

Coop Sverige AB
Englundavägen 4
17188 Solna

Diarienummer:
DI-2020-11368

Datum:
2023-06-30

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

Innehåll

Integritetsskyddsmyndighetens beslut.....	2
1 Redogörelse för tillsynsärendet	3
1.1 Handläggningen.....	3
1.2 Vad som anges i klagomålet.....	3
1.3 Vad Coop har uppgett.....	4
1.3.1 Vem som har implementerat Verktuget och i vilket syfte m.m.	4
1.3.2 Mottagare av uppgifterna	5
1.3.3 De uppgifter som behandlas i Verktuget och vad som utgör personuppgifter	5
1.3.4 Kategorier av personer som berörs av behandlingen	5
1.3.5 När koden för Verktuget exekveras och Mottagare bereds tillgång .	5
1.3.6 Hur länge de personuppgifter som behandlas lagras	5
1.3.7 Vilka länder personuppgifterna behandlas i	6
1.3.8 Coops relation till Google LCC.....	6
1.3.9 Säkerställande av att behandlingen inte sker för Mottagarnas egna ändamål	6
1.3.10 Beskrivning av Coops användning av Verktuget.....	6
1.3.11 Egna kontroller av överföringar som berörs av domen Schrems II	7
1.3.12 Överföringsverktyg enligt kapitel V i dataskyddsförordningen	8
1.3.13 Kontroll av hinder för fullgörande i lagstiftning i tredjeland.....	8
1.3.14 Vidtagna ytterligare skyddsåtgärder utöver de som Google vidtagit	8
1.4 Vad Google LCC har uppgett.....	10
2. Motivering av beslutet	11

Postadress:
Box 8114
104 20 Stockholm

Webbplats:
www.imy.se

E-post:
imy@imy.se

Telefon:
08-657 61 00

2.1 Ramen för granskningen.....	11
2.2 Det är fråga om behandling av personuppgifter.....	11
2.2.1 Tillämpliga bestämmelser m.m.	11
2.2.2 Integritetsskyddsmyndighetens bedömning	13
2.3 Coop är personuppgiftsansvarig för behandlingen	15
2.4 Överföring av personuppgifter till tredjeland	15
2.4.1 Tillämpliga bestämmelser m.m.	16
2.4.2 Integritetsskyddsmyndighetens bedömning	18
3 Val av ingripande	21
3.1 Rättslig reglering	21
3.2 Ska sanktionsavgift påföras?	21
3.3 Andra ingripanden.....	22
4 Överklagandehänvisning	23
4.1 Hur man överklagar	23

Integritetsskyddsmyndighetens beslut

Integritetsskyddsmyndigheten konstaterar att Coop Sverige Aktiebolag behandlar personuppgifter i strid med artikel 44 i dataskyddsförordningen¹ 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.coop.se, och därigenom överföra personuppgifter till tredjeland utan att villkoren enligt kapitel V i förordningen är uppfyllda.

Integritetsskyddsmyndigheten förelägger Coop Sverige Aktiebolag med stöd av artikel 58.2 d i dataskyddsförordningen att se till att bolagets behandling av personuppgifter inom ramen för Coop Sverige Aktiebolags användning av verktyget Google Analytics överensstämmer med artikel 44 och övriga bestämmelser i kapitel V. Detta ska särskilt ske genom att Coop Sverige 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 Coop Sverige AB (nedan "Coop" 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.coop.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.

1.2 Vad som anges i klagomålet

Av klagomålet framgår i huvudsak följande.

Den 14 augusti 2020 besökte klaganden Coops 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.

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).

bolagets) räkning. Google LLC ska därför enligt ovan nämnda villkor klassificeras som bolagets personuppgiftsbiträde.

Under klagandens besök på bolagets webbplats behandlades klagandens personuppgifter av Coop, åtminstone klagandens IP-adress och uppgifter insamlade genom kakor. En del av uppgifterna som samlades in, överfördes till Google. I enlighet med punkt 10 i villkoren om behandling av personuppgifter för Googles reklamprodukter, har Coop 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.

1.3 Vad Coop har uppgett

Coop Sverige AB har i huvudsak uppgett följande.

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

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

Syftet med Coops användning av Verkttyget är att uppfylla ändamålet att utveckla och förbättra Coops verksamhet, produkter och tjänster. Verkttyget används exempelvis för att analysera och utvärdera (i) hur registrerade användare använder coop.se, (ii) Coops kundpersonalisering på coop.se och (iii) Coops annonskampanjer. Baserat på de insikter som Verkttyget ger kan Coop ta beslut om åtgärder som förbättrar och optimerar Coops produkter, tjänster (t.ex. funktioner som erbjuds på coop.se samt deras placering eller personifiering på coop.se) och marknadsföring eller ta beslut om att nya produkter eller tjänster ska tas fram. För detta syfte är det nödvändigt att behålla relevanta unika identifierare för de analyser som utförs i syfte att skapa tillförlitliga och verifierbara resultat.

Verkttyget används för att skapa analyser och rapporter som underlättar beslutsfattande kopplat till ändamålen 1) ge en personlig upplevelse i Coops digitala kanaler och 2) marknadsföring och kommunikation i Coops och i tredje parts digitala kanaler.

² EU-domstolens dom Facebook Ireland och Schrems (Schrems II), C-311/18, EU:C:2020:559.

Coops ändamål med Verkytet kan uppfyllas även med implementeringen av en s.k. server side containern, som innebär att besökarens IP-adress inte ska skickas till Verkytet (se nedan). Coop behöver inte IP-adresser som identifierare för att uppfylla ändamålet med Verkytet. Syftet med Verkytet är att skapa rapporter till beslutsunderlag för ändamålet *utveckla och förbättra Coops verksamhet, produkter och tjänster*. Exempel på information som behövs i dessa rapporter. Kan vara vilka exponeringar som leder till ett köp i syfte att kunna utvärdera deras effektivitet, t.ex. produktvisningar, receptvisningar eller kampanjer. I detta sammanhang är det därför mätningen, inte IP-adressen, som är avgörande för om syftet med Verkytet kan uppfyllas.

Coops kunder finns på den svenska marknaden och Coop riktar sig endast mot den svenska marknaden. Praktiska skäl och förbudet avseende diskriminering av konsumenter, och i vissa fall även näringsidkare, enligt geoblockeringsförordningen³ gör dock att det inte sker någon begränsning av vem som kan besöka Coops webbplats. Coop analyserar inte särskilt från vilka länder trafik till webbplatsen kommer .

1.3.2 Mottagare av uppgifterna

Inom ramen för Coops användning av Verkytet på Webbplatsen lämnas personuppgifter ut till ett antal aktörer, vilka samtliga är personuppgiftsbiträden eller underbiträden till Coop, inbegripet Google LLC, Google Ireland Ltd och deras underbiträden.

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

Inom ramen för Coops användning av Verkytet på Webbplatsen behandlar bolaget och dess personuppgiftsbiträden (Mottagarna) nedan angivna uppgifter.

1. Användarbeteende på webbplatsen utifrån värden som skickas in via variabler på webbplatsen (t.ex. filterCombination, Page title, Referrer eller storeName).
2. Enhetsinformation (t.ex. flashVersion, javaEnabled, språk eller färgval på skärmen).
3. Kundstatus (dvs. om användaren besöker Coops webbplats i inloggat eller utloggat läge eller som företagskund).
4. Onlineidentifierare (t.ex. IP-adress, userID, transactionID, clientID, gclid, dclid eller Device ID).
5. Transaktionsdata utifrån värden som skickas in via variabler på webbplatsen (såsom antalKop, Transaction - dimension50 (boughtRecipe), Transaction - dimension7 (deliveryMethod), orderID eller deliveryTime).

1.3.4 Kategorier av personer som berörs av behandlingen

De kategorier av personer som berörs av behandlingen är besökare, privatkunder (icke medlem med konto), företagskunder och medlemmar i Coop Medlem.

Verkytet är inte uppsatt och används inte för att behandla särskilda kategorier av personuppgifter eller personuppgifter om särskilt utsatta personer.

³ Europaparlamentets och rådets förordning (EU) 2018/302 av den 28 februari 2018 om åtgärder mot omotiverad geoblockering och andra former av diskriminering på grund av kunders nationalitet, bosättningsort eller etableringsort på den inre marknaden.

1.3.5 När koden för Verkytget exekveras och Mottagare bereds tillgång

När en användare har gjort sina samtyckesval kommer användarens personuppgifter, i varierande omfattning, att skickas till Verkytget. Innehållet integreras och körs efter att villkor i Coops samtyckeshanterare är uppfyllda.

1.3.6 Hur länge de personuppgifter som behandlas lagras

De personuppgifter som behandlas i Verkytget lagras som längst i 38 månader och raderas därefter.

1.3.7 Vilka länder personuppgifterna behandlas i

Personuppgifterna behandlas bland annat i USA.

1.3.8 Coops relation till Google LCC

Coop köper licensen för Verkytget genom en återförsäljare som utgör Coops personuppgiftsbiträde. Coop och personuppgiftsbiträdet har ingått ett personuppgiftsbiträdesavtal som reglerar uppsättning och administration av Verkytget. Personuppgiftsbiträdet administrerar i sin tur självständigt samtliga förhållanden i förhållande till Google. Exempelvis hanterar personuppgiftsbiträdet hela uppsättningen av Verkytget, ersättning för tjänsten samt kontakter med Google avseende support. Google agerar med andra ord uteslutande på instruktioner från Coops personuppgiftsbiträde.

Google tillämpar vidare avtalsvillkor mellan sig och återförsäljaren som reglerar Googles personuppgiftsbehandling som personuppgiftsbiträde i förhållande till återförsäljaren varvid återförsäljaren är Coops personuppgiftsbiträde. Google blir därigenom Coops underbiträde. Denna syn på rollfördelningen överensstämmer med Coops personuppgiftsbiträdes och Googles syn. Utöver detta är de inställningar som möjliggör användning av personuppgifter i Verkytget för Googles egna ändamål inaktiverade.

Mot bakgrund av (i) att Coops personuppgiftsbiträde agerar i enlighet med Coops instruktioner, (ii) hur avtalsstrukturen ser ut och hur de inblandade parterna ser på rollfördelningen samt (iii) att datadelning för Googles egna ändamål är inaktiverat är Coops bedömning att Google utgör ett underbiträde till Coop kopplat till personuppgiftsbehandling i Verkytget.

1.3.9 Säkerställande av att behandlingen inte sker för Mottagarnas egna ändamål

Coop lämnar ut personuppgifterna till sina personuppgiftsbiträden. Coop har ingått personuppgiftsbiträdesavtal med dessa. I avtalen finns punkter som rör Coops rätt till revision/audit genom vilka Coop kan kontrollera att personuppgiftsbiträdet inte behandlar personuppgifter för egna ändamål eller för tredje parts ändamål.

Som en del av sitt arbete med dataskyddsförordningen tillämpar Coop en rutin för att säkerställa regelefterlevnad. Rutinen innefattar ett årshjul vars syfte är att säkra god regelefterlevnad över tid. Årshjulet är indelat i fyra delar där uppföljning av biträdesrelationer ingår i den tredje delen. Inom ramen för uppföljningsarbetet enligt årshjulet finns möjlighet att säkerställa att personuppgiftsbiträden endast behandlar personuppgifter på Coops vägnar.

I samband med arbetet gällande implementation av samtyckeshanteraren har därtill ytterligare åtgärder vidtagits för att säkerställa att Coop inte tillåter att Mottagare behandlar personuppgifter tillhörande Coops besökare, kunder och medlemmar för

sina egna ändamål. Det finns rutiner som anger att varje ansvarig medarbetare ska säkerställa att ingen delning av personuppgifter sker genom lösningar i tjänsten.

1.3.10 Beskrivning av Coops användning av Verktyget

Coop skickar olika identifierare via den mätning som satts upp på bolagets webbplats. Gemensamt för alla identifierare är att dessa är unika för de registrerades interaktioner relaterat till webbplatsen www.coop.se. En registrerad tillskrivs med andra ord inte en och samma identifierare som gäller för andra webbplatser än Coops webbplats.

Exemplet nedan beskriver en rapport där Coop vill förstå vilka produkter som är populära att handla online och hur dessa har exponerats för kunden på Coops webbplats. När kunden genomför sitt köp i Coops e-handel skickas följande information till Verktyget (på devisen variabel, beskrivning och exempel på värde):

- Id - Produktens ID – 3600542020855
- Variant – Storlek på förpackningen (tex 200 g etc.) – undefined
- Price – Produktens pris – 26.5
- List – Produkterna på sajt presenteras i en produktlista som kan ha olika namn, t.ex. produktsök, Sajt-sök, Sök-dropdown – produktsök
- listPosition – Vilken plats listan har bland andra produktlistor (från 0 och uppåt) – 0
- position – Vilken plats produkten har i produktlistan (från 0 och uppåt) – 0
- name – Produktnamn – Balsam Goodbye Damage
- brand – Varumärke – Fructis
- category – Produkt kategori område – Skönhet & Hygien -Hårvård - Balsam

De identifierare som överförs är följande:

1. *clientID* – används för att kunna avgöra om en registrerad är ny eller återkommande. Nya *clientID* genereras om en registrerad rensat sina cookies och går in på webbplatsen igen.
2. *userID* – genereras för registrerade med inloggningskonto på coop.se och används för att avgöra om en registrerad har ett inloggningskonto eller inte.
3. *gclid* och *dclid* – genereras för varje unikt annonsklick. Syftet är att kunna attribuera ett klick till en specifik annons för att exempelvis kunna få aggregerad information om hur många gånger annonsen har visats eller hur många som har interagerat med den.
4. *transactionID* – genereras i samband med ett köp på coop.se och motsvarar ett ordernummer.

Baserat på informationen, som anges ovan, kan Coop bland annat dra slutsatser kring populära produkter som leder till köp, hur kundresan startade samt vilken typ av registrerad som genomförde köpet (t.ex. ny eller återkommande medlem/kund eller medlem/kund med inloggningskonto). Dessa slutsatser är inte beroende av att registrerades publika IP-adresser skickas till Verktyget och syftet kan därmed uppfyllas oavsett av om publika IP-adresser skickas eller inte.

Mot bakgrund av implementeringen av server side-containern önskar Coop även förtydliga att registrerades IP-adresser endast behandlas genom följande behandlingar: 1) insamling på bolagets webbplats, 2) överföring till server side containern och 3) konvertering av de unika IP-adresserna till en generisk IP-adress för

server side containern. Insamling, överföring och konvertering sker i realtid och inga publika IP-adresser lagras.

1.3.11 Egna kontroller av överföringar som berörs av domen Schrems II

Mot bakgrund av domen Schrems II har Coop genomfört ett arbete med att se över sina tredjelandsöverföringar. Coop har under hösten 2021 även utfört en revision av Verktyget där Coop har kunnat konstatera att internationella dataöverföringar sker genom användning av Verktyget. Som en del av detta arbete har det vidtagits löpande åtgärder för att ytterligare höja integritetsskyddet relaterat till de registrerade vars personuppgifter berörs.

1.3.12 Överföringsverktyg enligt kapitel V i dataskyddsförordningen

Överföringar till tredjeland sker med stöd av EU-kommissionens standardavtalsklausuler (personuppgiftsbiträden), vilka finns inkorporerade i det avtal som ingåtts mellan Google och Coops personuppgiftsbiträde. Enligt avtalet utgör Coops personuppgiftsbiträde exportör av personuppgifterna till Verktyget.

Coop stödjer uppgiftsöverföringarna till USA på standardavtalsklausulerna för överföring av personuppgifter till personuppgiftsbiträden i tredjeland. Standardavtalsklausulerna har i detta fall ingåtts mellan Google LLC och bolagets personuppgiftsbiträde. I sammanhanget kan nämnas att Google tillhandahåller standardiserade tjänster och erbjuder inte sina kunder möjligheten att förhandla villkoren för sina tjänster. Eftersom det rör sig om villkor som inte är föremål för förhandling finns inga undertecknade kopior att tillgå. Coop har istället bifogat de databehandlingsvillkor vari standardavtalsklausulerna har inkorporerats och som gäller i enlighet med det avtal som ingåtts av Coops personuppgiftsbiträde.

Coop vidtar åtgärder för att säkerställa att de befintliga standardavtalsklausulerna alltid är uppdaterade enligt EU-kommissionens senaste version av standardavtalsklausuler.

1.3.13 Kontroll av hinder för fullgörande i lagstiftning i tredjeland

Kontroll av hinder i tredjelands lagstiftning ligger inom ramen för Coops arbete med att se över sina tredjelandsöverföringar. Coop har dock noterat den kritik som EU-domstolen har riktat mot amerikansk lagstiftning och tar hänsyn till denna i valet av kompletterande skyddsåtgärder.

1.3.14 Vidtagna ytterligare skyddsåtgärder utöver de som Google vidtagit

Genomförande av ytterligare skyddsåtgärder ligger inom ramen för Coops arbete med att se över sina tredjelandsöverföringar. Enligt uppgifter från Google, tillhandahålls flera säkerhetsåtgärder som Google bedömer utgör sådana ytterligare skyddsåtgärder som kan vidtas tillsammans med standardavtalsklausulerna.

Coop har även genomfört ett arbete med att inrätta en s.k. server side container, i syfte att utöka kontrollen över på vilket sätt data skickas till Verktyget.

Coop anser att Googles avtalsrättsliga och organisatoriska åtgärder får anses minimera den faktiska risken för att utlämnande av personuppgifter till tredjeland i slutändan äger rum. Av Googles Transparency Report, Global requests for user information, framgår dock att Googles löpande får förfrågningar från amerikanska myndigheter om vad som gäller vid åtkomst till personuppgifter som Google lagrar. Coops bedömning är att den reella risken för att uppgifter lämnas ut till amerikansk underrättelsetjänst är liten. Den går dock inte att eliminera genom vare sig åtgärder som Google eller Coop vidtar.

Vidare bedömer Coop att de kompletterande åtgärderna som vidtagit för att minimera övervakningsmöjligheterna också stärker Coops kunders fri-och rättigheter genom att dessa inte kan identifieras genom de uppgifter som överförs.

Sammanfattningsvis är det genom dessa åtgärder endast en och samma generiska IP-adress som överförs till Verktyget, oavsett vilken den registrerades unika IP-adress är. Coop har även aktiverat funktionen i Verktyget för så kallad IP-anonymisering, men mot bakgrund av server side containern är denna åtgärd enligt bolaget överflödigt.

1.3.14.1 Allmänt om server side container

En server side container implementeras i allmänhet för att antingen förbättra 1) webbplatsens prestanda eller 2) säkerhet. När det gäller prestanda kan färre taggar användas relaterat till den mätning som sätts upp på Webbplatsen, vilket betyder mindre kod på klient-sidan och exempelvis att webbplatsen kan laddas snabbare.

När det gäller säkerhet kan besökarens data bättre skyddas och webbplatsägaren behåller större kontroll över data som samlas in och distribueras i en miljö som kontrolleras av webbplatsägaren. När data först skickas till en molnbaserad lösning kan denna behandlas och vidare distribueras med taggar som webbplatsägaren kontrollerar.

1.3.14.2 Coops implementering av server side container

Syftet med den server side container som Coop har implementerat är att förbättra säkerheten relaterat till de data som skickas. Mer specifikt är syftet att på ett bra och säkert sätt kunna värna om de registrerades personliga integritet. Server side containern fungerar som en proxy mellan de registrerades webbläsare och Verktyget där Coop har valt att implementera server side containern på ett sätt som gör att de registrerades webbläsares publika IP-adress aldrig överförs till Verktyget.

Implementering kan beskrivas på följande sätt. En registrerad besöker webbplatsen www.coop.se i sin webbläsare. Google Analytics-scriptet laddas ner från server side containern istället för att laddas ner direkt från Google Analytics servrar. Detta resulterar i att den registrerades IP-adress samt information om användarbeteende, enhetsinformation, kundstatus, onlineidentifierare och transaktionsdata (enligt punkterna 1–5 ovan under avsnitt 1.3.10) överförs till server side containern, istället för direkt till Google Analytics. När Google Analytics-scriptet har laddats ner från server side containern sker ett nytt anrop från server side containern till Google Analytics servrar. Eftersom anropet sker från server side containern sker ingen överföring av den registrerades publika IP-adress till Google Analytics. Coop har konfigurerat server side containern på ett sätt som gör att alla data enligt ovan, förutom den registrerades publika IP-adress, passerar genom server side containern till Google Analytics. Google Analytics tar emot data som skickas från server side containern och den data (information) som har skickats publiceras i rapporter genom den mätning som satts upp på webbplatsen www.coop.se.

Behandlingarna som sker genom de ovan nämnda – dvs. att ta emot, konvertera och skicka vidare anropet – sker i arbetsminnet hos server side containern. Det betyder att all behandling sker i realtid och att ingen data lagras beständigt. Med andra ord lagras inte registrerades publika IP-adresser i server side containern och de exponeras inte heller mot Google Analytics servrar. All kommunikation från webbläsaren, via server side containern, till Verktyget är därtill krypterad.

Denna process går inte att reversera då informationen inte lagras och konverteringen inte baseras på ett ett-till-ett-förhållande som möjliggör användningen av en "nyckel" för att återskapa de publika IP-adresserna.

Coop har aktiverat Googles funktion för IP-anonymisering. Den innebär att den IP-adress som skickas till Verktuget trunkeras. Detta sker genom att Google tar bort en del av IP-adressen innan IP-adressen lagras på disk. För en IPv4 adress ersätts sista oktetten i adressen med en nolla. För en Ipv6 adress ersätts de sista 80 bitarna med nollor. Åtgärden går inte att reversera men eftersom denna åtgärd görs av Google i Verktuget har Coop även valt att implementera en server side container.

I Coops fall är funktionen IP-anonymisering aktiverad och tillämpas på den generiska IP-adress som skickas via server side containern. I sammanhanget är funktionen dock överflödig med hänsyn till att server side containern hindrar de registrerade publika IP-adresser från att skickas till Verktuget. Coops bedömning är att server side containern som åtgärd är en tillräcklig skyddsåtgärd, men att det inte skadar att även ha funktionen IP-anonymisering aktiverad i Verktuget.

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. Coop har beretts tillfälle att yttra sig över Googles LLC:s yttrande. Av Google LLC:s yttrande framgår följande om Verktuget.

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 Verktuget, som består av att samla in information relaterad till anropet på olika sätt och skickar informationen till Verktugets servrar.

En webbplatsansvarig som integrerat Verktuget 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 Verktuget kan göra olika inställningar, exempelvis avseende lagringstid. Verktuget 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 besöksstrafik eller avsaknad av trafik. Verktuget 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 Verktuget 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. Verktuget lagrar och läser cookies i besökarens webbläsare för att utvärdera besökarens session och annan information om anropet. Genom dessa cookies möjliggör Verktuget identifiering av unika användare (UUID) över surf-sessioner, men Verktuget kan inte identifiera unika användare i olika webbläsare eller enheter. Om en webbplatsägares webbplats har ett eget autentiseringsystem

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 Coop 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 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 lokaliseringssuppgift 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 knutna 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

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.

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 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 Verktuget utgör personuppgifter ska IMY ta ställning till om Google eller Coop genom implementeringen av Verktuget 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 Coop implementerat Verktuget 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 Coops (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. Den generiska IP-adress som skapats av Coops implementering av en s.k. server side container.

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

⁶ EU-domstolens dom Breyer, C-582/14, EU:C:2016:779, punkt 45–46.

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.

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 Coop 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. Coops åtgärd avseende den generiska IP-adress som skapats av Coops implementering av en s.k. server side container förhindrar överföring av IP-adress till tredjeland däremot möjliggörs fortfarande identifiering hos Coop, vilket i sig är tillräckligt för att uppgifterna tillsammans ska utgöra personuppgifter.

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.

IMY konstaterar att det även kan finnas skäl att jämföra IP-adresser (även generiska) 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.¹⁰

Dessutom har klagandens personuppgifter behandlats den 14 augusti 2020, genom att klaganden har varit inloggad på sitt Google-konto vid besöket på Webbplatsen, därigenom har 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 generiska IP-adresserna samt möjligheten att kombinera dessa med ytterligare uppgifter, att Coop:s användning av Verktyget på en webbsida innebär att personuppgifter behandlas.

2.3 Coop 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).

De svar som Coop lämnar visar att bolaget har fattat beslutet att implementera Verktyget på Webbplatsen. Vidare framgår att Coops 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 Coop genom att besluta att implementera Verktyget på webbplatsen i nämnda syfte har fastställt ändamålen och medlen med insamlingen och den

¹⁰ 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.

efterföljande överföringen av dessa personuppgifter. Coop 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 Coops överföring av personuppgifter till USA är förenlig med artikel 44 i dataskyddsförordningen och har stöd av ett överföringsverktyg 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 överförs 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.¹¹ 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*

¹¹ 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 sköden för skydd av privatlivet i Europeiska unionen och Förenta staterna.

fallet när lagstiftningen i det tredjelandet tillåter att myndigheterna i detta tredjeland gör ingrepp i de registrerade personernas rättigheter avseende dessa uppgifter.”¹²

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”.¹³

I Europeiska dataskyddsstyrelsens (EDPB) rekommendationer om följderna av domen¹⁴ 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”*.¹⁵

Av EDPB:s rekommendationer framgår att sådana ytterligare skyddsåtgärder kan delas in i tre kategorier: avtalsmässiga, organisatoriska och tekniska.¹⁶

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 [...]”*.¹⁷

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*

¹² Punkt 125-126.

¹³ Punkt 133, IMY:s.

¹⁴ 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”).

¹⁵ EDPB:s Rekommendationer 01/2020, punkt 75. IMY:s översättning.

¹⁶ EDPB:s Rekommendationer 01/2020, punkt 52.

¹⁷ 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".¹⁸

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".¹⁹ 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".²⁰

2.4.2 Integritetsskyddsmyndighetens bedömning

2.4.2.1 Tillämpligt överföringsverktyg

Av utredningen framgår att Coop 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 beslut av den 4 juni 2021 (2021/914/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 dock 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 nämligen, 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.

¹⁸ EDPB:s Rekommendationer 01/2020, punkt 128; IMY:s översättning.

¹⁹ EDPB:s Rekommendationer 01/2020, punkt 77; IMY:s översättning.

²⁰ EDPB:s Rekommendationer 01/2020, punkt 79; IMY:s översättning

EU-domstolen konstaterade därvid 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.²¹

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 Coop

Nästa fråga är om Coop vidtagit tillräckliga ytterligare skyddsåtgärder.

Som personuppgiftsansvarig och exportör av personuppgifterna är Coop 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 (Coop) 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 dessa åtgärder.

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

När det gäller de *avtalsmässiga och organisatoriska åtgärderna* kan konstateras att varken information till användare av Verktyget (såsom Coop),²² 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 oklart hur Google LLC:s "*noggranna prövning av varje begäran*" om "lagligheten" av sådana begäranden är effektiv som ytterligare skyddsåtgärd, med hänsyn till att även lagenliga rättsliga begäranden från amerikanska underrättelsetjänster enligt EU-domstolen inte är förenliga med kraven i EU:s dataskyddsregler.

När det gäller de *tekniska åtgärderna* som vidtagits kan konstateras att varken Google LLC eller bolaget 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.

²¹ Punkt 184 och 192. Punkt 259 och efterföljande.

²² Oavsett om en sådan anmälan ens skulle vara tillåten enligt amerikansk lagstiftning.

När det gäller krypteringsteknik – t.ex. 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.²³ 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 anför 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 trunkering²⁴ 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 Coop:s egna ytterligare skyddsåtgärder

Coop har uppgett att bolaget har vidtagit ytterligare skyddsåtgärder utöver de åtgärder som Google (trunkering²⁵ av sista oktetten när uppmätt data överförs) har vidtagit. Dessa består enligt bolaget av en s.k. server side container, som inrättats i syfte att utöka kontrollen över på vilket sätt data skickas till Verktyget och innebär att det endast är en och samma generiska IP-adress som överförs till Verktyget, oavsett vilken den registrerades unika IP-adress är.

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

IMY konstaterar att Coop även överför ett antal andra unika identifierare (clientID, userID, gclid och dclid samt transactionID),²⁶ vars syfte är att kunna särskilja den klagande hos Google. Den s.k. server side container innebär att IP-nummer, efter att IP-adressen som har samlats in av Coop (men innan överföringen till Google), ersatts med ett generiskt IP-nummer som är lika för alla besökare på Coops webbplats. De

²³ Se EDPB:s Rekommendationer 01/2020, punkt 81.

²⁴ 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).

²⁵ 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. Maskning av sista oktetten (Googles åtgärd) är inte en ytterligare integritetshöjande åtgärd än server side container, då denna åtgärd endast maskerar sista oktetten av en redan anonymiserad IP-adress.

unika identifierarna (clientID, userID, gclid och dclid samt transactionID) överförs även via s.k. server side container (och IP-anonymiseringen), men överförs i oförändrad form dvs. i klartext, som innebär att dessa uppgifter går att utskiljas och därmed kan sammankopplas. IMY konstaterar, eftersom det går att sammankoppla de överförda uppgifterna till andra uppgifter som också överförs till Google LLC, att de ytterligare skyddsåtgärderna inte är tillräckliga.

För att säkerställa effektiva skyddsåtgärder bör alla unika identifierare istället överföras i förändrad form (dvs. ej i klartext) som innebär att överförda uppgifter inte går att sammankoppla.

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 verkninglös.

2.4.2.3.3 *Integritetsskyddsmyndighetens slutsats*

Mot bakgrund av det ovan anförda finner IMY att Coop inte visat att något av de verktyg som anges i kapitel V i dataskyddsförordningen kan användas för att överföra personuppgifter om besökare på sin webbplats – särskilt unika identifierare, IP-adresser, webbläsardata och metadata – till Google LLC i USA.

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

IMY konstaterar därför att Coop Sverige AB bryter mot artikel 44 i dataskyddsförordningen.

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 Coop 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 Coop har överfört en stor mängd personuppgifter till tredjeland där uppgifterna inte kan garanteras den skydds nivå 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 skydds nivå i USA²⁷ 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.

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 Coop har gjort en analys av livscykeln för personuppgifter i Verktyget. Coop har även vidtagit åtgärder såsom en s.k. server side container, som inrättats i syfte att utöka kontrollen över på vilket sätt data skickas till Verktyget och som innebär att det endast är en och samma generiska IP-adress som överförs till Verktyget, oavsett vilken den registrerades unika IP-adress är. Bolaget har även aktiverat Googles åtgärd "anonymisering av IP-adresser" genom trunkering. Coop har således vidtagit omfattande tekniska åtgärder för att försöka begränsa riskerna för de registrerade och för att läka bristerna. Coop har därigenom också trots att de lyckats även om åtgärderna nu visat sig inte vara tillräckligt effektiva avseende att hindra amerikanska underrättelsetjänsters möjlighet att få åtkomst till uppgifterna eller för att göra sådan åtkomst verkningslös.

Vid en sammanvägd bedömning finner IMY att det finns anledning att i det här fallet avstå från att påföra Coop 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 av personuppgifter som åberopats av Coop 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 Coop föreläggas enligt artikel 58.2 d i dataskyddsförordningen att se till att bolagets behandling av

²⁷ 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 sköden för skydd av privatlivet i EU och Förenta staterna.

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 Coop 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.