Beet

Beet AB

Box 7140
103 87 Stockholm

Org.nr: 556911-3789
www.beet.se

4 JULI, 2023 – UPPDATERAD 17 JULI 2023

Information och rekommendationer relaterat till IMY:s beslut om Google Analytics 3/7-2023 & EC:s beslut om DPF 10/7-2023

Tomas
Lindqvist

Channel Lead – Analytics & Measurement

Innehåll

1. Vad har hänt & bakgrund

IMY (Integritetsskyddsmyndigheten) har 3/7 gjort ett utlåtande och beslut i likhet med tidigare myndigheter i Danmark, Frankrike, Italien och Österriket samt Norges preliminära utlåtande. Den största skillnaden för det svenska beslutet är att det är första beslutet där sanktionsavgift har delats ut, i övrigt är de till stor del likställda på vilken grund besluten tagits.

Beslutet innebär kortfattat att standardanvändning av Google Analytics (Universal Analytics - UA) inte är förenligt med GDPR och de fyra bolagen i fråga (Tele2, CDON, DI och Coop) har inte gjort tillräckliga tekniska åtgärder i användandet av UA för att säkerställa en likvärdig skyddsnivå av data som skickas till USA som garanteras inom EU under GDPR-lagen.

Ärendet kommer från en anmälning som intresseorganisationen NOYB (None of Your Business) gjort emot 101 EU-bolag (i Sverige fyra för Google Analytics och två för Facebook), där Sverige är femte landet att göra ett officiellt utlåtande om ett beslut. Anmälningarna gjordes av NOYB i koppling till, och strax efter, Schrems II-beslutet juli 2020 (vilket också drevs av NOYB).

Schrems II-beslutet var kortfattat att standardavtalsklausuler som Google och andra bolag stödjer sig på för användandet (såkallade SCCs - Standard Contractual Clauses) inte ger godtyckligt skydd i sig och att andra åtgärder behöver göras, där domen då fallit att bolagen inte gjort tillräckliga åtgärder.

Beslutet från IMY är därmed gjort på samma sätt som de tidigare länderna, men är först med att besluta om sanktionsavgifter.

Dessvärre ger IMY:s beslut begränsad information om exakt vad som tekniskt inte setts som “åtgärd nog” vid utredningarna och vi arbetar aktivt med att sammanställa och uppdatera information och rekommendationer efter vår bästa kunskap. Detta dokument kan därav komma att uppdateras med ny information och nya rekommendationer framåt.

Uppdatering 6/7-2023:
IMY byter titel på pressrelease artikeln från: "Bolag måste sluta använda Google

Analytics", till: "Fyra bolag måste sluta använda Google Analytics". Det förändrar inte konsekvensen att man behöver ta åtgärder men gör det tydligare att beslutet gäller dessa 4 bolag specifikt nu.

Uppdatering 17/7-2023:
Den 10e juli 2023 antog Europeiska kommissionen (European Commission - EC) antagit ett adekvat beslut för nya Data Protection Framework (DPF), som ersätter Privacy Shield, angående säkra och pålitliga dataöverföringar mellan EU-USA.

Användning av det nya ramverket som stöd för dataöverföringar mellan EU-USA har därmed blivit godkänt från och med den 10e juli 2023 för certifierade verksamheter.

En hemsida och information om vilka som är certifierade har släppts den 17e juli 2023 där man kan se vilka verksamheter som är certifierade. Därav att vi först den 17e kunnat veta vilka verksamheter som faktiskt är godkända även om beslutet träde i kraft direkt den 10e juli för att kunna sammanställa våra rekommendationer i samband med beslutet.

IMY har också släppt en pressrelease om EC:s adekvata beslut för DPF:
https://www.imy.se/nyheter/eu/

Vad innebär EC:s 'adekvata' beslut?
I praktiken betyder det att användningen av verktyg från certifierade partners nu är tillåten även för överföring av personuppgifter. I princip, om en överföring som görs inom EU är godkänd, skulle den nu också godkänd för överföring från EU till USA och vice versa USA till EU för överföringar som är godkända inom USA.

Länk till beslutet: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3721

Vilka verksamheter är nu certifierade?
För en fullständig lista, se den officiella webbplatsen. Men det kan nämnas direkt att Google, som berördes av IMY:s beslut angående Google Analytics, är certifierade enligt DPF tillsammans med Meta, Microsoft och många andra.

Därmed är användning av Google Analytics (UA & GA4) nu tillåten under DPF.

Observera att det fortfarande är viktigt att följa GDPR:s riktlinjer om minimering, obfuskering och tids-begränsning av datainsamling oavsett hur och var insamlingen görs och datan skickas.

Länk till DPF-certifierade verksamheter:
https://www.dataprivacyframework.gov/s/participant-search

Vad gäller då med våra rekommendationer i sektion 3 och 4?
Även om våra rekommendationer gjordes i en kontext utan DPF, är de fortfarande relevanta i en situation där DPF skulle ogiltigförklaras, i en 'Schrems-III' situation, likt hur Privacy Shield ogiltigförklarades av Schrems-II (NOYB har redan officiellt meddelat att de kommer att utmana det adekvata beslutet för DPF och vi kan förvänta oss att juridiska processerna inleds i början av 2024).

Det finns därmed en risk att en liknande situation uppstår som de tre åren mellan Schrems-II och DPF efter ett eventuellt Schrems-III beslut, och våra rekommendationer står fortfarande som vägledning för vilka potentiella risker de minimerar om en sådan situation uppstår.

Vi kommer fortsätta att utvärdera riskerna och vara tillgängliga för teknisk rådgivning angående dessa frågor för er specifika situation på begäran.

2. Nyckelfakta som är bra att veta

- Beslutet gäller **UA** kopplat till anmälan från 2020 gjord i relation till Schrems II. Vår bedömning är att **beslutet inte berör Google Analytics 4**.
  Observera att den bedömningen kan komma att ändras om vi ges ny kunskap.
- Tele2 använder idag GA4 genom vanlig GTM-implementering (Google Tag Manager). Det nämns i beslutet att Tele2 stängt av Google Analytics vilket betyder att det rör sig om UA (Universal Analytics).
- Google har i mer än ett år kommunicerat sunset (stängning) av datahantering via UA, med en milstolpe 1 juli 2023. Många konton har dock datahantering fortfarande aktiv och är inte "stängda". Läs mer på: https://support.google.com/analytics/answer/11583528?hl=en
- DI och Coop har, från vad vi kan förstå, gjort mer och större åtgärder för att få UA till likvärdig skyddsnivå (även om de också fick nedslag) men har inte drabbats av sanktionsavgifter.

OBS! Viktigt att notera är att UA inte anses vara avinstallerat bara för att "ny data" inte längre processas i det specifika kontot, utan **avinstallation av skripten från sajt eller Google Tag Manager (GTM)** krävs för att sluta skicka data till Google/USA.

3. Nuvarande rekommendationer

Dessa rekommendationer kan komma att ändras och är gjorda från vår bästa tolkning av den information vi har nu.

1. Tydliga "sluta nu" gällande användning av UA i IMY-besluten

Besluten har gjort det tydligt att användande av UAs IP-anonymiseringsfunktion (* se sektion 7) inte är tillräckligt. Coop och Dagens Industri som båda fick mildare domar implementerade en proxy för att helt ta bort IP-adresserna innan det skickades till Google vilket är en mer gedigen teknisk åtgärd.

1.1. <u>Sluta skicka besökares IP till Google vid användning av UA</u>
Alt. 1: Avinstallera UA-implementationer helt från sajt/GTM och sluta skicka data till UA.
(UA:s data-hantering skulle ändå ha stängts av den 1:a juli av Google, även om det i nuläget ser ut att fortsätta för många av de implementationer som Beet bevakar).
Alt. 2: Säkra att IP inte kan skickas till Google/USA vid användning av UA.

1.1.1. Vid implementationer direkt på sajt och via GTM, byt till server implementering och aktivera IP-borttagning (kräver uppsättning av en GTM-server).

1.1.2. Vid Implementationer via server, aktivera IP-borttagning om den funktionen inte är aktiverad idag.
Notering: Vid borttagning av IP förloras all GEO-IP-data och man får ingen location data.

1.2. <u>Skicka inte in/sluta skicka in personinformation eller data som enkelt kan identifieras till personinformation.</u>
Exakt vad som kan vara personinformation utöver IP-adress är tyvärr inte tydligt i IMY-besluten och därmed rekommenderas att applicera försiktighetsprincipen genom att minimera och abstrahera data för att minimera risken.

2. Försiktighetsåtgärder för UA och GA4 från IMY-besluten

Åtgärderna är grupperade under den nivå av risk vi ser skulle mitigeras vid implementering av åtgärden. “Hög Risk” kan då ses som åtgärder för att minska det vi ser som största riskerna etc.

2.1. Försiktighetsåtgärder vid användning av Universal Analytics:

Nedanstående åtgärder är avsedda att minimera risken att den data man har samlat/samlar till UA idag blir klassad som ”personinformation” i specifik användningssituation genom att isolera data till sitt UA-konto.

Hög risk:

- Stäng av/använd inte "Google-Signals"

Enligt vår tolkning av besluten verkar detta vara den största riskexponeringen utöver punkt 1.1 och 1.2 då Google vet vilka användarna är via Google-konton. Del av den datan delas till UA-kontot baserat på data man tillhandahåller Google och kan göra att datamängden blir klassad som personinformation även om man inte får all data från Google.

Medel risk:

- Stäng av/använd inte "Advanced Settings to Allow for Ads Personalization"

Låg risk:

- Dela inte/sluta dela ”Audiences och Konverteringar” till Google Ads

2.2. <u>Försiktighetsåtgärder vid användning av GA4:</u>

(inte del av IMY besluten just nu, men är liknande funktioner som i UA)

Hög risk

- Stäng av/använd inte "Google Signals" (se 2.2.a.)

Medel risk

- Implementera GTM-Sever som data-gateway för GA4 innan datan skickas till Google/USA, och där igenom filtrerar bort IP-adresserna i egna hanteringen.

GA4 har en teknisk skillnad emot UA där data först går till ett EU-baserat data-center innan det skickas till USA (och då blir en dataöverföring till USA). I det mellansteget tar de bort IP-adresserna som då inte skickas vidare. Därmed är GA4 säkrare och exponerar inte IP-adresser på samma sätt som UA. Dock behöver man inte ta för givet att Google faktiskt gör det och är dessutom något man själv inte kan bevisa om man blir granskad. Därmed ser vi det som en medelstor risk att göra vanlig implementering i GA4 och rekommenderar istället att implementering görs genom en GTM-server (data-gateway man själv äger).

- Stäng av/använd inte "Granular location and device data collection" inom EU. Slå av det för alla länder inom EU (** Se punkt 7).

Denna funktion ökar mängden detaljerad data relaterat till en användares device och plats som sparas och binds till besökarens datamängd. Risken här är huvudsakligen kopplad till att ha för många olika datapunkter på samma besök vilket ökar risken för identifieringsmöjligheter som därmed går emot GDPR-direktivet angående att minimera datasamling om den inte är strikt nödvändig.

Låg risk

- Stäng av/använd inte "Advanced Settings to Allow for Ads Personalization" inom EU (slå av det för alla länder inom EU) och därmed dela inte/sluta dela "Audiences" eller ”Konverteringar” till Google Ads.

Denna funktion kontrollerar vilken data som kan skickas vidare till Google Ads och användas för annonsering relaterat till de godkända regionerna. Avstängning av detta kan då ha stor effekt på ens Google Ads-marknadsföring om dessa funktioner används idag och kan behöva tas i beaktning. Funktionen styr alltså vad som får göras med

datan efter att den har överförts och vi bedömer att det är låg risk kopplat till frågan om själva data överföringen.

- Implementera data-hashning/extra pseudoanonymisering av olika potentiella identifierare som cookie-IDn, transaktions-IDn etc.

3. Alternativa plattformar att överväga för framtiden

Notera att ingen av dessa är fullvärdiga ersättare av UA/GA4, men är alternativ som är GDPR-godkända som vi kan hjälpa till med baserat på vår expertis:

- **PiwikPro** (ett alternativ för e-handel- och lead-sajter, liknar UA)
- **Matomo** (Open-source och byggt likt UA, OK för lead-sajter men har begränsad modul för e-handel)
- **Utvärdering av andra alternativ** (det finns fler verktyg där ute och nya som kommer, här kan vi bidra med vår expertis för utvärdering och hjälp)

4. Summering

Uppdatering 17/7-2023: Se detaljer om hur EC:s adekvat beslut för DPF den 10/7-2023 påverkar allt i allmänhet under ’Vad har hänt & bakgrund’ sektionen.

Beslutet är i linje med andra länders myndigheter, dock har man utfärdat sanktionsavgifter. Den överträdelse man fokuserar på som är tydligast är delning av IP-adresser till Google. Därutöver är det inte helt tydligt vad som ligger till grund för beslutet, men vi ser indikationer på att data-delning med Google, som Google Signals, gör att datamängden kan klassas som personinformation samt potentiellt för annan användning.

Våra rekommendationer fokuserar på att:

- **Eliminera risk -** *helt stänga av UA och byta till verktyg som är godkända som PiwikPro eller Matomo, alternativt använda GA4 som inte berörs av nuvarande ärenden och har bättre skydd än UA, även om det inte i dagsläget är certifierat godkänt.*
- **Minimera risk** - *stäng av funktioner och genomför tekniska åtgärder för att minimera risken i UA/GA4.*

En summering och riskbedömning för funktioner/data är för närvarande nedan:
Direkt risk: IP-adress och personinformation
Hög risk: Google Signals och “potentiell” personinformation
Medel risk: Andra delningsfunktioner som granulär device/platsdata
Låg risk: Icke-obfuskerade kund-IDn, användar-IDn, aggregerad data som audience-listor (antaget att consent nämner sådan potentiell användning som audiences)
Väldigt låg risk: Pseudoanonymiserade IDn, transaktions-IDn och liknande

5. Vad bör vi som bolag göra nu?

Ta inga förhastade beslut. Ja, detta är en seriös situation och agerande/ställningstagande kommer behövas, men säkerställ att beslut tas informerat.

1. Ta direkt ställning till våra rekommendationerna i punkt 1.1. och utvärdera 1.2.
2. Gör riskbedömning om var ni vill lägga er och vad som kan vara "affärskritiskt" av de funktioner som vi rekommender att eventuellt stänga av under punkt 2.
3. Om mer vägledning behövs kring våra rekommendationer, återkoppla med era frågor så hjälper vi att tydliggöra och säkra att information och rekommendationer uppfattas på rätt sätt.
4. Potentiellt boka in ett möte för att se över vår tekniska rådgivning för er enskilda situation och sätta en plan framåt.

6. Disclosure

Denna information är inte avsedd att utgöra juridisk rådgivning. Root Digital Group och dess dotterbolag samt anställda tillhandahåller inte juridisk rådgivning och kan därför inte hållas ansvariga för direkta eller indirekta förluster som uppstår till följd av denna information eller på grund av bristfällig eller felaktig information. För frågor som rör GDPR och datahantering rekommenderar Root Digital Group att man konsulterar juridisk expertis.

7. Term- och funktionsförklaringar

* **IP-anonymisering** är att sista okteten i IP-adress tas bort och 123.123.123.123 blir 123.123.123.000. Denna anonymisering görs enligt Google direkt när data når deras system men anses då inte ge godtyckligt skydd av IMY, troligen pga att man redan gjort själva dataöverföringen innan anonymisering sker men eventuellt också att det kanske inte ses som tillräckligt för att inte längre vara personinformation.

** Datapunkter som sparas vid användning av "**Granular location and device data collection**" och kan styras för vilka regioner det är aktivt och inte:

GEO: City, Latitude (of city), Longitude (of city)

Device: Browser minor version, Browser User-Agent string, Device brand, Device model, Device name, Operating system minor version, Platform minor version, Screen resolution

8. Uppdateringslogg

17/7-2023 – Under ’Vad har hänt & bakgrund’ lagt till relevant information om EC:s adekvat beslut för DPF och lagt till information om hur våra rekommendationer tolkas i samband med det

7/7-2023 – Ändrade ”ren kunddata” till ”Icke-obfuskerade kund-IDn” för tydlighet under ’Summering’

6/7-2023 - Språkmässiga justeringar och förtydligande, för ökad läsbarhet och förståelse

6/7-2023 – Under “Vad har hänt & bakgrund” sektion lagt till om IMYs Titel uppdatering för pressreleasen. Samt, ändrat “böter/bot” till “sanktionsavgift” för mer korrekt beskrivning

6/7-2023 – Tydliggjort information under sektion “Nyckelfakta som kan vara bra att veta” för alla punkterna samt gett mer detaljer och referenser

5/7-2023 – Adderade sektioner “Disclosure”, och “Term- och Funktionsförklaringar” samt expanderade information om IP-adress-problemet

5/7-2023 - Adderade en ny “Låg risk”-åtgärd under GA4-sektionen “Implementera data-hashning/extra pseudoanonymisering”

5/7-2023 – Under GA4 riskmitigerings-sektion har “Advanced Settings to Allow for Ads Personalization” flyttats från “Medel risk” till “Låg risk” och kombinerats med punkten “Dela inte/sluta dela “Audiences” eller Konverteringar till Google Ads”

5/7-2023 – Mer kontextuell information tillagd på flera åtgärder under försiktighetsåtgärder för GA4 och under sektion 7

5/7-2023 – Expanderat kontextuell förklaring under “Summering” för vad rekommendationer fokuserar på

5/7-2023 – Adderade mer info om DIs och Coops-situation under Nyckelfakta

5/7-2023 – Adderade introduktionstankar “Vad bör vi som bolag göra nu?” samt tydliggjorde och delade upp 3. till 3. och 4.