Vad din organisation behöver veta om det tredje adekvansbeslutet

I spåren av EU-kommissionens adekvansbeslut i juli 2023 så är det naturligt att organisationer frågar sig om de har fått grönt ljus att använda amerikanska molntjänstleverantörer.

I denna rapport analyserar vi vad adekvansbeslutet egentligen innebär och inte innebär. Vi fokuserar särskilt på vad som gäller när en organisation överväger att låta en molntjänstleverantör hantera personuppgifter inom EU. Det kommer vara vanligt även efter adekvansbeslutet, och innebär särskilda krav när adekvansbeslutet inte är relevant.

Vi granskar dessutom några av de förändringar som gjorts på den amerikanska sidan, särskilt genom att belysa delar av presidentdekretet Executive Order 14086 och bestämmelserna för den nya prövningsinstansen "Data Protection Review Court".

Vår förhoppning är att rapporten ska stötta organisationer som behöver avgöra vilka molntjänstleverantörer de kan förlita sig på. Det är relevant dels när en organisation köper molninfrastruktur, dels när en organisation överväger att använda en SaaS- eller PaaS-leverantör som i sin tur nyttjar underliggande molninfrastruktur.

Det finns givetvis en rad rättsliga och lämplighetsmässiga faktorer att beakta vid användning av molntjänster, utöver vad som är i fokus i denna rapport.

Arman Borghem, jurist och Regulatory and Compliance Advisor på Cleura

The report is also available in English here:
https://cleura.com/articles/new-adequacy-decision-fails-to-approve-us-cloud-services-in-the-eu/

cleura

An Iver company

Innehållsförteckning

Introduktion och sammanfattning

I juli 2023 fattade EU-kommissionen ett beslut om adekvat skyddsnivå, baserat på ramverket Data Privacy Framework. Många organisationer i EU frågar sig därför om de har grönt ljus att använda amerikanska molntjänstleverantörer.

Vi bedömer att svaret fortsatt är nej.

Till att börja med förväntar vi oss att EU-domstolen ogiltigförklarar det nya adekvansbeslutet inom ett par år. Några skäl för det berörs i avsnitt 3. Redan på grund av detta menar vi att det vore ett strategiskt felsteg att förlita sig på adekvansbeslutet för digitala satsningar av betydelse.

Den här rapporten fokuserar emellertid på en viktigare fråga än adekvansbeslutets öde.

Rapporten analyserar vad adekvansbeslutet kan – och *inte* kan – användas till och vad som gäller när adekvansbeslutet inte är relevant. Så är fallet när en molntjänstleverantör hanterar personuppgifter *inom EU*. Därmed hoppas vi reda ut frågetecken och förebygga missförstånd.

EU-kommissionens adekvansbeslut innebär inget generellt godkännande att använda amerikanska molntjänstleverantörer. Adekvansbeslutet möjliggör endast överföringar av personuppgifter *från EU till mottagare i USA* som har självcertifierat att de följer principerna i Data Privacy Framework och har tagits upp på det amerikanska handelsdepartementet lista.

En organisation i EU *kan* alltså använda adekvansbeslutet för överföringar från EU till en godkänd mottagare *i USA*. Adekvansbeslutet ger emellertid inte organisationen grönt ljus att använda amerikanska molntjänstleverantörer som ska hantera personuppgifter *i EU*.

De flesta organisationer i EU kommer också fortsättningsvis hantera personuppgifter i EU. Skälen kan exempelvis vara rättsliga eller lämplighetsmässiga. Fördröjningen till datacenter i EU kan också vara kortare än till datacenter på andra sidan Atlanten. Det finns rentav en trend där amerikanska molntjänstleverantörer åtminstone delvis erbjuder datalokalisering inom EU. Vid personuppgiftsbehandling just inom EU blir alltså adekvansbeslutet inte aktuellt.

Frågan är då vad som gäller när en organisation ska låta en molntjänstleverantör hantera personuppgifter inom EU. Vilka leverantörer kan organisationen förlita sig på?

Organisationen måste säkerställa den skyddsnivå för personuppgifter som gäller enligt EU-stadgan och GDPR. Av betydelse är då vilka skyldigheter amerikanska molntjänstleverantörer lyder under enligt amerikansk lag, och om dessa skyldigheter är i konflikt med EU:s regelverk.

Amerikanska lagar för underrättelseinhämtning, särskilt FISA 702, tillåter amerikanska myndigheter att tvinga amerikanska molntjänstleverantörer att lämna ut uppgifter oavsett om uppgifterna finns i EU. Det kallas extraterritoriell lagstiftning, det vill säga lagstiftning i tredjeland (t.ex. USA) som i praktiken reglerar personuppgiftsbehandling på EU:s territorium. GDPR föreskriver tydliga skyddsmekanismer mot sådan extraterritoriell lagstiftning.

När en organisation i EU ska låta en molntjänstleverantör behandla personuppgifter åt organisationen ska parterna ingå ett personuppgiftsbiträdesavtal. Personuppgiftsbiträdesavtalet ska ange att molntjänstleverantören *endast* får behandla personuppgifter enligt den personuppgiftsansvarige organisationens instruktioner. Det finns endast ett undantag där molntjänstleverantören får agera vid sidan av dessa instruktioner, exempelvis i syfte att lämna ut personuppgifter till en myndighet. Undantaget gäller endast om *unionsrätten eller en medlemsstats nationella rätt* kräver det av att leverantören. Det framgår av artikel 28.3 a i GDPR.

Kraven på säkerhet innebär på motsvarande sätt att personuppgiftsbiträden ska vidta åtgärder för att *säkerställa* att deras personal inte avviker från den personuppgiftsansvariges instruktioner (exempelvis för att lämna ut uppgifter till en myndighet) såvida inte *unionsrätten eller en medlemsstats nationella rätt* ålägger dem att göra det. Det framgår av artikel 32.4 i GDPR.

Amerikanska underrättelselagar som FISA 702 är varken unionsrätt eller en medlemsstats nationella rätt. Samtidigt kan underrättelselagarna tvinga amerikanska molntjänstleverantörer att lämna ut uppgifter i EU vid sidan av den personuppgiftsansvariges instruktioner.

Vi menar att detta visar att amerikanska molntjänstleverantörer i princip inte kan uppfylla de krav som följer av artikel 28.3 a samt 32.4 i GDPR.

Adekvansbeslutet kan inte heller användas som grund för överföringar från EU till amerikanska underrättelsemyndigheter i USA. Adekvansbeslutet kan endast användas för överföringar till mottagare i USA som har självcertifierat sig enligt Data Privacy Framework. Det har amerikanska underrättelsemyndigheter inte gjort, och de förväntas inte heller göra det.

Om en molntjänstleverantör lämnar ut personuppgifter på begäran av en myndighet så agerar molntjänstleverantören inte längre enligt sin kunds instruktioner, och blir då själv personuppgiftsansvarig för utlämnandet. All personuppgiftsbehandling måste ha en rättslig grund i GDPR och frågan blir då vilken rättslig grund en molntjänstleverantör kan använda.

Vi menar att den enda möjliga rättsliga grunden för en molntjänstleverantörs utlämnande till en myndighet finns i artikel 6.1 c i GDPR, eftersom utlämnandet är nödvändigt för att molntjänst-leverantören ska uppfylla en rättslig förpliktelse. Molntjänstleverantörens rättsliga förpliktelse är då skyldigheten att verkställa myndighetens beslut om att uppgifterna ska lämnas ut.

Problemet för amerikanska molntjänstleverantörer är att en sådan rättslig förpliktelse måste vara fastställd i *unionsrätten eller en medlemsstats nationella rätt*. Det framgår av artikel 6.3 i GDPR. Som noterats är amerikanska underrättelselagar som FISA 702 varken unionsrätt eller en medlemsstats nationella rätt. Adekvansbeslutet kan inte heller användas; amerikanska underrättelsemyndigheter ingår inte i Data Privacy Framework och är inte godkända mottagare. Sådana utlämnanden kan alltså inte genomföras i enlighet med GDPR – en rättslig grund saknas.

GDPR anger dock en rättslig möjlighet för molntjänstleverantörer att lämna ut personuppgifter i EU till tredjelands (exempelvis amerikanska) myndigheter. En möjlig grund i unionsrätten tydliggörs i artikel 48 i GDPR. Lösningen är en internationell överenskommelse mellan EU och tredjelandet i fråga. Adekvansbeslutet är dock ingen internationell överenskommelse. Det är ett ensidigt beslut från EU-kommissionen, som inte tar sikte på att reglera extraterritoriell åtkomst från myndigheter i USA till uppgifter i EU. Artikel 48 kan alltså inte användas.

Eftersom amerikanska molntjänstleverantörer säkerställer att de kan verkställa utlämnanden som är korrekta enligt amerikansk lag men strider mot EU:s rättsordning, snarare än att hindra sådana utlämnanden, menar vi att de inte ger de garantier som krävs av personuppgiftsbiträden enligt artikel 28.1 i GDPR. I avsnitt 2.3.5 beskriver vi hur EU-domstolspraxis kan anses stödja detta.

De regler i GDPR som vi har berört påverkas inte av adekvansbeslutet och i huvudsak inte heller av en bedömning av rättssäkerheten i amerikansk lagstiftning. I avsnitt 3 går vi ändå in på varför den exekutiva ordern 14086 och prövningsinstansen DPRC är otillräckliga för att tillgodose EU-rättens krav. I avsnitt 5 berör vi varför kryptering i molnet, och liknande åtgärder, sällan ger det skydd mot utlämnanden till tredjelands myndigheter som många organisationer hoppas på.

Slutsatsen är att molntjänster med verklig datasuveränitet, utan exponering mot amerikansk lagstiftning, fortsatt är det mest attraktiva alternativet.

1 Adekvansbeslutet möjliggör inte tredjelandsöverföringar till amerikanska underrättelsemyndigheter

EU-kommissionens adekvansbeslut från juli 2023 möjliggör endast överföringar av personuppgifter från EU till mottagare i USA som har självcertifierat att de följer principerna i Data Privacy Framework, anmält detta till det amerikanska handelsdepartementet och tagits upp på en särskild lista. Adekvansbeslutet möjliggör inte överföringar till USA generellt.

NSA och andra amerikanska underrättelsemyndigheter är inte självcertifierade mottagare. De finns således inte med på listan över godkända organisationer och förväntas inte heller adderas.

Det här innebär att adekvansbeslutet inte kan användas för att överföra personuppgifter från EU till amerikanska underrättelsemyndigheter i USA.

Samtidigt vill de flesta organisationer i EU hantera personuppgifter i EU. Det kan vara av regulatoriska skäl eller för att alternativen inte vore lämpliga. Ett annat skäl kan vara kortare fördröjning till datacenter i EU än på andra sidan Atlanten. Amerikanska molntjänstleverantörer erbjuder i högre utsträckning åtminstone delvis datalokalisering inom EU.

Frågan är då vad som gäller när en organisation ska hantera personuppgifter i datacenter inom EU. Vilka molntjänstleverantörer går egentligen att anlita?

Här behöver kunder ha i åtanke att amerikanska molntjänstleverantörer omfattas av regler som kan tvinga dem att ge amerikanska myndigheter tillgång till uppgifter i EU. Samtidigt har EU-lagstiftningen regler som i princip förbjuder sådana överföringar från EU till tredjelands myndigheter. Adekvansbeslutet gör varken från eller till i dessa situationer.

2 Skyddsnivån inom EU gäller oavsett adekvansbeslutet

2.1 Inledning

En personuppgiftsansvarig i EU måste säkerställa att dess personuppgiftsbehandling uppfyller den skyddsnivå som EU-stadgan och GDPR kräver. EU-regler såsom EU-stadgan och GDPR kallas gemensamt för *unionsrätten*. Dessa regler gäller även när adekvansbeslutet inte är aktuellt, det vill säga vid personuppgiftsbehandling inom EU.

För att en personuppgiftsansvarig organisation ska kunna avgöra om den kan hantera personuppgifter hos en molntjänstleverantör i EU behöver organisationen därför först förstå innebörden av unionsrättens skyddsnivå. Vilka krav innebär skyddsnivån när organisationen ska anlita en molntjänstleverantör, särskilt i relation till tredjelands lagstiftning?

EU-domstolen har klargjort att unionsrättens skyddsnivå omfattar alla personuppgifter oavsett om de är känsliga, oavsett hur uppgifterna används och oavsett om berörda personer fått utstå någon olägenhet (C-311/18 Schrems II p. 171). Mindre känsliga personuppgifter är alltså inte undantagna unionsrättens skydd.

2.2 EU-stadgans skydd

Unionsrättens skyddsnivå innebär att personuppgifter måste behandlas lagenligt för bestämda ändamål och med en legitim och lagenlig grund (EU-stadgan, artikel 8).

Dessutom gäller:

- rätten att få tillgång till insamlade personuppgifter,
- rätten att rätta (korrigera) felaktiga personuppgifter,
- att en oberoende myndighet kontrollerar att reglerna efterlevs, och
- rätten till en oavhängig och opartisk domstolsprövning för de vars rättigheter har kränkts.

Dessa punkter har ett slags grundlagsstatus eftersom de föreskrivs i Europeiska unionens stadga om de grundläggande rättigheterna (EU-stadgan, artikel 8 och 47). GDPR konkretiserar dessa och andra rättigheter och ska läsas i ljuset av EU-stadgan.

Rätten till domstolsprövning (eller effektiva rättsmedel som det också kallas) är särskilt viktig. Den rätten är avgörande för att en person ska kunna få en oberoende prövning av om personens andra rättigheter har kränkts. EU-domstolen har flera gånger framhållit det som en grundförutsättning för en rättsstat:

> Enligt fast rättspraxis är själva möjligheten till en effektiv domstolsprövning i syfte att säkerställa iakttagandet av unionsrätten en grundförutsättning för en rättsstat. En lagstiftning i vilken det inte föreskrivs någon möjlighet för enskilda att använda rättsmedel för att erhålla tillgång till, rätta eller radera personuppgifter som rör dem, respekterar inte det väsentliga innehållet i den grundläggande rätten till effektivt domstolsskydd, vilken är stadfäst i artikel 47 i [EU-stadgan]
> (C-311/18 Schrems II p. 187)

Det är därför särskilt viktigt att en personuppgiftsansvarig organisation säkerställer denna rättighet, så att den inte undergrävs till följd av valet av molntjänstleverantör.

De grundläggande rättigheterna är inte absoluta, de får alltså begränsas. Under en pågående, legitim underrättelseinhämtning kan det exempelvis vara rimligt att inte bevilja tillgång till insamlade personuppgifter. Varje sådan begränsning av en grundläggande rättighet måste emellertid uppfylla vissa krav i EU-stadgan. Bland annat måste begränsningens omfattning tydligt framgå i lag. EU-domstolen har i flera rättsfall klargjort var gränsen går för godtagbara begränsningar. Den lagstiftning där rättighetsbegränsningen framgår måste uppfylla krav på tydlighet och precision. Ett syfte är att lagstiftningen ska ge ett effektivt skydd mot riskerna för missbruk.

En rättighetsbegränsning får inte gå längre än vad som är strikt nödvändigt för att tillgodose begränsningens syfte. Lagstiftning som innebär ett ingrepp i rättigheter måste i sig innehålla tydliga och precisa bestämmelser som reglerar räckvidden och tillämpningen av ingreppet och som fastställer minimikrav, så att de personer vilkas uppgifter överförs har tillräckliga garantier som möjliggör ett effektivt skydd av deras personuppgifter mot riskerna för missbruk. Lagstiftningen måste i synnerhet precisera under vilka omständigheter och på vilka villkor en åtgärd för behandling av personuppgifter får vidtas, vilket säkerställer att ingreppet begränsas till vad som är strikt nödvändigt (artikel 52.1 EU-stadgan, C-311/18 Schrems II p. 175-176).

Ibland hävdas att amerikanska lagstiftning visserligen möjliggör omfattande underrättelseinhämtning, i strid med EU-stadgans krav, men att lagstiftningen inte används på ett så omfattande sätt i praktiken. Det talar emellertid inte till lagstiftningens fördel – tvärt om.

Eftersom amerikansk lagstiftning som Foreign Intelligence Surveillance Act (FISA) möjliggör en mer omfattande inhämtning än vad som är motiverat menar vi att lagstiftningen inte säkerställer ett effektivt skydd mot riskerna för missbruk.

Facit visar dessutom att amerikanska myndigheters verksamhet är kantad av övertramp och bristande rättssäkerhet såväl historiskt som i närtid, vilket vi återkommer till i avsnitt 4.

Vi menar också att eventuella begränsningar som införs genom presidentdekret eller myndighetsinterna regelverk inte är kapabla att åtgärda dessa brister, eftersom EU-domstolen anger att det är den lagstiftning som innebär en rättighetsbegränsning som också måste slå fast de minimikrav som skyddar mot riskerna för missbruk (C-311/18 Schrems II p. 175-176).

Bristerna i amerikansk lagstiftning och skälen till att förändringarna i USA är otillräckliga utvecklas i avsnitt 3.

Vi har här översiktligt förklarat några aspekter av det rättighetsskydd EU-stadgan kräver. En organisation som inte kan säkerställa detta rättighetsskydd för de personuppgifter som behandlas kan inte heller uppfylla unionsrättens krav. Vi menar att flera av de rättigheter som EU-stadgan slår fast undermineras om en organisation låter personuppgifter i EU exponeras mot amerikansk lagstiftning som ges företräde framför EU:s lagstiftning. Så är fallet när en amerikansk molntjänstleverantör tillåts hantera personuppgifterna i EU.

Utlämnanden av personuppgifter till myndigheter regleras även i GDPR. Där är det tydligt att ett utlämnande endast godtas om utlämnandet har stöd i unionsrätten eller en medlemsstats nationella rätt. Tredjelands lagstiftning gör sig alltså icke besvär. Detta behandlas i nästa avsnitt.

2.3 GDPR:s skydd mot åtkomst från tredjeland

2.3.1 När personuppgiftsbiträdet får avvika från sina instruktioner

När en organisation i EU ska låta en molntjänstleverantör behandla personuppgifter å organisationens vägnar måste parterna ingå ett personuppgiftsbiträdesavtal.

Personuppgiftsbiträdesavtalet måste ange att molntjänstleverantören bara får behandla personuppgifter enligt den personuppgiftsansvariges instruktioner, även när det gäller tredjelandsöverföringar. Utan instruktioner från den personuppgiftsansvarige får biträdet alltså inte göra några tredjelandsöverföringar. Det enda undantaget, där personuppgiftsbiträdet (molntjänstleverantören) ändå får genomföra tredjelandsöverföringar utan instruktioner från den personuppgiftsansvarige, är om unionsrätten eller en medlemsstats nationella rätt kräver att biträdet gör det. Det framgår av artikel 28.3 a i GDPR.

Kraven på säkerhet för personuppgifter innebär på motsvarande sätt att personuppgiftsbiträden ska vidta åtgärder för att säkerställa att deras personal inte avviker från den personuppgiftsansvariges instruktioner såvida inte unionsrätten eller en medlemsstats nationella rätt ålägger dem att göra det. Det framgår av artikel 32.4 i GDPR.

Amerikanska underrättelselagar som FISA 702 utgör varken unionsrätt eller en medlemsstats nationella rätt. Samtidigt kan underrättelselagarna tvinga amerikanska molntjänstleverantörer att lämna ut uppgifter de hanterar i EU vid sidan av den personuppgiftsansvariges instruktioner.

Som vi noterade i avsnitt 1 kan inte heller adekvansbeslutet användas som grund för dessa utlämnanden, inte minst eftersom det endast omfattar självcertifierade mottagare i USA.

2.3.2 Rättslig grund för utlämnanden till myndigheter

När en molntjänstleverantör lämnar ut personuppgifter på begäran av en myndighet så agerar molntjänstleverantören inte längre enligt sin kunds instruktioner, utan blir själv personuppgiftsansvarig för utlämnandet. All personuppgiftsbehandling måste ha en rättslig grund i GDPR och frågan blir då vilken rättslig grund som en molntjänstleverantör kan använda. Utan en giltig rättslig grund uppfyller utlämnandet inte GPDR.

EU-domstolen har slagit fast att en kommersiell aktörs utlämnanden till brottsbekämpande myndigheter i princip inte får ske med stöd av den rättsliga grunden intresseavvägning enligt artikel 6.1 f i GDPR. EU-domstolen pekar istället på den rättsliga grunden rättslig förpliktelse som åvilar den personuppgiftsansvarige enligt artikel 6.1 c i GDPR, se mål C-252/21 p. 124. Utifrån EU-domstolens skäl bedömer vi att samma rättsliga grund blir relevant vid utlämnanden till underrättelsemyndigheter.

Den rättsliga förpliktelse som åvilar den personuppgiftsansvarige enligt artikel 6.1 c i GDPR måste i sin tur vara fastställd i unionsrätten eller en medlemsstats nationella rätt som den personuppgiftsansvarige omfattas av. Det framgår av artikel 6.3 i GDPR.

Amerikanska underrättelselagar som FISA utgör inte unionsrätt eller en medlemsstats nationella rätt. Amerikanska molntjänstleverantörer synes därför inte kunna förlita sig på någon rättslig grund i GDPR för utlämnanden till amerikanska myndigheter enligt dessa lagar. Som vi noterade i avsnitt 1 kan inte heller adekvansbeslutet användas.

2.3.3 Utlämnanden till tredjelands myndigheter kräver en internationell överenskommelse

Artikel 48 i GDPR erbjuder en grund för molntjänstleverantörer att verkställa beslut enligt tredjelands lagstiftning, men endast om beslutet grundar sig på en internationell överenskommelse mellan tredjelandet och EU eller en medlemsstat.

Adekvansbeslutet är inte en sådan internationell överenskommelse, vilket vi går in på i nästa avsnitt.

Artikel 48 anger i sin helhet:

> Överföringar och utlämnanden som inte är tillåtna enligt unionsrätten
> Domstolsbeslut eller beslut från myndigheter i tredjeland där det krävs att en peronuppgiftsansvarig eller ett personuppgiftsbiträde överför eller lämnar ut personuppgifter får erkännas eller genomföras på något som helst sätt endast om det grundar sig på en internationell överenskommelse, såsom ett avtal om ömsesidig rättslig hjälp, som gäller mellan det begärande tredjelandet och unionen eller en medlemsstat, utan att detta påverkar andra grunder för överföring enligt detta kapitel.
> (Cleuras understrykning)

Om en personuppgiftsansvarig eller ett personuppgiftsbiträde tar emot ett beslut som kräver att personuppgifter överförs eller lämnas ut till tredjelands myndigheter, så får beslutet med stöd av artikel 48 alltså:

- endast
- erkännas eller genomföras (eller rentav bli verkställbart, det vill säga möjligt att genomföra[1])
- på något som helst sätt
- om det grundar sig på en internationell överenskommelse.

Här noterar vi hur strängt formulerad artikel 48 är, vilket bekräftas av hur beaktandesats 115 i GDPR tydliggör EU-lagstiftarens aversion mot extraterritoriell lagstiftning.

Artikel 48 föregriper inte andra grunder för tredjelandsöverföringar, men vi menar att förutsättningar saknas även enligt övriga grunder. Adekvansbeslutet enligt artikel 45 kan inte användas eftersom NSA och andra amerikanska underrättelsemyndigheter inte är självcertifierade mottagare. Vi förväntar oss inte heller att amerikanska underrättelsemyndigheter ingår standardavtalsklausuler med amerikanska molntjänstleverantörer eller medverkar till att använda andra verktyg i artikel 46. Slutligen menar vi att det i princip inte går att förlita sig på artikel 49 i denna kontext[2], bland annat eftersom en molntjänstleverantör normalt inte informeras om omständigheterna bakom varje utlämnande med stöd av exempelvis FISA.

Utan en tillämplig internationell överenskommelse som grund så är alltså amerikanska molntjänstleverantörer förhindrade att överföra personuppgifter till tredjeland baserat på beslut från tredjelands myndigheter.

Microsofts President Brad Smith är en av de som påtalat behovet av internationella överenskommelser mellan USA och EU, som lösning på problemet med ensidig extraterritoriell åtkomst till uppgifter i EU.[3]

2.3.4 Adekvansbeslutet är inte en grund i unionsrätten, en medlemsstats nationella rätt eller en internationell överenskommelse – för utlämnanden till tredjelands myndigheter

Som vi noterade i avsnitt 1 möjliggör adekvansbeslutet endast tredjelandsöverföringar till självcertifierade mottagare i USA som finns med på det amerikanska handelsdepartementets lista. Amerikanska underrättelsemyndigheter som NSA är inte självcertifierade enligt de två tidigare ramverken Safe Harbour och Privacy Shield. De förväntas inte heller bli det enligt det nya Data Privacy Framework.

Adekvansbeslutet varken kräver eller möjliggör tredjelandsöverföringar från en organisation i EU till amerikanska underrättelsemyndigheter. Adekvansbeslutet är alltså inte en grund i unionsrätten eller en medlemsstats nationella rätt som kan användas för utlämnanden vid sidan

[1] I flera andra språkversioner av GDPR används begrepp med en annan betydelse än ”genomföras”. Innebörden är snarare att besluten inte ens får *bli verkställbara*. Se t.ex. följande språkversioner: engelska (”enforceable”), tyska (”vollstreckbar werden”), franska (”rendue exécutoire”) och italienska (”assumere qualsivoglia carattere esecutivo”).
[2] Vad gäller artikel 49, se även EDPB-EDPS Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection, s. 6 f. https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-edps-joint-response-libe-committee-impact-us-cloud-act_sv.
[3] ”We also need a new generation of international agreements that define when and how governments will seek data stored within other countries’ borders, starting with our European allies.”, https://www.washingtonpost.com/opinions/2021/06/13/microsoft-brad-smith-trump-justice-department-gag-orders/. EU och USA har exempelvis inlett förhandlingar om effektivare åtkomst till e-bevisning. Vad gäller underrättelseinhämtning, vilket Schrems-domarna handlar om, är det emellertid tyst.

av den personuppgiftsansvariges instruktioner enligt artikel 28.3 a eller 32.4, eller som rättslig förpliktelse enligt artikel 6.1 c och 6.3.

Även om det ibland talas om ett ”dataöverföringsavtal” eller ”datapakt” så är adekvansbeslutet i sig ingen internationell överenskommelse. Det är ett ensidigt beslut från EU-kommissionen, som inte tar sikte på att reglera åtkomst från underrättelsetjänster i USA till uppgifter i EU. Även FISA, den amerikanska presidentens EO 14086 och DPRC-bestämmelserna är ensidiga och utgör inte internationella överenskommelser. Inget av dessa instrument är en internationell överenskommelse som kan användas som grund för tredjelandsöverföringar enligt artikel 48.

2.3.5 GDPR-skyldigheter vid anlitande av molntjänstleverantörer

Vi har hittills konstaterat att amerikanska molntjänstleverantörer på flera punkter saknar rättsliga förutsättningar i GDPR för att lämna ut personuppgifter som de hanterar i EU, till amerikanska myndigheter. Vad får det för konsekvenser för en organisation som överväger att anlita en sådan molntjänstleverantör?

Artikel 24 i dataskyddsförordningen beskriver den personuppgiftsansvariges ansvar – oavsett om ett biträde anlitas. Artikeln kräver lämpliga tekniska och organisatoriska åtgärder för att *säkerställa* och *kunna visa* att personuppgiftsbehandling utförs i enlighet med GDPR.

Ansvaret fortlöper när en personuppgiftsansvarig ska anlita ett personuppgiftsbiträde, såsom en molntjänstleverantör. Den personuppgiftsansvarige ska endast anlita personuppgiftsbiträden som ger tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder *på ett sådant sätt* att behandlingen *uppfyller* kraven i GDPR och *säkerställer* att personers rättigheter skyddas (artikel 28.1 i GDPR).

En molntjänstleverantörs garantier ska alltså avse åtgärder som genomförs på ett sådant sätt att personuppgiftsbehandlingen uppfyller kraven i GDPR och säkerställer skyddet för personers rättigheter.

Frågan är då vilka garantier, om några, som amerikanska molntjänstleverantörer ger. I samtliga fall vi känner till anger amerikanska molntjänstleverantörer att de lämnar ut personuppgifter enligt tvingande myndighetsbeslut. Eftersom molntjänstleverantörerna omfattas av amerikansk lag, även när de är verksamma i EU, kommer de därmed följa beslut om att göra personuppgifter i EU tillgängliga för amerikanska myndigheter.

En del molntjänstleverantörer hävdar samtidigt att de tagit emot ganska få begäranden från amerikanska myndigheter, åtminstone med utgångspunkt i specifika lagrum, kategorier av begäranden, kundsegment, tjänster eller uppgiftstyper. Med det vill molntjänstleverantörerna antyda en så låg sannolikhet för utlämnanden att den i praktiken borde bortses från. Trots det innebär alla villkor från amerikanska molntjänstleverantörer som vi har tagit del av att den amerikanska rättsordningen ges företräde framför EU:s rättsordning.

De amerikanska molntjänstleverantörerna framställer detta som en självklarhet, att de i egenskap av amerikanska bolag givetvis måste verkställa beslut enligt amerikansk jurisdiktion. De förväntar sig därmed med samma självklarhet att deras kunder i EU ska ge upp företrädet för sin egen rättsordning till förmån för amerikansk. Om sannolikheten för utlämnanden är så obetydlig frågar vi oss varför ingen amerikansk molntjänstleverantör är beredd att lova att den kommer att neka varje begäran om utlämnande, åtminstone inom vissa kundsegment eller tjänstetyper. Av samma skäl frågar vi oss varför amerikansk underrättelselagstiftning inte kan begränsas för att utesluta möjligheten till sådana utlämnanden som ändå inte påstås ske i verkligheten.

Som vi noterade i avsnitt 2.2 finns det ingenting tilltalande med lagstiftning som kan användas för omfattande inhämtning men som normalt sett inte används så brett i praktiken. Genom att lagstiftning som FISA möjliggör en mer omfattande inhämtning än vad som är motiverad menar vi att lagstiftningen inte säkerställer ett effektivt skydd mot riskerna för missbruk i enlighet med unionsrättens krav. Vi har i avsnitt 4 inkluderat ett axplock av övertramp och bristande rättssäkerhet vid amerikansk övervakning.

En molntjänstleverantör kan ha svårt att råda över antalet begäran om utlämnande som den tar emot, oavsett vad antalet varit historiskt. Vi ifrågasätter därför om statistiken över utlämnanden till amerikanska myndigheter kan anses vara en del av personuppgiftsbiträdets garantier. Däremot skulle statistik från ett tredjeland vars lagstiftning når upp till unionsrättens skyddsnivå kunna bekräfta bilden av att lagstiftningen efterlevs i praktiken.

Vi har dessutom noterat EU-domstolens syn på vad som krävs för att säkerställa unionsrättens skyddsnivå – och vad som är tillräckligt för att undergräva den. Vi menar att EU-domstolens uppfattning inte tycks ge utrymme för att bedöma sannolikheten för utlämnanden, typen av personuppgifter eller konsekvenserna för den enskilde.

EU-domstolen har vid en tredjelandsöverföring bedömt att ett effektivt skydd för personuppgifter inte kunde säkerställas när *lagstiftningen* i tredjeland *tillät* tredjelandets myndigheter att göra ingrepp i personers rättigheter. EU-domstolen har likaså angett att en tredjelandsöverföring måste avbrytas redan när *lagstiftningen* i tredjelandet föreskriver skyldigheter som *kan* äventyra det unionsrättsliga skydd som ska säkerställas.[4] EU-domstolen angav inte att det behövde ha skett något faktiskt utlämnande till amerikanska myndigheter eller att så ens behövde vara sannolikt. Den avgörande faktorn var *vad lagstiftningen tillät och kunde användas för*.

EU-domstolen har också angett att utlämnande av personuppgifter till en myndighet utgör ett ingrepp i grundläggande rättigheter oavsett hur uppgifterna används. Det förhåller sig på samma sätt med personuppgifter som lagras i syfte att myndigheter ska använda sig av dem. EU-domstolen har vidare angett att det i sammanhanget saknar betydelse om uppgifter som avser privatlivet är av känslig art eller om berörda personer har fått utstå eventuella olägenheter.[5]

Vi menar att detta borde tydliggöra vad som krävs för att säkerställa unionsrättens skyddsnivå vid personuppgiftsbehandling inom EU. När skyddsnivån vid en tredjelandsöverföring bedöms måste jämförelseobjektet vara skyddsnivån inom EU. Det är alltså skyddsnivån inom EU som tredjelandsöverföringen ska vara minst väsentligen likvärdig med. Som framgår av artikel 44: ”Alla bestämmelser i [kapitel V] ska tillämpas för att säkerställa att den nivå på skyddet av fysiska personer som säkerställs genom denna förordning inte undergrävs” (Cleuras understrykning). Det är vad det innebär att skyddet för personuppgifterna följer personuppgifterna *från EU* till tredjeland.

Vi har därför svårt att se att EU-domstolen skulle tillämpa en högre skyddsnivå vid tredjelandsöverföringar än vid behandling i EU enligt GDPR, inklusive enligt artikel 28, 32 och så vidare. Att kräva ett högre skydd vid tredjelandsöverföringar än den redan höga skyddsnivån inom EU vore till synes oproportionerligt och skulle dessutom motverka syftet med att

[4] C-311/18 Schrems II p. 126 och 135. Jfr även mål C-293/12 där EU-domstolen ogiltigförklarade datalagringsdirektivet i sin helhet trots att det kan förmodas att en mycket liten andel av de lagrade uppgifterna någonsin skulle komma att lämnas ut. Det målet gällde behandling och utlämnanden till myndigheter i EU.

[5] C-311/18 Schrems II p. 171. I den svenska språkversionen anges att det har *föga* betydelse om uppgifterna är av känslig art eller om personer drabbas av någon olägenhet, men i flera andra språkversioner är innebörden i stället *oavsett*. Se t.ex. engelska (”irrespective”), tyska (”es nicht darauf ankommt”), franska (”indépendamment”) och italienska (”indipendentemente”).

underlätta internationell handel och samarbete, som anges i skäl 101 i GDPR. Att skyddsnivån vid en tredjelandsöverföring endast behöver vara *väsentligen likvärdig* den inom EU talar också om något för ett utrymme för en *något lägre* skyddsnivå vid en tredjelandsöverföring än vid personuppgiftsbehandling inom EU. Det betyder att motsatt förhållande inte borde vara möjligt; personuppgiftsbehandling i EU kan inte omgärdas av en lägre skyddsnivå än vid en tredjelandsöverföring.

När EU-domstolen bedömer att en tredjelandsöverföring inte är tillåten redan när *lagstiftningen* i tredjeland *tillåter* tredjelandets myndigheter att göra ingrepp i personers unionsrättsliga rättigheter, samt att en tredjelandsöverföring måste avbrytas redan när *lagstiftningen* i tredjelandet föreskriver skyldigheter som *kan* äventyra det unionsrättsliga skyddet, drar vi därför slutsatsen att ribban för att säkerställa unionsrättens skydd vid personuppgiftsbehandling *i EU* måste vara i vart fall *minst lika hög*.

Unionsrättens skyddsnivå vid personuppgiftsbehandling inom EU, inbegripet enligt artikel 28 och 32 i GDPR, skulle därmed inte kunna säkerställas när amerikansk lagstiftning föreskriver skyldigheter gentemot en molntjänstleverantör som *tillåter* amerikanska myndigheter att göra ingrepp i personers rättigheter eller som *kan* äventyra unionsrättens skydd. Så är fortfarande fallet med exempelvis FISA 702, oavsett adekvansbeslutet.

Mot ovan bakgrund ser vi inte hur en amerikansk molntjänstleverantör kan anses ha vidtagit åtgärder som är tillräckliga för att uppfylla kraven i GDPR och säkerställa att individers rättigheter skyddas, när molntjänstleverantörens besked innebär att:

- Molntjänstleverantören omfattas av amerikansk extraterritoriell lagstiftning samt har klargjort att den kommer att lämna ut personuppgifter i EU till amerikanska myndigheter enligt sådan lagstiftning.

- Molntjänstleverantören tillåter sig att i strid med kraven i personuppgiftsbiträdesavtalet enligt artikel 28.3 a åsidosätta den personuppgiftsansvariges instruktioner samt i strid med artikel 32.4 i GDPR låter sin personal göra detsamma, för att lämna ut personuppgifter i EU till amerikanska myndigheter utan stöd i unionsrätten eller en medlemsstats nationella rätt.

- Molntjänstleverantören tillåter sig att i strid med artikel 6.1 c och 6.3 i GDPR lämna ut personuppgifter i EU till amerikanska myndigheter utan en korrekt rättslig grund i form av en rättslig förpliktelse i unionsrätten eller en medlemsstats nationella rätt.

- Molntjänstleverantören tillåter sig att i strid med artikel 48 i GDPR lämna ut personuppgifter i EU till amerikanska myndigheter utan stöd i en internationell överenskommelse.

Vad amerikanska molntjänstleverantörer faktiskt garanterar är därmed att de vidtar åtgärder som säkerställer att de *inte* uppfyller kraven i GDPR. Vi menar att sådana molntjänstleverantörer inte ger de garantier som krävs för att anlitas som personuppgiftsbiträden enligt artikel 28.1 i GDPR.

3 EO 14086 och DPRC-bestämmelserna

3.1 Inledning

Som vi tidigare noterat innebär GDPR att amerikanska molntjänstleverantörer inte får verkställa tredjelandsöverföringar till amerikanska underrättelsemyndigheter utan en grund i unionsrätten eller en medlemsstats nationella rätt.

Någon sådan grund finns inte idag. Adekvansbeslutet ger inte heller någon sådan grund. Eftersom amerikanska molntjänstleverantörer uppger att de ändå kommer att verkställa sådana beslut om utlämnanden menar vi att dessa leverantörer inte ger de garantier som krävs för att anlitas som personuppgiftsbiträden enligt GDPR. Skälen för detta utvecklas i avsnitt 2.3.

Dessa regler i GDPR gäller när personuppgifter ska behandlas *i EU*. Den springande punkten är att utlämnanden då inte får ske utan en grund i unionsrätten eller en medlemsstats nationella rätt. Utan en sådan grund får utlämnanden enligt tredjelands lag inte ske, oavsett om tredjelandets lag uppfyller krav på rättssäkerhet. Även om adekvansbeslutet skulle förbli giltigt består därmed de rättsliga problem som vi tar upp i avsnitt 2 i denna rapport, vilket utgör hinder för att använda amerikanska molntjänstleverantörer för personuppgiftsbehandling i EU.

Vi ska ändå gå igenom några av förändringarna på den amerikanska sidan, som det tredje adekvansbeslutet förlitar sig på. Syftet är att få en bättre bild av sannolikheten att EU-domstolen ogiltigförklarar adekvansbeslutet samt en förståelse för i vilka delar amerikansk rätt ännu brister i förhållande till unionsrätten. Den bedömningen är främst relevant om en organisation överväger tredjelandsöverföringar till USA, inte när organisationen behandlar personuppgifter i EU.

För att värdera amerikansk rätt börjar vi med EU-domstolens bedömning i Schrems II. EU-domstolen angav där att amerikanska övervakningsprogram som grundar sig på FISA 702, Executive Order 12333 och Presidential Policy Directive 28 inte motsvarar de minimikrav som unionsrätten kräver enligt proportionalitetsprincipen. Det innebär att övervakningsprogrammen som grundas på dessa bestämmelser inte kan anses vara begränsade till vad som är strikt nödvändigt.

EU-domstolen konstaterade dessutom att övervakningsprogrammen inte ger personer rättigheter som kan göras gällande mot amerikanska myndigheter i domstol, vilket innebär att personerna inte har rätt till ett effektivt rättsmedel.

USA har därefter gjort i huvudsak två förändringar som EU-kommissionen hänvisat till för att fatta adekvansbeslutet från juli 2023. Vi ska därför titta närmare på några relevanta delar av dessa förändringar för att se om de gör någon betydelsefull skillnad.

För det första har USA:s president utfärdat Executive Order 14086 med regler för signalspaning (EO 14086), vilka har implementerats av underrättelsetjänsterna. För det andra anger EO 14086 att USA:s justitieminister ska utfärda bestämmelser som inrättar en prövningsinstans kallad Data Protection Review Court (DPRC-bestämmelserna).

Frågan är då om EO 14086 och DPRC-bestämmelserna åtgärdar de brister som EU-domstolen identifierade i Schrems II. Andra aktörer har gjort djupgående analyser av detta.[6] I korthet bedömer vi att EO 14086 och DPRC-bestämmelserna är problematiska i förhållande till

[6] Se exempelvis https://www.justsecurity.org/83845/the-biden-administrations-sigint-executive-order-part-i-new-rules-leave-door-open-to-bulk-surveillance/ och https://www.justsecurity.org/83927/the-biden-administrations-sigint-executive-order-part-ii/.

unionsrätten. I följande avsnitt går vi närmare in på skälen för den slutsatsen. Redogörelsen gör inte anspråk på att vara fullständig.

3.2 EO 14086

För det första ifrågasätter vi av två skäl om EO 14086[7] kan uppfylla EU-stadgans krav på att rättighetsbegränsningar ska framgå i lag.

Dels koncentrerar en exekutiv order makten till en person, presidenten, som när som helst kan ändra eller upphäva en exekutiv order. Presidenten kan dessutom uppdatera delar av EO 14086 i hemlighet utifrån en bedömning presidenten själv råder över, se sektion 2(b)(i)(B) och sektion 2(c)(ii)(C). Ett sådant upplägg kännetecknar enligt vår mening inte ”lag”. Utöver detta är en exekutiv order i vart fall inte *lagstiftning*, samtidigt som EU-domstolen talar i termer av krav som ställs på just lagstiftning (”legislation”), se C-311/18 Schrems II p. 176.

Dels har EU-domstolen slagit fast att ”den rättsliga grund som gör ingreppet i rättigheterna möjligt i sig ska definiera räckvidden av begränsningen i utövandet av den aktuella rättigheten” (Cleuras understrykning). EU-domstolen anger att detta är en förutsättning för att uppfylla EU-stadgans krav på proportionalitet (C-311/18 Schrems II p. 175-176). Som vi förstår det är FISA 702 lagstiftning som gör övervakning möjlig vilket skulle vara fallet även utan EO 14086. Övervakning med stöd av FISA 702 innebär ett ingrepp i personers rätt till privatliv och skydd för personuppgifter, vilket är grundläggande rättigheter. EU-domstolen har slagit fast att FISA 702 inte uppfyller EU-stadgans krav på proportionalitet (C-311/18 Schrems II p. 184). För att åtgärda detta synes det därför behövas någon form av ändring av FISA 702 så att FISA 702 *i sig* definierar räckvidd och omfattning på de rättighetsbegränsningar övervakningen innebär. Någon sådan ändring har emellertid inte skett. Istället har EO 14086 införts med förhållningsregler för underrättelseverksamheten. Vi menar att EO 14086 inte synes vara kapabel att kompensera för bristen på proportionalitet i FISA 702 eftersom EO 14086 inte är den rättsliga grund som FISA 702 är.

För det andra ifrågasätter vi – alldeles oavsett bedömning i den första frågan – om skrivningarna i EO 14086 materiellt uppfyller kraven på tydlighet och precision utifrån EU-stadgans krav på proportionalitet (se avsnitt 2.2). Nödvändighet och proportionalitet nämns i EO 14086, men det är sparsamt med formuleringar som utvecklar vad begreppen innebär konkret. Skrivningarna är också vaga om när alternativ till signalspaning ska prioriteras. Så ska ske när alternativen är ”tillgängliga, görliga, och lämpliga” (”available, feasible, and appropriate”).

Begreppen ”necessary” och ”proportionate” i EO 14086 kan vid en första anblick se ut att anknyta till unionsrättsliga koncept, i synnerhet eftersom begreppen är centrala i EU-domstolens tolkning av EU-stadgan i Schrems II. Dessutom anger EO 14086 flera förhållningsregler avseende ”personal information”. Avsikten verkar dock inte vara att begreppen ska tolkas i linje med unionsrätten. DPRC, som ska pröva om övervakning har gått rätt till enligt EO 14086, ska nämligen tolka EO 14086 och dess begrepp uteslutande i ljuset av amerikansk rätt och rättstradition, inte någon annan rättskälla. Det framgår av § 201.10 i DPRC-bestämmelserna.

Mot ovan bakgrund betvivlar vi att EO 14086 uppfyller unionsrättens krav på tydliga bestämmelser som preciserar under vilka omständigheter och på vilka villkor underrättelse-inhämtning får ske. Vi har svårt att se hur EO 14086 på ett tillräckligt tydligt sätt, i enlighet med unionsrättens krav, reglerar räckvidden och tillämpningen av underrättelseinhämtningen och

[7] Executive Order 14086 On Enhancing Safeguards For United States Signals Intelligence Activities, https://www.whitehouse.gov/briefing-room/presidential-actions/2022/10/07/executive-order-on-enhancing-safeguards-for-united-states-signals-intelligence-activities/ även tillgänglig i strukturerad form här: https://noyb.eu/sites/default/files/2022-10/Biden%20EO%20on%20Surveillance%2C%20Structured.pdf

fastställer minimikrav som ger personer tillräckliga garantier som möjliggör ett effektivt skydd av deras personuppgifter mot riskerna för missbruk (se avsnitt 2.2 för mer om dessa krav). Saken blir inte bättre av att DPRC är förbjuden att tolka begreppen nödvändighet och proportionalitet utifrån unionsrätten, att ”personal information” inte tycks motsvara GDPR:s definition av personuppgifter samt att DPRC inte får beakta rättsutvecklingen inom EU när den tolkar hur EO 14086 tillämpas i praktiken.

3.3 DPRC-bestämmelserna

DPRC-bestämmelserna[8] utfärdades av det amerikanska justitiedepartementet utifrån presidentens uppdrag i EO 14086. DPRC-bestämmelserna inrättar prövningsinstansen Data Protection Review Court (DPRC). Syftet får förstås som att DPRC ska tillgodose unionsrättens krav på ett effektivt rättsmedel efter att EU-domstolen bedömde att Privacy Shield-ombudsmannen inte var tillräcklig (C-311/18 Schrems II p. 197).

För det första ifrågasätter vi om DPRC uppfyller EU-stadgans krav på rätten till en rättvis och offentlig rättegång ”inför en oavhängig och opartisk domstol som har inrättats enligt lag.”

Vad gäller kravet på att inrättas *enligt lag* är frågetecknen desamma som för EO 14086, vilket behandlas i första delen av avsnittet om EO 14086 ovan.

Vad gäller kravet på oavhängighet och opartiskhet noterar vi att USA:s styrelseskick präglas av maktdelningsläran, uppdelad i lagstiftaren (kongressen), den verkställande makten (presidenten) samt den dömande makten (federala domstolar). DPRC är inte en federal domstol tillhörande den dömande makten utifrån denna uppdelning. DPRC har inrättats av justitiedepartementet men är dessutom i sig *en del av* justitiedepartementet[9] och därmed den verkställande makten.

DPRC:s ledamöter tillsätts av justitieministern. Ledamöterna tycks emellertid också endast erhålla ett skydd för sitt förordnande och mot repressalier i förhållande till justitieministern, inte presidenten.[10] EU-domstolen har anmärkt att Privacy Shield-ombudsmannen inte tycktes omfattas av garantier *i förhållande till den verkställande makten* vad gällde sitt förordnade (C-311/18 Schrems II p. 195). Presidenten är den som ytterst utövar den verkställande makten i USA.

För det andra omfattar DPRC:s behörighet endast vissa typer av överträdelser, så kallade ”covered violations”. I korthet tycks denna definition kräva att en överträdelse *dels* negativt påverkar en persons integritet (”privacy”) och samhälleliga rättighetsintressen (”civil liberties interests”), *dels* är en överträdelse av den amerikanska konstitutionen, delar av FISA eller FISC-förfaranden, EO 12333 eller relaterade förfaranden, EO 14086 eller relaterade policyer och förfaranden, en efterföljande lag, order, policy eller förfarande, eller andra lagar, order, policyer eller förfaranden med liknande omfattning som EO 14086.[11]

Såvitt vi känner till innehåller ingen av dessa lagar eller bestämmelser en tillämplig rätt till tillgång till personuppgifter eller rätt till rättelse av felaktiga personuppgifter, åtminstone inte i en utsträckning som liknar unionsrätten där de utgör grundläggande rättigheter med tillhörande proportionalitetskrav vid begränsningar.[12] Vi ifrågasätter också om det tillräckligt tydligt går att

[8] Department of Justice, Data Protection Review Court Final Rule: https://www.justice.gov/d9/pages/attachments/2022/10/07/dprc_final_rule_signed.pdf
[9] ”The DPRC will be established within the Department of Justice”, s. 3 DPRC-bestämmelserna.
[10] § 201.7 (d) DPRC-bestämmelserna.
[11] § 201.2 DPRC-bestämmelserna, som pekar på definitionen av ”covered violation” i EO 14086, se sektion 4(d).
[12] Vi förmodar att det i så fall redan hade varit känt med tanke på att resursstarka aktörer på olika sätt har belyst amerikansk rätt under de rättsprocesser som ledde fram till Schrems II-domen.

läsa in dessa dataskyddsrättigheter i begreppen ”privacy” och ”civil liberties interests”. Integritet (privacy) brukar tillskrivas artikel 7 i EU-stadgan medan dataskydd hör till artikel 8. Det kan vara en bedömningsfråga hur integritetskänslig en personuppgiftsbehandling får vara medan dataskyddsrättigheter som tillgång och rättelse gäller oavsett integritetsintrånget. Till saken hör att när begrepp som ”privacy” och ”civil liberties interests” anges i EO 14086 ska de inte tolkas med unionsrätten i åtanke, utan uteslutande i ljuset av amerikansk rätt och rättstradition. Det framgår i § 201.10 DPRC-bestämmelserna.

När i unionsrätten grundläggande rättigheter inte uttryckligen erkänns eller preciseras i det amerikanska regelverket, är det möjligt att rättigheterna inte heller går att kränka i form av en överträdelse som omfattas (”covered violation”) från första början. DPRC verkar därför inte heller kunna besluta om korrigerande åtgärder i alla de fall där dessa unionsrättsliga rättigheter har kränkts.

För det tredje, och som vi berörde i föregående punkt, ger DPRC-bestämmelserna inte den klagande någon rätt till tillgång till en domstolsprövning för att erhålla tillgång till sina personuppgifter. En klagande synes därför inte heller vara tillförsäkrad sin rätt till rättelse eller radering. Som en konsekvens av det synes DPRC inte heller ha tillräckliga förutsättningar för att bedöma en övervakningsåtgärds proportionalitet och laglighet.

EU-domstolen har angett att ”Enligt fast rättspraxis är själva möjligheten till en effektiv domstolsprövning i syfte att säkerställa iakttagandet av unionsrätten en grundförutsättning för en rättsstat. En lagstiftning i vilken det inte föreskrivs någon möjlighet för enskilda att använda rättsmedel för att erhålla tillgång till, rätta eller radera personuppgifter som rör dem, respekterar inte det väsentliga innehållet i den grundläggande rätten till effektivt domstolsskydd, vilken är stadfäst i artikel 47 i [EU-stadgan]”. (C-311/18 Schrems II p. 187).

Rätten till domstolsprövning inbegriper alltså *att få sin rätt till tillgång eller rättelse av personuppgifter prövad av en domstol*. Rätten till tillgång och rätten till rättelse är inte absoluta, men varje begränsning ska vara proportionerlig utifrån EU-stadgans krav. Det kan alltså i vissa situationer vara möjligt att undanhålla information från en person, men det ska vara i undantagsfall. Ett viktigt syfte med en oberoende och oavhängig domstolsprövning blir då att slå fast om det verkligen är motiverat att undanhålla uppgifter från en person. Det är en sådan domstolsprövning som EU-domstolen anger är en grundförutsättning för en rättsstat.

I EU-kommissionens adekvansbeslut från juli 2023 hänvisas bland annat till möjligheten att begära ut uppgifter med stöd av den amerikanska Freedom of Information Act (FOIA), med reservation för olika undantag såsom när information är sekretessbelagd med hänsyn till nationell säkerhet. Utländska underrättelseuppgifter vars existens är hemligstämplad hos FBI är dessutom helt undantagna FOIA:s tillämpningsområde.[13] Vi förutsätter att EU-domstolen vid domen i Schrems II kände till befintliga vägar för att söka åtkomst till uppgifter, såsom FOIA. Vad gäller tillgången till rättslig prövning rörande FISA-övervakning noterade EU-domstolen hur EU-kommissionen uppmärksammat att den möjligheten är begränsad för icke-amerikaner, bland annat genom kravet på att visa talerätt, vilket synes ha varit ett skäl till att Privacy Shield-ombudsmannen infördes (C-311/18 Schrems II p. 45, i citaten av skäl 115-116).

EU-domstolen har även bedömt att det av FISA 702 inte kan utläsas några garantier för icke-amerikaner som eventuellt omfattas av övervakning samt att även om övervakningen måste följa reglerna i PPD-28 så ger PPD-28 inte individer rättigheter som de kan göra gällande *i domstol* mot amerikanska myndigheter (C-311/18 Schrems II p. 181). Vår slutsats är därmed att amerikansk rätt inte har räckt till för att ge icke-amerikaner effektiva rättsmedel, och att så förblir

[13] https://www.foia.gov/faq.html, ”What are exclusions?”

fallet såvida inte DPRC-bestämmelserna åtgärdar det som var otillräckligt med Privacy Shield-ombudsmannen.

DPRC-bestämmelserna anger att klagandeprocessen avslutas med ett slutligt besked ”utan att bekräfta eller förneka om den klagande var föremål för signalspaningsverksamhet”. Beskedet ska i samtliga fall att lyda ”Granskningen visade antingen inte på några överträdelser som omfattades eller så utfärdade Data Protection Review Court ett beslut som krävde lämpliga åtgärder”.[14] Även om DPRC måste tilldela den klagande en särskild ombudsperson (”Special Advocate”), får denne inte avslöja huruvida den klagande varit föremål för USA:s signalspaningsverksamhet.[15]

Eftersom DPRC inte ger de klagande någon rätt att veta om de varit föremål för signalspaning kan DPRC inte heller ge de klagande någon domstolsprövning av rätten att få tillgång till, rätta eller radera personuppgifter som rör dem. Även om DPRC på pappret kan besluta om exempelvis rättelse eller radering menar vi att det är närmast oundvikligt att DPRC får ett otillräckligt underlag för sina granskningar och åtgärder, och att DPRC därför i praktiken inte kan tillförsäkra att sådana åtgärder vidtas när det behövs.

En person kan nämligen svårligen beskriva för DPRC hur en uppgift borde rättas eller förklara varför den är irrelevant och borde raderas om personen inte först får tillgång till uppgiften för att värdera den. Utan att ta del av uppgiften kan personen inte heller påtala omständigheter som är relevanta för att DPRC ska kunna bedöma om själva insamlingen av uppgiften varit proportionerlig och lagenlig. Rätten till tillgång till uppgifter är alltså en förutsättning för att utöva andra grundläggande rättigheter. EU-domstolen har angett:

> Den rätt till tillgång som föreskrivs i artikel 15 i dataskyddsförordningen måste således göra det möjligt för den registrerade att försäkra sig om att de personuppgifter som rör honom eller henne är korrekta och att de behandlas på ett lagenligt sätt … I synnerhet är denna rätt till tillgång nödvändig för att möjliggöra för den registrerade att, i förekommande fall, kunna utöva sin rätt till rättelse, sin rätt till radering (”rätten att bli bortglömd”) och sin rätt till begränsning av behandling … liksom … sin rätt att föra talan till följd av skada (Mål C-487/21, p. 34-35.)

Vår slutsats är därför att DPRC inte ger personer *någon* rätt till en domstolsprövning av rätten till tillgång eller rättelse av personuppgifter. Som en konsekvens saknar DPRC även en effektiv möjlighet att pröva övervakningens laglighet samt personers rätt till begränsning av behandlingen och rätt att föra talan till följd av skada.

DPRC åtgärdar alltså inte det som EU-domstolen identifierade som otillräckligt med Privacy Shield-ombudsmannen, och amerikansk rätt når därför fortfarande inte upp till unionsrättens krav på effektiva rättsmedel.

Även om vi skulle bortse från DPRC, och en person i EU på något sätt skulle erhålla talerätt (”standing”) inför en amerikansk domstol, ifrågasätter vi dessutom om amerikanska domstolar är fullt ut behöriga att pröva relevanta omständigheter vid en fråga om rätten till tillgång till personuppgifter.

Vi förstår nämligen EU-domstolens praxis som att en begränsning av en persons rätt till tillgång till personuppgifter inte innebär att *domstolen* kan hindras från att ta del av uppgifterna för att pröva personens rätt till tillgång enligt artikel 47 i EU-stadgan.[16] Vi noterar härvid att den

[14] § 201.9 (h) DPRC-bestämmelserna, Cleuras översättning.
[15] § 201.11 (b) DPRC-bestämmelserna, Cleuras översättning.
[16] Se domen i de förenade målen C-584/10 P, C-593/10 P och C-595/10 P, p. 100-102 och 125-126, särskilt ”vilket inte påverkar den rätt som den behöriga domstolen har att kräva att den aktuella myndigheten

amerikanska rättsprincipen om State Secrets Privilege ger den verkställande makten (regeringen) i USA en möjlighet att helt undanta information från att behandlas i en domstolsprocess. En domare kan rentav behöva besluta att information ska undantas från ett mål utan att domaren själv fått ta del av informationen som regeringen hävdar omfattas av State Secrets Privilege.[17] Som ett resultat kan domaren sedan behöva skriva av målet.

Denna begränsning av domstolarnas möjlighet att ta del av information synes inte vara förenlig med EU-domstolens tolkning av rätten till ett effektivt rättsmedel enligt artikel 47 i EU-stadgan.

För det fjärde begränsas DPRC vad gäller de åtgärder DPRC kan besluta om vid en konstaterad överträdelse:

> Innan en DPRC-panel fastställer en lämplig åtgärd … ska den genom ODNI CLPO inhämta synpunkter från berörda delar av underrättelsegemenskapen om den lämpliga åtgärden, inbegripet en bedömning av effekterna på underrättelse-gemenskapens verksamhet och USA:s nationella säkerhet. Panelen ska ta vederbörlig hänsyn till dessa synpunkter (”due account of these views”) samt till sedvanliga sätt (”customary ways”) för att hantera den typ av överträdelse som identifierats.
> (DPRC-bestämmelserna, s. 15, Cleuras översättning)

Detta begränsar DPRC:s handlingsfrihet i val av åtgärd, eftersom DPRC är skyldig att ta hänsyn till synpunkter och sedvanliga arbetssätt som inte nödvändigtvis grundar sig på vad som är rättsligt påkallat.

3.4 Sammanfattande slutsatser om EO 14086 och DPRC-bestämmelserna

Vi ifrågasätter huruvida EO 14086 och DPRC-bestämmelserna når upp till unionsrättens skyddsnivå på flera punkter, i synnerhet:

- Huruvida EO 14086 kan anses utgöra lag i den mening som EU-stadgan kräver, särskilt till följd av maktkoncentrationen hos presidenten som när som helst kan ändra eller upphäva EO 14086 och i hemlighet kan ändra i delar av EO 14086.

---

redovisar sina skäl … Detta är nödvändigt … för att behörig domstol fullt ut ska kunna genomföra laglighetskontrollen av det aktuella beslutet … Ett påstående om kränkning av rätten till försvar och rätten till ett effektivt domstolsskydd måste dessutom prövas mot bakgrund av de specifika omständigheterna i varje enskilt fall … Det är riktigt att det finns tvingande hänsyn som rör unionens eller dess medlemsstaters säkerhet eller deras internationella relationer som kan utgöra hinder för att lämna ut vissa uppgifter eller viss bevisning till den berörda personen. I sådana fall ankommer det dock på unionsdomstolen, mot vilken det inte kan göras gällande att uppgifterna eller bevisen är sekretessbelagda eller hemliga, att inom ramen för sin domstolsprövning, använda sig av metoder som gör det möjligt att förena berättigade säkerhetshänsyn … med nödvändigheten av att i tillräcklig utsträckning säkerställa den enskildes processuella rättigheter, såsom rätten att yttra sig och principen om ett kontradiktoriskt förfarande … Domstolen ska härvid med beaktande av samtliga rättsliga och faktiska omständigheter som åberopats av den behöriga unionsmyndigheten, pröva om det finns stöd för de skäl för att motsätta sig en sådan utlämning som myndigheten har anfört” (Cleuras understrykning)

[17] ”*Reynolds*, on the other hand, expressly states that examination of the evidence at issue, ‘even by the judge alone, in chambers,’ should not be required if the Government shows ‘a reasonable danger that compulsion of the evidence’ will expose information that ‘should not be divulged’ in ‘the interest of national security.’ … Thus, the state secrets privilege … may sometimes preclude even *in camera, ex parte* review of the relevant evidence.” https://www.supremecourt.gov/opinions/21pdf/20-828_5ie6.pdf. Angående State Secrets Privilege, se även https://www.aktuellsakerhet.se/state-secrets-privilege-ett-forbisett-hinder-mot-tredjelandsoverforing-av-personuppgifter-till-usa

- Huruvida EO 14086 uppfyller kraven på proportionalitet, på grund av dess vaga skrivningar om nödvändighet och proportionalitet samt när alternativ till signalspaning ska prioriteras (när det är ”tillgängligt, görligt och lämpligt”). Dessutom ska begrepp som till synes relaterar till unionsrätten inte tolkas i enlighet med unionsrätten.

- Huruvida DPRC uppfyller EU-stadgans krav på rätten till en ”rättvis och offentlig rättegång … inför en oavhängig och opartisk domstol som har inrättats enligt lag”. Detta med tanke på att DPRC i sig självt är en del av justitiedepartementet och därmed den verkställande makten.

- Huruvida DPRC:s ledamöter får ett tillräckligt skydd för sitt förordnande och mot repressalier. DPRC-bestämmelserna tycks endast ge ett skydd i förhållande till USA:s justitieminister men inte mot presidenten, som ytterst utövar den verkställande makten.

- Att DPRC:s behörighet inte tycks omfatta alla kränkningar av grundläggande unionsrättsliga rättigheter, eftersom dessa inte alltid verkar anses utgöra s.k. ”covered violations”.

- Att DPRC-bestämmelserna inte tillförsäkrar individer någon rätt till tillgång till sina personuppgifter, och därmed inte heller möjligheten att utöva rätten till rättelse eller radering på ett effektivt sätt, eller att påtala omständigheter som är nödvändiga för att DPRC ska kunna bedöma en övervakningsåtgärds proportionalitet och laglighet.

- Att DPRC:s handlingsutrymme vid beslut om åtgärder är kringskuret genom att DPRC måste ta hänsyn till underrättelsetjänsternas synpunkter och arbetssätt, som inte nödvändigtvis grundar sig i vad som är rättsligt påkallat.

4 Exempel från verkligheten vid amerikansk övervakning

Amerikansk övervakning är kantad av övertramp och bristande rättssäkerhet, såväl historiskt som i närtid.

Här följer ett axplock där några exempel gäller olagligt agerande medan andra exempel visar på vad som helt lagligt fått äga rum.

- Redan 1975 slog den s.k. Church-kommittén fast att USA:s federala statsmakt under många årtionden ”avsiktligt åsidosatt” rättsliga begränsningar av sin övervakningsverksamhet och ”kränkt amerikanska medborgares konstitutionella rättigheter”.[18]

- I oktober 2015 framkom att NSA brutit mot ett övervakningsavtal med sin tyska motsvarighet. Nästan 70 % av de selektorer som Tyskland undersökte, och som NSA ville bedriva övervakning mot, avsåg regeringsorgan i EU-länder. Även europeiska företag var måltavlor.[19]

- I februari 2020 förklarade en amerikansk domstol att ett övervakningsprogram som NSA använt för att samla in miljarder uppgifter med samtalstrafik var olagligt. Domstolen

[18] https://www.intelligence.senate.gov/sites/default/files/94755_II.pdf, s. 137 (s. 153 i PDF-dokumentet).
[19] https://www.spiegel.de/politik/deutschland/nsa-selektorenliste-kurt-graulich-spricht-von-klarem-vertragsbruch-a-1060280.html

kritiserade dessutom amerikanska myndigheters uttalanden om övervakningsprogrammets nytta och effektivitet, uttalanden som domstolen menade inte var förenliga med hemlig dokumentation som domstolen tagit del av. När NSA tillfrågades om de fortfarande stod för sina tidigare uttalanden avböjde NSA att kommentera.[20]

- I juli 2020 avslöjades att en amerikansk säkerhetstjänst upprättat underrättelserapporter om journalister.[21]

- I en intervju från maj 2021 berättade en tidigare federal domare som tjänstgjorde i Houston mellan år 2004-2018, om hur bemyndiganden för inhemsk övervakning rutinmässigt hölls hemligstämplade. Inte bara under pågående utredningar utan långt efter att fallen avslutats. I hans domstol fanns över 15 år gamla begäran om bemyndiganden som fortfarande var hemligstämplade. Han undersökte saken vidare och fann att om ett fall någon gång hemligstämplats behölls hemligstämpeln i 99 % av fallen för alltid.[22]

- I juni 2021 publicerade Microsofts President Brad Smith en debattartikel i Washington Post där han beskrev hur missbruket av hemlig övervakning fortgått under såväl Trump som tidigare presidentadministrationer och att europeiska regeringar i allt högre grad försöker hålla sina uppgifter borta från datacenter som drivs av amerikanska företag.[23]

- I maj 2023 avslöjades att FBI gjort fler än 278 000 otillbörliga sökningar i en underrättelsedatabas med FISA 702-information.[24] En senator som varit ledamot i senatens underrättelsekommitté sedan 2001 krävde förändringar i amerikansk lagstiftning, inte bara uppdateringar av FBI:s interna riktlinjer. Senatorn uttalade därtill att ”Det finns viktig, hemlig information om hur regeringen har tolkat FISA 702 som kongressen och det amerikanska folket måste få ta del av innan lagen förnyas.”[25]

Exemplen gäller förstås bara sådant som framkommit i offentlighetens ljus.

Vi vill understryka att amerikansk underrättelseinhämtning givetvis kan tillföra ett värde när den bedrivs mot verkliga hot. Det vi vänder oss mot är lagstiftningens alltför lösa tyglar, den politiska inblandningen samt bristen på uppriktighet och effektiv tillsyn.

Microsofts President Brad Smith satte ord på problematiken i samband med ett mål gällande en brottsutredning för ett antal år sedan:

> (...) the U.S. Department of Justice's attempt to seize foreign customers' emails from other countries ignores borders, treaties and international law, as well as the laws those countries have in place to protect the privacy of their own citizens. As the French government stated on Monday, it's a path that creates "a significant

[20] https://techcrunch.com/2020/09/03/nsa-bulk-records-appeals-illegal/
[21] https://www.washingtonpost.com/national-security/dhs-compiled-intelligence-reports-on-journalists-who-published-leaked-documents/2020/07/30/5be5ec9e-d25b-11ea-9038-af089b63ac21_story.html och https://www.lawfareblog.com/what-if-j-edgar-hoover-had-been-moron
[22] https://themarkup.org/newsletter/hello-world/fighting-government-secrecy-about-surveillance
[23] https://www.washingtonpost.com/opinions/2021/06/13/microsoft-brad-smith-trump-justice-department-gag-orders/
[24] https://www.wsj.com/articles/fbi-improperly-searched-spy-database-for-information-on-americans-court-says-2f12bcd, se även https://www.theregister.com/2023/05/22/fbi_fisa_abuse/. Bland de som övervakades fanns en amerikansk senator, en delstatssenator och en domare på delstatsnivå, se https://www.theregister.com/2023/07/22/us_senator_caught_in_section_702/.
[25] https://www.wyden.senate.gov/news/press-releases/wyden-calls-for-reforms-to-fisa-surveillance-following-disclosure-of-new-abuses

> risk of conflict of laws." And as the tech sector appreciates all too well, that's a conflict that will leave tech companies and consumers caught in the middle.
>
> It's also a path that will lead to the doorsteps of American homes by putting the privacy of U.S. citizens' emails at risk. If the U.S. government obtains the power to search and seize foreign citizens' private communications physically stored in other countries, it will invite other governments to do the same thing. If we ignore other countries' laws, how can we demand that they respect our laws? That's part of why public interest groups, such as the Brennan Center for Justice and the Reporters Committee for Freedom of the Press, are watching this case so closely.
>
> The [Department of Justice's] position also bodes ill for the U.S. economy and American jobs. Right now, U.S. companies are world leaders in providing cloud services. That leadership position is based on trust. But if the U.S. government can assert this type of unilateral power to reach into datacenters that are operated by U.S. companies in other countries, foreign countries and foreign customers will question their ability to trust American companies.[26]

Som reaktion vidtog den amerikanska kongressen ändringar så att extraterritoriell åtkomst fick ett tydligt lagstöd. Sedan dess har farhågorna om eroderad tillit besannats. Adekvansbeslutet från juli 2023 löser inte problemet med denna extraterritoriella åtkomst. Det betyder att kränkningen av EU:s rättsliga suveränitet består.

5 Kryptering och liknande åtgärder

Kryptering eller pseudonymisering föreslås ibland som lösning för att hindra amerikanska myndigheter från att komma åt personuppgifter. Vi bedömer emellertid att sådana åtgärder, för att vara tillräckliga, i praktiken måste göra det omöjligt för amerikanska molntjänstleverantörer att lämna ut personuppgifterna.

Amerikanska molntjänstleverantörer kan åläggas att samarbeta med amerikanska myndigheter i syfte att tillhandahålla åtkomst till uppgifter – och kan få ersättning för åtgärder de vidtar för att ge sådan åtkomst.

För att kryptering effektivt ska skydda mot åtkomst från amerikanska underrättelsemyndigheter bedömer vi därför att molntjänstleverantören inte får ha teknisk möjlighet att kringgå krypteringen eller på annat sätt få åtkomst till uppgifter i klartext. Det innebär bland annat att molntjänstleverantören inte får ha teknisk möjlighet att använda sitt eget eller kundens behörighetssystem för att ge sig själv eller tredjelands myndigheter tillgång till personuppgifter, krypteringsfunktioner eller nycklar som kan dekryptera personuppgifter. Det är ofta här som krypteringsupplägg visar sig otillräckliga i denna kontext, när det visar sig att molntjänstleverantören vid något tillfälle:

- Hanterar uppgifterna i klartext i molnet.
- Hanterar kundens krypteringsnyckel i klartext i molnet.
- Har en egen krypteringsnyckel som hanteras i klartext i molnet.
- Har tillgång till nyckelhanteringssystemet eller behörighetssystemet som kontrollerar åtkomsten till nyckelhanteringssystemet.

[26] https://blogs.microsoft.com/on-the-issues/2018/01/19/something-extraordinary-happened-washington-d-c-yesterday/

Att uppgifter vid något tillfälle hanteras i klartext i molnet är en vanlig förutsättning för att molntjänster såsom SaaS-lösningar över huvud taget ska fungera. Även om uppgifter är krypterade vid vila (”at rest”) och under transport (”in transit”) kan de alltså behöva dekrypteras när de används (”in use”). Så är normalt sett fallet när uppgifterna ändras, används i en beräkning eller visas för en slutanvändare i en webbläsare.

Vi vill vara tydliga med att kryptering är en viktig åtgärd generellt. När en molntjänstleverantör utför molnkryptering vid vila och under transport kan det exempelvis skydda uppgifterna vid cyberattacker eller mot obehöriga insiders. Det innebär emellertid inte att en amerikansk molntjänstleverantör hindrats från att lämna ut uppgifterna enligt begäranden från amerikanska underrättelsemyndigheter.

Vi har inte sett något fall där en amerikansk molntjänstleverantör visat hur de krypterar uppgifter på ett sätt där kunden är i full kontroll, och där molntjänstleverantören inte har teknisk möjlighet att dekryptera uppgifterna, utan att kunden också berörs av en eller flera av följande:

- Krypteringen omfattar endast en delmängd av de uppgifter som behöver hanteras i molnet.
- Reducerad prestanda och funktionalitet eftersom det blir svårt eller omöjligt att bearbeta information i molnet samt söka efter, dela och samarbeta kring information.
- Högre licenskostnader.
- Administrativ börda för att hantera krypteringen samt tillhörande säkerhetsrisker.
- Ökade krav på medarbetare gällande i vilka system och digitala verktyg de får hantera information, krav som är svåra att upprätthålla fullt ut.

Därtill behöver beaktas att nuvarande krypteringsalgoritmer och deras implementering kan visa sig sårbara i framtiden, exempelvis med hänsyn till forskning inom kryptoteknik, att processorkraft blir billigare samt nya teknologiska paradigm såsom kvantteknik.

Utmaningarna med pseudonymisering, eller att dela upp data i mindre delar, är i stort sett de samma som vid kryptering.

Vi hävdar inte att kryptering, pseudonymisering eller andra tekniker omöjligen kan hindra åtkomst från amerikanska underrättelsetjänster. Vi frågar oss emellertid varför en organisation skulle vilja ta risken att dessa åtgärder inte räcker till rättsligt eller i realiteten samtidigt som organisationen måste dras med högre kostnader och praktiska begränsningar.

Vi tror att rättsligt hållbara samt lämpliga molntjänster, där uppgifter krypteras men också hanteras i klartext när och där det behövs, ger störst värde för pengarna och mest innovation. Molntjänster med verklig datasuveränitet, utan exponering mot amerikansk lagstiftning, kommer därför fortsatt vara det mest attraktiva alternativet.