Integritetsskydds myndigheten

CDON AB
Box 385
20123 Malmö

Diarienummer:
DI-2020-11397

Datum:
2023-06-30

Beslut efter tillsyn enligt dataskyddsförordningen - CDON AB:s överföring av personuppgifter till tredjeland

Innehåll

Postadress:
Box 8114
104 20 Stockholm

Webbplats:
www.imy.se

E-post:
imy@imy.se

Telefon:
08-657 61 00

Integritetsskyddsmyndighetens beslut

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

Integritetsskyddsmyndigheten förelägger med stöd av artikel 58.2 d i dataskyddsförordningen CDON AB att se till att bolagets behandling av personuppgifter inom ramen för bolagets användning av verktyget Google Analytics överensstämmer med artikel 44 och övriga bestämmelser i kapitel V. Detta ska särskilt ske genom att CDON AB ska upphöra 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.

IMY beslutar med stöd av artikel 58.2 och 83 i dataskyddsförordningen att CDON AB ska betala en administrativ sanktionsavgift på 300 000 (trehundra tusen) kronor för överträdelse av artikel 44 i dataskyddsförordningen.

1 Redogörelse för tillsynsärendet

1.1 Handläggningen

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

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

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

1.2 Vad som anges i klagomålet

I klagomålet anförs i huvudsak följande.

[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).

Den 14 augusti 2020 besökte klaganden CDON:s webbplats. Under besöket var klaganden inloggad på sitt Google-konto, som är kopplat till klagandens e-postadress. CDON 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. CDON) räkning och ska därför klassificeras som bolagets personuppgiftsbiträde.

Under besöket på bolagets webbplats behandlade CDON klagandens personuppgifter, åtminstone klagandens IP-adress och uppgifter insamlade genom kakor. En del av uppgifterna har överförts till Google. I enlighet med punkt 10 i villkoren om behandling av personuppgifter för Googles reklamprodukter, har CDON 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 enligt artikel 45 i dataskyddsförordningen för överföring av uppgifter till USA. CDON 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. CDON kan därför inte säkerställa ett lämpligt skydd av klagandens personuppgifter när dessa överförs till Google.

1.3 Vad CDON har uppgett

CDON AB har i yttranden den 15 januari 2021, den 15 februari 2022 och den 31 augusti 2022 i huvudsak uppgett följande.

1.3.1 Vem som har implementerat Verktyget och i vilket syfte m.m.
Koden för Verktyget var inbäddad på Webbplatsen vid tiden för klagomålet och är fortfarande inbäddad på Webbplatsen. Beslutet om att bädda in Verktyget på Webbplatsen fattades av CDON, ett bolag registrerat i Sverige. Data inhämtas från samtliga personer som besöker Webbplatsen, vilket sannolikt innefattar registrerade från mer än en EU/EES-medlemsstat.

CDON använder Verktyget i syfte att lära känna trafiken och använder Webbplatsen för att kunna fatta olika verksamhetskritiska beslut. Det är med hjälp av Verktyget t.ex. möjligt att ta reda på vilka produktkategorier som är mest populära och hur kunder navigerar, dels för att hitta till CDON, dels för att avsluta ett köp.

---

[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.

1.3.2 Mottagare av uppgifterna

Inom ramen för CDON:s användning av Verktyget på Webbplatsen lämnas personuppgifter endast ut till Google.

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

De uppgifter som behandlas inom ramen för CDON:s användande av Verktyget är olika egenskaper eller handlingar som besökaren vidtagit på webbplatsen, såsom:

1. Vilka element användaren sett när den navigerar och tittar runt på Webbplatsen,
2. Klickat på en Bild/Banner på Webbplatsen,
3. Lagt till eller tagit bort något i varukorgen,
4. Kommit till kassan eller slutfört ett köp,
5. Klickat på förslag på tillbehör på produktsidor eller lagt till något i önskelistan,
6. Om användaren är medlem i CDON:s kundklubb, samt
7. Vilken söksträng som användaren använt för att söka internt på Webbplatsen.

Utöver dessa uppgifter får Google även tillgång till respektive användares IP-adress.

1.3.4 Kategorier av personer som berörs av behandlingen

De kategorier av personer som berörs av behandlingen är samtliga kategorier av personer som besöker Webbplatsen. CDON har inte någon möjlighet att särskilja om uppgifter om särskilt utsatta personer behandlas. Detta beror på att CDON endast behandlar anonym ”beteendedata” avseende hur en användare navigerar på Webbplatsen. Den information som behandlas av CDON är inte mer än vad gäller själva överföringen av informationen till Google. CDON kan varken innan eller efter utlämnandet till Google identifiera enskilda användare. Vilken personkategori en unik användare tillhör har CDON således inte kännedom om.

1.3.5 När koden för Verktyget exekveras och mottagare bereds tillgång

Direkt efter att Webbplatsen har laddat klart i användarens webbläsare har det överförts information till Google om var användaren befinner sig på Webbplatsen. Sedan den 12 januari 2021 har CDON aktiverat ett verktyg som innebär att respektive användares samtycke krävs för att Verktygets innehåll ska integreras och köras i användarens webbläsare.

1.3.6 Hur länge lagras personuppgifterna

Uppgifter och annan information lagras inte av CDON utan överförs med hjälp av Verktyget i realtid från CDON till Google. CDON:s bedömning är att den anonymisering av IP-adresser som beskrivs nedan innebär de uppgifter som förs över till Google inte längre kan knytas till en specifik individ och därmed är inte att betrakta som personuppgifter. Hos Google lagras personuppgifter endast fram till dess att IP-adresserna har trunkerats[4]. Enligt information från Google utförs trunkeringen så snart det är tekniskt möjligt

1.3.7 Vilka länder personuppgifterna behandlas i

De uppgifter som överförs till Verktyget lagras bland annat i USA.

[4] 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).

1.3.8 CDON:s relation till Google LLC

CDON delar den bedömning som har gjorts av Google angående fördelningen av personuppgiftsansvaret som innebär att Google anses behandla uppgifter inom ramen för CDON:s användande av Verktyget såsom personuppgiftsbiträde åt CDON. CDON agerar som personuppgiftsansvarig.

De villkor som gäller för Verktyget är dels Googles användarvillkor, dels Googles villkor för behandling av uppgifter.

Den av Google och CDON överenskomna fördelningen av personuppgiftsansvaret framgår av Google Ads Data Processing Terms.

1.3.9 Säkerställande av att behandlingen inte sker för mottagarnas egna ändamål

CDON har inte haft skäl att anta att Google inte uppfyller de krav som följer av nämnda Google Ads Data Processing Terms, varför Googles efterlevnad av dessa ännu inte har kontrollerats ytterligare av CDON.

1.3.10 Beskrivning av CDON:s användning av Verktyget

CDON använder Verktyget i syfte att lära känna trafiken på Webbplatsen och för att kunna fatta olika verksamhetskritiska beslut utifrån den informationen. Det är med hjälp av Verktyget exempelvis möjligt att ta reda på vilka produktkategorier som är mest populära och hur kunder navigerar på Webbplatsen för att hitta till CDON och för att avsluta ett köp.

1.3.11 Egna kontroller av överföringar som berörs av domen Schrems II

Till följd av domen Schrems II har CDON vidtagit åtgärder i form av att identifiera vilka av CDON:s samarbetspartners som är belägna i länder utanför EU/EES och i förhållande till respektive samarbetspartners begärt information om vilka ytterligare säkerhetsåtgärder som dessa har vidtagit till följd av avgörandet.

CDON begärde den 26 oktober 2020 information av Google gällande effekten av CDON:s inbäddning av koden för Verktyget på Webbplatsen. Google har inte återkommit med svar på CDON:s begäran om information och CDON har av denna anledning, förutom att upprepa begäran till Google och påminna om svar, sökt allmänt tillgänglig information om vilka åtgärder som vidtagits av Google till följd av avgörandet.

Enligt allmänt tillgänglig information från Google har Google i tillägg till standardavtalsklausulerna vidtagit följande ytterligare skyddsåtgärder i relation till Verktyget:

- Google säkerställer en säker överföring av JavaScript-bibliotek och mätdata med hjälp av krypteringsprotokollet HTTP HSTS (Strict Transport Security).
- Verktyget har certifierats enligt de internationellt accepterade oberoende säkerhetsnormerna ISO 27001.

Utöver dessa åtgärder har CDON även valt att i koden för Verktyget aktivera IP-anonymisering, vilket innebär att IP-adresser trunkeras. IP-anonymiseringen (trunkeringen) innebär att den sista oktetten i IPv4-adresser respektive de sista 80 bitarna i IPv6-adresser raderas omedelbart efter att adresserna har skickats till insamlingsnätverket för Verktyget. Eftersom CDON:s uppfattning är att det är IP-adresserna som medför att övriga uppgifter som samlas in och överförs med hjälp av Verktyget är att betrakta som personuppgifter är CDON:s bedömning att trunkeringen

av IP-adresserna innebär att ingen information som överförs till Google är att betrakta som personuppgifter efter det att IP-anonymiseringen/trunkeringen har genomförts.

1.3.12 Överföringsverktyg enligt kapitel V i dataskyddsförordningen
Överföringar av personuppgiften till mottagare i tredjeländer inom ramen för CDON:s användning av Verktyget genomförs med stöd av EU-kommissionens standardavtalsklausuler (2010/87/EU).

I enlighet med de versioner av Googles villkor för behandling av uppgifter som har varit gällande sedan 12 augusti 2020, har Google och CDON ingått EU:s standardavtalsklausuler för överföring av uppgifter från en personuppgiftsansvarig inom EU till ett personuppgiftsbiträde utanför EU, baserat på EU-kommissionens mall 2010/87/EU.

1.3.13 Kontroll av hinder för fullgörande i lagstiftning i tredjeland
I syfte att säkerställa att avtalsförpliktelserna i standardavtalsklausulerna fullgörs har CDON skickat den begäran om information till Google angående tredjelandsöverföring som beskrivs ovan och CDON har inte fått något svar.

1.3.14 Vilken information omfattas av definitionen personuppgifter
Det är av vikt att skilja på begreppen att kunna särskilja användare och att inte kunna identifiera en specifik individ. Det senare, identifiering av en specifik individ är inte syftet med användandet av Verktyget och det är heller inte möjligt med den information som samlas in av unik(a) identifierare (som kan härledas till den webbläsare eller enhet (dvs. CDON:s konto-ID för Google Analytics)) varken ensamt eller i kombination med bland annat den informationen som genereras vid besök på Webbplatsen (dvs. Webbadress (URL) och HTML-titel på den Webbplatsen eller information om webbläsare). CDON är av den bestämda uppfattningen att IP-adresser är nödvändiga för att bland annat behandla informationen som generas vid besök på Webbplatsen (dvs. webbadress (URL) och HTML-titel på den Webbplatsen eller information om webbläsare) ska kunna anses utgöra personuppgifter. CDON vitsordar att dynamiska IP-adresser under vissa omständigheter kan anses utgöra personuppgifter. Det särskiljande av användare som möjliggörs genom informationen som samlas in av unik(a) identifierare är dock inte tillräckligt för att en specifik individ ska kunna identifieras, med eller utan hjälpmedel såsom tillexempelvis utgallring, utan det är endast i kombination med en fullständig IP-adress som informationen som samlas in av unik(a) identifierare och information som generas vid besök på Webbplatsen kan komma att utgöra personuppgifter.

Domarna Breyer[5] och M.I.C.M.[6] ger stöd för bedömningen att dynamiska IP-adresser i samtliga fall är att betrakta som personuppgifter. Dynamiska IP-adresser enligt EU-domstolen ska kunna betraktas som personuppgifter i förhållande till berörd leverantör av informations- eller kommunikationstjänster, inte i förhållande till varje aktör som får tillgång till en IP-adress. I målet Breyer avseende bedömningen av vilka hjälpmedel som rimligen kan komma att användas för att identifiera den aktuella personen, bedömde EU-domstolen att det enligt tysk rätt fanns lagliga medel som gör det möjligt för leverantören av elektroniska informations- eller kommunikationstjänster, att särskilt i händelse av it-attacker, vända sig till den behöriga myndigheten för att den ska vidta nödvändiga åtgärder för att erhålla sådana upplysningar från internetleverantören och inleda straffrättsliga förfaranden. Det kan ifrågasättas om en amerikansk myndighet med en trunkerad IP-adress, som kan utgöra en av 256 alternativa IP-adresser, har

[5] EU-domstolens dom Breyer, C-582/14, EU:C:2016:779.
[6] EU-domstolens dom M.I.C.M, C-597/19, EU:C:2021:492.

sådana lagliga medel som rimligen kan komma att användas för att möjliggöra identifieringen av en enskild individ, när det i fallet Breyer till och med ansågs problematiskt med en fullständig IP-adress i förhållande till den faktiska leverantören av den fysiska personens IT-tjänster.

1.3.15 Effektiviteten hos vidtagna skyddsåtgärder av Google och CDON
Med hänvisning till svaren ovan har CDON, utöver aktiveringen av IP-anonymiseringen, inte övervägt genomförandet av kompletterande åtgärder eftersom Google har informerat om att ytterligare åtgärder har vidtagits.

Trunkeringen av IP-adresserna är en effektiv skyddsåtgärd. Oaktat om trunkeringen av IP-adresserna sker inför, i samband med, eller i direkt anslutning till överföringen av informationen från CDON till Google. Trunkeringen av IP-adresserna innebär att informationen som lagras på Googles servrar i USA inte utgör personuppgifter. I en situation där trunkeringen genomförs först när uppgifterna har tagits emot av Google LCC, men senast i direkt anslutning till mottagandet, innebär trunkeringen att samtliga uppgifter som har överförts av CDON till Google och som lagras på Googles servrar inte kommer att utgöra personuppgifter eftersom IP-adressen, som är den unika identifierare som medför att övrig överförd information utgör personuppgifter, har anonymiserats. IP-adress utan den sista oktetten kan vara någon av 256 alternativa IP-adresser och därför *kan inte* en trunkerad IP-adress genom utgallring tillsammans med övrig information, anses utgöra personuppgifter.

1.3.16 Vidtagna ytterligare skyddsåtgärder utöver de som Google vidtagit
CDON har under ärendets hantering djupgående analyserat och utrett möjligheterna att byta till en annan lösning som inte innebär en användning av Verktyget. Coop har vidtagit förberedelser för en sådan förändring, som bolaget förhoppningsvis ska kunna verkställa skyndsamt för det fall IMY:s slutliga beslut innebär ett konstaterande att Verktyget inte är förenligt med dataskyddsförordningen och detta vinner laga kraft. Det ska dock understrykas att CDON:s analys visar att en sådan förändring kommer att vara mycket betungande för bolaget (särskilt i jämförelse för andra aktörer på marknaden) varför det inte kan genomföras innan klarhet finns i förhållande till vad som gäller för Verktyget avseende vad som är en tillräcklig skyddsåtgärd.

1.4 Vad Google LLC har uppgett

IMY har tillfört ärendet ett yttrande från Google LLC (Google) den 9 april 2021 som Google lämnat in till den österrikiska tillsynsmyndigheten. Yttrandet besvarar frågor som IMY och ett antal tillsynsmyndigheter har ställt till Google med anledning av delvis gemensam hantering av liknande klagomål som kommit in till dessa myndigheter. CDON 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 rättsliga, organisatoriska och tekniska skyddsåtgärder för att reglera överföringar av uppgifter inom ramen för Verktyget.

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

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

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

Utöver ovanstående åtgärder kan webbplatsägare använda IP-anonymisering genom att använda de inställningar som Verktyget tillhandahåller för att begränsa Googles användning av personuppgifter. Sådana inställningar inkluderar framför allt att i koden för Verktyget aktivera IP-anonymisering, vilket innebär att IP-adresser trunkeras och bidrar till dataminimering. Om IP-anonymiseringstjänsten används fullständigt sker anonymiseringen av IP-adressen nästan omgående efter att begäran har mottagits.

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

1.5 CDON:s kommentar på Googles yttrande

CDON vidhåller det som framförts i yttrandet av den 15 januari 2021. I tillägg till detta framför CDON följande med anledning av Googles yttrande av den 9 april 2021.

CDON har i sin användning av Verktyget vidtagit de säkerhetsåtgärder som Verktyget tillhandahåller.

Av Googles yttrande framgår bland annat följande:

> *"As a general matter, unless instructed to do so, Google does not attempt to link data it collects as a processor on behalf of website owners using Google Analytics with data it collects as a controller in relation to its users and the relevant policies and systems are designed to avoid such linking."*

Google anför alltså att ägaren av webbsidan har full kontroll över de personuppgifter som Google behandlar genom att det finns en möjlighet för användare av Verktyget att ge Google särskilda instruktioner om att koppla samman personuppgifterna med användare. CDON har inte gett Google några sådana instruktioner.

CDON har istället fokuserat på 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. CDON hade även begränsat lagringstiden för personuppgifterna och har inte heller aktiverat funktionen User-ID. CDON har alltså inte kunnat koppla ett fast ID för en enstaka användare till användarens engagemangsdata från en eller flera sessioner som har initierats från en eller flera enheter.

Sammanfattningsvis vidhåller CDON att användningen av Verktyget har skett i enlighet med de säkerhetsåtgärder som Verktyget erbjuder. Det ska även noteras att skyldigheter enligt kapitel V i dataskyddsförordningen primärt är skyldigheter som åläggs exportören, som i detta fall är CDON:s återförsäljare (se EDPB:s riktlinjer 05/2021 samt beslut av Österrikes dataskyddsmyndighet angående Google Analytics i mål 2021-0.586.257 (D155.027)).

2 Motivering av beslutet

2.1 Ramen för granskningen

IMY har med utgångspunkt i klagomålet i ärendet endast granskat om CDON överför personuppgifter till tredjelandet USA inom ramen för Verktyget och om CDON har rättsligt stöd för det i kapitel V i dataskyddsförordningen. Tillsynen omfattar inte om CDON:s 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.[7]

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.[8] 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

[7] EU-domstolens dom Nowak, C-434/16, EU:C:2017:994, punkt 34–35.
[8] 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.[9] 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.[10]

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 CDON genom implementeringen av Verktyget kan identifiera enskilda, t.ex. klaganden, vid besök på Webbplatsen eller om risken för det är försumbar.[11]

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

Av utredningen framgår att CDON 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 CDON (dvs. CDON:s 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.

---

[9] EU-domstolens dom Breyer, C-582/14, EU:C:2016:779, punkt 45–46.
[10] 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.
[11] Se Kammarrätten i Göteborgs dom den 11 november 2021 i mål nr 2232-21, med instämmande i underinstansens bedömning.

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 CDON 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.[12] 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[13] 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.

---

[12] 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.

[13] 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.

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, vilket i sig är tillräckligt för att avgöra att det handlar om behandling av personuppgifter.[14]

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.[15]

CDON 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 CDON:s användning av Verktyget på en webbsida, innebär behandling av personuppgifter.

[14] 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.
[15] Se till exempel EU-domstolens dom Latvijas Republikas Saeima (Points de pénalité), C-439/19, EU:C:2021:504, punkt 61, dom Nowak, C-434/16, EU:C:2017:994, punkt 33 och dom Rijkeboer, C-553/07, EU:C:2009:293, punkt 59.

2.3 CDON 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 CDON lämnar visar att CDON har fattat beslutet att implementera Verktyget på Webbplatsen. Vidare framgår att CDON:s 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 CDON 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. CDON 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 CDON:s 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.[16] 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

[16] 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.

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 fallet när lagstiftningen i det tredjelandet tillåter att myndigheterna i detta tredjeland gör ingrepp i de registrerade personernas rättigheter avseende dessa uppgifter.*”[17]

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”.*[18]*

I Europeiska dataskyddsstyrelsens (EDPB) rekommendationer om följderna av domen[19] 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”*.[20]

---

[17] Punkt 125-126.
[18] Punkt 133.
[19] 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”).
[20] EDPB:s Rekommendationer 01/2020, punkt 75; IMY:s översättning.

Av EDPB:s rekommendationer framgår att sådana ytterligare skyddsåtgärder kan delas in i tre kategorier: avtalsmässiga, organisatoriska och tekniska.[21]

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 [...]”.*[22]

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*”.[23]

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*”.[24] 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*”.[25]

2.4.2 Integritetsskyddsmyndighetens bedömning

2.4.2.1 Tillämpligt överföringsverktyg

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

---

[21] EDPB:s Rekommendationer 01/2020, punkt 52.
[22] EDPB:s Rekommendationer 01/2020, punkt 99; IMY:s översättning.
[23] EDPB:s Rekommendationer 01/2020, punkt 128; IMY:s översättning.
[24] EDPB:s Rekommendationer 01/2020, punkt 77; IMY:s översättning.
[25] EDPB:s Rekommendationer 01/2020, punkt 79; IMY:s översättning.

2.4.2.2 Lagstiftningen och situationen i tredjelandet

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

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

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

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.[26]

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 CDON

Nästa fråga är om CDON vidtagit tillräckliga ytterligare skyddsåtgärder.

Som personuppgiftsansvarig och exportör av personuppgifterna är CDON 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 (CDON) 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 CDON 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 CDON),[27] offentliggörandet av en

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

insynsrapport eller en allmänt tillgänglig ”*policy för hantering av regeringsförfrågningar*” hindrar eller minskar de amerikanska underrättelsetjänsternas möjligheter att få tillgång till personuppgifterna. Dessutom är det inte beskrivet vad det innebär att Google LLC:s gör en ”*noggrann prövning av varje begäran*” om ”lagligheten” från amerikanska underrättelsetjänster. IMY noterar att detta inte påverkar lagligheten av sådana begäranden eftersom de enligt EU-domstolen inte är förenliga med kraven i EU:s dataskyddsregler.

När det gäller de *tekniska åtgärder* som vidtagits kan det konstateras att varken Google LLC eller CDON 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.[28] 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[29] 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 CDON:s egna ytterligare skyddsåtgärder

CDON har uppgett att bolaget har vidtagit ytterligare skyddsåtgärder utöver de åtgärder som Google har vidtagit. Dessa består enligt CDON av aktivering av

[28] Se EDPB:s Rekommendationer 01/2020, punkt 81.
[29] 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).

funktionen för trunkering[30] av sista oktetten i IP-adress innan uppgifterna överförs till Google, som innebär att den sista oktetten maskeras.[31]

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 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 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 CDON 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 CDON 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 CDON åberopat kan ge sådant stöd för överföringen som anges i kapitel V i dataskyddsförordningen.

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

IMY konstaterar därför att CDON 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.

[30] 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).
[31] Se ovan i avsnittet om vad CDON har anfört, under rubriken ”Vidtagna kompletterande skyddsåtgärder”.

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.[32]

3.2 Ska sanktionsavgift påföras?

IMY har ovan funnit att de överföringar av personuppgifter till USA som sker via Google Analytics-verktyget och som CDON 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 CDON 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. CDON ska därför påföras en sanktionsavgift för den konstaterade överträdelsen. Se även vidare nedan under 3.3 för en utförlig beskrivning av överträdelsens allvar.

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.[33]

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 CDON:s årsredovisning för år 2022. Bolaget

[32] 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).
[33] Se Dom i Akzo Nobel, C-516/15, EU:C:2017:314, punkt. 48

omsatte cirka 461 000 000 kronor under det budgetåret. Detta belopp är mindre än 20 miljoner EUR och därav kan sanktionsavgiften bestämmas till ett belopp på upp till 20 miljoner EUR.

Vid bestämmande av sanktionsavgiftens storlek ska IMY med hänsyn till överträdelsen allvar och med beaktande av både försvårande och förmildrande omständigheter 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. CDON 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[34] 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/ESS 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.[35]

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 CDON inte vidtagit egna ytterligare skyddsåtgärder. Googles åtgärd avseende trunkering[36] 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.

CDON:s webbplats är dessutom en välbesökt e-handelsportal som erbjuder varor från många olika leverantörer och är tillgänglig i flera länder och på flera språk. Det rör sig om uppgifter om ett stort antal registrerade i EU/EES som kan identifieras indirekt och

---

[34] 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.
[35] 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.
[36] 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).

vars uppgifter kan sammankopplas med andra uppgifter om dem. När det gäller uppgifternas beskaffenhet följer redan av CDON:s 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 varor de är intresserad av över tid. CDON:s analys av Verktyget visar att det finns förslag på en annan lösning än Verktyget, men bolaget har valt att inte införa denna lösning med anledning av att sådan förändring skulle vara särskilt betungande för bolaget. CDON:s behandling av personuppgifter medför risker för allvarlig kränkning av enskildas fri och rättigheter vilket ger CDON ett särskilt ansvar som innebär höga krav vid överföringar till tredjeland, där IMY sammantaget bedömer att CDON 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 CDON vidtagit vissa, om än otillräckliga, åtgärder för att begränsa de personuppgifter som överfördes genom att aktivera ”anonymisering av IP-adresser” genom trunkering.[37] 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. För att säkerställa en proportionell sanktionsavgift i det enskilda fallet finns även skäl att redan i detta skede ytterligare justera utgångspunkten för den fortsatta beräkningen nedåt med beaktande av den omsättning som ligger till grund för beräkningen av sanktionsavgiften.

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 och mot bakgrund av att den administrativa sanktionsavgiften ska vara effektiv, proportionerlig och avskräckande bedömer IMY att sanktionsavgiften kan stanna vid 300 000 (trehundra tusen) kronor.

3.3 Andra ingripanden

Mot bakgrund av den konstaterade överträdelsen gör IMY bedömningen att CDON ska föreläggas enligt artikel 58.2 d i dataskyddsförordningen att se till att bolagets behandling av personuppgifter inom ramen för bolagets användning av verktyget Google Analytics överensstämmer med artikel 44 och övriga bestämmelser i kapitel V. Detta ska särskilt ske genom att upphöra med att använda den version av verktyget

[37] 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.

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)

Bilaga
Bilaga 1 – Information om betalning av sanktionsavgift

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.