

© Snoobi Technology 2025

Johdanto: evästeet tai ilman evästeitä



Evästeiden esto

Huoli yksityisyyden suojasta on johtanut kasvavaan evästeiden kieltoon, mikä näkyy suoraan analytiikkatyökalujen kehityksessä.

Lukuun ottamatta Google Chromea, useimmat selaimet estävät evästeet oletusarvoisesti, mikä haastaa markkinoijien ja data-analyttikoiden käyttämät perinteiset seurantamenetelmät.

Kolmannen osapuolen evästeitä tai vaihtoehtoisia tallennusratkaisuja tarkastellaan tiukemmin, kun yksityisyyttään suojelevat käyttäjät suhtautuvat epäluuloisesti tavanomaisiin seurantamenetelmiin.

Suostumushallinnalla pyritään kaventamaan tiedonkeruuvajetta, mutta nekin aiheuttavat usein ns.

"suostumusväsymystä" hukuttamalla käyttäjät evästekyselyihin. Analytiikan toteuttaminen edellyttää innovatiivista ratkaisua, joka tasapainottaa käyttäjätiedot ja vankan yksityisyyden suojan, sekä samalla kunnioittaa käyttäjien mieltymyksiä ja säilyttää verkkoanalytiikan ominaisuudet.

Evästeettömän analytiikan ja hybridianalytiikkaratkaisujen yleistyminen

Snoobi Analyticsin tarjoamat uudet analytiikkaratkaisut lähestyvät verkkotietojen keräämistä evästeettömän ja hybridilähestymistavan kautta. Perinteisen seurannan rajoitukset taklataan keräämällä dataa tallentamatta selainpohjaisia tietoja. Tietosuojasäädösten mukaisesti Snoobi Analytics tarjoaa joustavia, käyttäjien yksityisyyttä kunnioittavia tiedonkeruumenetelmiä.

Snoobi Analytics -alusta voi hyödyntää ensimmäisen osapuolen tietoja käyttäjän suostumuksella tai toimia kokonaan ilman evästeitä.

Tämä hybridimalli parantaa tietojen tarkkuutta ja luotettavuutta ja vähentää selaimen yksityisyysasetusten haavoittuvuutta. Hyödyntämällä näitä tekniikoita organisaatio voi varmistaa kattavan ja vaatimustenmukaisen verkkoanalytiikan, jossa yksityiskohtaiset tiedot ja tiukat yksityisyysstandardit ovat tasapainossa.

Muuttuvaan ympäristöön sopeutuminen on strateginen valinta

Siirtyminen evästeettömiin ja hybridianalyysimalleihin edellyttää tiedonseurantastrategioiden perusteellista uudelleensuunnittelua. Keskeistä on arvioida, mitkä tiedot ovat olennaisia ja käyttää yksityisyyttä kunnioittavia tiedonkeruumenetelmiä. Kehittyvät analytiikkaratkaisut eivät ole vain tekninen päivitys - vaan myös strateginen muutos.

Sopeutumalla aktiivisesti muutoksiin organisaatio voi turvata datan keruunsa tulevaisuudessa ja samalla rakentaa luottamusta. Uusi analytiikkaympäristö vaatii syvällistä ymmärrystä yksityisyydensuojaa kunnioittavista menetelmistä. Vain näin voidaan valita työkaluja, jotka tuottavat vakaata tietoa ympäristöissä, joissa data on rajoitettua.

On tärkeää pysyä ajan tasalla ja joustavana.

Tässä artikkelissa käsittelemme eri tapoja kerätä ja analysoida dataa yksityisyydensuojaa noudattamalla. Tarkastelemme käytettävissä olevia vaihtoehtoja, haasteita ja sitä, kuinka organisaatiot voivat hyödyntää analytiikan tietoja.

Charles W.Odinot, Snoobi Technology, 2025.

Indeksi

JOHDANTO: EVÄSTEET TAI ILMAN EVÄSTEITÄ.....	2
PSEUDOANONYMISOINTI VS. TÄYDELLINEN ANONYMISOINTI.....	4
VERKKOANALYTIikka & SELAIMEN EVÄSTEIDEN ESTO	5
'PAKOLLISET EVÄSTEET'	6
OIKEUTETTU ETU ANALYTIIKASSA	7
PALVELINPUOLEN SEURANTA	8
MIKSI SUOSTUMUKSENHALLINTA EI YKSIN RIITÄ	9
ANALYTIikka PORTAALEILLE TAI INTRANETILLE	10
YHTEENVETO: TIETOSUOJAYSTÄVÄLLINEN ANALYTIikka	11
ONKO YKSITYISYYDEN SUOJAA KUNNIOITTAVAA ANALYTIikkaA OLEMASSA?.....	12
LISÄTIETOJA.....	12

Kirjoittajasta

Charles Odinet on yksityisyydensuojaa kunnioittavien analytiikkateknologioiden asiantuntija, joka auttaa organisaatioita navigoimaan kehittyvässä digitaalisessa ympäristössä. Charlesilla on vahva asiantuntemus tietosuojasta, data-analytiikasta ja uusista seurantamenetelmistä, minkä avulla hän voi tarjota strategisia näkemyksiä eettisiin ja tehokkaisiin tiedonkeruukäytäntöihin. Snoobi Technologyn omistajana ja teknologiajohtajana Charles keskittyy työssään ratkaisuihin, jotka tasapainottavat liiketoiminnan tarpeita ja ensisijaisesti kunnioittavat yksityisyydensuojaa samalla hyödyntäen innovaatioita, kuten evästeetöntä seurantaa, yksityisyyttä ja ensimmäisen osapuolen tietostrategioita. Snoobi Analyticsin kehittäjätiimin johtamisen sekä tutkimuksen, konsultoinnin ja tuotekehittämisen kautta Charles osallistuu analytiikan tulevaisuuden muokkaamiseen yksityisyydensuojaa kunnioittaen.

snoobi

Pseudoanonymisointi vs. täydellinen anonymisointi

Mitä on tietojen anonymisointi

Tietosuoja on ratkaisevan tärkeää verkkosivustojen omistajille ja käyttäjille. Anonymisointistrategiat ovat olennaisen tärkeitä, jotta käyttäjätietoja voidaan suojella ja samalla saada tarvittavia tietoja.

Verkkoanalyysityökalut hyödyntävät erilaisia tekniikoita, kuten pseudoanonymisointia ja täydellistä anonymisointia, jotka tasapainottavat käyttäjien yksityisyyttä, tietojen analysointia ja organisaation vaatimustenmukaisuutta.

Pseudoanonymisointi: osittainen yksityisyyden suoja

Pseudoanonymisointia pidetään keskitason lähestymistapana tietosuojaan. Tässä menetelmässä henkilön tunnistettavat tiedot peitetään osittain tai korvataan keinotekoisilla tunnisteilla. Vaikka tämä tekniikka näyttää suojaavalta, siinä on kriittisiä heikkouksia, joita voidaan mahdollisesti käyttää hyväksi. Esimerkiksi niin sanotut seurantaevästeet säilyttävät edelleen yhteyden alkuperäisiin käyttäjätietoihin. Verkkosivustot, jotka käyttävät pseudoanonymisointia, voivat korvata käyttäjän suoran tunnisteiden satunnaisesti luodulla numerolla. Käyttäjä voidaan kuitenkin tunnistaa uudelleen, koska eväste tai käyttäjätiedot tallennetaan tulevaa käyttöä varten.

Pseudoanonymisointi tarjoaa vain vähäisen yksityisyyden suojan, joka voidaan helposti vaarantaa kehittyneillä tietojen korrelaatiotekniikoilla.

Täydellinen anonymisointi: kattava standardi käyttäjän yksityisyydelle

Täydellinen anonymisointi tarjoaa kattavan käyttäjätietojen suojan poistamalla yksilölliset tunnistamismahdollisuudet kokonaan ja palautumattomasti.

Snoobi Analytics varmistaa, että datasta tulee todella persoonatonta, jolloin verkkosivut voivat kerätä tietoa yksityisyyttä vaarantamatta.

Seurantaevästeitä ei tallenneta, ja istuntotiedot pysyvät yksilöllisinä vain yhden istunnon osalta.

Tämä lähestymistapa on täysin GDPR- ja CCPA-säädösten mukainen. Myöhempiä käyttäjäkäyntejä ei voida yhdistää analyttisesti, koska yksittäisten käyttäjien seuranta on tarkoituksella estetty.



Tietosuojakäytäntöjen ilmoittaminen

Verkkosivustojen on ilmoitettava avoimesti anonymisointistrategiasta ja selitettävä selkeästi mitä tietoja kerätään, käsitellään ja suojataan.

Selkokielen käyttäminen yksityisyyden suojaamisen kuvaamisessa auttaa organisaatioita rakentamaan luottamusta, täyttämään lain vaatimukset ja auttamaan käyttäjiä tekemään tietoon perustuvia päätöksiä.

Verkkoanalytiikka & selaimen evästeiden esto

Verkkoanalytiikka on kehittynyt yksityisyyteen liittyvien huolien ja tiukempien sääntöjen myötä. Monet selaimet estävät 3. osapuolen evästeet. Uudet yleistyvät menetelmät, kuten 1. osapuolen evästeet ja evästeetön analytiikka, korvaavat ne.

Miten selaimet estävät evästeet

- **Google Chrome:** Suunnitelmissa poistaa asteittain 3. osapuolen evästeet ja korvata ne Privacy Sandboxilla ja aihekohtaisella kohdentamisella.
- **Safari (Apple):** Käyttää Intelligent Tracking Prevention (ITP) -toimintoa 3. osapuolten evästeiden estämiseen ja 1. osapuolen evästeiden käyttöä rajoittamiseen.
- **Firefox:** ETP (Enhanced Tracking Protection) estää oletusarvoisesti 3. osapuolten evästeet.
- **Microsoft Edge:** Seurannan estoasetukset rajoittavat 3. osapuolten evästeitä ja muita seurantamekanismeja.
- Muissa selaimissa usein samankaltaisia mekanismeja, jotka estävät 3. osapuolen evästeet.

Organisaatioiden olisi siis syytä siirtyä kohti yksityisyyden suojaa edistäviä analytiikkaratkaisuja, jotka perustuvat vähemmän perinteisiin seurantamenetelmiin.



Mitä menetetään estäessä evästeet

Ilman evästeitä markkinointianalytiikat menettävät tärkeitä tietoja (käyttäjäkartoitusta, personointia ja konversiolukujen optimointia jne), mikä vaikeuttaa asiakaskäyttäytymisen ymmärtämistä ja mainosten kohdentamista.

Verkkoanalytiikassa käytettävät evästeet

Kolmannen osapuolen evästeet

- Voidaan asettaa verkkotunnukseksi tai verkkosivustolle, joka on eri kuin se, jolla käyttäjä vierailee (esim. mainosverkostot).
- Evästäettä voivat lukea muut työkalut kuin evästeen asettanut analytiikkatyökalu.
- Käytetään sivustojen väliseen seurantaan, kohdennettuun mainontaan ja uudelleenkohdentamiseen.
- Selaimet estävät ne yhä useammin, mikä vähentää tehokkuutta

Ensimmäisen osapuolen evästeet

- Tallentuvat verkkosivustolle, jolla käyttäjä vierailee (esim. kirjautumisistunto, kieliasetukset ja sivuston analytiikka).
- Vähemmän rajoituksia, mutta tietosuojasäännökset ja selainrajoitukset vaikuttavat silti.
- Elinkaarta lyhennetty joissakin selaimissa (esim. Safari rajoittaa ne enintään 7 päivään).

Evästeetön analytiikka

- Käyttää palvelinpuolen seuranta, suostumuksia, sormenjälkiä tai anonymisoituja 1. osapuolen tietoja.
- Luottaa tapahtumaseurantaan ja yhdistettyihin tietoihin yksittäisen käyttäjän seurannan sijaan.
- Noudattaa yksityisyyden suojaa koskevia lakeja (esim. GDPR, CCPA), mutta tarjoaa vähemmän yksityiskohtaista tietoa käyttäjistä.

Mihin tahansa muuhun kuin täysin anonymisoituun 1. osapuolen menetelmään sovelletaan tietosuojasäännöksiä, joihin tarvitaan käyttäjän suostumus.

Hybridiverkkoanalytiikka ongelmien ratkaisussa

Hybridiratkaisu mahdollistaa (1. osapuolen) evästeiden asettamisen käyttäjän antaessa siihen suostumuksensa vierailukohtaisesti. Käytettäessä suostumuksen tallennusvälinettä käyttäjän ei tarvitse antaa suostumusta tämän jälkeen, mutta hänen on voitava peruuttaa se.

Kun käyttäjä ei anna suostumustaan, Snoobi Analyticsin kaltainen verkkoanalytiikan työkalu ei tallenna evästeitä, vaan anonymisoi käyttäjän istunnon täysin. *Uudelleen kohdentaminen ja yleisön valinta eivät ehkä ole mahdollisia, mutta tärkeimmät mittarit ja sivukohtainen analyysi verkkosivuston liikenteestä on täysin mahdollista.*

'Pakolliset evästeet'

Pakolliset evästeet, eli välttämättömät evästeet, ovat kriittisiä verkkosivuston osia, jotka varmistavat asianmukaisen toiminnallisuuden ja lainsäädännön noudattamisen. Nämä pakolliset evästeet otetaan automaattisesti käyttöön ilman käyttäjän suostumusta ja ne varmistavat verkkosivuston optimaalisen toiminnan sekä täyttävät tekniset ja lainsäädännölliset vaatimukset.

Alla on tietoa siitä, mitä verkkosivuston analytiikan vaadittuihin evästeisiin tulisi sisällyttää ja mitä ei.

Mitä analytiikkaa varten vaadittavien evästeiden tulisi sisältää?

- **Istunnon tunnusevästeet:** Nämä auttavat seuraamaan käyttäjän istuntoa (esim. kirjautumisen muistaminen tai ostoskorissa olevien tuotteiden säilyttäminen).
- **Kuormituksen tasapainottamisen evästeet:** Nämä auttavat jakamaan liikennettä eri palvelimille, jotta verkkosivuston vaste olisi nopeampi.
- **Turvallisuus- ja petostentorjuntaevästeet:** Nämä suojaavat hyökkäyksiltä ja luvattomalta käytöltä.
- Kaikki muut evästeet, joita verkkosivusto tarvitsee toimiakseen oikein.

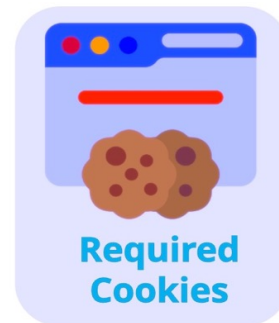
Nämä evästeet ovat rajattuja, ja ne voivat "elää" vain käyttäjän istunnon ajan.

Keskeinen sääntö

Välttämättömiä evästeitä pidetään "pakollisina", jos ne tukevat verkkosivuston toimivuutta (esim. turvallisuus, kirjautuminen, vakaus). Käyttäytymisen, myynnin tai markkinoinnin seurantaan käytettävät evästeet eivät ole pakollisia, ja niiden käyttöön tarvitaan käyttäjän suostumus.

Mitä analytiikkaan vaadittaviin evästeisiin EI pidä sisällyttää?

- **Henkilökohtaisesti tunnistettavat tiedot (PII):** Sähköpostit, nimet, puhelinnumerot tai osoitteet.
- **Tarkat sijaintitiedot:** Paikannus, ellei sitä nimenomaisesti vaadita ja ellei käyttäjä ole antanut siihen täyttä suostumusta.
- **Terveydelliset, taloudelliset tai oikeudelliset tiedot:** Voi johtaa säännösten noudattamatta jättämiseen.
- **Käyttäjän seurantaevästeet:** Evästeet, jotka seuraavat selauskäyttäytymistä (esim. millä sivuilla vieraillet tai miten navigoit sivulla).
- **Mainosevästeet:** Nämä tallentavat tietoja käyttäjän mieltymyksistä, jotta voidaan näyttää kohdennettuja mainoksia.
- **Cross-Site Tracking -tunnisteet:** Nämä "kolmannen osapuolen evästeet" voivat seurata käyttäjiä useilla eri verkkosivustoilla profilointia tai markkinointia varten, eikä niitä voi käyttää ilman suostumusta.



Vaaditut evästeet ja käytettävä teksti

Alla esimerkki käyttäjälle tarkoitetusta viestistä koskien välttämättömiä evästeitä.

"Käytämme välttämättömiä evästeitä, jotka ovat tarpeen verkkosivustomme asianmukaisen toiminnan ja palveluidemme turvallisuuden varmistamiseksi. Nämä evästeet tukevat tärkeitä toimintoja, kuten käyttäjätunnistusta, petosten havaitsemista ja turvallisuuden valvontaa. Ne auttavat meitä tunnistamaan ja estämään haitallisia toimia, suojaamaan käyttäjätilejä sekä varmistamaan verkkosivuston luotettavuuden. Näillä evästeillä ei kerätä henkilötietoja markkinointitarkoituksiin, eivätkä ne ole jaettavissa kolmansille osapuolille. Ne ovat välttämättömiä oikeudellisten, sääntely- ja turvallisuusvaatimusten täyttämiseksi. Verkkosivustomme toiminnan varmistamiseksi niitä ei voi poistaa käytöstä. Näitä evästeitä säilytetään vain niin kauan kuin laki edellyttää."

Oikeutettu etu analytiikassa

Verkkosivustojen tiedonhallinnan maailmassa "oikeutettu etu" on tärkeä, mutta usein väärin ymmärretty käsite. Organisaatioiden käyttäjätietojen hallintaa valvotaan yhä tiukemmin, joten oikeutetun edun ymmärtäminen ja asianmukainen toteuttaminen on ratkaisevan tärkeää. Mutta mitä se tarkalleen ottaen tarkoittaa, ja miksi se ei ole yksinkertainen ratkaisu verkkosivuston analytiikassa?

Mitä oikeutettu etu tarkalleen ottaen on?

Oikeutettu etu on yksi henkilötietojen käsittelyn laillisista perusteista useimmissa tietosuoja-säännöksissä, kuten GDPR:ssä. Yksinkertaistettuna oikeutettu etu antaa organisaatioille mahdollisuuden käsitellä henkilötietoja ilman erillistä suostumusta, jos siihen on perusteltu ja oikeutettu syy, eikä se ole ristiriidassa käyttäjien oikeuksien ja vapauksien kanssa.

Miten voit käyttää oikeutettua etua?

Hyvä esimerkki löytyy Iso-Britanniasta, jossa ICO (Information Commissioner's Office) suosittelee kolmivaiheista testiä, jota kutsutaan "LIA:ksi" (Legitimate Interest Assessment)".

- **Käyttötarkoitustesti:** Määrittää, onko tietojen käsittelyn tarkoitus oikeutettu.
- **Tarpeellisuustesti:** varmistaa, että käsittely on tarpeen mainittua tarkoitusta varten.
- **Tasapainotesti:** varmistaa, että yksilön oikeudet eivät syrjäytä oikeutettua etua.

Tämän testin avulla voit selvittää, onko oikeutetun edun käyttäminen perusteltua.

Voit käyttää heidän LIA-malliaan, joka löytyy heidän sivustoltaan [tai tästä linkistä](#).

Analytiikan osalta oikeutetun edun määrittäminen vaatii tasapainottelua organisaation tarpeiden ja tietosuojan välillä. Vaikka palvelun parantaminen analytiikan avulla voi olla oikeutettu etu, arvioinnissa on otettava huomioon sen tarpeellisuus ja suhteellisuus.

Tärkeintä on varmistaa, että organisaation edut eivät loukkaa käyttäjien oikeuksia liiallisesti. Esimerkiksi julkishallinnon organisaatio, joka käyttää analytiikkaa julkisten palvelujen parantamiseen, voi perustella oikeutetun etunsa paremmin kuin kaupalliset myyntipainotteiset strategiat.

On tärkeää, että käyttäjillä on aina mahdollisuus kieltäytyä tietojen käytöstä ja valvoa niiden käyttöä.

Oikeutettu etu voi jäädä vajaaksi

Oikeutettu etu vaatii subjektiivista tulkintaa, mikä voi helposti johtaa epä johdonmukaisuuksiin tietojenkäsittelyssä. Vaikka oikeutettu etu tarjoaa raamit, se ei riitä vastaamaan monimutkaisiin analyysivaatimuksiin. Suostumukseen perustuvat mallit tarjoavat selkeämmän ja konkreettisemmän tavan käsitellä tietoja. Opt-in-järjestelmät, joissa käyttäjä antaa nimenomaisen suostumuksensa, vahvistavat oikeudellista asemaa ja lisäävät avoimuutta.

Asettamalla käyttäjän suostumuksen etusijalle organisaatio voi vahvistaa vaatimustenmukaisuutta, rakentaa luottamusta ja varmistaa tietosuojastandardien mukaiset eettiset käytännöt.



Yhteenveto

Oikeutetun edun ymmärtäminen vaatii tasapainoa yksityisyyden suojan ja liiketoimintaetujen välillä. Organisaatioiden, jotka haluavat hyödyntää analytiikkaa ja säilyttää vaatimustenmukaisuuden, on yhdistettävä oikeutetun edun arviointi vahvoihin suostumusprosesseihin ja avoimuuteen.

Vaikka oikeutettu etu tukee analytiikkaa, työkalut kuten Snoobi Analytics osoittavat, että tarvitaan vahvat suostumuskehykset. Oikeutetun edun hallinta vaatii jatkuvaa arviointia lainsäädännön ja käyttäjien odotusten kehittyessä.

Palvelinpuolen seuranta

Palvelinpuolen seuranta siirtää tiedonkeruun käyttäjän selaimelta verkkosivuston omalle palvelimelle ennen kuin se lähetetään analytiikkatyökaluille, kuten Google Analytics tai vastaava. Tämä lähestymistapa voi tukea vaatimustenmukaisuutta, mutta siihen liittyy myös merkittäviä yksityisyyden suojaan liittyviä riskejä.

Palvelinpuolen seuranta ja tietosuojasäännöt

Edut

- Parempi tietojen valvonta: Sivuston omistaja valvoo, mitä tietoja lähetetään kolmansille osapuolille, mikä vähentää riippuvuutta evästeistä.
- Vähemmän riippuvuutta käyttäjän laitteista: Voidaan ohittaa joitakin selainrajoituksia, kuten kolmannen osapuolen evästeiden esto.
- Turvallisuus ja anonymisointi: Tietoja voidaan anonymisoida tai käsitellä ennen jakamista GDPR:n, CCPA:n ja muiden säännösten mukaisesti.

Mahdolliset oikeudelliset ja yksityisyyden suojaan liittyvät kysymykset

- Vaatii käyttäjän suostumuksen: Henkilötiedot (esim. IP-osoitteet, käyttäjätiedot, käyttäytyminen) edellyttävät useimmissa maissa suostumuksen, vaikka seuranta tapahtuisi palvelinpuolella.
- Avoimuuteen liittyvät huolenaiheet: Käyttäjät eivät välttämättä pääse helposti käsiksi tallennettuihin tietoihin tai hallitse palvelinpuolen seurantaa, mikä herättää eettisiä ja oikeudellisia kysymyksiä.
- Väärinkäytön riski: Jotkut organisaatiot käyttävät palvelinpuolen seurantaa yksityisyydensuojan ohittamiseen - voi johtaa rangaistuksiin.



Google Consent Manager ratkaisuna?

Miten auttaa:

- Kunnioittaa käyttäjän mieltymyksiä: Jos käyttäjä kieltäytyy seurannasta, Google Analytics ja Google Ads mukauttavat tiedonkeruuta vastaavasti.
- Tukee GDPR- ja CCPA-vaatimusten noudattamista: Toimii evästabannereiden kanssa, jotta voit valvoa, mitä tietoja lähetetään.
- Mahdollistaa rajoitetun tietojen seurannan: Joitakin rajoitettuja tietoja (ilman henkilötietoja) voidaan silti kerätä analytiikkaan, vaikka seuranta olisi kielletty.

Keskeiset rajoitukset EU:n alueella:

- Ei täysin GDPR:n mukainen, koska Google Consent Mode ei tarjoa GDPR:n edellyttämiä suostumuksen valintoja (esim. erilliset suostumukset eri evästetyypeille).
- Tukee ensisijaisesti Googlen palveluja (Google Analytics, Ads).
- Oikeutettua etua ei ole käsitelty asianmukaisesti, koska Google käyttää sitä tietyissä tietojenkäsittelytilanteissa, vaikka se ei ole GDPR:n mukaan hyväksyttävää ilman nimenomaista suostumusta. Huomaa, että monet EU:n viranomaiset eivät hyväksy oikeutettua etua perusteeksi seurannalle ilman suostumusta.
- Tietojen siirto Yhdysvaltoihin voi olla ongelma, koska Google tallentaa tietoja sinne, ja tämä herättää GDPR-huolia Schrems II -päätöksen vuoksi. Vaikka Google on tehnyt EU:n tietosuojasitoumuksia, viranomaiset voivat silti katsoa, että ne eivät ole riittäviä.
- Ei automaattista evästeiden estämistä, koska Google Consent Mode ei estä evästeitä automaattisesti. Verkkosivustojen on otettava Googlen sovellusrajapinnat käyttöön tietojen keräämisen estämiseksi ennen suostumuksen antamista.
- Jos Googlen palvelut on määritetty väärin, ne voivat kerätä osittaisia tietoja (esim. käyttämällä evästeettömiä pingejä) ennen kuin täysi suostumus on annettu.
- Sääntelyerot eri EU-maissa: Joillakin tietosuojaviranomaisilla on standardi GDPR:ää tiukempia tulkintoja suostumussäännöistä, ja näitä Google Consent Mode ei välttämättä täysin täytä.

Yhteenveto

Palvelinpuolen seuranta voi parantaa vaatimustenmukaisuutta, mutta se ei poista suostumuksen tarvetta. Google Consent Manager auttaa seurannan hallinnassa, mutta se ei ratkaise kaikkia tietosuojaan liittyviä ongelmia. Täydellinen vaatimustenmukaisuus edellyttää, että organisaatiot varmistavat edelleen avoimuuden, sallivat opt-out-mahdollisuuden ja käsittelevät tietoja lainmukaisesti.

Miksi suostumuksenhallinta ei yksin riitä

Selaimet kehittyvät jatkuvasti yksityisyyden suojan suhteen, ja suostumustenhallinnan rooli muuttuu. Niiden tehokkuus heikkenee, kun selaimet estävät seurannan oletuksena. Suostumustenhallintatyökalujen, jotka ovat tärkeitä evästekyselyissä ja GDPR- tai CCPA-vaatimusten noudattamisessa, on sopeuduttava, koska suostumuksia tarvitaan vähemmän. Niiden on mukauduttava käyttäjien tarpeisiin, sisällön räätälöintiin ja digitaaliseen markkinointiin.

Miksi tietoja voi silti jäädä puuttumaan, vaikka suostumustenhallintaa käytetään?

Monet verkkosivustot käyttävät Cookiebotin® kaltaisia suostumustenhallinta-alustoja (CMP) noudattaakseen tietosuojalakeja. Nämä alustat pyytävät käyttäjiltä lupaa seurata heidän tietojiaan, jolloin markkinoijat voivat kerätä tietoja vain suostumuksen saatuaan. Vaikka CMP on käytössä, markkinoijat voivat silti kohdata puutteellista verkkoanalytiikkaa.

(1) Käyttäjät voivat hylätä seurannan

Useimmat suostumusbannerit antavat käyttäjille mahdollisuuden kieltäytyä yhdestä tai useammasta seurantavaihtoehdosta, eli:

- Evästeitä ei voida asettaa (ensimmäisen tai kolmannen osapuolen evästeet).
- Mitään seurantaskriptejä (analytiikka, sosiaalisen median seuranta jne.) ei suoriteta.
- Käyttäjistä ei tallenneta käyttäytymistietoja (sivunäkymiä, klikkauksia, konversioita).

Tämä aiheuttaa tietopuutteita, mikä vaikeuttaa verkkosivuston suorituskyvyn tarkkaa mittaamista.

(2) Osittainen suostumus heikentää tietojen laatua

Jotkut käyttäjät sallivat seurannan valikoivasti:

- Vain välttämättömät evästeet ovat sallittuja, kun taas analytiikka- ja markkinointievästeet on estetty.
- Toteutuksesta riippuen on myös mahdollista, että suostumus annetaan useiden sivujen jälkeen, mikä vaikuttaa tietojen laatuun.

Markkinoijat ja analytiikot saavat hajanaisia tietoja, joista puuttuvat keskeiset toimet, kuten liikenteen lähde, välitön poistuminen tai usean istunnon käyttäytyminen.

Jos käyttäjä esimerkiksi antaa suostumuksensa vain välttämättömiin evästeisiin, hän voi edelleen selata verkkosivustoa, mutta hänen toimiaan ei seurata. Tästä seuraa liian vähäiset käynnit analytiikassa.

(3) Selaimen ja laitteen rajoitukset ovat voimassa

Vaikka käyttäjä hyväksyisi evästeet ensimmäisellä sivulla, nykyaikaiset selaimet ja tietosuojatyökalut voivat:

- Estää seurantapyynnöt (esim. Safarin älykäs seurannan esto).
- Rajoittaa evästeiden käyttöikää (esim. Safari ja Firefox poistavat ensimmäisen osapuolen evästeet 7 päivän kuluttua).

Tämän seurauksena analytiikan tiedot ovat edelleen epätäydellisiä, vaikka käyttäjät olisivat antaneet suostumuksensa.

Vaikka käyttäjät eivät hyväksy evästeitä, niin markkinoijat ja analytiikot voivat kerätä tietoa ja noudattaa GDPR:ää käyttämällä evästeettömiä seurantamenetelmiä ja UTM-parametreja. On tärkeää pysyä läpinäkyvänä ja tarjota selkeitä opt-in-vaihtoehtoja, jotka ovat käyttäjälle ymmärrettäviä. Yksityisyydensuojaa korostavien analytiikkaratkaisujen, kuten Snoobi Analyticsin, käyttäminen auttaa säilyttämään näkemyksellisyyden ilman GDPR:n rikkomista.



Kattava analytiikka Snoobin avulla

Käyttämällä Cookiebot®:n kaltaista suostumuksenhallintatyökalua yhdessä Snoobi Analyticsin kanssa, voidaan seurata vierailijoiden reittejä "hybridi"-mallilla, jossa suostumuskäyttäytyminen sisältyy web-analytiikkaan rikkomatta GDPR:ää tai muita yksityisyydensuojaa koskevia sääntöjä.

Analytiikka portaaleille tai intranetille

Verkkosivuston tilastoissa voi paljastua henkilötietoja, kuten sähköpostiosoitteita. Tämä koskee erityisesti portaaleja ja intranetteja, jotka vaativat kirjautumistietoja. Henkilötietojen lisääminen URL-osoitteisiin tai sallia portaalin lisätä niitä voi aiheuttaa yksityisyyteen liittyviä riskejä.

Tässä alla on muutamia keskeisiä riskejä ja huomioita.

URL-osoitteissa olevien henkilötietojen paljastumisen riski

Henkilökohtaiset tiedot voivat päätyä URL-osoitteeseen, jos sovellus tarvitsee niitä toimiakseen tai jos sovellusta ei ole määritetty oikein. Esimerkiksi lähetettäessä sähköpostia:

<https://this.sample.com/usr?email=jdoe@this.com>

Tähän liittyy useita riskejä

Useimmat suostumusbannerit antavat käyttäjille mahdollisuuden kieltäytyä yhdestä tai useammasta seurantavaihtoehdosta, eli:

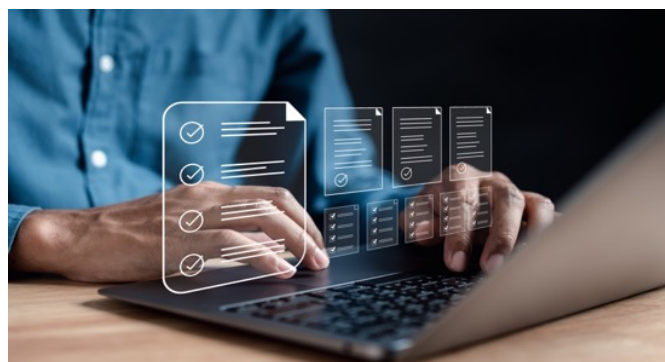
- **Tietovuoto:** URL-osoitteet kirjataan eri paikkoihin, kuten palvelin- ja palomuurilokeihin sekä analytiikkatyökaluihin.
- **Phishing- ja roskapostiriskit:** Jos sähköpostiosoitteet näkyvät URL-osoitteissa, ne voidaan jäljittää ja käyttää phishing-hyökkäyksiin.
- **GDPR ja vaatimustenmukaisuuden rikkomukset:** URL-osoitteissa olevien henkilötietojen paljastaminen on GDPR:n kaltaisten säädösten mukaan tietosuojarikkomus, koska URL-osoitteet tallennetaan turvattomasti ja käyttäjän valvonnan ulkopuolella.
- **Istunnon kaappaus:** Jos todennuskoodit tai istunnotiedot on upotettu URL-osoitteeseen sähköpostin mukana, hyökkääjät voivat päästä sisään kaappaamalla URL-osoitteen.

Mikä on sallittua portaaleissa tai intranetissä?

Yrityksen intranetissä sisäisten käytäntöjen ja työntekijöiden sopimusten tulisi selventää, miten analytiikkatietoja käytetään. Jos ulkoiset käyttäjät tai asiakkaat kirjautuvat sisään, tulisi soveltaa kaikkia tavanomaisia tietosuojasäännöksiä.

Voitdaanko evästeet asettaa automaattisesti?

- **Kyllä**, todella välttämättömien evästeiden osalta. Jos evästeet ovat välttämättömiä todennuksen, turvallisuuden tai ydintoimintojen kannalta, ne eivät vaadi suostumusta.
- **Ei**, analytiikkaevästeille ilman suostumusta. Jopa kirjautumisessa intranettiin GDPR edellyttää edelleen nimenomaista suostumusta analytiikkaevästeille, ellet voi perustella niitä oikeutetun edun mukaan (vaikeaa seurannan osalta).
- **Ratkaisu:** Jotkut organisaatiot käyttävät evästeetöntä analytiikkaa (täysin anonymisoitua) suostumusvaatimusten ohittamiseksi ja ovat samalla vaatimustenmukaisia.



Yleiset suuntaviivat

Tietosuojasäännökset ovat siis voimassa, vaikka sinulla olisi suljettu, vain työntekijöille tarkoitettu portaal

Muutamia ohjeita:

- Käytä raakojen sähköpostiosoitteiden sijasta käyttäjätunnuksia tai hajautettuja arvoja
- Käytä istuntopohjaista todennusta sen sijaan, että välität henkilötietoja kyselyparametreissa.
- Älä nimeä henkilökohtaisia kansioita henkilökohtaisilla nimillä.
- Vältä käyttäjätunnuksia, puhelinnumeroita tai muita henkilökohtaisia tunnisteita kyselymerkkijonoissa.
- Älä sisällytä henkilötietoja URL-osoitteessa näkyviin lomakemerkintöihin.
- Jos käyttäjän on haettava tietonsa, hae ne palvelimelta istunnon todennuksen perusteella sen sijaan, että ne upotettaisiin URL-osoitteeseen.
- Määritä lokijärjestelmät (esim. Apache, Nginx, IIS) siten, että arkaluonteiset kyselyparametrit jätetään pois.
- Jos käytät Snoobi Portal Analytics -ratkaisua, neuvottele Snoobin kanssa henkilötietoelementtien poissulkemisesta ja häivyttämisestä.
- Jos intranet tai portaalit toimii SharePoint Online-, SharePoint Server- tai Microsoft 365 -palvelimella, kannattaa noudattaa Microsoftin parhaita käytäntöjä.

Yhteenveto: Tietosuojaystävällinen analytiikka

Yksityisyyden suojaan liittyy monia näkökohtia, mutta tärkeintä on, että käyttäjille annetaan kontrolli, ollaan läpinäkyviä ja huolehditaan tietosuojasta ja tietoturvasta. Tietosuojaystävällinen analytiikka kunnioittaa oikeuksia ja luo samalla oivalluksia. Kun analytiikka ja yksityisyyden suoja ovat linjassa keskenään, luodaan parhaat edellytykset kaikille osapuolille, ja käyttäjät ovat halukkaampia jakamaan tietoaan.



Yksityisyys ja teknologia

Yksityisyyden suojan osalta teknologia tarjoaa monia vaihtoehtoja. Jotkut suojaavat yksityisyyttään, toiset taas eivät. DuckDuckGo® esimerkiksi on hakukone ja mainosalusta, joka ei kerää henkilötietoja. Sen sijaan DuckDuckGo tarjoaa kävijöille hakusanoihin perustuvia kontekstisidonnaisia mainoksia. Tällä lähestymistavalla vältetään Googlen yhä useammin kohtaamat yksityisyysongelmat.

Toinen vaihtoehto on analytiikka-alusta, joka mahdollistaa tietojen keräämisen käyttäjistä sekä evästeiden kanssa että ilman niitä. Henkilötietoja kerätään vain, jos käyttäjä antaa suostumuksensa. Ilman suostumusta kerätään vain nimettömiä tietoja. Snoobi käyttää Cookiebot®-asetuksia ja sallii evästeiden asettamisen käyttäjän mieltymysten mukaan.

Neljä tärkeää elementtiä tietosuojaa edistävään analytiikkaan

(1) Salli henkilötietojen käytön kontrolli.

- Henkilötietojen käsittelyyn tarvitaan suostumus. Suostumuksen on oltava vapaa ja kiistaton, ja siihen on sisällyttävä selkeä, myönteinen toimenpide. Esimerkiksi painikkeen "Hyväksyn" klikkaaminen. Pelkkä oletus siitä, että verkkosivustolla jatkaminen on suostumus, riittää vain "välttämättömien evästeiden" osalta, jotka ovat välttämättömiä verkkosivuston toiminnan kannalta.
- On myös tärkeää, että kerätään vain ne tiedot, joiden jakamiseen on annettu suostumus, ja tietoja käytetään vain siihen tarkoitukseen, jota varten ne on kerätty. Henkilötietoja, jotka on rekisteröity ensimmäisen osapuolen käyttöön, ei saa jakaa esimerkiksi kumppaneille tai kolmansille osapuolille.
- Tietoja keräävien organisaatioiden on ilmoitettava selkeästi tietojensa käyttötarkoitukset. Yllättävää kyllä, laajoja henkilötietoja kerätään edelleen ilman yksilöiden tietoa tästä. Käyttäjille on ilmoitettava muutoksista tietojen käytössä ja annettava mahdollisuus kieltäytyä uusista käyttötavoista sääntöjen mukaisesti. Heidän tulisi myös sallia pyytää henkilökohtaisten tietojen tarkastelua ja poistamista. Avoimuus ja valvonta ovat keskeisiä tiedonkeruukäytännöissä.

(2) Avoin raportointi ja tietojen käsittely

- On oltava täysin selvää, jaetaanko tietoja, miten, kenelle ja mihin tarkoitukseen. Suostumus on helpompi antaa, jos käyttötarkoitus ilmoitetaan selkeästi. Tällöin organisaatiot voivat hyötyä suoraan käyttäjiltä saaduista ensimmäisen osapuolen tiedoista.
- Luottamus on tärkeää, sillä ilman sitä käyttäjät saattavat käyttää mainosten esto-ohjelmia tai muita estotyökaluja, mikä heikentää organisaation kykyä parantaa palvelujaan. Tallennuspaikalla on merkitystä, sillä "pilvipalvelu" ei riitä – yksityisyyden suoja riippuu alueellisesta lainsäädännöstä.
- Henkilötietoja eri maissa käsittelevien organisaatioiden on tunnettava paikallinen tietosuojalainsäädäntö. EU:n kansalaisten tietojen säilyttäminen EU:n alueella on suositeltavaa. Snoobi Analytics säilyttää kaikki kerätyt tiedot palvelimilla Suomessa ja EU:n alueella. Läpinäkyvyys ja vaatimustenmukaisuus ovat keskeisiä sekä käyttäjille että organisaatioille.

(3) Sisäänrakennettu tietosuojaja

- Yksityisyyden suoja edistävät analyysimenetelmät perustuvat "sisäänrakennetun yksityisyyden suojan" periaatteisiin, joissa korostetaan ennakoivaa ja ennaltaehkäisevää lähestymistapaa. Keskeinen lähtökohta on ehkäistä yksityisyyden suojan loukkauksia sen sijaan, että niihin puututtaisiin reaktiivisesti.
- Kaksi keskeistä ennakoivaa strategiaa ovat tietojen minimointi (käytetään vain välttämättömiä tietoja tiettyihin tarkoituksiin) ja käyttötarkoituksen rajoittaminen (käyttäjille tiedotetaan avoimesti tietojen tarkasta käytöstä ennen käsittelyä).
- Tietojen käsittelyn jälkeen tietoja ei saa säilyttää tarpeellista pidempään. Toteutusmekanismit vaihtelevat käyttökäytännöittäin, kuten tietojen anonymisointi tai yksityisyyden suojaavat analyysitoiminnot.

Snoobi Analytics mahdollistaa tietojen täydellisen anonymisoinnin, mikä takaa vankan yksityisyyden suojan ja nykyaikaisten tietojenkäsittelystandardien noudattamisen. Tietoja ei koskaan jaeta verkkosivuston omistajan valvonnan ulkopuolelle.

(4) Tietoturva

Tietoturva ja yksityisyyden suoja ovat erillisiä, mutta toisiinsa liittyviä. Tietoturva suojaa tietoja luvattomalta käytöltä, varkauksilta ja turmeltumiselta, ja siihen kuuluvat laitteistojen suojaus, menettelyt ja käytännöt. Tietosuojaystävällisissä analytiikkaratkaisuuksissa on tärkeää priorisoida vahvat turvatoimet. Hyvä tietoturva estää mainehaittoja ja taloudellisia tappioita. Käyttäjien on luotettava siihen, että heidän tietonsa ovat turvassa, tai he eivät halua jakaa niitä, vaikka siitä olisi hyötyä.

Onko yksityisyyden suoja kunnioittavaa analytiikkaa olemassa?

Monia yleisiä analytiikka-alustoja ei ole suunniteltu yksityisyyden suoja silmällä pitäen. Ne hoitavat tietoturvan hyvin, mutta jäävät jälkeen avoimuuden ja käyttäjien oman kontrollin sallimisen osalta. Monille osapuolille on hyödyllistä analysoida käyttäjien käyttäytymistä. Esimerkiksi Googlen liiketoimintamalli perustuu tiedonkeruun maksimoimiseen. Hyvä uutinen on, että on olemassa analytiikkatyökaluja, kuten Snoobi Analytics, joka kunnioittaa yksityisyyttä ja kerää mahdollisimman paljon tietoa verkkosivustolla käyttäytymisestä lain sallimissa rajoissa.

Lisätietoja

Tietoja Snoobi c

- ◇ [Snoobin Turvatoimet](#)
- ◇ [Snoobi & Cookiebot](#)
- ◇ [Evästeetön Analytiikka](#)
- ◇ [Snoobin turvallinen Tietosuojattu seuranta](#)
- ◇ [Snoobin verkkosivusto](#)
- ◇ [Snoobin Tietopankki](#)
- ◇ [Pyydä ilmainen kokeilujakso](#)

Tietosuojaja säännökset

- ◇ [Evästeohjeistus - Suomi](#)
- ◇ [Iso-Britannian tietosuojavaltuutetun toimisto](#)
- ◇ [Euroopan sähköisen viestinnän tietosuojadirektiivi](#)
- ◇ [CNIL:n ohjeet \(ranskaksi\)](#)
- ◇ [Tiedonkeruu ja evästeet Alankomaissa](#)
- ◇ [Saksan BfDI:n tietosuojasivu](#)
- ◇ [Wikipedia 3. osapuolen evästeistä](#)

