2023-08-25 Förvaltningar och bolag i Göteborgs Stad

Dataskyddsenhetens uppdaterade rekommendationer om tredjelandsöverföringar med anledning av nytt adekvansbeslut för USA

Bakgrund

Genom EU-kommissionens adekvansbeslut den 10 juli 2023 har förutsättningarna förändrats för överföringar av personuppgifter från EU till de amerikanska organisationer som har anslutit sig till ”EU-US Data Privacy Framework.”[1] Mot bakgrund av detta har det uppstått ett behov av att uppdatera dataskyddsenhetens rekommendation gällande tredjelandsöverföringar till USA specifikt. I denna rekommendation ger vi en bakgrund och beskrivning av det nya rättsläget samt ger rekommendationer kring vad verksamheter behöver tänka på ifall de använder USA-baserade leverantörer och/eller underleverantörer.

Tidigare lämnade rekommendationer

Dataskyddsenheten skickade den 18 september 2020 ut skrivelsen ”Information till personuppgiftsansvariga styrelser och nämnder med anledning av EU-domstolens dom i mål C-311/18 (Schrems II-målet)” till samtliga förvaltningar och bolag i Göteborgs Stad. I maj 2022 skickades uppdaterade rekommendationer i frågan ut (”Dataskyddsenhetens uppdaterade rekommendationer om tredjelandsöverföringar efter Schrems II”).

Tidigare rekommendation för andra länder kvarstår

Tidigare lämnade rekommendationer gällande hanteringen av tredjelandsöverföringar som inte avser specifikt USA kvarstår. Om överföring av personuppgifter sker till ett land utanför EU/EES **som inte är USA** och mottagarlandet saknar adekvansbeslut rekommenderar dataskyddsenheten även fortsatt att förvaltningar och bolag i Göteborgs Stad följer metoden TIA (Transfer Impact Assessment) enligt EDPB:s rekommendationer 01/2020 om åtgärder som komplement till överföringsverktyg för att säkerställa överensstämmelsen med EU-nivån för skydd av personuppgifter.

Reglering av tredjelandsöverföringar i GDPR

Syftet med GDPR är att säkerställa rätten till privatliv och rätten till skydd för personuppgifter, samt möjliggöra personuppgifternas fria flöde inom EU/EES. För att dessa rättigheter inte ska urholkas krävs tydliga regler för överföring av personuppgifter till länder som inte ingår i EU/EES. Tredjelandsöverföringar är inte tillåtna om den personuppgiftsansvarige eller personuppgiftsbiträdet inte kan säkerställa att GDPR

[1] Europeiska kommissionen, Beslut om adekvat skydd för säkra uppgiftsflöden mellan EU och USA; Beslut om adekvat skydd för säkra uppgiftsflöden mellan EU och USA (europa.eu)

efterlevs och att förutsättningarna i kapitel 5 i GDPR är uppfyllda. Bestämmelserna i kapitel 5 ska tillämpas så att nivån på skyddet av fysiska personer som säkerställs genom förordningen inte undergrävs (artikel 44 i GDPR).

Vad är ett adekvansbeslut?

EU-kommissionen har möjlighet att fatta beslut om att ett specifikt tredjeland eller en internationell organisation säkerställer adekvat skyddsnivå. Detta görs genom ett så kallat adekvansbeslut (artikel 45.1 i GDPR). Ett sådant beslut innebär antingen att EU-kommissionen fastslår att ett helt tredjeland, ett avgränsat territorium eller en eller flera specificerade sektorer i tredjelandet, alternativt att en specifik internationell organisation säkerställer en skyddsnivå för personuppgifter som är väsentligt likvärdig med den skyddsnivå som finns inom EU/EES. Personuppgifter kan därmed överföras med stöd av adekvansbeslutet utan att ytterligare skyddsåtgärder enligt kapitel 5 i GDPR vidtas. En uppdaterad lista på vilka länder som omfattas av adekvansbeslut finns på EU-kommissionens hemsida.[2]

Nytt adekvansbeslut för USA

Det nya adekvansbeslutet från 10 juli 2023 gäller tillsvidare från och med beslutsdatumet och kommer regelbundet att ses över för att säkerställa att skyddsnivån är effektiv och fortsatt adekvat (artikel 45.3–5 i GDPR). En första översyn av beslutet kommer att ske inom ett år från och med ikraftträdandet.

Adekvansbeslutet gäller inte överföringar till USA generellt, utan bara överföringar till organisationer som är etablerade i USA som omfattas av ett nytt ramverk för självcertifiering – ”EU-US data privacy framework” eller som det kallas på svenska ”ramverket för dataskydd mellan EU och USA” (härefter ”ramverket”). Alla organisationer som ingår i ramverket och som därmed omfattas av adekvansbeslutet förekommer på en lista som är sökbara på en särskild hemsida.[3]

Bakgrunden till att det nya adekvansbeslutet kunde fattas är inte bara att man har låtit inrättat ett nytt ramverk för certifiering, men också att amerikanska myndigheter efter påtryckningar från EU har vidtagit vissa skyddsåtgärder som gäller amerikansk dataskyddslagstiftning och som innebär vissa förbättringar jämfört med hur det såg ut tidigare.[4] Mot bakgrund av detta har EU-kommissionen i dagsläget bedömt att skyddsåtgärderna vad gäller amerikansk dataskyddslagstiftning tillsammans med de åtaganden som enskilda organisationer tar på sig genom ramverket, innebär ett tillräckligt starkt skydd för personuppgifter och därför bedöms överföringar till dessa organisationer vara förenliga med kraven i kapitel 5 GDPR. Detta innebär att det inte krävs några ytterligare skyddsåtgärder eller överföringsmekanismer för att en sådan tredjelandsöverföring ska bli laglig.

Organisationer som har blivit självcertifierade behöver årligen genomgå en process för att förnya certifieringen. Om det visar sig att organisationen misslyckats med att leva upp till ramverkets principer eller om den självmant väljer att frånträda dem kommer organisationen att plockas bort från listan och inte längre vara certifierad.

[2] Europeiska kommissionen, Adekvansbeslut; Adequacy decisions (europa.eu)
[3] Data Privacy Framework, Data privacy framework list: Participant Search (dataprivacyframework.gov).
[4] Europeiska kommissionen; Questions & Answers: EU-US Data Privacy Framework (europa.eu)

Det är viktigt att understryka att även om överföringen till tredjeland kan stödjas på ett adekvansbeslut innebär det inte att behandlingen i sig är laglig. Principerna i GDPR behöver fortsatt följas och lämpliga tekniska och organisatoriska säkerhetsåtgärder behöver vidtas enligt artikel 32 i GDPR.

Certifiering för vissa typer av uppgifter

I ramverket delas personuppgifter upp i 1) personuppgifter som ej utgör ”HR-data” och 2) ”HR-data”. Begreppet ”HR-data” avser personlig information om tidigare eller nuvarande anställda, insamlade inom ramen för anställningsförhållandet. Det finns särskilda krav för certifiering gällande överföring av personuppgifter inom HR, och mot bakgrund av detta är det viktigt att ta reda på vilken typ av uppgifter som certifieringen för en viss organisation omfattar.

Vad gäller för överföringar till organisationer i USA som inte är certifierade?

Vad gäller tredjelandsöverföringar till organisationer i USA som inte ingår i ramverket så kan överföringar till dessa inte baseras på adekvansbeslutet, utan i dessa fall krävs att det finns en tillämplig överföringsmekanism enligt artikel 46 GDPR. För mer information om hanteringen hänvisas till den information som tillhandahållits av Europeiska dataskyddsstyrelsen (EDPB).[5]

Vad gäller nu?

Risker kvarstår för överföring av personuppgifter till USA

Det nya adekvansbeslutet innebär att ni som personuppgiftsansvariga numera har möjlighet att stödja era överföringar av personuppgifter till USA på adekvansbeslutet i de fall överföringarna sker till certifierade organisationer och typen av uppgifter omfattas av certifieringen. Samtidigt är det viktigt att komma ihåg att verksamheter som önskar använda tjänster som innebär att personuppgifter överförs till USA även har andra lagkrav att ta hänsyn till, till exempel offentlighet- och sekretesslagstiftningen (OSL). Det är därför viktigt att varje verksamhet har kunskap om de lagar, regler och föreskrifter som gäller för den egna verksamheten och vid användning av en tjänst, eller inför anlitande av ett biträde och/eller underbiträde, säkerställer att samtliga av dessa kan efterlevas.

Adekvansbeslutets giltighet ifrågasatt

En kort tid innan EU-kommissionens adekvansbeslut fattades antog Europaparlamentet en resolution i vilken det bland annat anfördes att de av USA hittills vidtagna skyddsåtgärderna inte var tillräckliga. EU-kommissionen valde ändå att fatta adekvansbeslutet. Även efter att adekvansbeslutet fattades och trädde i kraft har det blivit ifrågasatt, bland annat av intresseorganisationen noyb (None of your business) som uttalat att man avser utmana beslutet.[6] Mot bakgrund av detta, samt att de tidigare ramverk som har funnits mellan EU och USA har genomgått rättsliga prövningar och ogiltigförklarats av EU-domstolen, är sannolikheten stor att även nuvarande ramverk kommer att utmanas och prövas rättsligt inom en snar framtid.

[5] EDPB, Information note on data transfers under the GDPR to the United States after the adoption of the adequacy decision on 10 July 2023; edpb_informationnoteadequacydecisionus_en.pdf (europa.eu)
[6] European Commission gives EU-US data transfers third round at CJEU (noyb.eu)

Rekommendationer för hantering av avtal och licenser

Trots att en personuppgiftsansvarig nu har rättsliga möjligheter att stödja överföring av personuppgifter till USA på det nya adekvansbeslutet, rekommenderar dataskyddsenheten verksamheter i Göteborgs Stad att iaktta stor försiktighet. Det nya beslutet kommer att följas upp och utvärderas och för det fall de överenskommelser som har gjorts mellan EU och USA inte efterföljs kan beslutet komma att upphävas. Vidare är det ett krav att varje organisation årligen blir certifierad, vilket medför att det kan ske förändringar i listan över certifierade organisationer med förhållandevis korta intervall. Därtill är det sannolikt att beslutet om adekvat skyddsnivå prövas i domstol, vilket precis som Schrems-målen tidigare gjort, kan leda till att beslutet ogiltigförklaras som tillräcklig grund för överföringar av personuppgifter till USA. Mot denna bakgrund rekommenderar dataskyddsombudet stadens förvaltningar och bolag att vänta med att fatta beslut som påverkar överföringar av personuppgifter till USA på lång sikt.

Nedan följer rekommendationer för hanteringen av dels befintliga avtal/licenser, dels nya avtal/licenser.

För hantering av befintliga avtal/licenser som innebär en direkt eller indirekt tredjelandsöverföring till USA

- Kontrollera att de biträden och/eller underbiträden som ni använder är certifierade.
- Kontrollera att de kategorier av personuppgifter (den data) som ska behandlas omfattas av certifieringen.
- Uppdatera er information till de registrerade gällande överföringar till tredjeland.
- Tänk långsiktigt och arbeta fram utträdesstrategier för att ha en plan för hur ni ska kunna hantera en situation där ramverket ogiltigförklaras eller en organisation förlorar sin certifiering och överföringen därför inte kan stödjas på adekvansbeslutet.

För hantering av nya avtal/licenser som innebär en direkt eller indirekt tredjelandsöverföring till USA

- Ingå inte nya långa avtal samt licenser som medför användning av ett biträde och/eller underbiträde som innebär en direkt eller indirekt överföring av personuppgifter till USA. Samma rekommendation gäller också för förlängning av befintliga avtal och/eller licenser.

Rekommendation för användning av molntjänster

För användande av molntjänster rekommenderas verksamheter, oavsett leverantör, att ta hänsyn till de iakttagelser som gjorts av Integritetsskyddsmyndigheten (IMY) i rapporten om användning av molntjänster i offentlig sektor.[7] Tillsynsmyndigheten lyfter bland annat att det föreligger svårigheter att förhandla med molntjänstleverantörer och därmed påverka utformningen och/eller villkor för användningen av tjänsten. Vidare konstaterar IMY att de är svårt att identifiera och fastställa rollfördelningen mellan personuppgifts-ansvarig och personuppgiftsbiträde, eller gemensamt personuppgiftsansvar. Slutligen framkommer att bristen på kunskap i dataskydd hos leverantörer ställer större krav på upphandlande myndigheter för att fortsatt säkerställa laglighet vid användning av system.

[7] Användning av molntjänster inom offentlig sektor – en sammanställning av en undersökning av sju myndigheter (imy.se)

När det gäller användningen av molntjänster tillhandahållna av amerikanska leverantörer, såsom Microsoft, Google och Amazon, gäller rekommendationerna ovan. Vidare behöver verksamheter, innan nya tjänster införs, säkerställa lagefterlevnad gentemot GDPR såväl som andra lagar och regler som kan styra användningen. Verksamheter som hanterar stora mängder särskilt skyddsvärda och/eller känsliga personuppgifter, till exempel inom skola och socialtjänst, bör även ta hänsyn till att det i många fall kan vara direkt olämpligt att hantera information i en molntjänst med tanke på de höga risker som föreligger för de registrerade vid en eventuell incident. Då informationen som hanteras i en molntjänst även innebär att uppgifterna röjs[8] för leverantören behöver verksamheterna också bedöma huruvida användningen är förenlig med kraven i OSL.[9]

Rekommendation för användning av sociala medier

Vid användandet av sociala medier finns fler aspekter att ta hänsyn till än bara tredjelandsproblematiken. I de fall användandet av sociala medier innebär att behandling i form av profilering sker, behöver även reglerna om detta i artikel 22 i GDPR följas. Vid användandet av sociala medier kan detta bli aktuellt ifall verksamheten använder till exempel annonseringstjänster.

Verksamheter som vill använda sociala medier behöver säkerställa att personuppgifts-behandlingen följer reglerna i GDPR. Det förutsätter att verksamheten som första steg identifierar vilka behandlingar som genomförs vid användandet av sociala medier. Därefter behöver verksamheten, utifrån faktiska omständigheter, identifiera vem som är personuppgiftsansvarig för vilka behandlingar.[10] Det gäller både i förhållande till leverantören av tjänsten (t.ex. Meta) och till tjänsteleverantören i staden. Om leverantören är personuppgiftsbiträde ska ett personuppgiftsbiträdesavtal finnas på plats som reglerar ansvaret mellan aktörerna. För att säkerställa att verksamheten uppfyller sin ansvarsskyldighet och omsorgsplikt enligt GDPR behöver även, innan avtalstecknande, både leverantörer och eventuella underleverantörer kontrolleras. För att tredjelands-överföringar till amerikanska biträden/underbiträden ska vara lagenlig behöver samtliga biträden/underbiträden vara certifierade enligt ramverket, annars måste den personuppgiftsansvarige ha en annan grund för överföring.

Den personuppgiftsansvarige bör även väga in den egna verksamhetens möjlighet att uppfylla omsorgsplikten vid val av leverantör. Detta är särskilt aktuellt för leverantörer av sociala medietjänster i nuläget, då Meta, som levererar flera av de sociala medieplattformarna, vid flera tillfällen under det senaste året har belagts med sanktionsavgifter för felaktig hantering av personuppgifter. Överträdelserna gällde bland annat olaglig överföring av personuppgifter till USA, bristande säkerhetsåtgärder och olaglig behandling av personuppgifter. Meta har också nyligen förbjudits att använda profilering på det sätt som man hittills gjort på användare i Norge.[11]

Även om en personuppgiftsansvarig nu har rättsliga möjligheter att stödja överföring av personuppgifter till USA på det nya adekvansbeslutet, rekommenderar dataskyddsenheten

[8] SOU 2021:1, Säker och kostnadseffektiv it-drift – rättsliga förutsättningar för utkontraktering
[9] För mer information och vägledning se bl.a. underlag från e-sam; Molnfrågan - eSamverka
[10] Se b.la. Datainspektionen beslut 2010-07-02, dnr 685-2010, 868-2010 och 687-2010 samt EU-domstolens dom C-210/17 ”Wirtschaftsakademie Schleswig-Holstein, dom C-25/17 Jehovas vittne och dom C-40/17 Fashion ID.
[11] Tvangsmulkt til Meta hvis forbud ikke følges | Datatilsynet

verksamheter i Göteborgs Stad att iaktta stor försiktighet. Det nya beslutet innebär förvisso att *överföringar* av personuppgifter till USA har stöd i lag. Samtidigt har den senaste rättsutvecklingen visat att användning av sociala medier innebär *andra* stora risker för registrerade. Utifrån den osäkerhet som nu råder kring de sociala medieplattformarnas hantering av personuppgifter, och huruvida denna är förenlig med kraven i GDPR, är det därför extra viktigt att de verksamheter som behandlar personuppgifter i dessa tjänster kontrollerar att behandlingar uppfyller samtliga krav i GDPR.

Frågor?

Har ni frågor kring tredjelandsöverföring eller behöver råd och stöd är ni välkomna att kontakta dataskyddsenheten på dso@intraservice.goteborg.se.