylgjast með hegðun notenda í þágu markaðssetningar.

Þá skiptast vefkökur einnig í flokka eftir *uppruna* en þær teljast annað hvort fyrstu aðila vefkökur eða þriðju aðila vefkökur. Fyrstu aðila vefkökur eru vefkökur sem verða til á tilteknu vefsvæði og stafa t.d. frá eiganda vefsíðu sem notandi er að heimsækja. Þessar vefkökur eru almennt notaðar til að geyma upplýsingar um samskipti notandans við þá tilteknu vefsíðu, s.s. innskráningarupplýsingar, stillingar og innihald innkaupakörfu og geta bætt notendaupplifun á vefsíðunni. Fyrstu aðila vefkökur eru aðeins aðgengilegar viðkomandi vefsíðueiganda. Þriðju aðila vefkökur eru hins vegar tilkomnar vegna þjónustu sem viðkomandi vefsvæði notar og miðla upplýsingum um notanda til þriðju aðila. Þjónusta þriðja aðila getur farið fram með margvíslegum hætti og þriðju aðila vefkökur geta t.d. gert vefþjónustuaðilum kleift að stjórna innviðum vefsíðu með auðveldum hætti. Þær geta einnig verið hluti af svokölluðum greiningarpökkum (e. analytics packages) sem gera vefþjónustuaðilum kleift að fylgjast með því hvernig vefsíða þeirra er notuð. Þá geta ýmis frammistöðutól (e. performance suites) á vegum þriðja aðila einnig gert vefþjónustuaðilum kleift á sambærilegan hátt að fylgjast með notkun vefsvæðis, s.s. hversu margir nýir notendur heimsækja það, hversu oft, hvernig notendur vafra um vefsvæði og hvaða tenglar eru notaðir. Loks geta þriðju aðila vefkökur gert vefþjónustuaðilum kleift að birta notendum sérsniðnar auglýsingar og fylgjast með notkun þeirra á ólíkum vefsvæðum, oft í skiptum fyrir auglýsingatekjur. Þriðju aðilar sem koma markaðssetningar vefkökum fyrir í endabúnaði notenda gera það kleift að persónugreina notendur þvert á vefsíður með því að úthluta þeim viðvarandi, einkvæmu auðkenni (e. persistent unique ID). Þetta auðkenni tengist notendasniði (e. user profiles) sem búið er til með því að fylgjast með hegðun viðkomandi á netinu. Þessi notendasnið geta verið aðlaðandi fyrir lögaðila þar sem hægt er að nota þau til þess að útbúa sérsniðnar og persónubundnar auglýsingar fyrir notanda en vefþjónustuaðili fær eftir atvikum hluta af auglýsingatekjum eftir að notandi smellir á auglýsingu. Þá geta þriðju aðila vefkökur jafnframt talist nauðsynlegar í ákveðnum tilvikum þó algengara sé að styðjast við þriðju aðila vefkökur í þágu markaðssetningar.

2.2. Mikilvægi trausts í viðskiptum á netinu

Það hvernig vefþjónustuaðilar og eigendur vefsvæða nota vefkökur og haga vefkökustillingum á vefsvæði getur haft áhrif á traust notenda þegar þeir stunda viðskipti á netinu. Unnt er að halda utan um og afla samþykkis notenda fyrir notkun vefkaka með mismunandi hætti og eins er misjafnt hvort og með hvaða hætti notendur fái tækifæri til að afturkalla samþykki eða breyta stillingum fyrir notkun á vefkökum.

Ekki allir vefkökuborðar gefa notendum sömu valkosti varðandi samþykki fyrir notkun vefkaka. Í framkvæmd eru algengustu leiðirnar, sem notendum er boðið upp á til að taka afstöðu til notkunar á vefkökum eftirfarandi:

- Notendur geta *valið að samþykkja notkun á vefkökum sem ekki eru nauðsynlegar (e. opt-in)* áður en þær eru teknar í notkun. Notandi veitir þannig samþykki með ótvíræðri aðgerð með því að velja hvaða vefkökur hann heimilar að sé komið fyrir.
- Notendur geta *afþakkað eða hafnað vefkökum sem ekki eru nauðsynlegar (e. opt-out)*.
- Notendur eru beðnir um að *staðfesta notkun á vefkökum eða loka vefkökuborða* eftir að hafa verið upplýstir um að vefkökur séu notaðar í skýrum tilgangi við heimsókn á

vefsvæði. Segja má að með þessu sé notanda ekki veitt raunverulegt tækifæri á að taka afstöðu til vefkökunotkunar, þ.e. veita samþykki eða hafna notkuninni.

- Þögn, reitir sem þegar er búið að haka við eða aðgerðarleysi, s.s. ef notendur andmæla ekki notkun á vefkökum, fela almennt ekki í sér upplýst samþykki eins og það er skilgreint í persónuverndarlögum.

Það þekkist að vefþjónustuaðilar beiti ýmsum aðferðum til að þrýsta á notendur til að samþykkja allar vefkökur, þ.m.t. vefkökur sem ekki eru nauðsynlegar, í stað þess að óska eftir samþykki notanda fyrir ólíkum tegundum vefkaka og/eða gefa þeim færi á að hafna öðrum vefkökum en þeim sem eru nauðsynlegar. Sem dæmi er algengt að notaðir séu vefkökuborðar sem innihalda hnapp til að samþykkja allar vefkökur sem er stór og áberandi, t.d. grænn eða í öðrum áberandi lit, á meðan hnappur sem gerir notanda kleift að hafna vefkökum er minna áberandi í útliti t.d. hvað lit eða stærð hnappsins varðar. Eins er algengt að notendur þurfi að hafa meira fyrir því að hafna vefkökum, s.s. með því að fara í gegnum röð stillinga, á vefsvæði eða í netvafra, á meðan möguleiki til að samþykkja allar vefkökur er strax aðgengilegur.

Frjálst og óþvingað samþykki fyrir notkun á vefkökum er til þess fallið að auka gagnsæi, ánægju og traust neytenda í viðskiptum á netinu og stuðla að reglufylgni við viðeigandi ákvæði fjarskipta- og persónuverndarlaga.

2.3. Kröfur til notkunar á vefkökum eru ólíkar eftir tegund þeirra

Í fjarskiptalögum eru gerðar mismunandi kröfur til samþykkis í tengslum við notkun á vefkökum m.a. eftir tilgangi með notkun þeirra eins og að framan hefur verið rakið. Sem dæmi má nefna að ekki er gerð krafa um samþykki fyrir notkun hvers konar kerfa og búnaðar sem safnar og/eða geymir upplýsingar um athafnir eða samskipti notanda í endabúnaði hans ef slík notkun fer fram samkvæmt heimild í lögum. Þá er notkun slíks búnaðar, þ.m.t. vefkökur, heimil til að fá aðgang að upplýsingum og/eða til tæknilegrar geymslu í lögmætum tilgangi, að því gefnu að notkunin fari fram með vitund hlutaðeigandi notanda.

Almennt styðst notkun á frammistöðu-/tölfræði vefkökum og virkni vefkökum við upplýst samþykki nema þegar notkunin fer fram í lögmætum tilgangi. Markaðssetningar vefkökur, óháð því hvort þær eru fyrstu aðila eða þriðju aðila vefkökur, eru hins vegar alltaf háðar upplýstu samþykki notandans enda er eðli þeirra og virkni oftast slík að markaðssetningarkökum er ætlað að fylgjast með hegðun og aðgerðum notenda á vefsíðum í þeim megintilgangi að sérsníða markaðs-, auglýsinga- og kynningarefni að notendum.

Algennt er að eigendur vefsvæða og vefþjónustuaðilar feli utanaðkomandi þjónustuaðila að upplýsa um og/eða afla samþykkis fyrir notkun á vefkökum á vefsvæðum sínum. Þjónusta slíkra aðila getur verið hagkvæm, t.d. vegna sérfræðipækkingar viðkomandi á vefkökum, en einnig haft í för með sér áhættumeiri vinnslu persónuupplýsinga sem vefþjónustuaðili ber ábyrgð á t.d. vegna miðlunar og eftir atvikum frekari vinnslu persónuupplýsinga sem kann að fara fram hjá þjónustuaðila vegna þessa. Í samræmi við bestu venjur ættu vefþjónustuaðilar að tryggja að engum öðrum vefkökum en nauðsynlegum vefkökum sé komið fyrir í endabúnaði notanda án þess að notandi hafi verið upplýstur um tilgang þeirra og veitt samþykki fyrir slíkri notkun. Vefþjónustuaðilar ættu sömuleiðis að gæta þess að upplýsingagjöf til notenda sé

reglulega uppfærð samhliða breyttri notkun eða virkni vefsvæðis sem m.a. getur haft áhrif á þær vefkökur sem stuðst er við.

3. Lög og reglur sem við eiga

Í grundvallaratriðum er óheimilt að nota eða koma fyrir kerfum og búnaði þ.m.t. hugbúnaði, sem safnar og/eða geymir upplýsingar um athafnir eða samskipti notanda í endabúnaði hans eins og snjalltæki eða tölvu nema samkvæmt upplýstu samþykki notanda eða samkvæmt heimild í lögum, sbr. 2. mgr. 88. gr. fjarskiptalaga. Þrátt fyrir framangreint er notkun slíks búnaðar heimil til að fá aðgang að upplýsingum og/eða til tæknilegrar geymslu í lögmætum tilgangi en einungis með vitund hlutaðeigandi notanda. Vefkökum sem komið er fyrir í endabúnaði notanda falla undir framangreint þar sem þær safna og/eða geyma upplýsingar um athafnir notanda á tilteknu vefsvæði. Um skilyrði samþykkis og upplýsingaskyldu fer eftir ákvæðum laga nr. 90/2018 um persónuvernd og vinnslu persónuupplýsinga (hér eftir „persónuverndarlög“).

3.1. Lög nr. 70/2022 um fjarskipti

Fjallað er um vefkökur, smygildi eða aðra slíka tækni sem safnar eða geymir upplýsingar um notanda eða athafnir hans, í 2. mgr. 88. gr. fjarskiptalaga. Af 2. mgr. 88. gr. fjarskiptalaga leiðir að óheimilt er að nota vefkökur, sem komið er fyrir í nettengdum endabúnaði notanda og veita aðgang að upplýsingum um hann, nema notandi hafi veitt *upplýst samþykki* fyrir slíku eða ef notkunin byggist á *heimild í lögum*.

Í undantekningartilvikum er, samkvæmt 3. málsl. 2. mgr. 88. gr. fjarskiptalaga, heimilt að nota hvers konar kerfi og búnað þ.m.t. vefkökur án þess að afla samþykkis notanda, til að fá aðgang að upplýsingum og/eða til tæknilegrar geymslu þegar notkunin er í *lögmætum tilgangi* og með *vitund* hlutaðeigandi notanda. Í athugasemdum við ákvæðið í frumvarpi því er varð að lögum nr. 77/2022 er tekið fram að slíkur lögmætur tilgangur skuli túlkaður þröngt og geti aðeins átt við í tveimur tilfellum:

- þegar um er að ræða tæknilega geymslu eða aðgang að upplýsingum í þeim eina tilgangi að framkvæma fjarskiptin yfir fjarskiptanet, þ.e. að auðkenna endapunkt fjarskiptanna, til að skiptast á gagnapökkum í rétttri röð og til að uppgötva sendingarvillur eða gagnatap.
- þegar notkunin er nauðsynleg forsenda þess að unnt sé að veita ákveðna þjónustu sem sérstaklega hefur verið óskað eftir.

Við mat á því hvort notkun falli undir lögmætan tilgang samkvæmt framangreindu þarf því að greina hvort um sé að ræða upplýsingar sem eru í raun nauðsynlegar til að tryggja virkni viðkomandi síðu eða veita umbeðna þjónustu, eða hvort notkun á vefkökum fari einungis fram til bæta virkni á tilteknu vefsvæði og auðvelda notendum að nota vefsvæði.

Í athugasemdum við 2. mgr. 88. gr. í frumvarpi því er varð að fjarskiptalögum nr. 77/2022 kemur fram að með upplýstu samþykki, fyrir notkun búnaðar sem safnar eða geymir upplýsingar um notanda í endabúnaði hans eins og vefkökur, er átt við að upplýsingaskylda samkvæmt

persónuverndarlögum sé uppfyllt gagnvart notanda áður en samþykki er aflað þegar notkun þeirra fer fram í öðrum tilgangi en þeim lögmæta tilgangi sem ákvæðið heimilar.

3.2. Lög nr. 90/2018 um persónuvernd og vinnslu persónuupplýsinga

Samþykki er skilgreint í 8. tl. 1. mgr. 3. gr. persónuverndarlaga sem óþvinguð, sértæk, upplýst og ótvíræð viljayfirlýsing hins skráða þess efnis að hann samþykki vinnslu persónuupplýsinga um sig, með yfirlýsingu eða ótvíræðri staðfestingu. Svo að samþykki teljist upplýst þarf einstaklingur, í þessu tilviki notandi vefsvæðis, að staðfesta að hann sé samþykkur vinnslu tiltekinna upplýsinga um sig og að honum sé kunnugt um tilgang hennar, hvernig hún fari fram, hvernig persónuvernd verði tryggð, um að honum sé heimilt að afturkalla samþykki sitt o.s.frv. Þannig telst samþykki ekki upplýst nema einstaklingur viti hvað hann er að samþykkja og hvaða afleiðingar meðferð upplýsinganna hefur eða getur haft fyrir viðkomandi.

Samþykki fyrir vinnslu almennra persónuupplýsinga er mögulegt að veita í verki, þ.e. með ótvíræðri aðgerð, en sú aðgerð notanda að smella á hnapp á vefsvæði til að samþykkja vefkökur hefur talist til ótvíræðs samþykkis samkvæmt túlkun Persónuverndar að því gefnu að upplýsingagjöf eða fræðsla um vinnslu persónuupplýsinga og tilgang hennar, sem samþykki varðar, sé veitt á skýran og aðgengilegan hátt. Þegar notendur fá ekki raunverulegt val um að samþykkja notkun á vefkökum, s.s. vegna þess að samþykki er eini valmöguleiki notenda, þá telst slíkt ekki frjálst og óþvingað. Þögn, reitir sem þegar er búið að haka við eða aðgerðarleysi fela því almennt ekki í sér samþykki.

Vefþjónustuaðili, eða sá sem tekur ákvörðun um tilgang og aðferð við vinnslu persónuupplýsinga með vefkökum á vefsvæði sínu, telst ábyrgðaraðili að vinnslu persónuupplýsinga sem fram fer með vefkökum samkvæmt persónuverndarlögum og skal hann geta sýnt fram á að notanda hafi verið veitt lögbundin fræðsla áður en upplýsts samþykkis hans er aflað. Samkvæmt leiðbeiningum bæði Persónuverndar⁷ og Evrópska persónuverndarráðsins⁸ þarf að lágmarki að upplýsa um eftirfarandi atriði til þess að samþykki teljist upplýst samkvæmt persónuverndarlögum:

- heiti ábyrgðaraðila
- tilgangur hvernar vinnsluáðgerðar sem óskað er samþykkis fyrir
- hvaða persónuupplýsingar er fyrirhugað að vinna með
- rétt til að afturkalla samþykki
- hvort fram fari sjálfvirk ákvörðunartaka
- hvort miðla eigi persónuupplýsingum til ríkis utan Evrópska efnahagssvæðisins án þess að fullnægjandi vernd liggi fyrir

Eftir atvikum kann að vera nauðsynlegt að veita frekari upplýsingar til þess að gera hinum skráða raunverulega kleift að átta sig á hvað felst í fyrirhugaðri vinnslu persónuupplýsinga með vefkökum áður en hann veitir samþykki fyrir vinnslunni.

⁷ Persónuvernd, „Leiðbeiningar um samþykki“ bls. 6-7. Sótt af: https://www.personuvernd.is/media/leidbeiningar-personuverndar/Leiðbeiningar-um-samthykki_5.4.2018.pdf

⁸ European Data Protection Board, „Guidelines 05/2020 on consent under Regulation 2016/679: Version 1.1: 4 May 2020“ bls. 15-16. Sótt af: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf

Ábyrgðaraðilum samkvæmt framansögðu t.d. eigendum vefsvæða eða vefþjónustuaðilum ber að afla upplýsts samþykkis notenda í öllum tilvikum þegar notkun á vefkökum fer ekki fram á grundvelli lagaheimildar eða í lögmætum tilgangi samkvæmt fjarskiptalögum, óháð því hvort notkunin feli í sér vinnslu persónuupplýsinga eða ekki. Þrátt fyrir að notkun á vefkökum fari fram í lögmætum tilgangi, sem felur í sér undanþágu frá öflun upplýsts samþykkis notanda, þarf engu að síður ávallt að veita notendum upplýsingar um notkunina. Framangreind upplýsingaskylda endurspeglar þannig áðurnefnda grundvallarreglu 1. mgr. 88. gr. fjarskiptalaga um fjarskiptaleynd. Með því að upplýsa um notkun vefkaka í t.d. vefkökuborða, persónuverndaryfirlýsingu eða vefkökustefnu er unnt að veita fræðslu um öll framangreind atriði sem fjarskipta- og persónuverndarlög áskilja.

Þrátt fyrir að tæknilega sé unnt að koma vefkökum fyrir í endabúnaði notanda án þess að slíkar vefkökur safni persónuupplýsingum eða persónugreinanlegum upplýsingum, t.d. með tímabundnum vefkökum sem úthluta sérhverjum notanda tilfallandi númeri (e. random number), verður ekki annað ráðið en að þær vefkökur sem frumkvæðisskoðun þessi nær til, sem og vefkökur almennt, safni persónugreinanlegum upplýsingum um notanda.

Persónuupplýsingar eru allar upplýsingar sem gera það kleift að persónugreina einstakling, beint eða óbeint, s.s. með tilvísun í auðkenni eins og nafn, kennitölu, staðsetningargögn, netauðkenni eða einn eða fleiri þætti sem einkenna hann í líkamlegu, lífeðlisfræðilegu, erfðafræðilegu, andlegu, efnalegu, menningarlegu eða félagslegu tilliti. Hafi persónuupplýsingar verið aftengdar einstaklingi þannig að ekki sé lengur unnt að persónugreina viðkomandi með öryggisráðstöfunum, s.s. aðgangstakmörkunum, dulkóðun eða notkun gerviauðkenna, teljast upplýsingar engu að síður persónugreinanlegar ef hægt er að rekja þær til einstaklings með notkun viðbótarupplýsinga t.d. ef dulkóðunarlykli hefur ekki verið eytt. Í því sambandi hefur Evrópudómstóllinn m.a. staðfest að ákvæði 3. mgr. 5. gr. tilskipunar 2002/58/EB um persónuvernd í fjarskiptum, sem innleitt er í íslenskan rétt með ákvæði 2. mgr. 88. gr. fjarskiptalaga, er ætlað að vernda allar upplýsingar, sem geymdar eru í endabúnaði notanda, óháð því hvort um persónuupplýsingar eða persónugreinanlegar upplýsingar sé að ræða⁹.

Þegar kerfi og búnaður þ.m.t. hugbúnaður, eru notuð til að safna og/eða geyma upplýsingar um athafnir eða samskipti notanda í endabúnaði hans á grundvelli upplýsts samþykkis samkvæmt skilyrðum persónuverndarlaga þarf vefþjónustuaðili að geta sýnt fram á að notandi hafi samþykkt vinnslu persónuupplýsinga um sig. Samþykki ber að veita með skýrri staðfestingu sem m.a. getur verið veitt með rafrænum hætti. Dæmi um ótvírætt samþykki fyrir vinnslu almennra persónuupplýsinga er rafræn staðfesting eða hak við reit þegar farið er inn á vefsvæði á netinu, val á tæknilegum stillingum eða annars konar athöfn í verki sem gefur skýrt til kynna að fyrirhuguð vinnsla persónuupplýsinga með vefkökum sé samþykkt. Í því samhengi felur þögn, reitur sem þegar er búið að haka við, andmælaréttur eða aðgerðarleysi ekki í sér ótvíræða staðfestingu á að einstaklingur samþykki vinnslu persónuupplýsinga, sbr. athugasemdir við 10. gr. í frumvarpi er varð að lögum nr. 90/2018, um persónuvernd og vinnslu persónuupplýsinga. Samþykki ætti að ná til allrar vinnslustarfsemi sem fram fer í sama tilgangi, einum eða fleiri.

⁹ Sjá dóm Evrópudómstólsins í máli C-673/17, *Planet 49*, [2019] EU:C:2019:801 frá 1. október 2019, mgr. 70-71.

Þegar vinnsla fer fram í margvíslegum tilgangi ætti að gefa samþykki fyrir hverjum og einum þeirra¹⁰, t.d. ólíkum tilgangi vefkaka eða flokka vefkaka þar sem það á við.

Svo skilyrðum samþykkis sé mætt samkvæmt persónuverndarlögum eiga notendur rétt á að draga samþykki sitt til baka á jafn auðveldan hátt og samþykki var veitt.¹¹ Í tengslum við notkun á vefkökum þýðir þetta að notendur eiga almennt að geta afturkallað samþykki sitt með sömu aðgerð og samþykki var veitt t.d. í vefkökuborða á vefsvæði eða með breytingu á vefkökustillingum á vefsvæðinu. Það er jafnframt í samræmi við bestu venjur að bjóða upp á skýra leið fyrir notendur til að „samþykkja“ eða „hafna“ sérhverri tegund vefköku eða ólíkum tilgangi og hafa vefkökuborða sýnilegan á tilteknu vefsvæði svo notandi hafi tækifæri á að breyta vefkökustillingum síðar, og með því í reynd draga samþykki til baka, með auðveldum hætti.

4. Frumniðurstöður

Í júlí - desember 2024 var framkvæmd skönnun á vefsvæðum valinna vefþjónustuaðila í þeim tilgangi að greina þær vefkökur sem umrædd vefsvæði koma fyrir í endabúnaði notanda þegar tiltekið vefsvæði er skoðað í netvafra. Vefsvæðin gera neytendum kleift að kaupa vörur og/eða bóka þjónustu hjá fjölbreyttum hópi lögaðila. Eigendur vefsvæðanna bera ábyrgð á að upplýsa notendur um notkun á vefkökum á vefsvæðum sínum og eftir atvikum afla samþykkis fyrir þeirri notkun í samræmi við ákvæði fjarskiptalaga sem að framan hafa verið rakin. Skönnunin fór fram með opnum hugbúnaði hins Evrópska persónuverndarráðs sem að framan hefur verið lýst og beindist að þeirri útgáfu vefsvæðanna sem birtast í netvafra borðtölvu.

Þegar vefkökur eru notaðar til að fá aðgang að upplýsingum, safna upplýsingum eða fylgjast með athöfnum notenda án vitundar þeirra og samþykki eftir því sem við á samrýmist slík notkun ekki kröfum fjarskiptalaga og telst ólöglegt. Það hvernig vefþjónustuaðilar og eigendur vefsvæða nota vefkökur og haga vefkökustillingum á vefsvæði getur haft áhrif á traust notenda þegar þeir stunda viðskipti á netinu. Þá er upplýst samþykki fyrir notkun á vefkökum til þess fallið að auka gagnsæi, ánægju og traust neytenda í viðskiptum á netinu og stuðla að reglufylgni við viðeigandi ákvæði fjarskipta- og persónuverndarlaga.

Niðurstöður úr skönnuninni voru ólíkar eftir vefsvæðum og þeirri fræðslu eða framkvæmd sem viðhöfð er hverju sinni. Engu að síður er unnt að setja niðurstöður fram almennt varðandi tiltekin atriði sem lúta að veittri fræðslu og/eða öflun upplýst samþykkis fyrir notkun á vefkökum og eru sambærileg þvert á vefsvæði þeirra vefþjónustuaðila sem skoðun þessi náði til. Frumniðurstöður eru þríþættar og varða eftirfarandi atriði:

Veitt fræðsla til notenda um notkun á vefkökum

Upplýsingagjöf um vefkökur er unnt að veita á ólíkan hátt til að mynda er algengt að fjalla um vefkökur í persónuverndar- og/eða sérstakri vefkökustefnu en jafnframt er unnt að tilkynna

¹⁰ Sjá 32. lið formála reglugerðar Evrópuþingsins og ráðsins (ESB) 2016/679 frá 27. apríl 2016 um vernd einstaklinga í tengslum við vinnslu persónuupplýsinga og um frjálsa miðlun slíkra upplýsinga og niðurfellingu tilskipunar 95/46/EB („almenna persónuverndarreglugerðin”).

¹¹ Sjá 1. mgr. 10. gr. persónuverndarlaga og 3. mgr. 7. gr. almennu persónuverndarreglugerðarinnar.

sérstaklega um notkun vefkaka í svokölluðum vefkökuborða sem birtist um leið og notandi opnar vefsvæði. Óháð framsetningu slíkrar upplýsingagjafar leiddi skoðun Fjarskiptastofu í ljós að meirihluti valinna vefþjónustuaðila býður upp á einhvers konar fræðslu eða upplýsingagjöf um vefkökur og tilgang þeirra. Algengast er að upplýsingar séu veittar í persónuverndarstefnu vefþjónustuaðila og/eða í sérstakri vefkökustefnu sem eftir atvikum inniheldur ítarlegri upplýsingar um tegund, tilgang og líftíma vefkaka. Þrátt fyrir að flestir vefþjónustuaðilar sem skoðunin varðaði upplýsi um vefkökunotkun að einhverju leyti er upplýsingagjöf ekki alltaf efnislega í samræmi við þær vefkökur og/eða flokka vefkaka sem notaðar eru í framkvæmd. Þegar vefþjónustuaðili upplýsir ekki um tegund, tilgang og líftíma þeirra flokka vefkaka sem hann notar í reynd á vefsvæði sínu leiðir slíkt til þess að notandi fær ekki nauðsynlegar upplýsingar um notkun vefkaka, hvort heldur sem notaðar eru vefkökur sem krefjast upplýsts samþykkis notanda eða vefkökur sem notaðar eru í lögmætum tilgangi og ekki þarf að samþykkja sérstaklega.

Upplýst samþykki notenda vegna notkunar á vefkökum

Fjarskiptalög gera kröfu um upplýst samþykki notanda fyrir notkun kerfis eða búnaðar, t.a.m. vefkökur, sem safna og/eða geyma upplýsingar um athafnir eða samskipti notanda í endabúnaði hans, veita aðgang að upplýsingum sem geymdar eru í endabúnaði hans eða fylgjast með athöfnum hans. Um skilyrði samþykkis fyrir notkun vefkaka og upplýsingaskyldu fer eftir ákvæðum laga nr. 90/2018, um persónuvernd og vinnslu persónuupplýsinga. Nauðsynlegar upplýsingar skal veita áður en samþykki er aflað. Svo samþykki teljist upplýst þarf notandi að staðfesta, m.a. að hann sé samþykkur vinnslu tiltekinna upplýsinga og að honum sé kunnugt um tilgang hennar ella telst veitt samþykki ekki fullnægjandi samkvæmt persónuverndarlögum. Slíkt samþykki er unnt að veita á ólíkan hátt en samþykki þarf að veita með ótvíræðri staðfestingu s.s. skriflegri yfirlýsingu þar sem við á eða með aðgerð, s.s. með rafrænu haki, með því að smella á samþykkishnapp í vefkökuborða eða með annars konar athöfn sem gefur skýrt til kynna að notandi samþykki fyrirhugaða notkun á vefkökum að undangenginni fullnægjandi fræðslu. Þögn, reitir sem þegar er búið að haka við eða aðgerðarleysi fela almennt ekki í sér samþykki.

Rúmlega helmingur þeirra vefþjónustuaðila sem skoðun þessi beinist að býður notendum upp á að samþykkja notkun á valkvæðum vefkökum með því að smella á þar til gerðan hnapp þ.e. með sérstakri aðgerð. Einungis tveir vefþjónustuaðilar af þeim átta sem skoðunin náði til gera notendum kleift annað hvort að breyta stillingum fyrir valkvæðar vefkökur eða hafna þeim í vefkökuborða. Það hvort samþykki teljist upplýst veltur á þeirri upplýsingagjöf eða fræðslu um vefkökur sem að framan hefur verið rakin þá sérstaklega hvað varðar tilgang þeirra. Þrátt fyrir að flestir vefþjónustuaðilar sem skoðun þessi varðar bjóði notendum upp á að samþykkja vefkökur í vefkökuborða leiddi skoðun þessi í ljós að slíkt samþykki er annað hvort ekki virt í framkvæmd eða telst ekki frjálst og óþvingað í skilningi persónuverndarlaga þar sem notendur geta einungis samþykkt allar vefkökur sem notaðir eru í ólíkum tilgangi.

Notkun á vefkökum í framkvæmd

Í ákveðnum tilvikum leiddi skoðun Fjarskiptastofu í ljós misræmi milli veittrar fræðslu tiltekinna vefþjónustuaðila um notkun þeirra á vefkökum annars vegar og notkunar þeirra í framkvæmd hins vegar. Þegar raunveruleg notkun á vefkökum samrýmist almennt ekki veittri fræðslu og samþykki notenda, til dæmis ef fleiri valkvæðum vefkökum er komið fyrir á nettengdum endabúnaði notanda en samþykki hans nær til, getur samþykki ekki talist upplýst svo fullnægjandi sé.

Markverðar niðurstöður finnast þegar raunveruleg notkun á vefkökum er skoðuð sem og hvort val notenda hvað varðar notkun á vefkökum, þ.m.t. samþykki eða höfnun, sé virt í framkvæmd. Frumniðurstöður bera með sé að allir vefþjónustuaðilar sem skoðunin nær til koma fyrir vefkökum í endabúnaði notenda sem annað hvort er ekki greint frá í veittri fræðslu um vefkökur og/eða áður en notandi hefur veitt upplýst samþykki sitt fyrir slíkum vefkökum og í einhverjum tilvikum eftir að slíkum vefkökum hefur verið sérstaklega hafnað. Hefur því enginn þeirra vefþjónustuaðila sem frumkvæðisskoðunin nær til gengið úr skugga um að valkvæðum vefkökum, þ.m.t. markaðssetningar vefkökum, sé ekki komið fyrir í endabúnaði notenda áður en notandi hefur samþykkt valkvæðar vefkökur í reynd. Í ljósi þess að markaðssetningar vefkökur eru almennt notaðar til þess að greina hegðun notenda í þágu markaðs- og kynningarstarfs eru þær ekki notaðar í lögmætum tilgangi samkvæmt fjarskiptalögum, þ.e. til að tryggja virkni viðkomandi síðu eða eru forsenda þess að unnt sé að veita notendum umbeðna þjónustu, og kalla því á upplýst samþykki.

Samandregið

Með einfaldri framsetningu má draga saman helstu niðurstöður úttektarinnar í yfirlitstöflu hér að neðan:

Vefþjónustuaðili	A	B	C	D	E	F	G	H
Vefkökuborði	Nei	Nei	Já	Já	Já	Já	Já	Já
Boðið upp á samþykkja/hafna/breyta stillingum á vefsvæði	Nei	Nei	Nei	Já (samþykkja og breyta stillingum)	Nei (með notkun)	Já (Samþykkja)	Nei (með notkun)	Já (Samþykkja, hafna og breyta stillingum)
Fræðsla veitt í persónuverndarstefnu	Nei	Já (ekki fullnægjandi)	Nei	Já	Já (ekki fullnægjandi)	Já	Já	Já (ekki fullnægjandi)
Fræðsla veitt í vefkökustefnu	Nei	Nei	Nei	Já	Já (ekki fullnægjandi)	Já	Já (ekki fullnægjandi)	Já (ekki fullnægjandi)
Samþykki	Nei	Nei	Nei	Já (ekki virt)	Nei (ekki óþvingað)	Nei (ekki óþvingað)	Nei (ekki óþvingað)	Já (ekki virt)
Valkvæðar vefkökur notaðar án samþykkis	Já	Já	Já	Já	Já	Já	Já	Já
Niðurstaða	Ekki í samræmi við 2. mgr. 88. gr. fjarskiptalaga	Ekki í samræmi við 2. mgr. 88. gr. fjarskiptalaga	Ekki í samræmi við 2. mgr. 88. gr. fjarskiptalaga	Ekki í samræmi við 2. mgr. 88. gr. fjarskiptalaga	Ekki í samræmi við 2. mgr. 88. gr. fjarskiptalaga	Ekki í samræmi við 2. mgr. 88. gr. fjarskiptalaga	Ekki í samræmi við 2. mgr. 88. gr. fjarskiptalaga	Ekki í samræmi við 2. mgr. 88. gr. fjarskiptalaga
	↓	↓	↓	↓	↓	↓	↓	↓
Fræðsla/vitund	✗	✗	✗	✓	✗	✓	✗	✗
Framkvæmd	✗	✗	✗	✗	✗	✗	✗	✗
Samþykki	✗	✗	✗	✓	✗	✗	✗	✓

12

¹² Taflan er ekki sundurliðuð eftir nöfnum vefþjónustuaðila.