Integritetsskydds myndigheten

Dagens Industri Aktiebolag
Gjörwellsgatan 30
11260 Stockholm

Diarienummer:
DI-2020-11370

Datum:
2023-06-30

Beslut efter tillsyn enligt dataskyddsförordningen – Dagens Industri Aktiebolags överföring av personuppgifter till tredjeland

Innehåll

Postadress:
Box 8114
104 20 Stockholm

Webbplats:
www.imy.se

E-post:
imy@imy.se

Telefon:
08-657 61 00

Integritetsskyddsmyndighetens beslut

Integritetsskyddsmyndigheten konstaterar att Dagens Industri Aktiebolag behandlar personuppgifter i strid med artikel 44 i dataskyddsförordningen[1] genom att sedan den 14 augusti 2020 och till dagen för detta beslut använda verktyget Google Analytics, som tillhandahålls av Google LLC, på sin webbplats www.di.se, och därigenom överföra personuppgifter till tredjeland utan att villkoren enligt kapitel V i förordningen är uppfyllda.

Integritetsskyddsmyndigheten förelägger Dagens Industri Aktiebolag med stöd av artikel 58.2 d i dataskyddsförordningen att se till att bolagets behandling av personuppgifter inom ramen för Dagens Industris användning av verktyget Google Analytics överensstämmer med artikel 44 och övriga bestämmelser i kapitel V. Detta ska särskilt ske genom att Dagens Industri Aktiebolag ska upphöra att använda den version av verktyget Google Analytics som användes den 14 augusti 2020, om inte tillräckliga skyddsåtgärder vidtagits. Åtgärderna ska vara genomförda senast en månad efter att detta beslut vunnit laga kraft.

1 Redogörelse för tillsynsärendet

1.1 Handläggningen

Integritetsskyddsmyndigheten (IMY) har inlett tillsyn beträffande Dagens Industri Aktiebolag (nedan ”Dagens Industri” eller ”bolaget”) med anledning av ett klagomål. Klagomålet gäller en påstådd överträdelse av bestämmelserna i kapitel V i dataskyddsförordningen kopplat till överföring av klagandens personuppgifter till tredjeland. Överföringen påstås ha skett när klaganden besökte bolagets webbplats, www.di.se (nedan ”bolagets webbplats” eller ”Webbplatsen”) genom verktyget Google Analytics (nedan ”Verktyget”) som tillhandahålls av Google LLC.

Klagomålet har lämnats över till IMY, i egenskap av ansvarig tillsynsmyndighet enligt artikel 56 i dataskyddsförordningen. Överlämnandet har skett från tillsynsmyndigheten i det land där klaganden har lämnat in sitt klagomål (Österrike) i enlighet med förordningens bestämmelser om samarbete vid gränsöverskridande behandling.

Handläggningen vid IMY har skett genom skriftväxling. Mot bakgrund av att det gäller gränsöverskridande behandling har IMY använt sig av de mekanismer för samarbete och enhetlighet som finns i kapitel VII i dataskyddsförordningen. Berörda tillsyns-myndigheter har varit myndigheterna i Tyskland, Norge, Danmark, Estland och Portugal.

1.2 Vad som anges i klagomålet

I klagomålet anförs i huvudsak följande.

Den 14 augusti 2020 besökte klaganden Dagens Industris webbplats. Under besöket var klaganden inloggad på sitt Google-konto, som är kopplat till klagandens e-postadress. Bolaget hade på sin webbplats implementerat en Javascript-kod för Googles tjänster, inklusive Google Analytics. I enlighet med punkt 5.1.1 b i villkoren för

[1] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

Googles behandling av personuppgifter för Googles reklamprodukter och även Googles villkor för behandling av ”the New Order Data Processing Conditions for Google Advertising Products” behandlar Google personuppgifter för den personuppgiftsansvariges (dvs. bolagets) räkning. Google LLC ska därför enligt ovan nämnda villkor klassificeras som bolagets personuppgiftsbiträde.

Under klagandens besök på bolagets webbplats behandlades klagandens personuppgifter av Dagens Industri, åtminstone klagandens IP-adress och uppgifter insamlade genom kakor. En del av uppgifterna som samlades in, överfördes direkt till Google. I enlighet med punkt 10 i villkoren om behandling av personuppgifter för Googles reklamprodukter, har Dagens Industri godkänt att Google får behandla personuppgifter om klaganden i USA. Sådan överföring av uppgifter kräver rättsligt stöd i enlighet med kapitel V i dataskyddsförordningen.

Enligt EU-domstolens dom Facebook Ireland and Schrems (Schrems II)[2] kunde bolaget inte längre förlita sig på ett beslut om adekvat skyddsnivå för överföring av uppgifter till USA enligt artikel 45 i dataskyddsförordningen. Bolaget bör inte basera överföringen av uppgifter på standardiserade dataskyddsbestämmelser enligt artikel 46.2 c i dataskyddsförordningen om mottagarlandet inte säkerställer ett lämpligt skydd med hänsyn till unionsrätten för de personuppgifter som överförs.

Google ska klassificeras som leverantör av elektroniska kommunikationstjänster i den mening som avses i 50 US Code § 1881 (4)(b) och är därmed föremål för övervakning av amerikanska underrättelsetjänster i enlighet med 50 US § 1881a (section 702 i Foreign Intelligence Surveillance Act, nedan ”702 FISA”).[3] Google förser den amerikanska regeringen med personuppgifter i enlighet med dessa bestämmelser. Bolaget kan därför inte säkerställa ett lämpligt skydd av klagandens personuppgifter när dessa överförs till Google.

1.3 Vad Dagens Industri har uppgett

Dagens Industri Aktiebolag har i huvudsak uppgett följande.

1.3.1 Vem som har implementerat Verktyget och i vilket syfte m.m.

Dagens Industri har fattat beslutet att implementera Verktyget på Webbplatsen, vilket har skett genom att koden för Verktyget har bäddats in på Webbplatsen. Verktyget är fortfarande aktivt. Bolaget är etablerat i Sverige och har inte fattat ett sådant beslut för någon annan europeisk webbplats.

Syftet med att bädda in koden för Verktyget på Webbplatsen är att Dagens Industri ska kunna analysera hur Webbplatsen används, i synnerhet att kunna följa användningen av Webbplatsen över tid.

Webbplatsen riktar sig mot svenska besökare, men det kan inte uteslutas att enskilda från andra länder har besökt Webbplatsen och således kan omfattas av statistiken.

---

[2] EU-domstolens dom Facebook Ireland och Schrems (Schrems II), C-311/18, EU:C:2020:559.
[3] Se https://www.govinfo.gov/content/pkg/USCODE-2011-title50/html/USCODE-2011-title50-chap36-subchapVI-sec1881.htm och https://www.govinfo.gov/content/pkg/USCODE-2011-title50/html/USCODE-2011-title50-chap36-subchapVI-sec1881a.htm.

Den data (inklusive eventuella personuppgifter) som överförs till Verktyget kan komma att lagras på servrar i olika länder, inklusive USA. Som användare av Verktyget går det inte att styra vilka servrar som används för att lagra data i Verktyget.

1.3.2 Mottagare av uppgifterna
Inom ramen för Dagens Industris användning av Verktyget på Webbplatsen lämnas personuppgifter ut till ett antal aktörer, vilka samtliga är personuppgiftsbiträden eller underbiträden till Dagens Industri, inbegripet Google LLC, Google Ireland Ltd och deras underbiträden.

1.3.3 De uppgifter som behandlas i Verktyget och vad som utgör personuppgifter
Inom ramen för Dagens Industris användning av Verktyget på Webbplatsen behandlar bolaget och dess personuppgiftsbiträden (Mottagarna) nedan angivna uppgifter.

- *Sidvisningsdata* – exempelvis URL, klick i menyer, artiklar som besöks, lästid och hur länge besökaren tittar på en video.
- *Teknisk information om enhet* – exempelvis cookie-värde (som är hashat innan det överförs till Verktyget, men var ej hashat när klagande besökte Webbplatsen), operativsystem och skärmstorlek.
- *Användarkategori* – exempelvis en flagga som visar om besökaren är prenumerant eller inte.[4]
- *S.k. "egna dimensioner"* – exempelvis vilken version av publiceringsplattform som en sidvisning skedde på, information om artikel (till exempel författare).
- *IP-adresser* – IP-adress behandlas dels när Google Analytics mätscript *läses in*, dels när uppmätt data ska *överföras* till Verktyget. Den IP-adress som behandlas tillsammans med uppmätt data (sidvisningsdata etc.) anonymiseras genom bolagets egenutvecklade process och som hanteras på en EU-baserad infrastruktur innan den skickas tillsammans med den uppmätta datan till Verktyget (se mer om detta nedan).

Dagens Industri bedömer att *kategorierna* Sidvisningsdata, Teknisk information om enhet, Användarkategori och "egna dimensioner" kan betraktas som personuppgifter endast i de fall då bolaget kan knyta dessa uppgifter till en individ genom kompletterande information som bolaget har i andra system, vilket inte alltid är fallet. Dagens Industri betraktar IP-adresser som personuppgifter till dess att dessa anonymiseras.

1.3.4 Kategorier av personer som berörs av behandlingen
De *kategorier* av personer som berörs av behandlingen är besökare av Webbplatsen. Det kan vara Dagens Industris betalande prenumeranter eller besökare utan ett digitalt konto.

Uppgifter om särskilt utsatta personer behandlas inte. Webbplatsen riktar sig i första hand till vuxna i deras yrkesroll eller som har ett intresse för ekonomi- och närings-livsfrågor. Den riktar sig inte till barn eller andra särskilt utsatta grupper.

1.3.5 När koden för Verktyget exekveras och mottagare bereds tillgång
Koden för Verktygets innehåll, dvs. scriptet som mäter den data som skickas till Verktyget, körs endast om besökaren har gett sitt samtycke till att Dagens Industri

[4] Observera att identifierande uppgifter såsom faktiskt prenumerations-ID inte överförs, utan enbart ett värde som representerar kategorin "prenumerant" eller "inte prenumerant" (1 eller 0).

använder analys-cookies på Webbplatsen. Om besökaren har gett sitt samtycke kommer den data som mäts av scriptet först att skickas till Dagens Industris proxyserver, där flertalet säkerhetshöjande åtgärder genomförs, exempelvis anonymisering av IP-adress. En delmängd av den uppmätta datan överförs därefter krypterat från proxyservern till Verktyget som tillhandahålls av Google (se nedan).

Google LLC, Google Ireland och övriga personuppgiftsbiträden och underbiträden får tillgång till den pseudonymiserade data som lagras i Verktyget i den utsträckning som krävs för att personuppgiftsbiträdet eller underbiträdet ska kunna utföra tjänsten, inklusive support- och felsökningstjänster.

1.3.6 Hur länge lagras personuppgifterna
Den data som uppmätts på Webbplatsen och som överförs till Verktyget sparas i Verktyget i 26 månader och raderas därefter. Dagens Industri sparar uppgifterna för att kunna analysera användningen av Webbplatsen över tid, närmare bestämt för att kunna göra årsjämförelser och därigenom analysera hur användningen förändras. Dagens Industri har bedömt att det är nödvändigt att i vart fall kunna jämföra användningen över två årscykler. För att kunna analysera och ta fram statistik över dessa förändringar behöver bolaget spara den uppmätta datan i 26 månader.

1.3.7 Vilka länder personuppgifterna behandlas i
De uppgifter som överförs till Verktyget lagras bland annat i USA.

1.3.8 Dagens Industris relation till Google LLC
Verktyget tillhandahålls genom avtal mellan Dagens Industri och ett svenskt aktiebolag (nedan ”Leverantören”). Google Ireland Ltd är i sin tur underleverantör till leverantören. Dagens Industri har ingått personuppgiftsbiträdesavtal med leverantören, som reglerar Leverantörens och dess underbiträdens personuppgiftsbehandling.

Eftersom ändamålen och medlen för behandlingen i sin helhet bestäms av Dagens Industri är Google LLC och Google Ireland Ltd personuppgiftsbiträden för den personuppgiftsbehandling som blir aktuell i förhållande till Verktyget.

Dagens Industri har även ingått ett personuppgiftsbiträdesavtal direkt med Google LLC för att uppfylla de formella kraven enligt standardavtalsklausulerna, dvs. att dessa formellt ska ingås direkt mellan den personuppgiftsansvarige och biträde i tredjeland.

1.3.9 Säkerställande av att behandlingen inte sker för mottagarnas egna ändamål

1.3.9.1 Generellt
Dagens Industri månar om att enbart anlita sådana leverantörer som kan uppfylla bolagets högt ställda krav på en säker och lagenlig personuppgiftsbehandling. Innan en viss leverantör väljs ut görs en bedömning av leverantörens förmåga att upprätthålla en godtagbar säkerhetsnivå, inklusive att skydda personuppgifter som ska behandlas. Dagens Industri har även arbetat fram en revisionsplan där bolaget avser att genomföra revisioner av de viktigaste leverantörerna, utifrån ett rullande schema. Dagens Industri för även en kontinuerlig dialog med Google, där säkerhets- och dataskyddsfrågor diskuteras.

1.3.9.2 Avtal med Leverantören
Genom biträdesavtalet med Leverantören och de dokumenterade instruktioner som lämnats från Dagens Industri i detta avseende har det säkerställts kontraktuellt att Leverantören och dess underbiträden inte behandlar personuppgifter för egna eller

tredje parts ändamål. Biträdesavtalet innehåller således särskilda bestämmelser (avsnitt 3.2.1) om att Leverantören endast får behandla personuppgifter i enlighet med Dagens Industris dokumenterade instruktioner. I bilaga 2 till biträdesavtalet tydliggörs att Leverantören under inga omständigheter har rätt att behandla personuppgifter för egna ändamål.

Som incitament för att efterleva de krav som ställs enligt biträdesavtalet och för att poängtera dess vikt har Leverantören en ersättningsskyldighet gentemot Dagens Industri om Leverantören skulle bryta mot avtalet eller tillämplig dataskyddslagstiftning och detta medför skada för Dagens Industri.

Biträdesavtalet med Leverantören möjliggör även för Dagens Industri att begära dokumentation och genomföra revisioner av system och rutiner för att säkerställa att behandlingen sker i enlighet med Dagens Industris dokumenterade instruktioner och tillämplig dataskyddslagstiftning.

För det fall Dagens Industri har skäl att anta att Leverantören inte efterlever kraven som ställs i biträdesavtalet har Dagens Industri för avsikt att genomföra en sådan revision. Leverantören har även rätt att begära dokumentation och genomföra revisioner i förhållande till Google (avsnitt 7.5 i Googles biträdesavtal).

Dagens Industri kan också begära att genomföra revision av Googles system och rutiner i enlighet med biträdesavtalet med Leverantören (avsnitt 8.5).

1.3.10 Beskrivning av Dagens Industris användning av Verktyget
Dagens Industri använder Verktyget för att samla in kvantitativa data, webbstatistik, om hur Webbplatsen används, och göra analyser utifrån dessa uppgifter. Webbstatistik kan till exempel visa vilka sidor som är mest besökta, vilken väg besökare tar genom Webbplatsen, och från vilka sidor besökare lämnar Webbplatsen. Webbanalys kan även ge insikt i besöksfrekvens och vilket innehåll som besöks under längst tid. Den analys som görs med hjälp av Verktyget kan exempelvis ligga till grund för produktförbättringar.

1.3.11 Egna kontroller av överföringar som berörs av domen Schrems II
Efter att domen Schrems II publicerades den 16 juli 2020 inledde Dagens Industri under slutet av juli 2020 ett projekt för att generellt kartlägga överföringar av personuppgifter till tredjeland. Projektet avsåg inte Verktyget specifikt utan gällde tredjelandsöverföringar generellt. I samband med att Dagens Industri fick kännedom om bland annat det aktuella klagomålet inleddes den 18 augusti 2020 ett projekt som särskilt avsåg användningen av Verktyget. Relativt omgående efter domen, kunde bolaget konstatera att den är relevant för den dataöverföring som sker inom ramen för Verktyget och Dagens Industri har därefter vidtagit relevanta skyddsåtgärder, se nedan.

1.3.12 Överföringsverktyg enligt kapitel V i dataskyddsförordningen
Dagens Industri har ingått ett personuppgiftsbiträdesavtal direkt med Google LLC. Googles standardavtalsklausuler är en del av biträdesavtalet. Av biträdesavtalet framgår att Google är bunden av klausulerna (punkt 10.2). Klausulerna baseras på kommissionens beslut 2010/87/EU för överföringar från en personuppgiftsansvarig inom EU/EES till ett personuppgiftsbiträde utanför EU/EES. Dessa avtalsvillkor gäller automatiskt vid ingåendet av Googles personuppgiftsbiträdesavtal och behöver således inte undertecknas separat för att vara tillämpliga. Det framgår av ingressen till

Googles standardavtalsklausuler. Enligt svensk lag, som ska tillämpas på standardavtalsklausulerna, innebär det att dessa blir en del av avtalet.

Googles standardavtalsklausuler utgör även del av personuppgiftsbiträdesavtalet med Leverantören i enlighet med bilaga 2 i biträdesavtalet med Leverantören.

Dagens Industri har även ingått ett personuppgiftsbiträdesavtal med Leverantören, där Google Ireland Ltd agerar underbiträde och som i sin tur har vissa underbiträden i tredjeland. Även i detta avtal tillämpas Googles standardavtalsklausuler som överföringsverktyg.

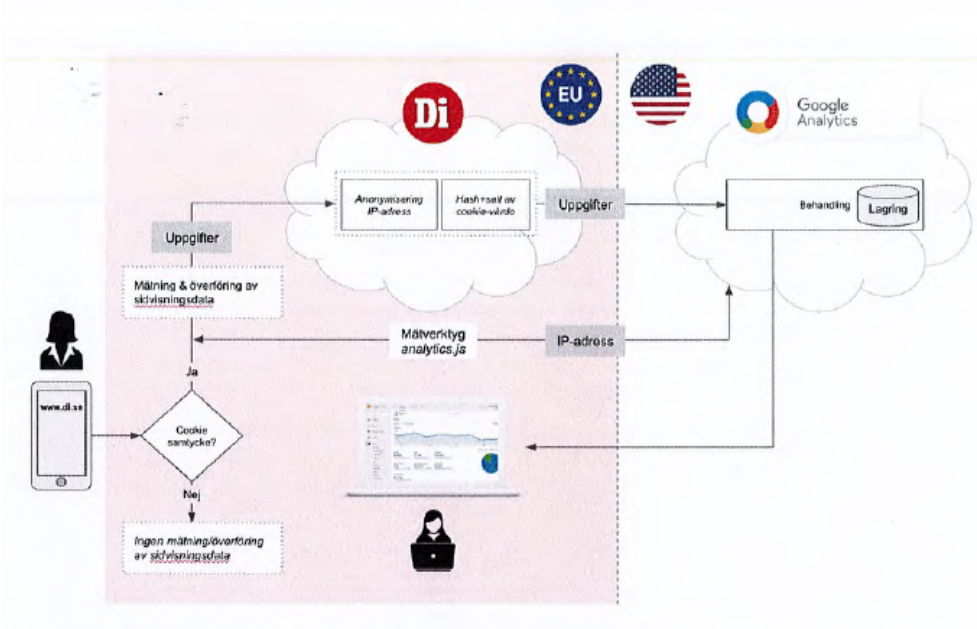
1.3.13 Kontroll av hinder för fullgörande i lagstiftning i tredjeland

Dagens Industri har ännu inte med säkerhet kunnat konstatera om det finns något i tredjelands lagstiftning som förbjuder mottagarna att uppfylla sina avtalsförpliktelser enligt standardavtalsklausulerna. Bolaget har därför i förebyggande syfte utgått från att så är fallet och vidtagit särskilda tekniska skyddsåtgärder för att säkerställa att skyddet för de uppgifter som behandlas i Verktyget uppnår en acceptabel nivå.

1.3.14 Vidtagna ytterligare skyddsåtgärder utöver de som Google vidtagit

1.3.14.1 Inledning

Dagens Industri har genomfört en utförlig kartläggning av livscykeln för person-uppgifter som behandlas i Verktyget, och har därvid identifierat och implementerat ett antal ytterligare skyddsåtgärder. Åtgärderna visualiseras översiktligt i bilden nedan, och kommenteras ytterligare i efterföljande avsnitt.



1.3.14.2 Kontroll över insamling och överföring av uppgifter till Verktyget

Ett vanligt förekommande sätt att använda Verktyget, om inte ytterligare skyddsåtgärder vidtas, innebär att den data som mäts via Webbplatsens mätscript överförs direkt till Verktygets servrar, utan att först gå via en kontrollpunkt hos den personuppgiftsansvarige som använder verktyget.

Eftersom Verktygets servrar kan finnas inom och utanför EU/EES kan användning av Verktyget leda till att uppmätt data överförs till tredjeland. I Verktyget finns en funktion som innebär att användare av Verktyget kan välja att anonymisera IP-adressen (trunkering)[5] som överförs tillsammans med uppmätt data. Eftersom anonymiseringen sker först efter att IP-adressen överförts till Google Analytics servrar uppstår enligt Dagens Industri en tredjelandsöverföring innan anonymiseringen äger rum.

Dagens Industri har vidtagit skyddsåtgärder innan data överförs till Verktyget. För att ta kontroll över vilken data som överförs till Verktygets servrar utanför EU/EES har bolaget implementerat tekniska åtgärder som innebär att de uppgifter som samlas in via Google Analytics mätscript på Webbplatsen i ett första steg överförs till en proxyserver som finns inom EU där uppgifterna behandlas för att undvika att de kan användas för att identifiera en individ därefter. Mjukvaran som används har utvecklats och ägs av Dagens Industri, och hostas (inhysas) hos Google Ireland Ltd som en del av Google Cloud Platform ("GCP"). GCP:en används således enbart som hyrd infrastruktur för att köra proxyserverns kod på. Den data som behandlas på GCP:en sker uteslutande på datacenter inom EU. Dagens Industri är personuppgiftsansvarig för den behandling som sker i proxyservern.

Genom att Dagens Industri har infört denna kontrollpunkt kan bolaget säkerställa att ingen data överförs till servrar utanför EU/EES utan att först ha genomgått skydds-åtgärder (se vidare nedan). Överföring till proxyservern är krypterad med Secure Sockets Layer (”SSL”), en teknik som möjliggör krypterad kommunikation mellan en webbläsare och en server).

1.3.14.3 Anonymisering av IP-adress och algoritm

De uppgifter som i vissa fall kan knytas till en individ och som överförs från Webb-platsen till proxyservern är IP-adress och cookie-värde. Exemplen nedan illustrerar hur dessa nummer kan se ut före och efter att de behandlats på proxyservern.

Före behandling på proxyserver:

Uppgifter

- IP-adress: klartext, t.ex. 176.10.253.34
- Cookie-värde: klartext, t.ex. 744100309.1604572939

Innan uppmätt data överförs till Verktyget genomförs följande på proxyservern:

- *Anonymisering av IP-adress*. Besökarens IP-adress anonymiseras genom generalisering och aggregering där den sista oktetten i IPv4-adressen ersätts med ”.0”.
- *Hashning av cookie-värdet*. Det cookie-värde som uppmätts på Webbplatsen kan antingen vara helt anonymt (när bolaget *inte* kan koppla cookie-värdet till uppgifter i sina andra system) eller utgöra en pseudonymiserad personuppgift (när bolaget kan koppla cookie-värdet till uppgifter i sina andra system). Som en ytterligare skyddsåtgärd innan överföring sker till Verktyget hashas cookie-värdet från besökarens klient med ett "salt".[6] Hashningen av cookie-värdet utgör ytterligare ett skydd mot

[5] Trunkering av IP-adress innebär att asterisk eller nollor ersätter andra siffror i sista oktetter (sista siffrorna i en IP-adress, ett tal mellan 0 och 255).
[6] Jfr information om "Keyed-hash function with stored key" i Artikel 29-gruppens vägledning om anonymiseringstekniker.

risken att amerikanska myndigheter kan koppla ”avlyssnad data” (dvs. data som eventuellt skulle kunna avläsas genom signalspaningsprogram antingen "at rest" i Verktyget eller "in transfer") med identifierande data som amerikanska myndigheter eventuellt skulle kunna få tillgång till på annat sätt.

Efte*r* att ovan beskrivna åtgärder har genomförts kan IP-adressen och cookie-värdet exempelvis se ut enligt följande:

Uppgifter

- IP-adress: anonymiserad, t.ex. 176.10.253.00
- Cookie-värde: hashad, t.ex. 35009a79-1a05-49d7-b876-2b884d0f825b

Överföringen av uppgifterna sker sedan via SSL-kryptering från proxyservern till Verktyget.

Anonymisering av besökarens IP-adress sker när denna ska överföras tillsammans med den uppmätta sidvisningsdatan etc. (se ovan för vilka datapunkter som mäts).

Dessförinnan har IP-adressen exponerats för Verktyget vid det tillfälle Google Analytics mätscript via krypterad överföring lästes in i besökarens webbläsare från Verktygets server. Det går inte att koppla samman IP-adressen med den sidvisnings-data etc. som vid ett senare tillfälle uppmäts på Webbplatsen. Dagens Industri har därför bedömt att denna exponering av IP-adressen inte utgör någon integritetsrisk för besökare på Webbplatsen.

Avseende tidpunkten för besök på Webbplatsen kan Google LLC visserligen indirekt härleda tidpunkt för besöket, men denna möjlighet är mycket begränsad. Google har konfigurerat servern varpå 'analytics.js' tillhandahålls på så sätt att JavaScript-filen cachas i den mottagande terminalens applikations-cache i två timmar, oberoende av vilken hemsida den först inhämtas via (d.v.s. inte nödvändigtvis på Webbplatsen). Under denna tidsperiod görs inga fler anrop där IP-adressen exponeras i dess helhet, vilket innebär att de uppmätta sidvisningsdata som överförs via Dagens Industris proxyserver till Google LLC (första överföringen) mycket sällan har en tidsmässigt motsvarande maskinlogg hos Google LLC kopplad till överföringen via 'analytics.js' (andra överföringen). I kombination med att besökare oftast nyttjar Webbplatsen som informationskälla i arbetet och/eller under föregående två timmar besökt en annan webbplats som använder Google Analytics (högst sannolikt givet att cirka 74 % av världens 10 000 mest populära hemsidor föreliggande) gör att en stor andel av besöken på Webbplatsen bara resulterar i överförda sidvisningsdata från Dagens Industris proxyserver och ingen inläsning av Verktyget med tillhörande överföring av IP-adress. Därmed försvåras kraftigt eventuella försök att sammankoppla maskinloggar från överföring av Verktyget och överförda sidvisningsdata från Dagens industris proxyserver och reducerar enligt Dagen enligt risk till bortom ”rimlig sannolikhet”.

1.3.14.4 Mer om kontroll av att ytterligare åtgärder kan genomföras i praktiken m.m.
Dagens Industris överväganden gällande de åtgärder som bolaget har implementerat är baserade på EDPB:s rekommendationer om hur enskilda tredjelandsöverföringar ska bedömas utifrån sin specifika legala kontext (punkt 33).[7]

De säkerhetshöjande åtgärderna består främst av det ansvar för och den kontroll som Dagens Industri tagit över faserna av livscykeln innan överföringen av uppgifterna sker till Verktyget. Riskbedömningen har haft som utgångsläge att de registrerades skydd bäst uppnås genom att de uppgifter som överförs utanför EU/EES är frånkopplade från den registrerade och dennes tekniska enhet som använts för att besöka Webbplatsen, och att bolaget kontrollerar den process som säkerställer att dessa åtgärder utförs.

1.3.14.5 Dagens Industris slutsats av tillräcklig säkerhetskyddsnivå
Med beaktande av de genomförda åtgärderna bedömer Dagens Industri att risken för att de registrerades integritet eller rättigheter skulle kränkas genom användandet av Verktyget är mycket liten. Bolagets samlade bedömning är således att en tillräcklig skyddsnivå uppnås genom de genomförda åtgärderna.

1.3.15 Dagens Industris bedömning och slutsats avseende om uppgifterna kan anses vara identifierbara

1.3.15.1 Bolagets bedömning avseende om uppgifterna kan anses vara identifierbara
Dagens Industri anser att det inte är självklart att en bedömning leder till att uppgifterna ifråga – IP-adress, viss systeminformation och besökt webbadress – utgör personuppgifter.

I skäl 26 i dataskyddsförordningen anges bland annat följande:

”*För att avgöra om en fysisk person är identifierbar bör man beakta alla hjälpmedel, som t.ex. utgallring, som, antingen av den personuppgiftsansvarige eller av en annan person, rimligen kan komma att användas för att direkt eller indirekt identifiera den fysiska personen. För att fastställa om hjälpmedel med rimlig sannolikhet kan komma att identifiera den fysiska personen bör man beakta alla objektiva faktorer, som kostnader och tidsåtgång för identifiering, med beaktande av tillgänglig teknik vid tidpunkten för behandlingen som den tekniska utvecklingen*.”

Artikel 29-arbetsgruppen har i sin vägledning[8] om begreppet personuppgifter ytterligare konkretiserat hur bedömningen ska gå till:

I skäl 26 till direktiv 95/46[9] (upphävda) ägnas särskild uppmärksamhet åt termen ”identifierbar” när det står att ”*för att avgöra om en person är identifierbar bör hänsyn tas till alla medel som rimligen kan användas antingen av den personuppgiftsansvarige eller av någon annan person för att identifiera personen”. Detta innebär att en rent hypotetisk möjlighet att peka ut den enskilde inte är tillräcklig för att betrakta personen som ”identifierbar”. Om denna möjlighet, med beaktande av ”alla medel som rimligen kan komma att användas av den personuppgiftsansvarige eller någon annan person”, inte existerar eller är försumbar, bör personen inte anses vara ”identifierbar”, och informationen skulle inte betraktas som ”personuppgifter”. Kriteriet ”alla medel som*

[7] EDPB:s Rekommendationer 01/2020 om åtgärder som komplement till överföringsverktyg för att säkerställa överensstämmelsen med EU-nivån för skydd av personuppgifter Version 2.0 Antagna den 18 juni 2021
[8] WP 136. Artikel 29-gruppens yttrande 4/2007 om begreppet personuppgifter, antagna den 20 juni 2007
[9] Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter.

rimligen kan komma att användas antingen av den personuppgiftsansvarige eller av någon annan person" bör särskilt ta hänsyn till alla faktorer som står på spel. Kostnaden för att genomföra identifiering är en faktor, men inte den end[a]. [O]m uppgifterna är avsedda att lagras i en månad kan identifiering inte förväntas vara möjlig under informationens "livstid" och de bör inte betraktas som personuppgifter."[10]

Vidare uttalas följande i vägledningen:

"En relevant faktor, som nämnts tidigare, för att bedöma "alla medel som rimligen kan komma att användas" för att identifiera personerna kommer i själva verket att vara det ändamål som den registeransvarige eftersträvar vid behandlingen av uppgifter."[11]

1.3.15.2 Bolagets slutsats avseende om uppgifterna kan anses vara identifierbara
Dagens Industri har dragit slutsatsen att för att det ska vara fråga om personuppgifter enligt Dataskyddsförordningen så ska bedömningen av om enskilda är identifierbara utgå från alla relevanta omständigheterna och bedöma den rimliga sannolikheten för identifiering, varav syftet med behandlingen är en omständighet. Eftersom syftet med behandlingen inte är att identifiera enskilda, utgör tekniska skyddsåtgärder en extra viktig faktor vid bedömningen av om enskilda kan komma att identifieras.

Dagens Industri kommer mot den bakgrunden fram till att det inte är självklart att en bedömning i enlighet med artikel 29-gruppens vägledning leder till att uppgifterna ifråga – IP-adress, viss systeminformation och besökt webbadress – utgör personuppgifter.

Bedömningen av att enskilda inte är identifierbara har gjorts med beaktade av de omständigheter som framgår av dvs. (i) kostnaden för identifiering, (ii) syftet med behandlingen, (iii) hur behandlingen är strukturerad, (iv) fördelarna som den personuppgiftsansvarige förväntar sig med behandlingen, (v) vilka intressen som står på spel för den fysiska personen, samt (vi) behandlingens varaktighet. Syftet med behandlingen är inte att identifiera enskilda, utan utgör tekniska skyddsåtgärder. Det är enligt Dagens Industri inte alls självklart att en bedömning i enlighet med vägledningen leder till att uppgifterna ifråga – IP-adress, viss systeminformation och besökt webbadress – utgör personuppgifter.

1.4 Vad Google LLC har uppgett

IMY har tillfört ärendet ett yttrande från Google LLC (Google) den 9 april 2021 som Google lämnat in till den österrikiska tillsynsmyndigheten. Yttrandet besvarar frågor som IMY och ett antal tillsynsmyndigheter har ställt till Google med anledning av delvis gemensam hantering av liknande klagomål som kommit in till dessa myndigheter. Dagens Industri har beretts tillfälle att yttra sig över Googles LLC:s yttrande. Av Google LLC:s yttrande framgår följande om Verktyget.

En JavaScript-kod inkluderas på en webbsida. När en användare besöker (anropar) en webbsida utlöser koden en nedladdning av en JavaScript-fil. Därefter utförs spårningsoperationen för Verktyget, som består av att samla in information relaterad till anropet på olika sätt och skickarinformationen till Verktygets servrar.

[10] WP 136. Artikel 29-gruppens yttrande 4/2007 om begreppet personuppgifter, antagna den 20 juni 2007, sida 15.
[11] WP 136. Artikel 29-gruppens yttrande 4/2007 om begreppet personuppgifter, antagna den 20 juni 2007, sida 16 och 17.

En webbplatsansvarig som integrerat Verktyget på sin webbplats kan skicka instruktioner till Google för behandling av de uppgifter som samlas in. Dessa instruktioner överförs via den så kallade tagghanteraren som hanterar den spårningskod som den webbansvarige har integrerat i sin webbplats och via tagghanterarens inställningar. Den som integrerat Verktyget kan göra olika inställningar, exempelvis avseende lagringstid. Verktyget gör det också möjligt för den som integrerat det att övervaka och upprätthålla stabiliteten på sin webbplats, exempelvis genom att hålla sig informerad om händelser såsom toppar i besökstrafik eller avsaknad av trafik. Verktyget gör det också möjligt för en webbplatsansvarig att mäta och optimera effektiviteten av reklamkampanjer som genomförs med hjälp av andra verktyg från Google.

I detta sammanhang samlar Verktyget in besökarens http-anrop och information om bland annat besökarens webbläsare och operativsystem. Enligt Google innehåller ett http-anrop för vilken sida som helst information om webbläsaren och enheten som gör anropet, exempelvis domännamn, och information om webbläsaren, exempelvis typ, referens och språk. Verktyget lagrar och läser cookies i besökarens webbläsare för att utvärdera besökarens session och annan information om anropet. Genom dessa cookies möjliggör Verktyget identifiering av unika användare (UUID) över surfsessioner, men Verktyget kan inte identifiera unika användare i olika webbläsare eller enheter. Om en webbplatsägares webbplats har ett eget autentiseringssystem kan webbplatsägaren använda ID-funktionen, för att mer exakt identifiera en användare på alla enheter och webbläsare som de använder för att komma åt webbplatsen.
När informationen samlas in överförs den till Verktygets servrar. Alla uppgifter som samlas in via Verktyget lagras i USA.

Google har infört bland annat nedanstående rättsliga, organisatoriska och tekniska skyddsåtgärder för att reglera överföringar av uppgifter inom ramen för Verktyget.

Google har vidtagit rättsliga och organisatoriska skyddsåtgärder såsom att bolaget alltid genomför en noggrann prövning om en begäran om tillgång från statliga myndigheter om användardata kan genomföras. Det är jurister/specialutbildad personal som genomför dessa prövningar och undersöker om en sådan begäran är förenlig med gällande lagar och Googles riktlinjer. De registrerade informeras om utlämnandet, såvida det inte är förbjudet i lag eller skulle inverka negativt på en nödsituation. Google har även publicerat en policy på bolagets webbplats om hur en sådan begäran om tillgång från statliga myndigheter av användardata ska genomföras.

Google har vidtagit tekniska skyddsåtgärder såsom att skydda personuppgifter från avlyssning vid överföring av data i Verktyget. Genom att som standard använda HTTP Strict Transport Security (HSTS), som instruerar webbläsare som http till SSL (HTTPS) att använda ett krypteringsprotokoll för all kommunikation mellan slutanvändare, webbplatser och Verktygets servrar. Sådan kryptering förhindrar inkräktare från att passivt lyssna av kommunikation mellan webbplatser och användare.

Google använder även en krypteringsteknik för att skydda personuppgifter s.k. ”data i vila” (”data at rest”) i datacenter, där användardata lagras på en disk eller säkerhetskopieringsmedia för att förhindra obehörig åtkomst till datan.

Utöver ovanstående åtgärder kan webbplatsägare använda IP-anonymisering genom att använda de inställningar som Verktyget tillhandahåller för att begränsa Googles användning av personuppgifter. Sådana inställningar inkluderar framför allt att i koden

för Verktyget aktivera IP-anonymisering, vilket innebär att IP-adresser trunkeras och bidrar till dataminimering. Om IP-anonymiseringstjänsten används fullständigt sker anonymiseringen av IP-adressen nästan omgående efter att begäran har mottagits.

Google begränsar även åtkomsten till datan från Verktyget genom behörighetsstyrning samt genom att all personal ska ha genomgått en utbildning avseende informationssäkerhet.

2 Motivering av beslutet

2.1 Ramen för granskningen

IMY har med utgångspunkt i klagomålet i ärendet endast granskat om Dagens Industri överför personuppgifter till tredjelandet USA inom ramen för Verktyget och om bolaget har rättsligt stöd för det i kapitel V i dataskyddsförordningen. Tillsynen omfattar inte om bolagets personuppgiftsbehandling i övrigt är förenlig med dataskyddsförordningen.

2.2 Det är fråga om behandling av personuppgifter

2.2.1 Tillämpliga bestämmelser m.m.

För att dataskyddsförordningen ska vara tillämplig krävs att personuppgifter behandlas.

Dataskyddsförordningen syftar enligt artikel 1.2 till att skydda fysiska personers grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter. Enligt artikel 4.1 i dataskyddsförordningen är personuppgifter ”*varje upplysning som avser en identifierad eller identifierbar fysisk person (nedan kallad en registrerad), varvid en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller onlineidentifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet*”. För att avgöra om en fysisk person är identifierbar bör man beakta alla hjälpmedel som, antingen av den personuppgiftsansvarige eller av en annan person, rimligen kan komma att användas för att direkt eller indirekt identifiera den fysiska personen (skäl 26 till dataskyddsförordningen).

Begreppet personuppgifter kan innefatta samtliga upplysningar, såväl objektiva som subjektiva upplysningar, under förutsättning att de ”avser” en bestämd person, vilket de gör om de på grund av sitt innehåll, syfte eller verkan är knuten till personen.[12]

Ordet ”indirekt” i artikel 4.1 i dataskyddsförordningen tyder på att det inte är nödvändigt att informationen i sig gör det möjligt att identifiera den registrerade för att det ska vara en personuppgift.[13] I skäl 26 i dataskyddsförordningen anges dessutom att för att kunna avgöra om en fysisk person är identifierbar bör alla hjälpmedel, som t.ex. utgallring (engelska ” singling out”), som, antingen av den personuppgiftsansvarige eller av en annan person, rimligen kan komma att användas för att direkt eller indirekt identifiera den fysiska personen, beaktas. För att fastställa om hjälpmedel med *rimlig*

[12] EU-domstolens dom Nowak, C-434/16, EU:C:2017:994, punkt 34–35.
[13] EU-domstolens dom Breyer, C-582/14, EU:C:2016:779, punkt 41.

sannolikhet kan komma att användas för att identifiera den fysiska personen bör samtliga objektiva faktorer, såsom kostnader och tidsåtgång för identifiering, med beaktande av såväl tillgänglig teknik vid tidpunkten för behandlingen, beaktas. Av artikel 4.5 i förordningen framgår att med *pseudymisering* avses behandling av personuppgifter på ett sätt som innebär att personuppgifterna inte längre kan tillskrivas en specifik registrerad utan att kompletterande uppgifter används, under förutsättning att dessa kompletterande uppgifter förvaras separat och är föremål för tekniska och organisatoriska åtgärder som säkerställer att personuppgifterna inte tillskrivs en identifierad eller identifierbar fysisk person.

S.k. ”nätidentifierare” (ibland benämnda ”onlineidentifierare”) – t.ex. IP-adresser eller information som lagras i cookies – kan användas för att identifiera en användare, särskilt när de kombineras med andra liknande typer av information. Enligt skäl 30 till dataskyddsförordningen kan fysiska personer knytas till nätidentifierare som lämnas av deras utrustning, t.ex. IP-adresser, kakor eller andra identifierare. Detta kan efterlämna spår som, särskilt i kombination med unika identifierare och andra uppgifter som samlas in, kan användas för att skapa profiler för fysiska personer och identifiera dem.

Artikel 29-arbetsgruppen har i yttrandet från 2007 klargjort vad de avser är hjälpmedel som rimligen kan komma att användas för identifiering avseende bland annat IP-adresser.[14] I yttrandet anges att *alla medel som rimligen kan komma att* för att identifiera vederbörande är b.la följande kostnaden för att genomföra identifieringen, det avsedda syftet, hur behandlingen är strukturerad och tekniska fel. Å andra sidan bör hänsyn tas till den senaste tekniken vid tidpunkten för behandlingen och utvecklingsmöjligheterna under den period då uppgifterna kommer att behandlas, faktorerna är således dynamiska och kan komma ändras över tid.

Ordalydelsen i skäl 26 i direktiv 95/46 antyder, genom hänvisningen till alla hjälpmedel som *rimligen* kan komma att användas av den personuppgiftsansvarige eller en annan person, att det inte krävs att en enda person innehar all information som är nödvändig för att identifiera den registrerade.[15]

I Artikel 29-gruppens yttrande från 2007 anges i exempel nummer 15 följande om dynamiska IP-adresser på en dator som finns hos ett internetcafé där ingen identifiering krävs för att kunna använda internet. [M]an kan hävda att de uppgifter som samlats in angående användningen av dator X under en viss tid inte gör det möjligt att identifiera användaren med rimliga medel och att det därför inte är personuppgifte[r].[16]

EU-domstolen har i dom Breyer slagit fast att en person inte anses identifierbar genom en viss uppgift om risken för identifiering i praktiken är försumbar, vilket den är om identifiering av den aktuella personen är förbjuden i lag eller omöjlig att genomföra i praktiken.[17] EU-domstolen har dock i dom M.I.C.M. från 2021 och i dom Breyer slagit fast att dynamiska IP-adresser utgör personuppgifter i förhållande till den som behandlar dem, när denne även har en laglig möjlighet att identifiera innehavarna av internetanslutningarna med hjälp av de ytterligare upplysningar som tredje part förfogar över.[18]

---

[14] Yttrande 4/2007 om begreppet personuppgifter, 01248/07/SV WP 136, sida 16.
[15] EU-domstolens dom Breyer, C-582/14, EU:C:2016:779, punkt 43.
[16] Yttrande 4/2007 om begreppet personuppgifter, 01248/07/SV WP 136, sida 17 och 18.
[17] EU-domstolens dom Breyer, C-582/14, EU:C:2016:779, punkt 45–46.
[18] EU-domstolens dom M.I.C.M, C-597/19, EU:C:2021:492, punkt 102–104 samt dom Breyer, C-582/14, EU:C:2016:779, punkt 49.

2.2.2 Integritetsskyddsmyndighetens bedömning

För att avgöra om de uppgifter som behandlas genom Verktyget utgör personuppgifter ska IMY ta ställning till om Google eller Dagens Industri genom implementeringen av Verktyget kan identifiera enskilda, t.ex. klaganden, vid besök på Webbplatsen eller om risken för det är försumbar.[19]

IMY anser att de uppgifter som behandlas utgör personuppgifter av följande skäl.

Av utredningen framgår att Dagens Industri implementerat Verktyget genom att infoga en JavaScript-kod (en tagg), som angetts av Google, i källkoden för Webbplatsen. Medan sidan laddas i besökarens webbläsare laddas JavaScript-koden från Google LLC:s servrar upp och körs lokalt i besökarens webbläsare. En kaka (cookie) sätts samtidigt av i besökarens webbläsare och sparas på datorn. Kakan innehåller en textfil som samlar information om besökarens manövrering på Webbplatsen. Bland annat fastställs en unik identifierare i värdet på kakan och denna unika identifierare genereras och hanteras av Google.

När klaganden besökte Webbplatsen, eller en undersida på Webbplatsen, överfördes följande information via JavaScript-koden från klagandens webbläsare till Google LLC:s servrar:

1. Unik(a) identifierare som identifierat den webbläsare eller enhet som använts för att besöka Webbplatsen samt en unik identifierare som identifierat bolaget (dvs. bolagets konto-ID för Google Analytics).
2. Webbadress (URL) och HTML-titel på den webbplats och webbsida som klaganden har besökt.
3. Information om webbläsare, operativsystem, skärmupplösning, språkinställning samt datum och tidpunkt för åtkomst till Webbplatsen.
4. Klagandens IP-adress.

Vid klagandens besök sattes (enligt punkt 1 ovan) nämnda identifierare i kakor med namnen ”_gads”, ”_ga” och ”_gid” och överfördes därefter till Google LLC. Dessa identifierare har skapats med syftet att kunna särskilja individuella besökare, såsom klaganden. De unika identifierarna gör därmed besökarna på Webbplatsen identifierbara. Även om sådana unika identifierare (enligt punkt 1 ovan) i sig inte skulle anses göra enskilda identifierbara, måste det dock beaktas att dessa unika identifierare i det aktuella fallet kan kombineras med ytterligare element (enligt punkterna 2–4 ovan) samt att det är möjligt att dra slutsatser i förhållande till information (enligt punkterna 2–4 ovan) som medför att uppgifter utgör personuppgifter, oaktat om IP-adressen inte överförts i sin helhet.

Kombineras uppgifter (enligt punkterna 1–4 ovan) innebär det att enskilda besökare på Webbplatsen blir ännu mer särskiljbara. Det är således möjligt att identifiera individuella besökare av Webbplatsen. Det är i sig tillräckligt för att det ska anses vara personuppgifter. Det krävs inte kännedom om den faktiska besökarens namn eller fysiska adress, eftersom särskiljandet (genom ordet ”utgallring” i skäl 26 i dataskyddsförordningen, ”singling out” i den engelska versionen) i sig är tillräckligt för att göra besökaren indirekt identifierbar. Det krävs inte heller att Google eller Dagens Industri har för avsikt att identifiera klaganden, utan möjligheten att göra det är i sig tillräckligt för att avgöra om det är möjligt att identifiera en besökare. *Objektiva hjälpmedel som rimligen kan användas* antingen av den personuppgiftsansvarige eller

[19] Se Kammarrätten i Göteborgs dom den 11 november 2021 i mål nr 2232-21, med instämmande i underinstansens bedömning.

av någon annan, är *alla hjälpmedel som rimligen* kan användas i syfte att identifiera klaganden. Exempel på *objektiva hjälpmedel som rimligen kan användas* är tillgång till ytterligare information hos en tredje part som skulle göra det möjligt att identifiera klaganden med beaktande av såväl tillgänglig teknik vid tidpunkten för identifieringen samt kostnaden (tidsåtgången) för identifieringen.

IMY konstaterar att EU-domstolen genom dom M.I.C.M. och dom Breyer slagit fast att dynamiska IP-adresser utgör personuppgifter i förhållande till den som behandlar dem, när denne även har en laglig möjlighet att identifiera innehavarna av internetanslutningarna med hjälp av de ytterligare upplysningar som tredje part förfogar över.[20] IP-adresser förlorar inte sin karaktär av att vara personuppgifter enbart på grund av att medlen för identifiering ligger hos tredje part. Breyer-domen och M.I.C.M-domen bör tolkas utifrån det som faktiskt uttalas i domarna, dvs. att om det finns en laglig möjlighet att få tillgång till kompletterande information i syfte att identifiera klaganden är det objektivt klart att det finns ett ”*medel som rimligen kan komma att användas*” för att identifiera klaganden. Domarna ska enligt IMY inte läsas motsatsvis, på det sättet att det måste påvisas en lagreglerad möjlighet att få tillgång till uppgifter som kan knyta IP-adresser till fysiska personer för att IP-adresserna ska anses vara personuppgifter. En tolkning av begreppet personuppgift som innebär att det alltid måste påvisas en *laglig möjlighet* att knyta sådana uppgifter till en fysisk person skulle enligt IMY innebära en betydande begränsning av förordningens skyddsområde, och öppna upp möjligheter att kringgå skyddet i förordningen. Denna tolkning skulle bland annat strida mot förordningens syfte enligt artikel 1.2 i dataskyddsförordningen. Breyer-domen är beslutad under tidigare gällande direktiv 95/46 och begreppet ”singling out” enligt skäl 26 till nuvarande förordning (att det inte krävs kännedom om den faktiska besökarens namn eller fysiska adress, eftersom särskiljandet i sig är tillräckligt för att göra besökaren identifierbar), angavs inte i tidigare gällande direktiv som en metod för identifiering av personuppgifter.

I sammanhanget tillkommer också andra uppgifter (enligt punkterna 1–3 ovan) som IP-adressen kan kombineras med för att möjliggöra identifiering. Även om trunkeringen[21] av sista oktetten och ”hashning” av cookie-värdet utgör integritetshöjande åtgärder, då de begränsar omfattningen av de uppgifter som myndigheter kan få tillgång till (i tredjeland) konstaterar IMY att det ändå går att koppla de överförda uppgifterna till andra uppgifter som också överförs till Google LLC (till USA). Därigenom möjliggörs identifiering, vilket i sig är tillräckligt för att uppgifterna tillsammans ska utgöra personuppgifter.

IMY konstaterar att det även kan finnas skäl att jämföra IP-adresser med pseudonymiserade personuppgifter. Pseudonymisering av personuppgifter innebär enligt artikel 4.5 i dataskyddsförordningen att uppgifterna – i likhet med dynamiska IP-adresser – inte direkt kan tillskrivas en specifik registrerad utan att kompletterande uppgifter används. Enligt skäl 26 till dataskyddsförordningen bör sådana uppgifter anses vara uppgifter om en identifierbar fysisk person.

En snävare tolkning av begreppet personuppgifter skulle enligt IMY undergräva räckvidden för rätten till skydd av personuppgifter, som garanteras i artikel 8 i

[20] EU-domstolens dom M.I.C.M, C-597/19, EU:C:2021:492, punkt 102–104 och dom Breyer, C-582/14 EU:C:2016:779, punkt 49.
[21] Trunkering av IP-adress innebär att asterisk eller nollor ersätter andra siffror i sista oktetter (sista siffrorna i en IP-adress, ett tal mellan 0 och 255), vilket i sig endast kan vara något av 256 alternativ. Effekten av denna åtgärd innebär att det fortfarande går att särskilja IP-adressen från de övriga IP-adresser (255 alternativ), eftersom IP-adressen kan sammankopplas med övriga överförda uppgifter (t.ex. uppgift om enhet och tidpunkt för besöket) till tredjeland.

Europeiska unionens stadga om de grundläggande rättigheterna, eftersom det skulle göra det möjligt för personuppgiftsansvariga att särskilt peka ut enskilda tillsammans med personuppgifter (t.ex. när de besöker en viss webbplats) samtidigt som enskilda nekas rätt till skydd mot att sådana uppgifter om dem sprids. En sådan tolkning skulle undergräva skyddsnivån för enskilda och vore inte förenligt med det vida tillämpningsområde som dataskyddsreglerna getts i EU-domstolens praxis.[22]

Dagens Industri har dessutom, genom att klaganden varit inloggad på sitt Google-konto vid besöket på Webbplatsen, behandlat uppgifter där man kunnat dra slutsatser om den enskilde baserat på dennes registrering hos Google. Av Googles yttrande framgår att implementering av Verktyget på en webbplats gör det möjligt att få information om att en användare av ett Google-konto (dvs. en registrerad) har besökt webbplatsen i fråga. Google anger visserligen att vissa villkor måste vara uppfyllda för att Google ska kunna ta emot sådan information, t.ex. att användaren (klaganden) inte har avaktiverat behandling för och visning av personliga annonser. Eftersom klaganden var inloggad på sitt Google-konto vid besöket på Webbplatsen, kan Google fortfarande därmed ha haft möjlighet att få information om den inloggade användarens besök på Webbplatsen. Det faktum att det inte framgår av klagomålet att inga personliga annonser har visats, medför inte att Google inte kan få information om den inloggade användarens besök på Webbplatsen.

IMY finner mot bakgrund av de unika identifierarna som kan identifiera webbläsaren eller enheten, möjligheten att härleda den enskilde genom dennes Google-konto, de dynamiska IP-adresserna samt möjligheten att kombinera dessa med ytterligare uppgifter, att Dagens Industris användning av Verktyget på en webbsida, innebär behandling av personuppgifter.

2.3 Dagens Industri är personuppgiftsansvarig för behandlingen

Personuppgiftsansvarig är bland annat en juridisk person som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter (artikel 4.7 i dataskyddsförordningen). Personuppgiftsbiträde är bland annat en juridisk person som behandlar personuppgifter för den personuppgifts-ansvariges räkning (artikel 4.8 i dataskyddsförordningen).

De svar som Dagens Industri har lämnat visar att har fattat beslutet att implementera Verktyget på Webbplatsen. Vidare framgår att Dagens Industris syfte med implementeringen av verktyget har varit att bolaget ska kunna analysera hur Webbplatsen används, och i synnerhet kunna följa användningen av Webbplatsen över tid.

IMY finner att Dagens Industri genom att besluta att implementera Verktyget på Webbplatsen i nämnda syfte, har fastställt ändamålen och medlen med insamlingen och den efterföljande behandlingen av dessa personuppgifter. Dagens Industri är därför personuppgiftsansvarig för denna behandling.

[22] Se till exempel EU-domstolens dom Latvijas Republikas Saeima (Points de pénalité), C-439/19, EU:C:2021:504, punkt 61, dom Nowak, C-434/16, EU:C:2017:994, punkt 33 och dom Rijkeboer, C-553/07, EU:C:2009:293, punkt 59.

2.4 Överföring av personuppgifter till tredjeland

Av utredningen framgår att de uppgifter som samlas in via Verktyget lagras av Google LLC i USA. Således överförs de personuppgifter som samlas in via Verktyget till USA.

Frågan är därmed om Dagens Industris överföring av personuppgifter till USA är förenlig med artikel 44 i dataskyddsförordningen och har rättsligt stöd för det i kapitel V.

2.4.1 Tillämpliga bestämmelser m.m.

Enligt artikel 44 i dataskyddsförordningen, som har rubriken ”Allmän princip för överföring av uppgifter”, får bland annat överföring av personuppgifter som är under behandling eller är avsedda att behandlas efter det att de överförts till ett tredjeland – dvs. ett land utanför EU/EES – bara ske under förutsättning att den personuppgifts-ansvarige och personuppgiftsbiträdet, med förbehåll för övriga bestämmelser i dataskyddsförordningen, uppfyller villkoren i kapitel V. Alla bestämmelser i nämnda kapitel ska tillämpas för att säkerställa att den skyddsnivå som garanteras genom dataskyddsförordningen inte undergrävs.

I kapitel V i dataskyddsförordningen finns verktyg som kan användas vid överföringar till tredjeländer för att säkerställa en skyddsnivå som i huvudsak motsvarar den som garanteras inom EU/EES. Det kan t.ex. vara överföring med stöd av ett beslut om adekvat skyddsnivå (artikel 45) och överföring som omfattas av lämpliga skyddsåtgärder (artikel 46). Därtill finns undantag för särskilda situationer (artikel 49).

EU-domstolen har i domen Schrems II ogiltigförklarat det beslut om adekvat skydds-nivå som tidigare gällde överföring av personuppgifter till USA.[23] Eftersom ett beslut om adekvat skyddsnivå sedan juli 2020 saknas får överföringar till USA inte grundas på artikel 45.

I artikel 46.1 föreskrivs bland annat att i avsaknad av ett beslut i enlighet med artikel 45.3 får en personuppgiftsansvarig eller ett personuppgiftsbiträde endast överföra personuppgifter till ett tredjeland efter att ha vidtagit lämpliga skyddsåtgärder, och på villkor att lagstadgade rättigheter för registrerade och effektiva rättsmedel för registrerade finns tillgängliga. I artikel 46.2 c stadgas att sådana lämpliga skyddsåtgärder får ta formen av standardiserade dataskyddsbestämmelser som antas av kommissionen i enlighet med det granskningsförfarande som avses i artikel 93.2.

I domen Schrems II underkände inte EU-domstolen standardavtalsklausuler som överföringsverktyg. Domstolen konstaterade dock att de inte är bindande för myndigheterna i tredjelandet. EU-domstolen uttalade därvid att ”*[ä]ven om det således finns situationer där mottagaren av en sådan överföring, beroende på rättsläget och gällande praxis i det berörda tredjelandet, kan garantera det nödvändiga skyddet av uppgifter enbart med stöd av de standardiserade dataskyddsbestämmelserna, finns det andra situationer i vilka bestämmelserna i dessa klausuler inte kan vara ett tillräckligt medel för att i praktiken säkerställa ett effektivt skydd av de personuppgifter som överförs till det berörda tredjelandet.”* Enligt EU-domstolen är så *”bland annat*

[23] Kommissionens genomförandebeslut (EU) 2016/1250 av den 12 juli 2016 i enlighet med Europaparlamentets och rådets direktiv 95/46/EG om huruvida ett adekvat skydd säkerställs genom skölden för skydd av privatlivet i Europeiska unionen och Förenta staterna och EU-domstolens dom Facebook Ireland och Schrems (Schrems II), C-311/18, EU:C:2020:559.

fallet när lagstiftningen i det tredjelandet tillåter att myndigheterna i detta tredjeland gör ingrepp i de registrerade personernas rättigheter avseende dessa uppgifter.”[24]

Anledningen till att EU-domstolen ogiltigförklarade beslutet om adekvat skyddsnivå med USA var på grund av hur de amerikanska underrättelsetjänsterna kan få åtkomst till personuppgifter. Enligt domstolen kan ingåendet av standardavtalsklausuler inte i sig säkerställa en skyddsnivå som krävs enligt artikel 44 i dataskyddsförordningen, eftersom de garantier som där anges inte tillämpas när sådana myndigheter begär åtkomst. EU-domstolen uttalade därför följande:

> ”Det framgår således att de standardiserade dataskyddsbestämmelser som kommissionen antagit med stöd av artikel 46.2 c i samma förordning endast syftar till att tillhandahålla de personuppgiftsansvariga eller deras personuppgiftsbiträden etablerade i unionen avtalsenliga skyddsåtgärder som tillämpas på ett enhetligt sätt i alla tredjeländer och således oberoende av den skyddsnivå som säkerställs i vart och ett av dessa länder. Eftersom dessa standardiserade dataskyddsbestämmelser, med hänsyn till deras art, inte kan leda till skyddsåtgärder som går utöver en avtalsenlig skyldighet att säkerställa att den skyddsnivå som krävs enligt unionsrätten iakttas, kan det vara nödvändigt, beroende på den situation som råder i ett visst tredjeland, för den personuppgiftsansvarige att vidta ytterligare åtgärder för att säkerställa att skyddsnivån iakttas”.*[25]*

I Europeiska dataskyddsstyrelsens (EDPB) rekommendationer om följderna av domen[26] klargörs att om bedömningen av lagstiftning och praxis i tredjelandet innebär att det skydd som överföringsverktyget ska garantera inte kan upprätthållas i praktiken måste exportören, inom ramen för sin överföring, som regel antingen avbryta överföringen eller vidta lämpliga ytterligare skyddsåtgärder. EDPB konstaterar därvid att ”*ytterligare åtgärder kan endast anses vara effektiva i den mening som avses i EU-domstolens dom ”Schrems II” om och i den mån de – ensamt eller i kombination – åtgärdar de specifika brister som konstaterats vid bedömningen av situationen i tredjelandet när det gäller dess lagar och praxis som är tillämpliga på överföringen”*.[27]

Av EDPB:s rekommendationer framgår att sådana ytterligare skyddsåtgärder kan delas in i tre kategorier: avtalsmässiga, organisatoriska och tekniska.[28]

När det gäller *avtalsmässiga* åtgärder uttalar EDPB att sådana åtgärder ”*[...] kan komplettera och förstärka de skyddsåtgärder som överföringsverktyget och relevant lagstiftning i tredjelandet tillhandahåller [...]. Med hänsyn till att de avtalsmässiga åtgärderna är av sådan art att de i allmänhet inte kan binda myndigheterna i det tredjelandet eftersom de inte är parter i avtalet, kan dessa åtgärder ofta behöva kombineras med andra tekniska och organisatoriska åtgärder för att tillhandahålla den nivå av uppgiftsskydd som krävs [...]”.*[29]

När det gäller *organisatoriska* åtgärder betonar EDPB ”*[a]tt välja och genomföra en eller flera av dessa åtgärder kommer inte nödvändigtvis och systematiskt att säkerställa att [en] överföring uppfyller den grundläggande likvärdighetsnorm som*

---

[24] Punkt 125-126.
[25] Punkt 133.
[26] EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Version 2.0, antagna den 18 juni 2021 (nedan “EDPB:s Rekommendationer 01/2020”).
[27] EDPB:s Rekommendationer 01/2020, punkt 75: IMY:s översättning.
[28] EDPB:s Rekommendationer 01/2020, punkt 52.
[29] EDPB:s Rekommendationer 01/2020, punkt 99; IMY:s översättning.

krävs enligt EU-lagstiftningen. Beroende på de särskilda omständigheterna kring överföringen och den bedömning som gjorts av tredjelandets lagstiftning *krävs organisatoriska åtgärder för att* komplettera avtalsmässiga och/eller tekniska åtgärder *för att säkerställa en skyddsnivå för personuppgifter som är väsentligen likvärdigt den som garanteras inom EU/EES*".[30]

När det gäller *tekniska* åtgärder påpekar EDPB att "*dessa åtgärder kommer särskilt att vara nödvändiga när lagstiftningen i det landet ålägger importören skyldigheter som strider mot garantierna i artikel 46 i dataskyddsförordningens överföringsverktyg och som i synnerhet kan inkräkta på den avtalsenliga garantin om ett i allt väsentligt likvärdigt skydd mot att myndigheterna i det tredjelandet får tillgång till dessa uppgifter*".[31] EDPB uttalar därvid att *"de åtgärder som anges [i Rekommendationerna] är avsedda att säkerställa att åtkomsten till de överförda uppgifterna för offentliga myndigheter i tredjeländer inte inkräktar på ändamålsenligheten i de lämpliga skyddsåtgärderna i artikel 46 i dataskyddsförordningens överföringsverktyg. Dessa åtgärder skulle vara nödvändiga för att garantera en i allt väsentligt likvärdig skyddsnivå som den som garanteras inom EU/EES, även om de offentliga myndigheternas tillgång är förenlig med lagstiftningen i importörens land, där sådan tillgång i praktiken går utöver vad som är nödvändigt och proportionerligt i ett demokratiskt samhälle. Syftet med dessa åtgärder är att förhindra potentiellt otillåten åtkomst genom att hindra myndigheterna från att identifiera de registrerade, dra slutsatser om dem, peka ut dem i ett annat sammanhang eller koppla de överförda uppgifterna till andra datamängder som bland annat kan innehålla nätidentifierare som tillhandahålls av de enheter, applikationer, verktyg och protokoll som används av registrerade i andra sammanhang*".[32]

2.4.2 Integritetsskyddsmyndighetens bedömning

2.4.2.1 Tillämpligt överföringsverktyg

Av utredningen framgår att Dagens Industri och Google har ingått standardiserade dataskyddsbestämmelser (standardavtalsklausuler) i den mening som avses i artikel 46 för överföring av personuppgifter till USA. Dessa klausuler är i linje med dem som offentliggjorts av Europeiska kommissionen i beslut 2010/87/EU och alltså ett överföringsverktyg enligt kapitel V i dataskyddsförordningen.

2.4.2.2 Lagstiftningen och situationen i tredjelandet

Som framgår av domen Schrems II kan användande av standardavtalsklausuler kräva ytterligare skyddsåtgärder som komplement. Därför behöver en analys av lagstiftningen i det aktuella tredjelandet göras.

IMY anser att den analys som EU-domstolen redan gjort i domen Schrems II, som avser liknande förhållanden, är relevant och aktuell, och att den därmed kan läggas till grund för bedömningen i ärendet utan att någon ytterligare analys av den rättsliga situationen i USA behöver göras.

Google LLC ska, i egenskap av importör av uppgifterna till USA, klassificeras som leverantör av elektroniska kommunikationstjänster i den mening som avses i 50 US Code § 1881 (b)(4). Google är därför föremål för övervakning av amerikanska underrättelsetjänster i enlighet med 50 US § 1881a ("702 FISA") och därmed skyldigt att förse den amerikanska regeringen med personuppgifter när 702 FISA används.

---

[30] EDPB:s Rekommendationer 01/2020, punkt 128; IMY:s översättning.
[31] EDPB:s Rekommendationer 01/2020, punkt 77; IMY:s översättning.
[32] EDPB:s Rekommendationer 01/2020, punkt 79; IMY:s översättning.

EU-domstolen konstaterade i domen Schrems II att de amerikanska övervakningsprogrammen som grundar sig på 702 FISA, Executive Order 12333 (nedan ”E.O. 12333”) och Presidential Policy Directive 28 (nedan ”PPD-28”) i den amerikanska lagstiftningen inte motsvarar de minimikrav som i unionsrätten gäller enligt proportionalitetsprincipen. Det innebär att de övervakningsprogram som grundas på dessa bestämmelser inte kan anses vara begränsade till vad som är strikt nödvändigt. Domstolen konstaterade dessutom att övervakningsprogrammen inte ger de registrerade rättigheter som kan göras gällande mot amerikanska myndigheter i domstol, vilket innebär att dessa personer inte har rätt till ett effektivt rättsmedel.[33]

IMY konstaterar mot denna bakgrund att användningen av EU-kommissionens standardavtalsklausuler inte i sig är tillräckligt för att uppnå en godtagbar skyddsnivå för de överförda personuppgifterna.

2.4.2.3 Ytterligare skyddsåtgärder som genomförts av Google och Dagens Industri

Nästa fråga är om Dagens Industri vidtagit tillräckliga ytterligare skyddsåtgärder.

Som personuppgiftsansvarig och exportör av personuppgifterna är Dagens Industri skyldigt att se till att reglerna i dataskyddsförordningen efterlevs. I detta ansvar ingår bland annat att i varje enskilt fall vid överföringar av personuppgifter till tredjeland bedöma vilka ytterligare skyddsåtgärder som ska användas och i vilken utsträckning, inbegripet att utvärdera om de åtgärder som mottagaren (Google) och exportören (Dagens Industri) sammantaget vidtagit är tillräckliga för att uppnå en godtagbar skyddsnivå.

2.4.2.3.1 Googles ytterligare skyddsåtgärder

Google LLC har i egenskap av importör av personuppgifter vidtagit avtalsmässiga, organisatoriska och tekniska åtgärder för att komplettera standardavtalsklausulerna. Google har i yttrande den 9 april 2021 beskrivit att bolaget har vidtagit åtgärder.

Frågan är om de ytterligare skyddsåtgärder som vidtagits av Dagens Industri och Google LLC är effektiva, med andra ord hindrar amerikanska underrättelsetjänsters möjligheter att få åtkomst till de överförda personuppgifterna.

När det gäller de *rättsliga och organisatoriska åtgärderna* kan konstateras att varken information till användare av Verktyget (såsom Dagens Industri),[34] offentliggörandet av en insynsrapport eller en allmänt tillgänglig ”*policy för hantering av regeringsförfrågningar*” hindrar eller minskar de amerikanska underrättelsetjänsternas möjligheter att få tillgång till personuppgifterna. Dessutom är det inte beskrivet vad det innebär att Google LLC:s gör en ”*noggrann prövning av varje begäran*” om ”lagligheten” från amerikanska underrättelsetjänster. IMY noterar att detta inte påverkar lagligheten av sådana begäranden eftersom de enligt EU-domstolen inte är förenliga med kraven i EU:s dataskyddsregler.

När det gäller de *tekniska åtgärder* som vidtagits kan det konstateras att varken Google LLC eller Dagens Industri har klargjort hur de beskrivna åtgärderna – såsom skydd av kommunikation mellan Googles tjänster, skydd av data vid överföring mellan datacenter, skydd av kommunikation mellan användare och webbplatser eller ”fysisk säkerhet” – hindrar eller minskar amerikanska underrättelsetjänsters möjligheter att bereda sig tillgång till uppgifterna med stöd av det amerikanska regelverket.

---

[33] Punkt 184 och 192. Punkt 259 och efterföljande.
[34] Oavsett om en sådan anmälan ens skulle vara tillåten enligt amerikansk lagstiftning.

När det gäller den krypteringsteknik som används– tillexempel. för s.k. ”data i vila” (”data at rest”) i datacenter, som Google LLC nämner som teknisk åtgärd – har Google LLC som importör av personuppgifter ändå en skyldighet att bevilja åtkomst till eller lämna över importerade personuppgifter som Google LLC förfogar över, inklusive eventuella krypteringsnycklar som krävs för att göra uppgifterna begripliga.[35] Således kan en sådan teknisk åtgärd inte anses vara effektiv så länge Google LLC har möjlighet att få tillgång till personuppgifterna i klartext.

Beträffande vad Google LLC:s anfört om att *”i den mån information för mätning i Google Analytics som överförs av webbplatsinnehavare utgör personuppgifter, får de anses vara pseudonymiserade*” kan konstateras att universella unika identifierare (UUID) inte omfattas av begreppet pseudonymisering i artikel 4.5 i dataskydds-förordningen. Pseudonymisering kan vara en integritetshöjande teknik, men de unika identifierarna har, som beskrivits ovan, det specifika syftet att särskilja användare och inte att fungera som skydd. Därtill görs enskilda identifierbara genom vad som ovan angetts om möjligheten att kombinera unika identifierare och andra uppgifter (t.ex. metadata från webbläsare eller enheter och IP-adressen) och möjligheten att länka sådan information till ett Google-konto för inloggade användare.

När det gäller Googles åtgärd avseende anonymisering av IP-adresser i form av trunkering[36] framgår det inte av Googles svar om denna åtgärd sker före överföringen, eller om hela IP-adressen överförs till USA och förkortas först efter överföringen till USA. Ur teknisk synvinkel har det således inte visats, att det inte finns potentiell tillgång till hela IP-adressen innan den sista oktetten trunkeras.

Vad gäller det faktum att Google LLC har konfigurerat lösningen så att JavaScript-filen cachas i den mottagande terminalens applikations-cache i två timmar (vilket kan innebära en fördröjning mellan första och andra anropet på upp till två timmar) så innebär detta att anropen kan få olika tidstämplar, som i sig skulle kunna innebära ett försvårande avseende identifieringen av vilken besökare som har avgett det unika anropet. IMY konstaterar dock att Dagens Industri inte kan säkerställa att en fördröjning av anropen faktiskt sker, dels då det rent tekniskt inte går d att säkerställa när (eller om) en fördröjning mellan första och andra anropet sker, och då styrningen (aktiveringen) av cachningen ligger utanför bolagets kontroll.

Mot denna bakgrund konstaterar IMY att de ytterligare skyddsåtgärder som vidtagits av Google inte är effektiva, eftersom de inte hindrar amerikanska underrättelse-tjänsters möjlighet att få åtkomst till personuppgifterna eller gör sådan åtkomst verkningslös.

2.4.2.3.2 Dagens Industris egna ytterligare skyddsåtgärder

Dagens Industri har uppgett att bolaget har vidtagit ytterligare skyddsåtgärder utöver de åtgärder som Google har vidtagit. Dessa består enligt Dagens Industri av att bolaget har genomfört omfattande kartläggning av livscykeln för personuppgifter som behandlas i Verktyget och att bolaget på egna dataservrar (*överföringen genom proxyservern)* maskerar sista oktetten av IP-adressen och hashar värdet i kakorna innan uppgifterna överförs till Google.[37]

---

[35] Se EDPB:s Rekommendationer 01/2020, punkt 81.
[36] Trunkering av IP-adress innebär att asterisk eller nollor ersätter andra siffror i sista oktetter (sista siffrorna i en IP-adress, ett tal mellan 0 och 255).
[37] Se ovan i avsnittet om vad bolaget har anfört, under rubriken ”Vidtagna kompletterande skyddsåtgärder”.

IMY finner dock att dessa åtgärder inte är tillräckliga av följande skäl.

Det framgår av bolagets egna uppgifter att *två separata* överföringar av den enskildes IP-adress sker till Google LLC – *dels* genom ett anrop från *mätverktyget ”analytics.js”* med hela IP-adressen exponerad, *dels* med trunkering[38] av sista oktetten när uppmätt data överförs *(och hashning av cookie-värdet*).[39]

Dagens Industri gör gällande att det som kan utläsas ur den första överföringen (där hela IP-adressen exponeras) enbart är vilken webbsida som IP-adressen har besökt och att det inte går att koppla samman IP-adressen med den sidvisningsdata etc. som vid ett senare tillfälle uppmäts på Webbplatsen. IMY konstaterar dock att överföringen i sig innebär en överföring av en personuppgift (IP-adressen), trots vidtagna skyddsåtgärder.

När det gäller den andra överföringen innehåller den dessutom ytterligare uppgifter om besöket på Dagens Industris webbplats (såsom besökarens enhet och tidpunkt för besöket) och sammankopplingen torde därmed kunna göras med IP-adressen då skillnaden efter trunkeringen endast är att sista oktetten maskerats, vilket för IP-adresser innebär enbart 256 alternativ (dvs. ett nummer mellan 0–255). Även om maskningen av sista oktetten och ”hashning” av cookie-värdet utgör integritetshöjande åtgärder, då de begränsar omfattningen av de uppgifter som myndigheter kan få tillgång till (i tredjeland) konstaterar IMY att det ändå går att koppla de överförda uppgifterna till andra uppgifter som också överförs till Google LLC.

Mot denna bakgrund konstaterar IMY att inte heller de ytterligare åtgärder som vidtagits av bolaget, utöver de ytterligare åtgärder som Google vidtagit, är tillräckligt effektiva för att hindra amerikanska underrättelsetjänsters möjlighet att få åtkomst till personuppgifterna eller göra sådan åtkomst verkningslös.

2.4.2.3.3 Integritetsskyddsmyndighetens slutsats

IMY finner att Dagens Industris och Googles åtgärder varken var för sig eller sammantaget är tillräckligt effektiva för att hindra amerikanska underrättelsetjänsters möjlighet att få åtkomst till personuppgifterna eller göra sådan åtkomst verkningslös.

Mot denna bakgrund finner IMY att varken standardavtalsklausuler eller de övriga åtgärder som Dagens Industri åberopat kan ge sådant stöd för överföringen som anges i kapitel V i dataskyddsförordningen.

I och med denna överföring av uppgifter undergräver Dagens Industri därför den skyddsnivå för personuppgifter för registrerade som garanteras i artikel 44 i dataskyddsförordningen.

IMY konstaterar därför att Dagens Industri Aktiebolag bryter mot artikel 44 i dataskyddsförordningen.

---

[38] Trunkering av IP-adress innebär att asterisk eller nollor ersätter andra siffror i sista oktetter (sista siffrorna i en IP-adress, ett tal mellan 0 och 255), vilket i sig endast kan vara något av 256 alternativ. Effekten av denna åtgärd innebär att det fortfarande går att särskilja IP-adressen från de övriga IP-adresser (255 alternativ), eftersom IP-adressen kan sammankopplas med övriga överförda uppgifter (t.ex. uppgift om enhet och tidpunkt för besöket) till tredjeland.
[39] Se ovan i avsnitt 1.3.17.1, illustration av dataflöden (s. 8 i bolagets yttrande).

3 Val av ingripande

3.1 Rättslig reglering

IMY har vid överträdelser av dataskyddsförordningen ett antal korrigerande befogenheter att tillgå enligt artikel 58.2 a–j i dataskyddsförordningen, bland annat reprimand, föreläggande och sanktionsavgifter.

IMY ska påföra sanktionsavgifter utöver eller i stället för andra korrigerande åtgärder som avses i artikel 58.2, beroende på omständigheterna i varje enskilt fall.

Varje tillsynsmyndighet ska säkerställa att påförandet av administrativa sanktionsavgifter i varje enskilt fall är effektivt, proportionellt och avskräckande. Det anges i artikel 83.1 i dataskyddsförordningen.

I artikel 83.2 i dataskyddsförordningen anges de faktorer som ska beaktas för att bestämma om en administrativ sanktionsavgift ska påföras, men också vid bestämmandet av sanktionsavgiftens storlek. Om det är fråga om en mindre överträdelse får IMY enligt vad som anges i skäl 148 i stället för att påföra en sanktionsavgift utfärda en reprimand enligt artikel 58.2 b i förordningen. Hänsyn ska vid bedömningen tas till försvårande och förmildrande omständigheter i fallet, såsom överträdelsens karaktär, svårighetsgrad och varaktighet samt tidigare överträdelser av relevans.

Enligt artikel 83.5 c i dataskyddsförordningen ska det vid överträdelse av bland artikel 44 i enlighet med 83.2 påföras administrativa sanktionsavgifter på upp till 20 miljoner EUR eller, om det gäller ett företag, på upp till 4 % av den totala globala årsomsättningen under föregående budgetår, beroende på vilket värde som är högst.

3.2 Ska sanktionsavgift påföras?

IMY har ovan funnit att de överföringar av personuppgifter till USA som sker via Google Analytics-verktyget och som Dagens Industri är ansvarigt för strider mot artikel 44 i dataskyddsförordningen. Överträdelser av den bestämmelsen kan, som framgår ovan, föranleda sanktionsavgifter. Det är i det aktuella fallet fråga om en allvarlig överträdelse som i normalfallet bör föranleda en sanktionsavgift.

Vid bedömningen i detta fall om sanktionsavgift ska påföras ska i *försvårande* riktning beaktas att överträdelsen har skett genom att Dagens Industri har överfört en stor mängd personuppgifter till tredjeland där uppgifterna inte kan garanteras den skyddsnivå som ges i EU/EES. Behandlingen har skett systematiskt och under en längre tid. Efter att EU-domstolen genom dom den 16 juli 2020 underkände kommissionens beslut om adekvat skyddsnivå i USA[40] förändrades förutsättningarna för överföringar av personuppgifter till USA. Det har nu förflutit cirka 3 år sedan domen meddelades och EDPB har under den tiden lämnat rekommendationer om konsekvenserna av domen för publik konsultation den 10 november 2020 och i slutlig form den 18 juni 2021.

[40] Kommissionens genomförandebeslut (EU) 2016/1250 av den 12 juli 2016 enligt Europaparlamentets och rådets direktiv 95/46/EG om huruvida ett adekvat skydd säkerställs genom skölden för skydd av privatlivet i EU och Förenta staterna.

I *förmildrande* riktning ska det beaktas den särskilda situation som uppstått efter domen och tolkningen av EDPB:s rekommendationer, där det funnits ett tomrum efter att överföringsverktyget till USA enligt Kommissionens tidigare beslut underkänts av EU-domstolen. Det ska därtill särskilt beaktas att det av utredningen framgår att Dagens Industri har gjort en seriös analys och kartläggning av livscykeln för personuppgifter i Verktyget. Dagens Industri har även vidtagit åtgärder såsom att bolaget på egna dataservrar (överföringen genom proxyservern) maskerar sista oktetten av IP-adressen (trunkering) och hashar värdet i kakorna innan uppgifterna överförs till Google. Bolaget har även aktiverat Googles åtgärd ”anonymisering av IP-adresser” genom trunkering. Dagens Industri har således vidtagit förhållandevis omfattande åtgärder för att försöka begränsa riskerna för de registrerade och för att läka bristerna. Dagens Industri har därigenom också trott att de lyckats även om åtgärderna i praktiken nu visat sig inte vara effektiva.

Vid en sammanvägd bedömning finner IMY att det finns anledning att i det här fallet avstå från att påföra Dagens Industri en sanktionsavgift för den konstaterade överträdelsen och stanna vid ett föreläggande om att åtgärda bristen.

3.3 Andra ingripanden

Det framgår av utredningen att de skyddsåtgärder för överföring som åberopats av Dagens Industri inte kan ge stöd för överföringen enligt kapitel V i dataskyddsförordningen. Överföringen innebär således en överträdelse av förordningen. För att säkerställa att överträdelsen upphör ska Dagens Industri föreläggas enligt artikel 58.2 d i dataskyddsförordningen att se till att bolagets behandling av personuppgifter inom ramen för användningen av verktyget Google Analytics överensstämmer med artikel 44 och övriga bestämmelser i kapitel V. Detta ska särskilt ske genom att Dagens Industri upphör med att använda den version av verktyget Google Analytics som användes den 14 augusti 2020, om inte tillräckliga skyddsåtgärder vidtagits. Åtgärderna ska vara genomförda senast en månad efter att detta beslut vunnit laga kraft.

Detta beslut har fattats av generaldirektören Lena Lindgren Schelin efter föredragning av juristen Sandra Arvidsson. Vid den slutliga handläggningen har även rättschefen David Törngren, enhetschefen Catharina Fernquist och IT- och informationssäkerhetsspecialisten Mats Juhlén deltagit.

Lena Lindgren Schelin, 2023-06-30 (Det här är en elektronisk signatur)

4 Överklagandehänvisning

4.1 Hur man överklagar

Om ni vill överklaga beslutet ska ni skriva till Integritetsskyddsmyndigheten. Ange i skrivelsen vilket beslut ni överklagar och den ändring som ni begär. Överklagandet ska ha kommit in till Integritetsskyddsmyndigheten senast tre veckor från den dag ni fick del av beslutet. Om överklagandet har kommit in i rätt tid sänder Integritetsskyddsmyndigheten det vidare till Förvaltningsrätten i Stockholm för prövning.

Ni kan e-posta överklagandet till Integritetsskyddsmyndigheten om det inte innehåller några integritetskänsliga personuppgifter eller uppgifter som kan omfattas av sekretess. Myndighetens kontaktuppgifter framgår av beslutets första sida.