Integritetsskydds myndigheten

Tele2 Sverige Aktiebolag
Box 62
16494 Kista

Diarienummer:
DI-2020-11373

Datum:
2023-06-30

Beslut efter tillsyn enligt dataskyddsförordningen – Tele2 Sverige AB:s överföring av personuppgifter till tredjeland

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 Tele2 Sverige Aktiebolag behandlar personuppgifter i strid med artikel 44 i dataskyddsförordningen[1] genom att under perioden den 14 augusti 2020 till och med maj 2023 använda verktyget Google Analytics, som tillhandahålls av Google LLC, på sin webbplats www.tele2.se, och därigenom överföra personuppgifter till tredjeland utan att villkoren enligt kapitel V i förordningen är uppfyllda.

IMY beslutar med stöd av artikel 58.2 och 83 i dataskyddsförordningen att Tele2 Sverige Aktiebolag ska betala en administrativ sanktionsavgift på 12 miljoner (tolv miljoner) kronor för överträdelse av artikel 44 i dataskyddsförordningen.

1 Redogörelse för tillsynsärendet

1.1 Handläggningen

Integritetsskyddsmyndigheten (IMY) har inlett tillsyn beträffande Tele2 Sverige Aktiebolag (nedan Tele2 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.tele2.se (nedan ”Tele2s 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.

1.2 Vad som anges i klagomålet

I klagomålet anförs i huvudsak följande.

Den 14 augusti 2020 besökte klaganden Tele2s 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 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 Tele2, åtminstone klagandens IP-adress och uppgifter insamlade genom kakor. En del av uppgifterna som samlades in, överfördes direkt till Google. I

[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).

enlighet med punkt 10 i villkoren om behandling av personuppgifter för Googles reklamprodukter, har Tele2 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 Tele2 har uppgett

Tele2 Sverige Aktiebolag har i huvudsak uppgett följande.

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

Tele2 har fattat beslutet att implementera Google Analytics (”Verktyget”) på Webbplatsen, vilket har skett genom att koden för Verktyget har bäddats in på Webbplatsen. Bolaget började avveckla den versionen av Verktyget som omfattas av IMY:s tillsyn under våren 2022 och slutade att använda den versionen under juni 2023 men har inte kunnat uppge ett exakt datum för detta. Bolaget är etablerat i Sverige och har inte fattat ett sådant beslut för någon annan europeisk webbplats.

Syftet med användningen av Verktyget är för att kunna sammanställa och analysera statistik avseende besöken på Webbplatsen.

Statistiken avseende besöken på Webbplatsen som erhållits via Verktyget har endast utvärderats av Tele2 i Sverige.

Det finns inte någon möjlighet att i Verktygets inställningar göra några val avseende överföring av uppgifter till USA.

1.3.2 Mottagare av uppgifterna

Inom ramen för Tele2s användning av Verktyget på Webbplatsen lämnas information ut till ett antal aktörer, vilka samtliga är personuppgiftsbiträden eller underbiträden till bolaget, inbegripet Google LLC, Google Ireland Ltd och deras underbiträden.

---

[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.

1.3.3 De uppgifter som behandlas i Verktyget och vad som utgör personuppgifter

Den information som behandlas av Tele2 och Google inom ramen för Verktyget omfattar (i) information om besöket på Webbplatsen t.ex. vilka sidor som visas eller vilka klick som görs, (ii) information om den enhet som anropar Webbplatsen och (iii) information i cookien (_ga cookie) som utgörs av Client ID.

Tele2 använder tjänsten Verktyget för att analysera statistik avseende besöken på webbplatsen www.tele2.se. All statistik och alla rapporter som genereras via Verktyget framställs på aggregerad nivå och kan inte användas för att direkt eller indirekt identifiera någon fysisk person.

Framställning av statistik och rapporter via Verktyget möjliggörs genom att cookies används på Webbplatsen. Om en besökare på Webbplatsen har samtyckt till att cookies används, placeras en cookie i besökarens webbläsare. Den information som behandlas genom användning av Verktyget utgörs således av följande kategorier: (i) information om besöket på Webbplatsen t.ex. vilka sidor som visas eller vilka klick som görs, (ii) information om den enhet som besöker Webbplatsen och (iii) information i cookien (_ga cookie) som utgörs av Client ID.

(i) Informationen om besöket på Webbplatsen
Information avseende besöket på Webbplatsen innehåller inte i sig någon information som kan användas för att direkt eller indirekt identifiera någon fysisk person dvs. en sidvisning eller ett klick utgör i sig helt anonym information.

(ii) Information om den enhet som besöker Webbplatsen
Information om den enhet som anropar och besöker Webbplatsen består t.ex. av vilken typ av webbläsare och vilken IP-adress som används vid besöket. Vad gäller IP-adresser används numera statiska IP-adresser enbart av ett fåtal företag och organisationer. I övrigt används uteslutande dynamiska IP-adresser för alla konsumenter. En dynamisk IP-adress betyder förenklat att en enhet tilldelas en IP-adress vid varje uppkoppling till internet och enheten tilldelas därefter helt nya IP-adresser vid senare uppkopplingstillfällen. En enhet är inte nödvändigtvis en dator, mobiltelefon eller en surfplatta utan kan i många fall utgöras av en router eller annan enhet som sedan flera datorer, mobiler eller surfplattor ansluter sig till och IP-adressen kan då således inte härledas till datorn, mobiltelefon eller surfplattan utan till routern. För att indirekt kunna identifiera en person med hjälp av en dynamisk IP-adress krävs att den kompletteras med en tidpunkt då den användes samt att ytterligare upplysningar inhämtas om vem som tilldelats IP-adressen från besökarens internetleverantör.

I Verktyget används IP-adress endast för ändamålet att analysera statistik avseende besöken på en webbplats. För det ändamålet torde en användare av Verktyget inte förfoga över några lagliga medel enligt svensk rätt som gör det möjligt att inhämta de kompletterande upplysningar som krävs för att indirekt kunna identifiera en fysisk person.

Den IP-adress som samlas in genom Verktyget anonymiseras dessutom i princip omgående efter insamlingen genom att siffrorna efter sista punkten i IP-adressen ersätts av 0 (exempelvis 192.169.0.100 blir 192.168.0.0). Sådan IP-anonymisering sker i tidigast möjliga skede under insamlingsprocessen och den fullständiga IP-adressen sparas eller behandlas aldrig på disk. För mer information om anonymisering

av IP-adress i Verktyget, se
https://support.google.com/analytics/answer/2763052?hl=en.

Anonymisering av IP-adressen innebär således att användaren av Verktyget aldrig har tillgång till den fullständiga IP-adressen och det finns då inga hjälpmedel som en användare av Verktyget rimligen kan använda för att indirekt identifiera en fysisk person (jfr. beaktandesats 26 i GDPR) med följden att risken för identifiering i praktiken kan anses försumbar.

(iii) Information i _ga cookien
Den information som behandlas genom användning av _ga cookien utgörs av ett Client ID. Client ID utgörs av ett slumpmässigt nummer med en tidsstämpel som sparas i _ga cookien. Detta Client ID kan användas för att se om en webbläsare tidigare har kopplat upp sig mot Webbplatsen. Tele2 kan dock inte använda Client ID enskilt eller tillsammans med en anonymiserad IP-adress för att direkt eller indirekt identifiera en fysisk person.

Med anledning av ovan anser Tele2 att det kan ifrågasättas om Tele2 i överhuvudtaget behandlar och överför personuppgifter till tredjeland. Med hänsyn till att viss osäkerhet får anses föreligga avseende den rättsliga bedömningen av ovannämnda förhållanden, har Tele2 av försiktighetsskäl valt att tillämpa reglerna i dataskyddsförordningen för de uppgifter som behandlas inom ramen för Verktyget.

1.3.4 Kategorier av personer som berörs av behandlingen
Uppgifterna rör besökare på Webbplatsen. Inga särskilda kategorier av personuppgifter enligt definitionen i artikel 9.1 i dataskyddsförordningen behandlas inom ramen för Verktyget. Tele2 kan inte genom Verktyget identifiera olika kategorier av personer som besöker Webbplatsen. Webbplatsen riktar sig vare sig till barn, eller någon annan särskild kategori av registrerade och besökare på Webbplatsen behöver inte ange någon ålder, eller någon annan personuppgift som behandlas i Verktyget.

1.3.5 När koden för Verktyget exekveras och mottagare bereds tillgång
Verktyget aktiveras och cookies placeras i användarens webbläsare efter att besökaren har gett sitt samtycke till användning av cookies. Anonymisering av IP-adress sker i tidigast möjliga skede under insamlingsprocessen och den fullständiga IP-adressen sparas eller behandlas aldrig på disk av Google (https://support.google.com/analytics/answer/2763052?hl=en&ref_topic=2919631).

1.3.6 Hur länge de personuppgifter som behandlas lagras
Under den tid Verktyget används kan lagringsperiod upp till 26 månader ställas in i Verktyget. Om avtalet för Verktyget upphör att gälla åtar sig Google enligt personuppgiftsbiträdesavtalet att radera personuppgifter i Verktyget så snart det praktiskt är möjligt efter avtalets upphörande, men senast inom 180 dagar.

1.3.7 Vilka länder personuppgifterna behandlas i
Enligt den information Tele2 har erhållit från Google anonymiseras besökarens IP-adress på det datacenter som ligger närmast där besökaren kopplar upp sig ifrån. Enligt villkoren i avtalet med Google kan Google inom ramen för Verktyget behandla uppgifterna i bl.a. USA.

1.3.8 Tele2s relation till Google LCC
Tele2 betraktar Google som personuppgiftsbiträde för den behandling som sker inom ramen för Verktyget dvs. Google behandlar informationen i Verktyget endast för

Tele2:s räkning. Detta stöds även av avtalet mellan Tele2 och Google avseende Verktyget och det personuppgiftsbiträdesavtal som gäller för Verktyget.

1.3.9 Säkerställande av att behandlingen inte sker för mottagarnas egna ändamål
Enligt punkt 5.3 i personuppgiftsbiträdesavtalet med Google får Google enbart behandla personuppgifter i enlighet med Tele2s instruktioner. Tele2s användning av Verktyget innebär att IP-adresser anonymiseras i tidigast möjliga skede under insamlingsprocessen och att den fullständiga IP-adressen aldrig sparas eller behandlas på disk av Google. Det innebär således att Google inte kan behandla den fullständiga IP-adressen för egna eller för tredje parts ändamål.

1.3.10 Beskrivning av bolagets användning av Verktyget
Tele2 använder Verktyget för att analysera statistik avseende besöken på Webbplatsen. All statistik och alla rapporter som genereras via Verktyget framställs på aggregerad nivå och inga åtgärder vidtas i förhållande till enskilda besökare på Webbplatsen inom ramen för Verktyget.

1.3.11 Egna kontroller av överföringar som berörs av domen Schrems II
Efter domen Schrems II initierade Tele2 ett internt arbete med att se över samtliga internationella dataöverföringar i Tele2s verksamhet. Denna översyn har även omfattat Verktyget.

Tele2 har haft en löpande dialog med Google som har inneburit att sedan den 12 augusti 2020 har överföringen av uppgifter till Google i USA baserats på standardavtalsklausuler för dataskydd som antagits av kommissionen. Eftersom EU-domstolen i domen Schrems II ansåg att den lagstiftning som Google omfattas av i USA inte motsvarar den skyddsnivå som finns i europeisk dataskyddslagstiftning, så är kompletterande skyddsåtgärder nödvändiga vid användning av de standardavtalsklausuler för dataskydd som antagits av kommissionen.

I dialogen med Google har Tele2 därför diskuterat vilka ytterligare skyddsåtgärder som kan vidtas i förhållande till Verktyget. Det har då konstaterats att de skyddsåtgärder som används i förhållande till Verktyget är IP-anonymisering (vilket har varit aktiverat av Tele2 ända sedan Verktyget infördes). Därtill har Google ISO270001-certifiering för Verktyget och Google använder även olika krypteringslösningar i samband med Verktyget och överföringen av uppgifter till USA.

1.3.12 Överföringsverktyg enligt kapitel V i dataskyddsförordningen
I den mån personuppgifter överförs till USA baseras överföringen på artikel 46.2 c i dataskyddsförordningen (standardavtalsklausuler för dataskydd som antagits av kommissionen). Standardavtalsklausuler gäller för uppgiftsöverföringen i Verktyget. Standardavtalsklausulerna är inte undertecknade av parterna utan ingår som en del i personuppgiftsbiträdesavtalet med Google genom hänvisning till dessa standardavtalsklausuler i punkt 10.2 i personuppgiftsbiträdesavtalet.

1.3.13 Kontroll av hinder för fullgörande i lagstiftning i tredjeland
I EDPBs rekommendation 01/2020 anges bland annat att pseudonymisering och anonymisering är sådana ytterligare skyddsåtgärder som kan vidtas för att uppnå en skyddsnivå motsvarande den som finns i Europa och därmed möjliggöra en överföring av personuppgifter till USA baserat på standardavtalsklausuler för dataskydd som antagits av kommissionen.

Tele2s bedömning, baserat på de ytterligare skyddsåtgärder som används i samband med Verktyget, är därför att uppgifterna skyddas på ett adekvat sätt och att skyddsnivån då motsvarar den som finns i europeisk dataskyddslagstiftning.

Tele2 har kontrollerat att de kompletterande skyddsåtgärder som vidtagits kan genomföras i praktiken och att det inte finns något i tredjelandslagstiftningen som hindrar mottagarna där från att genomföra åtgärderna för att säkerställa att nivån på uppgiftsskyddet för fysiska personer som garanteras inom EU/EES inte undergrävs.

1.3.14 Vidtagna ytterligare skyddsåtgärder utöver de som Google vidtagit
Tele2 har ställt in IP-anonymisering för Verktyget.

1.4 Vad Google LCC 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. Tele2 har beretts tillfälle att yttra sig över Googles yttrande. Av Googles 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 skicka informationen till Verktygets servrar.

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 avtalsrättsliga, organisatoriska och tekniska skyddsåtgärder för att reglera överföringar av uppgifter inom ramen för Verktyget.

Google har vidtagit avtalsrättsliga 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 Tele2 överför personuppgifter till tredjelandet USA inom ramen för Tele2s användning av Verktyget och om Tele2s har rättsligt stöd för det i kapitel V i dataskyddsförordningen. Tillsynen omfattar inte om Tele2s 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 förordningen 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.[4]

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.[5] 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 (”singling out” i den engelska språkversionen), 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 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.

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.[6] 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

[4] EU-domstolens dom Nowak, C-434/16, EU:C:2017:994, punkt 34–35.
[5] EU-domstolens dom Breyer, C-582/14, EU:C:2016:779, punkt 41.
[6] EU-domstolens dom Breyer, C-582/14, EU:C:2016:779, punkt 45–46.

internetanslutningarna med hjälp av de ytterligare upplysningar som tredje part förfogar över.[7]

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 Tele2 genom implementeringen av Verktyget kan identifiera enskilda, t.ex. klaganden, vid besök på Webbplatsen eller om risken för det är försumbar.[8]

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

Av utredningen framgår att Tele2 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 och körs lokalt i besökarens webbläsare. En kaka (cookie) sätts samtidigt 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 Tele2 (dvs. Tele2s 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 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

[7] 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.
[8] Se Kammarrätten i Göteborgs dom den 11 november 2021 i mål nr 2232-21, med instämmande i underinstansens bedömning.

dataskyddsförordningen, ”singling out” i den engelska versionen) i sig är tillräckligt för att göra besökaren indirekt identifierbar. Det krävs inte heller att Google eller Tele2 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 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.[9] 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 inte enligt IMY 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. Googles åtgärd avseende trunkering[10] av en IP-adress innebär att det fortfarande går att särskilja IP-adressen, eftersom den kan sammankopplas med övriga överförda uppgifter till tredjeland (till USA). Därigenom möjliggörs identifiering, vilket i sig är tillräckligt för att uppgifterna tillsammans ska utgöra personuppgifter.

Dessutom har flera andra tillsynsmyndigheter inom EU/ESS beslutat att överföring av personuppgifter till tredjeland har skett vid användningen av Verktyget eftersom det har varit möjligt att kombinera IP-adresser med andra uppgifter (enligt punkterna 1–3 ovan), och därmed möjliggjort särskiljande av uppgifter och identifiering av IP-adress,

---

[9] 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.

[10] 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.

vilket i sig är tillräckligt för att avgöra att det handlar om behandling av personuppgifter.[11]

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 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.[12]

Tele2 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 Tele2s användning av Verktyget på en webbsida, innebär behandling av personuppgifter.

2.3 Tele2 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 personuppgiftsansvariges räkning (artikel 4.8 i dataskyddsförordningen).

---

[11] Österrikes tillsynsmyndighet (Datenschultzbehörde) beslut av den 22 april 2022 avseende klagomål Google Analytics representerad av NOYB med lokalt ärendenummer 1354838270, Frankrikes tillsynsmyndighet (CNIL) beslut av den 10 februari 2022 representerad av NOYB och Italiens tillsynsmyndighet (Garante) beslut av den 9 juni 2022 avseende klagomål Google Analytics representerad av NOYB, lokalt ärendenummer 9782890.
[12] 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.

De svar som Tele2 lämnar visar att bolaget har fattat beslutet att implementera Verktyget på Webbplatsen. Vidare framgår att Tele2s syfte med detta varit att bolaget ska kunna analysera hur Webbplatsen används, i synnerhet att kunna följa användningen av webbplatsen över tid.

IMY finner att Tele2 genom att besluta att implementera Verktyget på Webbplatsen i nämnda syfte har fastställt ändamålen och medlen med insamlingen och den efterföljande överföringen av dessa personuppgifter. Tele2 är därför personuppgiftsansvarig för denna behandling.

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 Tele2s 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 personuppgiftsansvarige 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 nivå på skyddet av fysiska personer som säkerställs 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 skyddsnivå som tidigare gällde avseende USA.[13] 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*

[13] 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.

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 fallet när lagstiftningen i det tredjelandet tillåter att myndigheterna i detta tredjeland gör ingrepp i de registrerade personernas rättigheter avseende dessa uppgifter."*[14]

Anledningen till att EU-domstolen ogiltigförklarade beslutet om adekvat skyddsnivå med USA var 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”.*[15]*

I Europeiska dataskyddsstyrelsens (EDPB) rekommendationer om följderna av domen[16] 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”*.[17]

Av EDPB:s rekommendationer framgår att sådana ytterligare skyddsåtgärder kan delas in i tre kategorier: avtalsmässiga, organisatoriska och tekniska.[18]

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*

---

[14] Punkt 125-126.
[15] Punkt 133.
[16] 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”).
[17] EDPB:s Rekommendationer 01/2020, punkt 75; IMY:s översättning.
[18] EDPB:s Rekommendationer 01/2020, punkt 52.

kombineras med andra tekniska och organisatoriska åtgärder för att tillhandahålla den nivå av uppgiftsskydd som krävs [...]”.[19]

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 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*”.[20]

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*”.[21] 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*”.[22]

2.4.2 Integritetsskyddsmyndighetens bedömning

2.4.2.1 Tillämpligt överföringsverktyg

Av utredningen framgår att Tele2 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 2021/914 av den 4 juni 2021 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

[19] EDPB:s Rekommendationer 01/2020, punkt 99; IMY:s översättning.
[20] EDPB:s Rekommendationer 01/2020, punkt 128; IMY:s översättning.
[21] EDPB:s Rekommendationer 01/2020, punkt 77; IMY:s översättning.
[22] EDPB:s Rekommendationer 01/2020, punkt 79; IMY:s översättning.

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.

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.[23]

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 Tele2

Nästa fråga är om Tele2 vidtagit tillräckliga ytterligare skyddsåtgärder.

Som personuppgiftsansvarig och exportör av personuppgifterna är Tele2 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 (Tele2) 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 Tele2 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 Tele2),[24] 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

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

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 Tele2 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.

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.[25] 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 dataskyddsförordningen. 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 ”anonymisering av IP-adresser” i form av trunkering[26] 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.

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

2.4.2.3.2 Tele2s egna ytterligare skyddsåtgärder

Tele2 har uppgett att bolaget har vidtagit ytterligare skyddsåtgärder utöver de åtgärder som Google har vidtagit. Dessa består enligt Tele2 av aktivering av funktionen för trunkering[27] av sista oktetten i IP-adress innan uppgifterna överförs till Google, som innebär att den sista oktetten maskeras.

Som anförts ovan avseende Googles åtgärder framgår det inte av Googles svar om denna åtgärd sker före överföringen eller om hela IP-adressen överförs till USA och

[25] Se EDPB:s Rekommendationer 01/2020, punkt 81.
[26] 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).
[27] 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).

trunkeras först efter överföringen till USA. Ur teknisk synvinkel har det således inte visats att det efter överföringen inte finns potentiell tillgång till hela IP-adressen innan den sista oktetten trunkeras.

Även om trunkeringen skulle ske innan överföringen sker är det inte en tillräcklig åtgärd, eftersom den trunkerade IP-adressen kan sammankopplas med övriga uppgifter, såsom IMY konstaterat ovan i avsnitt 2.2.2. En trunkering av en IP-adress innebär att endast sista oktetten maskeras, vilket i sig endast kan vara något av 256 alternativ (dvs. i spannet 0–255) och på grund av att den trunkerade IP-adressen går att särskilja från andra IP-adresser kan denna uppgift sammankopplas med övriga uppgifter (enligt ovan i avsnitt 2.2.2) och möjliggöra identifiering, vilket i sig är tillräckligt för att avgöra om uppgifterna tillsammans är en personuppgift. Även om maskningen av sista oktetten utgör en integritetshöjande åtgärd, då den 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 (i tredjeland).

Mot denna bakgrund konstaterar IMY att inte heller de ytterligare åtgärder som vidtagits av Tele2 utöver de ytterligare åtgärder som Google vidtagit är tillräckligt effektiva för att hindra amerikanska underrättelsetjänsters möjlighet att få åtkomst till personuppgifterna eller gör sådan åtkomst verkningslös.

2.4.2.3.3 Integritetsskyddsmyndighetens slutsats
IMY finner att Tele2 och Googles åtgärder varken var för sig eller sammantaget är tillräckligt effektiva för att hindra amerikanska underrättelsetjänsters möjlighet att få åtkomst till personuppgifterna eller gör sådan åtkomst verkningslös.

Mot denna bakgrund finner IMY att varken standardavtalsklausuler eller de övriga åtgärder som Tele2 åberopat kan ge sådant stöd för överföringen som anges i kapitel V i dataskyddsförordningen.

I och med denna överföring av uppgifter undergräver Tele2 därför den skyddsnivå för personuppgifter för registrerade som garanteras i artikel 44 i dataskyddsförordningen.

IMY konstaterar därför att Tele2 Sverige AB bröt mot artikel 44 i dataskyddsförordningen i vart fall under perioden den 14 augusti 2020 till och med maj 2023.

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.

EDPB har antagit riktlinjer om beräkning av administrativa sanktionsavgifter enligt dataskyddsförordningen som syftar till att skapa en harmoniserad metod och principer för beräkning av sanktionsavgifter.[28]

3.2 Ska sanktionsavgift påföras?

IMY har ovan funnit att de överföringar av personuppgifter till USA som sker via Google Analytics-verktyget och som Tele2 är ansvarigt för strider mot artikel 44 i dataskyddsförordningen. Överträdelser av den bestämmelsen kan enligt artikel 83 föranleda sanktionsavgifter.

Mot bakgrund bland annat av att Tele2 överfört en stor mängd personuppgifter, att behandlingen pågått under en lång tid samt att överföringen inneburit att personuppgifterna inte kunnat garanteras den skyddsnivå som ges i EU/EES är det inte fråga om en mindre överträdelse. Tele2 ska därför påföras en sanktionsavgift för den konstaterade överträdelsen.

3.2.1 Till vilket belopp ska sanktionsavgiften bestämmas?

Vid bestämmande av maxbeloppet för en sanktionsavgift som ska påföras ett företag ska den definition av begreppet företag användas som EU-domstolen använder vid tillämpning av artiklarna 101 och 102 i EUF-fördraget (se skäl 150 i dataskyddsförordningen). Av domstolens praxis framgår att detta omfattar varje enhet som utövar ekonomisk verksamhet, oavsett enhetens rättsliga form och sättet för dess finansiering samt även om enheten i juridisk mening består av flera fysiska eller juridiska personer.[29]

Enligt artikel 83.5 c i dataskyddsförordningen ska det vid överträdelse av bland annat 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.

IMY bedömer att det företags omsättning som ska läggas till grund för beräkning av den administrativa sanktionsavgiften är Tele2 Sverige AB:s årsredovisning för år 2022. Bolaget omsatte cirka 28 102 000 000 kronor under det budgetåret. Det högsta sanktionsbelopp som kan fastställas i ärendet är fyra procent av detta belopp, det vill säga cirka 1 124 080 000 kronor.

Vid bestämmande av sanktionsavgiftens storlek ska IMY med hänsyn till överträdelsen allvar och med beaktande av både försvårande och förmildrande omständigheter

[28] EDPB:s riktlinjer 8/2020 Guidelines 04/2022 on the calculation of administrative fines under the GDPR (antagna för publik konsultation den 12 maj 2022).
[29] Se Dom i Akzo Nobel, C-516/15, EU:C:2017:314, punkt. 48

bestämma ett administrativt sanktionsbelopp som i det enskilda fallet är effektiv, proportionell och avskräckande.

IMY bedömer att följande faktorer har betydelse för bedömningen av överträdelsens allvarlighet.

När det gäller bedömningen av överträdelsens allvarlighetsgrad finns det till en början faktorer som medför att de finns skäl att se allvarligare på överträdelsen. Tele2 har överfört en stor mängd personuppgifter till tredjeland. Överföringen har inneburit att personuppgifterna inte har kunnat garanteras den skyddsnivå som ges i EU/EES vilket i sig är en allvarlig överträdelse. Därtill är det försvårande att överföringen av personuppgifter har pågått under en längre tid, dvs. från och med den 14 augusti 2020 och pågår fortfarande, och att de har skett systematiskt. IMY beaktar även att det nu har förflutit cirka 3 år sedan EU-domstolen genom dom den 16 juli 2020 underkände kommissionens beslut om adekvat skyddsnivå i USA[30] varigenom förutsättningarna för överföringar av personuppgifter till USA förändrades.

EDPB har under den tiden lämnat rekommendationer om konsekvenserna av domen som varit ute för publik konsultation den 10 november 2020 och antagits i slutlig form den 18 juni 2021. Dessutom har flera andra tillsynsmyndigheter inom EU/EES meddelat förelägganden om att upphöra med användningen av Verktyget tills tillräckligt effektiva säkerhetsskyddsåtgärder har vidtagits av de personuppgiftsansvariga. Besluten har omfattat fall där de personuppgiftsansvariga även har vidtagit åtgärder såsom ”anonymisering av IP-adresser” i form av trunkering.[31]

Trots att dessa rekommendationer och beslut tydligt pekar på riskerna med och svårigheterna att säkerställa en tillräcklig skyddsnivå för uppgiftsöverföringar till företag i USA har Tele2 har fortsatt att använda Verktyget under perioden den 14 augusti 2020 till och med i vart fall maj 2023 utan att vidta egna ytterligare skyddsåtgärder. Googles åtgärd avseende trunkering[32] av IP-adress innebär att det fortfarande går att särskilja IP-adressen, eftersom den kan sammankopplas med övriga överförda uppgifter till tredjeland (till USA). Därigenom möjliggörs identifiering vilket medför att uppgifterna tillsammans utgör personuppgifter.

Tele2 är en av de stora aktörerna inom telekombranschen i Sverige. Det rör sig om uppgifter om ett stort antal registrerade som kan identifieras indirekt och vars uppgifter kan sammankopplas med andra uppgifter om dem. När det gäller uppgifternas beskaffenhet följer redan av Tele2s eget syfte med behandlingen – dvs. att bland annat kunna dra slutsatser om hur de registrerade navigerar på och hittar till Webbplatsen, att uppgifterna sammantagna – gör det möjligt att dra förhållandevis precisa slutsatser om privatlivet för de registrerade och kartlägga dem, såsom beträffande vad de köper och vilka tjänster de är intresserad av över tid och inneha hos bolaget. Tele2s behandling av personuppgifter medför risker för allvarlig kränkning

[30] 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.
[31] Österrikes tillsynsmyndighet (Datenschultzbehörde) beslut av den 22 april 2022 avseende klagomål Google Analytics representerad av NOYB med lokalt ärendenummer 1354838270, Frankrikes tillsynsmyndighet (CNIL) beslut av den 10 februari 2022 representerad av NOYB och Italiens tillsynsmyndighet (Garante) beslut av den 9 juni 2022 avseende klagomål Google Analytics representerad av NOYB, lokalt ärendenummer 9782890.
[32] Trunkering av IP-adress ”anonymisering 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 (till USA).

av enskildas fri- och rättigheter vilket ger Tele2s ett särskilt ansvar som innebär höga krav vid överföringar till tredjeland, där IMY sammantaget bedömer att Tele2 inte har visat att bolaget gjort en tillräcklig analys och kartläggning och inte heller har vidtagit nödvändiga säkerhetsåtgärder för att begränsa riskerna för de registrerade.

IMY konstaterar samtidigt att det finns faktorer som talar i motsatt riktning. IMY beaktar 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. IMY beaktar även att Tele2 vidtagit vissa, om än otillräckliga, åtgärder för att begränsa de personuppgifter som överfördes genom att aktivera ”anonymisering av IP-adresser” genom trunkering.[33] Tele2 har gjort en analys och kartläggning av livscykeln för personuppgifter i Verktyget. Även detta förhållande beaktas vid bedömningen av överträdelsernas allvar.

Sammantaget bedömer IMY, mot bakgrund av de redovisade omständigheterna, att de aktuella överträdelserna är av låg allvarlighetsgrad. Utgångspunkten för beräkningen av sanktionsavgiften bör därför sättas lågt i förhållande till det aktuella maxbeloppet.

Utöver bedömningen av överträdelsens allvar ska IMY bedöma om det föreligger några försvårande eller förmildrande omständigheter som får betydelse för sanktionsavgiftens storlek. IMY bedömer att det saknas ytterligare försvårande eller förmildrande omständigheter, utöver de som beaktas vid bedömningen av allvarlighetsgraden, som påverkar sanktionsavgiftens storlek.

Utifrån en samlad bedömning av nämnda omständigheter, den höga omsättningen i förhållande till de konstaterade överträdelserna och mot bakgrund av att den administrativa sanktionsavgiften ska vara effektiv, proportionerlig och avskräckande bedömer IMY att sanktionsavgiften kan stanna vid 12 000 000 (tolv miljoner) kronor.

_____

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)

Bilaga
Bilaga 1 – Information om betalning av sanktionsavgift

[33] Österrikes tillsynsmyndighet (Datenschultzbehörde) beslut av den 22 april 2022 avseende klagomål Google Analytics representerad av NOYB med lokalt ärendenummer 1354838270, Frankrikes tillsynsmyndighet (CNIL) beslut av den 10 februari 2022 representerad av NOYB och Italiens tillsynsmyndighet (Garante) beslut av den 9 juni 2022 avseende klagomål Google Analytics representerad av NOYB, lokalt ärendenummer 9782890.

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.