Analys av tredjelandsöverföring av behandlingar i O365 för Lunds kommun

Transfer Impact Assessment

2021-01-27

Security Solution Scandinavia AB
Flöjelbergsgatan 20 C
431 37 Mölndal, Sverige

Office +46 31 98 90 00
www.securitysolution.se

Datum	Version	Beskrivning	Ändrat av
2021-01-19	0.9	Utkast	Marcus Broman
2021-01-27	1.0	Analys färdigställd	Marcus Broman

Innehållsförteckning

1 Generell information

1.1 Importör (Leverantör)

Identifiera importörens/leverantörens organisation.

Microsoft Corporation/Microsoft AB.

1.2 Placeringsort

Huvudkontorets placeringsort

Microsoft Corporation har sitt huvudkontor i Redmond, Washington, USA. Microsoft AB har sitt huvudkontor i Stockholm, Sverige.

1.3 Produkt/typ av tjänst

Vilken typ av produkt eller tjänst tillhandahåller leverantören för vår organisation?

Microsoft Office 365

Beskriv produkten/tjänsten.

Microsoft 365 (M365) är SaaS-tjänst som tillhandhålls av Microsoft. M365 är en samlad benämning på produkter som innehåller Office 365 samt även lokala applikationer, operativsystemet Windows 10 Enterprise, Enterprise Mobility + Security (EMS) och maskininlärning. Office 365 (O365) är en molnbaserad serie med appar och tjänster med bekanta applikationer som Microsoft Outlook, Word, Powerpoint och Excel, vilka görs tillgängliga både via dator, mobila enheter och webbläsare. Tjänsten licensieras genom olika typer av licenser, där Lunds kommun använder sig av E3 och E1.

1.4 Personuppgiftsbehandling

Vilka behandlingar utför leverantören för vår organisation?

Den kommungemensamma interna tjänsten har liksom många andra tjänster med IT-innehåll personuppgifter i flera nivåer av data. Med nivåer av data avses Innehållsdata, Gemensamma innehållsdata, Funktionsdata och Diagnosdata (definition av dessa, se nedan). Omfattningen av funktionella data samt diagnosdata varierar mellan olika tjänster och dess IT-stöd. Omfattningen av personuppgiftsbehandling i innehållsdata i dokument, e-post, kalendrar med mera bestäms av den förvaltning som använder tjänsten.

Omfattningen av personuppgiftsbehandling i gemensamma innehållsdata, diagnosdata samt funktionsdata som genereras vid användningen av komponenter i Office 365 kan inte bestämmas av varje enskild personuppgiftsansvarig.
Innehållsdata är innehåll i Word-filer, Powerpoint-filer, Excel-filer, OneNote, Teams-ytor etc. Innehållsdata (Content data) är data som användare skapar med Office 365 komponenter, till exempel text som skrivs in i ett Word-dokument, och används i samband med den anslutna upplevelsen. Annan innehållsdata (Customer data) är Signaturer, kontaktkortsinformation som användaren kompletterar med, personlig information i Delve etc.
Gemensamma innehållsdata som är användarinformation som härrör från HR-system och Skatteverkets befolkningsregister. Exempel på gemensamma innehållsdata är kontaktkort från Active Directory (AD), gemensamma metadatastrukturer, och visualisering av organisation.
Funktionella data är konfigurationsdata för komponenter, metadata som t.ex. rättigheter, tillgång, ändringar om innehållsdata, (t.ex. filnamn, ägare, eventloggar) samt funktionella data som Microsoft tillfälligt måste bearbeta för att låta användare ansluta till internet och använda Microsofts onlinetjänster. Det är data som behövs för t.ex. autentisering och konfiguration av appar mm.
Diagnosdata Obligatorisk diagnostiska data är den data som Microsoft samlar in och lagrar om den individuella användningen av komponenter i Office 365. Diagnostiska data för tjänster, som är de data som krävs för att hålla tjänsten säker, uppdaterad och fungera som förväntat. Individuellt användande av Office-applikationer som lagras och inte endast transporteras. Inkluderar systemgenererade eventloggar, telemetridata som samlas in samt 'required service data' för Connected Services. Kommunkontoret samlar också in loggar etc. som diagnosdata.

1.5 Produkter/tjänster (tillgångar)

Vilken specifik produkt eller tjänst tillhandahåller leverantören för vår organisation?

- Teams
- Onedrive/Sharepoint
- Microsoft 365 Apps - Word, Excel, Powerpoint (lokalt installerade program)
- Outlook online (kalender, kontakter)
- Office Mobile Apps
- Office för webben
- Planner
- Forms
- Fler tjänster ingår i licensen, men används inte eller är underliggande tjänster, se (Säkerhetsanalys Office 365)

1.6 Kategorier av registrerade och kategorier av personuppgifter

Vilka kategorier av registrerade finns i behandlingen, och vilka kategorier av personuppgifter behandlas för respektive kategori av registrerad?

Kategorier av registrerade

Anställda och konsulter i Lunds kommun samt deras externa kontakter som hanteras i tjänsten.

Kategorier av personuppgifter

Den kommungemensamma interna tjänsten har liksom många andra tjänster med IT-innehåll personuppgifter i flera nivåer av data. Med nivåer av data avses Innehållsdata, Gemensamma innehållsdata, Funktionsdata och Diagnosdata (definition av dessa, se avsnitt 1.4). Omfattningen av funktionella data samt diagnosdata varierar mellan olika tjänster och dess IT-stöd.

Enligt kommunens juridiska riktlinjer är det inte tillåtet att behandla känsliga personuppgifter eller uppgifter som är reglerade av sekretess i tjänsten. Riktlinjerna omfattar samtliga förvaltningar i kommunen, och därmed samtliga personuppgiftsansvariga nämnder, samt det kommunala bolaget Visit Lund AB.

Vilka kategorier av personuppgifter som behandlas i innehållsdata i dokument, e-post, kalendrar med mera bestäms av den förvaltning som använder tjänsten.

Vilka kategorier av personuppgifter som behandlas i gemensamma innehållsdata, diagnosdata samt funktionsdata som genereras vid användningen av komponenter i Office 365 kan inte bestämmas av varje enskild personuppgiftsansvarig, men påverkas av de bedömningar och åtgärder som görs av kommunkontoret för kommunen som helhet.

2 Tredjelandets generella skyddsnivå

Denna del innehåller analys av hur tredjelandets skyddsnivå generellt kan beskrivas på makronivå som ett underlag för bedömning.

I GDPR:s artikel 44 framgår att personuppgifter som är under behandling eller är avsedda att behandlas efter det att de överförts till ett tredjeland får bara ske under förutsättning att den personuppgiftsansvarige och personuppgiftsbiträdet efterlever kraven i Kapitel V som säkerställer att GDPR inte undergrävs.

I målet Schrems II[1] konstaterade EU-domstolen i GDPR att överföring av personuppgifter till ett tredjeland bara får ske under förutsättning att det aktuella tredjelandet säkerställer en adekvat skyddsnivå för dessa uppgifter. Vidare konstaterade domstolen att personer vars personuppgifter överförs till ett tredjeland med stöd av standardiserade dataskyddsbestämmelser ska åtnjuta en skyddsnivå som är *väsentligen likvärdig* med den som garanteras inom unionen genom denna GDPR, jämförd med artikel 8 i EU-stadgan. Se domslut.

Enligt GDPR:s artikel 45(2) bedömer EU-kommissionen när en adekvat skyddsnivå uppnås. Kriterierna för att uppnå en tillräcklig (adekvat) skyddsnivå baseras olika aspekter som:

- tredjelandets rättsstatsprinciper
- respekten för de mänskliga rättigheterna och de grundläggande friheterna
- relevant lagstiftning, både allmän lagstiftning och sektorslagstiftning, inklusive avseende allmän säkerhet, försvar, nationell säkerhet och straffrätt och offentliga myndigheters tillgång till personuppgifter
- tillämpningen av relevant lagstiftning, dataskyddsregler, yrkesregler och säkerhetsbestämmelser
- regler för vidare överföring av personuppgifter till ett annat tredjeland eller en annan internationell organisation, som ska följas i det landet eller den internationella organisationen
- rättspraxis samt faktiska och verkställbara rättigheter för registrerade och effektiv administrativ och rättslig prövning för de registrerade vars personuppgifter överförs
- effektiv fungerande oberoende tillsynsmyndighet för att säkerställa och kontrollera att dataskyddsregler följs, inklusive lämpliga verkställighetsbefogenheter, ge de registrerade råd och assistans när det gäller utövandet av deras rättigheter och samarbeta med medlemsstaternas tillsynsmyndigheter
- vilka internationella åtaganden det berörda tredjelandet eller den berörda internationella organisationen har gjort, eller andra skyldigheter som följer av rättsligt bindande konventioner eller instrument samt av dess deltagande i multilaterala eller regionala system, särskilt rörande skydd av personuppgifter.

Vad avser statlig tillgång och övervakning, se de europeiska nödvändiga garantierna (*European Essential Guarantees- EEG)* att "[...]övervakningsåtgärder vid överföring av personuppgifter, inte går utöver vad som är nödvändigt och proportionellt i ett demokratiskt samhälle", vilket förklaras i Europeiska dataskyddsstyrelsens (EDPB) dokument Rekommendationer 02/2020 om europeiska nödvändiga garantier för övervakningsåtgärder

- Garanti A – Uppgifter bör behandlas utifrån tydliga, precisa och tillgängliga bestämmelser
- Garanti B – Nödvändighet och proportionalitet ska säkerställas för legitima mål
- Garanti C – En oberoende tillsynsmekanism bör finnas
- Garanti D – Enskilda personer ska ha tillgång till effektiva rättsmedel

[1] Europeiska unionens domstolsbeslut i mål C-311/18 (Schrems II)

2.1 Rättsstatsprincipen

Bedöm rättsstatsprincipen i det land där leverantören behandlar personuppgifter för personuppgiftsansvarigs räkning.

För att hjälpa till med bedömningen av tredjelandets rättsstatsprincip kan man ta del av följande källor:

- Transparency Internationals rankning av världens länder efter korruptionsnivåer
- Landsguiden hos Utrikespolitiska institutet
- The World Justice Project Rule of Law Index® 2020
- Freedom House's Freedom in the World report

Förklara på vilket sätt landet respekterar rättsstatsprincipen.

☐ Svag
☐ Medel
☒ Stark

Förklaring:

Enligt The World Justice Project Rule of Law Index 2020 placeras USA på plats 21, av 128. Flera EU-länder ligger lägre.
USA ligger på plats 23 av 180 länder i Transparency Internationals rankning av världens länder efter korruptionsnivåer, eller strax under hälften bland de 36 OECD-länderna. [2]
USA är i grunden en stabil demokratisk rättsstat med ett starkt skydd för yttrandefrihet och fria regelbundna val. Pressen är fri och oberoende från staten, men media har varit utsatt för attacker under Donald Trumps presidentskap. En polarisering har skett i befolkningen, men har inte påverkat de demokratiska institutionerna, även om förtroendet har sjunkit sedan 2017. Domstolarnas oberoende ses som en grundpelare i demokratin i USA och Högsta domstolen utgör en motvikt mot den politiska makten, vilket har visat sig i 2020 års presidentval.
I Economist Intelligence Units (EIU) demokrati-index har USA för första gången halkat ned till kategorin "bristfälliga demokratier" där de ligger på plats 25 år 2019. Endast 22 länder räknas som fullgoda demokratier enligt EIU. De nordiska länderna och Nya Zealand toppar listan. Emellertid efter maktskiftet 2021 bör USA hamna som fullgod demokrati igen.

2.2 Respekt för mänskliga och medborgerliga rättigheter

Bedöm de mänskliga fri- och rättigheterna i det land där leverantören behandlar personuppgifter för personuppgiftsansvarigs räkning.

För att hjälpa till med bedömningen av tredjelandets rättsstatsprincip kan man ta del av följande källor:

- Transparency Internationals rankning av världens länder efter korruptionsnivåer
- Landsguiden hos Utrikespolitiska institutet

[2] Mer info om USA:s demokrati och rättigheter på finns i Landsguiden hos Utrikespolitiska institutet

- The World Justice Project Rule of Law Index® 2020
- Freedom House's Freedom in the World report

Förklara på vilket sätt landet respekterar internationella normer och standarder för mänskliga rättigheter.

☐ Svag
☐ Medel
☒ Stark

Förklaring:

Enligt Freedom in the World report ligger USA på 86 av 100 poäng (enbart Sverige, Norge och Finland har 100 poäng).
Efter terrorattentatet mot World Trade Center antog kongressen 2001 en lagstiftning mot terrorism (Patriot Act), som bland annat gav myndigheterna stora befogenheter att avlyssna brottsmisstänkta och att hålla terrormisstänkta utlänningar fängslade utan konkreta anklagelser. Patriot Act har förlängts två gånger, 2006 samt 2011. Kritik från främst människorättsorganisationer hävdar att lagarna inkräktar på rättigheter som garanteras i författningen. Kritiken växte när Edward Snowden 2013 avslöjade att National Security Agency, NSA, kontinuerligt bedriver massövervakning världen över av tele- och internetkommunikation.
Patriot Act har använts flitigt av myndigheter för att begära ut information från till exempel telefonbolag, banker och internetbolag. I en rapport från 2014 förekom 11 000 fall där myndigheterna begärt ut uppgifter om enskilda personer mellan 2001 och 2014. I endast 51 fall rörde sig misstankarna om terrorism. Omstridda inslag i Patriot Act som gällde främst massavlyssning av telekomtrafik löpte ut 2015 men återkom genast, om än med vissa inskränkningar, i en ny lag (Freedom Act).

2.3 Allmän dataskyddslagstiftning/integritets- och dataskyddslagstiftning

Har det land där leverantören behandlar personuppgifter för personuppgiftsansvarigs räkning en omfattande, samlad lagstiftning inom integritets- och dataskydd?

Beskriv implementeringen av landets lagstiftning.

☐ Ja
☒ Nej

Förklaring:

Det finns ingen allmän federal dataskyddslagstiftning i USA, men flera sektorsspecifika lagar gäller på federal nivå.

2.4 Sektorsspecifik integritets- och dataskyddslagstiftning

Har det land där leverantören behandlar personuppgifter för personuppgiftsansvarigs räkning sektorsspecifik integritets- och dataskyddslagstiftning?

Uppge de relevanta lagarna och beskriv implementeringen av landets lagstiftning.

☒ Ja
☐ Nej

Förklaring:

Förslag för en allmän federal dataskyddslagstiftning i USA har pågått under lång tid men ännu inte resulterat i ett ramverk som är allmänt tillämpbart. De sektorsspecifika lagarna som gäller över hela USA är:

- Health Insurance Portability and Accountability Act från 1996 ('HIPAA'), som reglerar integriteten och säkerheten för hälsoinformation.
- Gramm-Leach-Bliley Act från 1999 ('GLBA'), som kräver att finansinstitut förklarar sin praxis för informationsutbyte för sina kunder och skyddar känsliga uppgifter.
- Children's Online Privacy Protection Act of 1998 ('COPPA'), som ställer krav på leverantörer av webbplatser eller onlinetjänster riktade till barn under 13 år.

Andra federala lagar som innehåller integritets- och dataskyddsaspekter:

- Electronic Communications Privacy Act of 1986
- Health Information Technology for Economic and Clinical Health Act of 2009 ('HITECH')
- Telemarketing and Consumer Fraud and Abuse Prevention Act of 1994 ('TCFAPA')
- Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 ('CAN-SPAM')
- Fair Credit Reporting Act of 1970 ('FCRA')
- Telephone Consumer Protection Act of 1991 ('TCPA')
- Privacy Act of 1974
- Fair and Accurate Credit Transactions Act of 2003 ('FACTA')
- Video Privacy Protection Act of 1988 ('VPPA')

Vidare har frånvaron av en allmän federal dataskyddslagstiftning eller en tillsynsmyndighet gjort Federal Trade Commission ('FTC') till *de facto*- tillsynsmyndigheten, vilket har resulterat i en rad rättspraxis och förlikningar. Exempelvis finns regleringar för brott mot konsumenternas integritetsrättigheter eller underlåtenhet att upprätthålla säkerheten för känslig konsumentinformation.

2.5 Allmän säkerhet, försvar, nationell säkerhet och straffrätt

Har det land där leverantören behandlar personuppgifter för personuppgiftsansvarigs räkning allmän säkerhet, försvar, nationell säkerhet och/eller straffrätt som tillåter offentliga eller brottsbekämpande myndigheter tillgång till de överförda uppgifterna?

Med andra ord, gäller tredjelandets nationella säkerhetslagar för överföringar (t.ex. via elektroniska eller digitala medel). dvs. är bägge, tillsammans med överföringarna, uttryckligen föremål för dessa nationella säkerhetslagar)?

☒ Ja
☐ Nej

Förklaring:

Den amerikanska lagstiftningen gäller för amerikanska bolag, även om data hanteras inom Microsofts molntjänst i EU.
De tre huvudsakliga lagarna som är aktuella för amerikanska leverantörer är

- Foreign Intelligence Surveillance Act Executive ("FISA")
- Executive Order 12,333 ("EO 12,333")
- Presidential Policy Directive 28 ("PPD28").

EO 12,333 utfärdades av Ronald Reagan 1981 och används utanför USA med ändamålen att förse presidenten och nationella säkerhetsrådet med nödvändig information som beslutsunderlag i frågor rörande nationell säkerhet och policy. FISA är från 1978 och ändamålen är mer specifika och anges som nödvändiga att skydda en faktisk eller potentiell attack eller andra allvarliga fientliga handlingar av utländsk makt eller agent för utländsk makt; sabotage, internationell terrorism, spridning av massförstörelsevapen; eller hemliga utländska underrättelseaktiviteter. FISA avsnitt § 702 tillkom 2008 och uppdaterades 2017. Med detta avsnitt kan amerikanska staten (NSA) övervaka utländska personer, utan att specificera målen eller individuella godkännanden. Generellt godkännande av övervakningsprogrammen sker genom certifiering årligen av justitieministern samt underrättelsechefen, vilket kan anses vara en ren formalitet.
PDD-28, som utfärdades av Barack Obama 2014, ger generella utgångspunkter med ett visst skydd under FISA § 702 för att signalspaningen ska bedrivas lagligt och med hänsyn till den personliga integriteten och mänskliga rättigheter. Dock är skydd för icke-amerikaner i praktiken inte möjliga att verkställa juridiskt.
Den amerikanska signalspaningen är omfattande vilket visselblåsaren Edward Snowden avslöjade 2013. Det innebär att amerikansk underrättelsetjänst kan kräva att amerikanska företag delar med sig av den information (personuppgifter) som överförts till den amerikanska leverantören, även om informationen lagras i EU.

2.6 Övergripande rättsligt ramverk

Beskriv landets rättsliga principer som rör offentliga myndigheters tillgång till och behandling av överförda personuppgifter från EU.

Identifiera de allmänna rättsliga principerna som är relevanta för statlig åtkomst, inklusive följande:

- Konstitutionell ram och reservation av lagprincip
- Särskilda regler för skydd av personuppgifter

Förklaring:

USA:s rättssystem är uppdelat mellan federala lagar och delstatslagar. Vissa federala lagar gäller över hela landet, se ovan under Sektorsspecifik integritets- och dataskyddslagstiftning. Den primära källan för rättsliga principer i USA är deras konstitution, vilken innehåller de 27 tilläggen (amendments), där de första tio är rättighetsförklaringen (Bill of Rights). Konstitutionen har grundläggande regler för staten där personlig integritet för amerikanska medborgare är skyddat mot intrång från det allmänna bland annat genom det fjärde tillägget

> *" The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath of affirmation, and particularly describing the place to be searched, and the persons or things to be seized.".*

Detta skydd inskränks av antingen skälighet (*probable cause)* eller rannsakningsorder (warrant). Enligt prejudicerande mål i Högsta domstolen omfattar skyddet även elektronisk kommunikation. Skyddet omfattar "the people", som enligt annan praxis innebär "the people of the United States". Utländska medborgare omfattas alltså inte av skyddet i fjärde tillägget.
The Federal Trade Commission Act ställer krav på att personuppgifter ska ha samma skydd, oavsett om data behandlas hos ett företag i USA, utomlands eller hos en tredje part. Det är till en stor del FTC som ser till att de nationella reglerna för dataskydd och personuppgiftsbehandling tillämpas. FTC agerade även som en tillsynsmyndighet i ärenden som skedde under Safe Harbor och Privacy Shield, innan dessa ogiltigförklarades.
Vidare fastställer the Privacy Act från 1974 att en myndighet inte får avslöja personuppgifter om en enskild, om inte denne har gett sitt samtycke, såvida inte avslöjandet är tillåtet enligt något av tolv lagstadgade undantag.
Judicial Redress Act som ger medborgare i vissa länder (inkl. EU) rätt att i domstol klaga på att deras personuppgifter har överlämnats till myndigheter inom det amerikanska rättsväsendet.
USA Patriot Act ger polisen möjligheter att övervaka misstänkta personer med koppling till terrorism. Vidare finns det få rättsliga begränsningar av hur personuppgifter får överföras från USA till andra länder.

2.7 Generellt – Tydliga, precisa och tillgängliga regler för personuppgiftsbehandling

Baseras de statliga myndigheternas personuppgiftsbehandling (för övervakning) på tydliga, precisa och tillgängliga regler?

För mer information, se *Garanti A - Uppgifter bör behandlas utifrån tydliga, precisa och tillgängliga bestämmelser*, som förklaras i Europeiska dataskyddsstyrelsen (EDPB) Recommendations 02/2020 on the European Essential Guarantees for surveillance measures

☒ Ja
☐ Nej

Förklaring:

US CLOUD Act (Clarifying Lawful Overseas Use of Data Act eller kort Cloud Act) är en amerikansk lag som antogs 2018 av USA:s kongress. Lagen gör det möjligt för amerikanska myndigheter att begära ut data som lagras utanför USA:s territorium från tjänsteleverantörer som omfattas av USA:s jurisdiktion. Syftet med lagen är att underlätta utredningsarbetet för brottsbekämpande myndigheter.
Cloud Act ger USA:s brottsbekämpande myndigheter omfattande befogenheter att beordra vissa typer av tjänsteleverantörer (inklusive telekomoperatörer och molntjänstleverantörer) att bland annat lämna ut data om användare. Data som en tjänsteleverantör kan behöva lämna ut omfattar även innehållet i kommunikation som till exempel e-post och chattmeddelanden. Tjänsteleverantören måste lämna ut denna data oavsett om den lagras i eller utanför USA. För att en amerikansk myndighet ska kunna begära ut uppgifter från en tjänsteleverantör med stöd av Cloud Act krävs vanligtvis ett beslut av en amerikansk domstol. Domstolen gör då en bedömning om det är sannolikt att ett specifikt brott har ägt rum eller kommer att göra det.
Åtgärder som vidtas med stöd av FISA är begränsade till USA:s territorium medan Cloud Act gör det möjligt för amerikanska myndigheter att begära ut data som lagras utanför USA:s territorium.
Foreign Intelligence Surveillance Act (FISA) är en amerikansk lag som introducerades 1978 och som har uppdaterats flera gånger sedan 11 september-attackerna. FISA reglerar insamling av ”foreign intelligence information” för ändamål som är relaterade till nationell säkerhet. Metoderna som får användas av amerikanska

myndigheter i detta syfte är bland annat avlyssning av kommunikation och tillgång till data som lagras i molntjänster. Exempel på sådana metoder är övervakningsprogrammen PRISM och Upstream.
Executive Order 12,333 (EO 12,333) utfärdades 4 december 1981 och gör det möjligt för National Security Agency (NSA) att få åtkomst till uppgifter som befinner sig "i transit" på väg till USA, genom att NSA har åtkomst till undervattenskablar på Atlantens botten, varvid NSA kan samla in och lagra dessa uppgifter innan de anländer till Förenta staterna där de omfattas av bestämmelserna i FISA. Verksamhet som grundar sig på EO 12,333 regleras inte i lag.
Presidential Policy Directive 28 (PPD-28) utfärdades den 17 januari 2014, och medförde ett antal begränsningar av USA:s signalspaningsverksamhet. Detta presidentdirektiv är bindande för USA:s underrättelsemyndigheter.

2.8 Generellt – Nödvändighet och proportionalitet

Påvisar de statliga myndigheterna nödvändighet och proportionalitet med hänsyn till de uppsatta legitima målen?

För mer information, se *Garanti B - Nödvändighet och proportionalitet ska säkerställas för legitima mål*, som förklaras i europeiska dataskyddsstyrelsen (EDPB) Recommendations 02/2020 on the European Essential Guarantees for surveillance measures

☒ Ja
☐ Nej

Förklaring:

EU-domstolen fastslog i sin dom C-311-18 (Schrems II) att varken avsnitt 702 FISA eller EO 12,333, jämförda med PPD-28, motsvarar de minimikrav som gäller i unionsrätten enligt proportionalitetsprincipen, varför det inte kan anses att de övervakningsprogram som grundar sig på dessa bestämmelser är begränsade till vad som är strikt nödvändigt.
EU-kommissionen har vid underkännandet av Privacy Shield konstaterat att den lämpliga metoden för tredjelandsöverföring till USA är SCC. Olika aktörer och utredningar har pekat på att problemen med SCC är desamma som för Privacy Shield. Dock har inte detta blivit prövat av EU-domstolen. Den svenska It-driftsutredningen framför i ett delbetänkande (SOU 2021:1) att de har:

> "*...svårt att se att det i en situation som gäller tredjelandsöverföring vid utkontraktering av it-drift finns några ytterligare skyddsåtgärder som kan vidtas som läker de brister som EU-domstolen i Facebook Irland och Schrems bedömer finns i amerikansk lagstiftning.* "

Detta ställningstagande kan tolkas som att de antingen inte prövat olika möjligheter som EDPB rekommenderar eller avstår från att göra ett ställningstagande. De pekar ut att lösningen finns i ändring av den amerikanska lagstiftningen. Samtidigt föreslår It-driftsutredningen en lagstiftning som skulle lösa problem med Cloud Act och uppgifter som omfattas av sekretess enligt OSL. Detta leder till ett antagande att utredarna förmodar en lösning på problemen med överföring av personuppgifter till USA och att någon ny mekanism eller lagändring i USA är att vänta.
EDPB framför i sina rekommendationer att tredjelandets rätt till tillgång av uppgifter för nationella säkerhetsändamål inte ska gå utöver vad som är rimligt och proportionerligt i ett demokratiskt samhälle. Motiven för signalspaning skiljer sig inte åt från svensk lagstiftning, där syftet enligt lagen (2008:717) om signalspaning i

försvarsunderrättelsetjänst (LSF) är att kartlägga yttre militära hot, utveckling och spridning av massförstörelsevapen och utländska konflikter.
I en komparativ studie vid Stockholms universitet av skyddet för den personliga integriteten mellan Sverige och USA görs en jämförelse.[3] Bland likheterna är kraven på proportionalitet och skälighet.
Vad gäller tillgång till och behandling av personuppgifter enligt Cloud Act motsvaras de minimikrav som gäller i unionsrätten enligt proportionalitetsprincipen, framförallt eftersom en begäran om tillgång enligt Cloud Act vanligtvis kräver ett beslut av en amerikansk domstol.

2.9 Generellt – Opartiskt tillsynssystem

Finns det ett opartiskt tillsynssystem som övervakar statliga myndigheters tillgång till och behandling av personuppgifter?

För mer information, se *Garanti C - En oberoende tillsynsmekanism bör finnas*, som förklaras i Europeiska dataskyddsstyrelsen (EDPB) Recommendations 02/2020 on the European Essential Guarantees for surveillance measures

☒ Ja
☐ Nej

Förklaring:

För att en amerikansk myndighet ska kunna begära ut uppgifter från en tjänsteleverantör med stöd av Cloud Act krävs vanligtvis ett beslut av en amerikansk domstol. Domstolen gör då en bedömning om det är sannolikt att ett specifikt brott har ägt rum eller kommer att göra det.
Foreign Intelligence Surveillance Court (FISC) är en specialdomstol som skapades i samband med att FISA introducerades. FISC:s uppgift är att övervaka åtgärderna som vidtas med stöd av FISA. Enligt avsnitt 702 i FISA godkänner FISC dock inte individuella övervakningsåtgärder, utan snarare övervakningsprogram som till exempel Prism och Upstream. Detta godkännande sker utifrån årliga certifieringar som tas fram av justitieministern och chefen för nationella underrättelsetjänsten. Certifieringarna som ska godkännas av FISC avser inte enskilda personer utan gäller kategorier av uppgifter som ska samlas in av underrättelsemyndigheterna. Därutöver bedömer FISC inte huruvida det är lämpligt att övervaka enskilda individer på ett visst sätt i det enskilda fallet. FISC bedömer endast om övervakningen kan klassas som övervakningsåtgärd.
FISC kan också pröva bestridanden av direktiv om samarbete från de som tillhandahåller elektroniska kommunikationstjänster (exempelvis Microsoft). FISC kan även utfärda föreläggande att följa ett direktiv, om det efter prövning är legitimt. Underlåtenhet att följa ett föreläggande är straffbart. FISC:s beslut kan överklagas till Foreign Intelligence Surveillance Court Review (FISCR) och FISCR:s beslut kan överklagas till Högsta domstolen.
NSA har även intern kontroll, men dessa är mer rådgivande för att upprätthålla skydd för personlig integritet vid strategiska beslut.

[3] Wiklund, Marlene (2020) Signalspaning i Sverige och USA: En komparativ studie av skyddet för den personliga integriteten vid signalspaning i försvarsunderrättelseverksamhet

Ytterligare kontroll bedrivs av justitiedepartementet gällande efterlevnad av FISA avsnitt 702, vilket rapporteras till justitieministern, den nationella underrättelsechefen, kongressens underrättelseutskott samt både representanthusets och senatens justitieutskott.
En angivet oberoende statlig nämnd är Privacy and Civil Liberties Oversight Board (PCLOB), vars medlemmar är utsedda av presidenten. PCLOB har till uppgift att väga intressen för personlig integritet och medborgerliga friheter mot intresset att förebygga terrorism. PCLOB rapporterar till kongressen och presidenten med rekommendationer.[4]

2.10 Generellt – Individers rätt till prövning

Finns det effektiva rättsmedel – rätt till prövning – tillgängligt för individer vars personuppgifter är tillgängligt för statliga myndigheter (för övervakning)?

För mer information, se *Garanti D - Enskilda personer ska ha tillgång till effektiva rättsmedel*, som förklaras i Europeiska dataskyddsstyrelsen (EDPB) *Recommendations 02/2020 on the European Essential Guarantees for surveillance measures*

☐ Ja
☒ Delvis
☐ Nej

Förklaring:

Amerikanska medborgares rätt till privatliv skyddas av USA:s konstitution, skyddet gäller däremot inte för utländska medborgare.
De rättsmedel som FISA föreskriver för att bestrida olaglig elektronisk övervakning från de amerikanska underrättelsemyndigheterna är flera. Dessa rättsmedel kan i teorin även användas av utländska medborgare som till exempel EU-medborgare. Ett sådant rättsmedel är att enskilda kan kräva skadestånd från USA när personlig information har använts eller lämnats ut på ett olagligt och medvetet sätt. Därutöver har de rätt att stämma de amerikanska regeringens tjänstemän och begära skadestånd. Enskilda kan också bestrida lagenligheten i övervakningen och begära att informationen hemlighålls.
Även om det i princip finns möjligheter för utländska medborgare att söka rättslig prövning är de praktiska möjligheterna för att öppna och föra en sådan talan ytterst begränsade. Därutöver kan en talan som väcks av enskilda personer komma att förklaras som oacceptabel när de saknar grund, vilket begränsar enskildas möjligheter att väcka en sådan talan vid allmänna domstolar. Utländska medborgare omfattas inte av samma grundlagsskydd för rätten till privatliv som amerikanska medborgare.
Övervakningsprogrammen som grundas på avsnitt 702 FISA måste visserligen genomföras med iakttagande av kraven enligt PPD-28. Emellertid hade den amerikanska regeringen som svar på en fråga från EU-domstolen angett att PPD-28 inte ger registrerade personer några bindande rättigheter som kan göras gällande mot amerikanska myndigheter i domstol.

[4] Länk till rapporter med rekommendationer av Privacy and Civil Liberties Oversight Board

Den verksamhet hos NSA som grundar sig på EO 12,333 kan inte bli föremål för rättsmedel vid domstol. Det finns därmed inga rättigheter för individer som kan göras gällande mot amerikanska myndigheter vid domstol vad avser denna typ av verksamhet.

2.11 Brottsbekämpande ändamål

Beskriv de offentliga myndigheternas tillgång till och behandling av de överförda personuppgifterna för brottsbekämpande ändamål.

Cloud Act ger USA:s brottsbekämpande myndigheter omfattande befogenheter att beordra vissa typer av tjänsteleverantörer (inklusive telekomoperatörer och molntjänstleverantörer) att bland annat lämna ut data om användare. Cloud Act omfattar endast data som är relevanta för att skydda allmän säkerhet och bekämpa allvarliga brott (terrorism).

Data som en tjänsteleverantör kan behöva lämna ut omfattar även innehållet i kommunikation som till exempel e-post och chattmeddelanden. Tjänsteleverantören måste lämna ut denna data oavsett om den lagras i eller utanför USA. För att en amerikansk myndighet ska kunna begära ut uppgifter från en tjänsteleverantör med stöd av Cloud Act krävs vanligtvis ett beslut av en amerikansk domstol. Domstolen gör då en bedömning om det är sannolikt att ett specifikt brott har ägt rum eller kommer att göra det och utfärdar en så kallad rannsakningsfullmakt (Warrant).

2.12 Rättslig grund och tillämpliga begränsningar/säkerhetsåtgärder (brottsbekämpning)

Beskriv den rättsliga grunden för de tredjelandets myndigheters tillgång till och behandling av personuppgifter för brottsbekämpning och tillämpliga begränsningar/säkerhetsåtgärder

Artikel 6c i GDPR - rättslig förpliktelse, vilket vilar på att det måste föreligga sannolika skäl för att ett konkret lagbrott har begåtts och att begärda uppgifter är relevant för och har koppling till brottet. Detta förutsätter att artikel 48 i GDPR kan tillämpas, eftersom det inte är EU-lag eller lag i ett medlemsland som ställer förpliktelsen. Ett domstols- eller myndighetsbeslut som sker inom ramen för den bilaterala överenskommelsen MLAT[5] är godtagbart. EDPS och EDPB anser att Cloud Act kringgår MLAT, att rättsliga förutsättningar i nuläget inte är tillfredställande och att ett annat instrument för överföring är därför lämpligare. [6]
Vad gäller begränsningar i Cloud Act gäller att polis och åklagare endast begär innehåll från tjänsteleverantörer om *den fysiska eller juridiska person som innehar rättigheterna till datan* har samtyckt eller om en rannsakningsfullmakt har utfärdats av en amerikansk domstol i enlighet med Cloud Act eller i enlighet med ett bilateralt avtal (MLAT). Data behöver vara åtkomligt från USA och Cloud Act erkänner tjänsteleverantörers rätt att bestrida en begäran som strider mot ett annat lands lagstiftning eller nationella intressen.
Cloud Act begränsar inte möjligheten till kryptering av data eller ett enkelt sätt för avkodning som polis och åklagare kan använda. Kryptering av kunden kan alltså begränsa möjligheten till vad som kan lämnas ut.

[5] Mutual legal assistance treaty mellan EU och US är en internationell överenskommelse om brottsbekämpning.

[6] EDPB-EDPS till LIBE-kommittén om inverkan av US Cloud Act på EUs skydd av personuppgifter.

EU-kommissionen arbetar med en förordning om tillgång till e-bevisning, vilket motsvarar Cloud Act. Risken för konflikt mellan Cloud Act och GDPR beror på om USA och EU kan förhandla fram ett avtal som tillfredsställer båda parter. Med en förordning om e-bevisning på plats finns goda möjligheter till ett bilateralt avtal.

2.13 Oberoende tillsyn (brottsbekämpning)

Genomförs det opartisk tillsyn på offentliga myndigheter som samlar in personuppgifter för brottsbekämpningsändamål?

☒ Ja

☐ Nej

Förklaring:

Amerikanska justitiedepartementet (Department of Justice) utför tillsyn över på federal nivå av brottsbekämpande myndigheter i enlighet med olika lagar som innefattar även insamling och transparens gällande personuppgifter, t.ex. *Violent Crime Control and Law Enforcement Act of 1994* samt *Title VI of the Civil Rights Act of 1964.*[7]

2.14 Individers rätt till prövning (brottsbekämpning)

Har individer, inkluderat tredjelandsmedborgare och europiska medborgare, vars personuppgifter görs tillgänglig och behandlas för brottsbekämpningsändamål effektiva juridiska och/eller administrativa rättigheter?

☒ Ja
☐ Nej

Förklaring:

Cloud Act erkänner möjligheten för en molntjänstleverantör att försöka ogiltigförklara en rannsakningsfullmakt om åtkomst till en kunds information. Det finns en möjlig konflikt för en amerikansk medborgare som är bosatt i EU. Förutsättningarna är att motsätta sig utlämning gäller om:

- kunden är en fysisk person som inte är en amerikansk medborgare och inte är bosatt i USA,

eller om

- kunden är en juridisk person som inte har sitt säte i, eller utgår från USA. Utelämnandet som krävs skulle skapa en reell risk att leverantören skulle strida mot de lokala lagarna (t.ex. EU eller medlemsstater).

Det är dock svårt för registrerade själva att praktiskt bestrida en begäran om utlämnande hos en amerikansk åklagare eller polismyndighet.

[7] Conduct of law enforcement agencies

2.15 Nationella säkerhetsändamål

Beskriv de offentliga myndigheternas tillgång till och behandling av personuppgifter för nationella säkerhetsändamål.

De tre huvudsakliga lagarna som är aktuella för amerikanska leverantörer är Foreign Intelligence Surveillance Act Executive ("FISA"), Executive Order 12,333 ("EO 12,333") (Ronald Reagan 1981) och Presidential Policy Directive 28 ("PPD28").

2.16 Oberoende tillsyn (Nationella säkerhetsändamål)

Genomförs det opartisk tillsyn på offentliga myndigheter som samlar in personuppgifter för nationella säkerhetsändamål?

☒ Ja
☐ Nej

Förklaring:

På en generell nivå är det amerikanska systemet uppdelat mellan lagstiftande, exekutiva och dömande funktioner där respektive funktion fungerar som en kontrollmekanism för de övriga. Exempelvis är de polisiära myndigheterna en av den exekutiva funktionen och kan då kontrolleras av United States House Committee on the Judiciary som är en del av den lagstiftande funktionen.
De polisiära myndigheterna på federal nivå som har befogenheter att samla in personuppgifter är många och uppdelade på minst 15 olika departement. Exempelvis ligger Federal Bureau of Investigation (FBI) under Justitiedepartementet medan CIA ligger under United States Intelligence Community (IC) som i förlängningen ligger direkt under presidenten.
Många av de federala myndigheterna har även specifika tillsynsfunktioner, som kallas för Office of Inspector General (OIG), för respektive myndighet och som ansvarar för tillsynen av myndighetens verksamhet. Exempelvis ansvarar CIA Office of Inspector General (CIA-OIG) för kontroll av CIA medan United States Department of Justice Office of the Inspector General (DOJ-OIG) bl.a. ansvarar för FBI.

2.17 Registrerades rätt till prövning (Nationella säkerhetsändamål)

Har individer, inkluderat tredjelandsmedborgare och europiska medborgare, vars personuppgifter görs tillgänglig och behandlas för nationella säkerhetsändamål effektiva juridiska och/eller administrativa rättigheter?

☐ Ja
☒ Nej

Förklaring:

Det finns möjligheter för organisationer och företag att bestrida utlämnandet av uppgifter men det finns i nuläget inga mekanismer för europeiska medborgare att ifrågasätta att ens uppgifter utlämnas till amerikanska

myndigheter och det finns heller inga rättigheter till att bli underrättad att ens uppgifter har varit föremål för signalspaning.
Det finns vidare likheter av förutsättningarna för signalspaning med lagen (2008:717) om signalspaning i försvarsunderrättelsetjänst (LSF) och hur tekniken används. Myndigheten som bedriver signalspaning i Sverige är Försvarets radioanstalts (FRA). Det ska också finnas en möjlighet för individer att utöva sina rättigheter. Det finns en teoretisk skyldighet att underrätta enskilda som blivit föremål för FRA:s signalspaning. Personer som är föremål för svensk signalspaning kan hindras från att bli underrättade om det föreligger sekretess. Finns sekretess går det att skjuta upp underrättelsen. Efter ett år behöver underrättelsen inte längre utföras. Således är skyldigheten att underrätta enskilda praktiskt taget meningslös. Detta förfarande liknar alltså i praktiken hur det fungerar med amerikansk signalspaning enligt FISA och gällande utländska medborgare. Det finns förvisso i Sverige enligt § 10 a LSF en möjlighet för enskilda att begära kontroll om dennes uppgifter har behandlats otillbörligt genom att skicka en begäran till Statens inspektion för försvarsunderrättelseverksamheten (SIUN). Detta ger enskilda en möjlighet till att ta vara på integritetsaspekter, men i realiteten är även eventuell förekomst av behandling av personuppgifter praktiskt svårt att bevisa, då SIUN kan bara svara om behandling har skett otillbörligt. Ändamål gällande nationell säkerhet ligger utanför GDPR:s omfattning och därför kan en begäran enligt GDPR artikel 15 inte ge svar på om personuppgifter behandlats i signalspaningen i Sverige.

2.18 Offentliga myndigheters tillgång – proportionalitet

Är de offentliga myndigheternas tillgång till och behandling av personuppgifter begränsad på ett sätt som uppfyller kraven och kan i princip likställas med det EU-lagstiftningen kräver, enligt principen om proportionalitet, i den mån övervakningsprogrammen baserat på dessa bestämmelser är begränsade till enbart det som är absolut nödvändigt?

☐ Ja
☒ Nej

Förklaring:

EU-domstolen fastslog i sin dom C-311-18 (Schrems II) att varken FISA avsnitt 702 eller EO 12,333, jämförda med PPD-28, motsvarar de minimikrav som gäller i unionsrätten enligt proportionalitetsprincipen, varför det inte kan anses att de övervakningsprogram som grundar sig på dessa bestämmelser är begränsade till vad som är strikt nödvändigt.

2.19 Yrkesregler och säkerhetsbestämmelser

Har landet där leverantören behandlar personuppgifter för personuppgiftsansvarigs räkning yrkesregler och säkerhetsbestämmelser?

Identifiera och beskriv dessa regler och bestämmelser.

☒ Ja
☐ Nej

Förklaring:

American Bar Association tillhandahåller en ackrediterad certifiering som **Privacy Law Specialist** för professionella jurister genom IAPP (International Association of Privacy Professionals). Enligt amerikansk lag har jurister rätt att annonsera att de är specialiserade på ett visst rättsområde om de är certifierade som sådana av en "bona fide" - organisation.

2.20 Relevant rättspraxis

Har landet där leverantören behandlar personuppgifter för personuppgiftsansvarigs räkning relevant rättspraxis för dataskydd/integritetsskydd?

Identifiera relevant rättspraxis gällande tredjelandets myndigheters övervakning av registrerade.

☐ Ja
☒ Nej

Förklaring:

Gällande FISA, EO 12,333 pågår ett antal rättstvister gentemot PRISM och tillämpningen av FISA-domstolar (FISC). Ett par relevanta fall är

- 2013 American Civil Liberties Union vs NSA om massövervakning efter Snowdens avslöjanden. Fallet är inte löst, utan inväntar regeringens svar.
- 2013 FreedomWatch (Klayman) för en grupptalan mot myndigheter och tjänstemän som förmodades vara ansvariga för PRISM. Ärendet avslogs 2017, men har överklagats.
- 2014 Rand Paul och Freedom Works, Inc. för en grupptalan mot ex-president Obama m.fl. om inrikes avlyssning. Inväntar överklagan i Klayman-fallet.
- 2014 Schuchardt mot Obama för att NSA samlar in all e-post i USA. Ev. kommer fallet avslås.

2.21 Regelverk för vidareöverföring av personuppgifter

Har landet där leverantören behandlar personuppgifter för personuppgiftsansvarigs räkning regler för vidareöverföring av personuppgifter till ett annat tredjeland eller internationell organisation?

Identifiera och förklara dessa regler.

☒ Ja
☐ Nej

Förklaring:

Det finns få regler som reglerar överföring från USA till andra länder, men det finns överenskommelser med andra länder, t.ex. deltar USA i reglering av överföring av personuppgifter inom Asien och Stillahavsområdet.[8]

Privacy Shield med Schweiz var en motsvarande överenskommelses som Privacy Shield med EU. Den blev ogiltigförklarad den 8 september 2020 av Federal Data Protection and Information Commissioner (FDPIC)[9].

2.22 Registrerades rättigheter och rätt till prövning

Tillhandahåller det land där leverantören behandlar personuppgifter för personuppgiftsansvarigs räkning effektiva och verkställbara rättigheter för den registrerade samt effektiv administrativ och rättslig prövning för de registrerade vars personuppgifter överförs (från EU/EES)?

Med andra ord, har de registrerade vars personuppgifter är föremål för åtkomst av tredjelandets offentliga myndigheter verkställbara rättigheter och effektiva rättsmedel i domstol mot dessa myndigheter (dvs. effektiv administrativ och rättslig prövning)?

Se dataskyddsförordningens beaktandesatser:

- **Skäl 104:** "de registrerade bör tillförsäkras effektiva och lagstadgade rättigheter samt effektiv administrativ och rättslig prövning".
- **Skäl 108:** Lämpliga säkerhetsåtgärder, som SCC:s eller BCR:s "bör säkerställa iakttagande av de krav i fråga om dataskydd och registrerades rättigheter som är lämpliga för behandling inom unionen, inbegripet huruvida bindande rättigheter för de registrerade och effektiva rättsmedel är tillgängliga, inbegripet en faktisk rätt att föra talan på administrativ väg eller inför domstol och att kräva kompensation i unionen eller i ett tredjeland".
- **Skäl 114:** "bör den personuppgiftsansvarige eller personuppgiftsbiträdet i alla fall använda sig av lösningar som ger de registrerade verkställbara och effektiva rättigheter vad gäller behandlingen av deras personuppgifter inom unionen när dessa uppgifter väl har överförts, så att de fortsatt kan utöva sina grundläggande rättigheter och att skyddsåtgärder fortsatt gäller i förhållande till dem."

☐ Ja
☒ Delvis
☐ Nej

Förklaring:

För brottsbekämpande ändamål finns möjlighet till prövning i domstol för att bestrida utlämnande.

Denna möjlighet saknas för nationella säkerhetsändamål enligt FISA avsnitt 702 eller EO 12,333.

[8] APEC Cross-Border Privacy Rules (CBPR) System

[9] FDPIC considers CH-US Privacy Shield does not provide adequate level of data protection

2.23 Oberoende tillsynsmyndighet

Har det land där leverantören behandlar personuppgifter för personuppgiftsansvarigs räkning en eller flera oberoende tillsynsmyndigheter med ansvar att säkerställa och upprätthålla enlighet med dataskyddsregler, ge stöd och rådgivning för registrerade om deras rättigheter, samt samarbetar med EU-medlemsstaters tillsynsmyndigheter?

☐ Ja
☒ Nej

2.24 Oberoende tillsynsmyndighet - effektivitet

Fungerar den oberoende tillsynsmyndigheten effektivt (till exempel genom adekvata befogenheter)?

Skäl 104: Det tredjelandet bör säkerställa effektiv oberoende dataskyddsövervakning.

☐ Ja
☐ Nej
☒ Ej tillämpbar

2.25 Internationella åtaganden/förpliktelser

Har det land där leverantören behandlar personuppgifter för personuppgiftsansvarigs räkning gått med i någon internationell överenskommelse eller andra skyldigheter från rättsligt bindande överenskommelser eller instrument, likväl medlemskap i multilaterala eller regionala system relaterat till personuppgiftsskydd?

Förklara landets internationella åtaganden och förpliktelser i enlighet med landets deltagande i multilaterala eller regionala system, särskilt vad gäller skyddet av personuppgifter, samt genomförandet av sådana förpliktelser.

Har landet till exempel undertecknat och ratificerat Europarådets konvention av den 28 januari 1981 för skydd av enskilda med avseende på automatisk behandling av personuppgifter och dess tilläggsprotokoll?

☒ Ja
☐ Nej

Förklaring:

Multilaterala överenskommelser saknas.

- USA är med i OECD:s ramverk Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.
- USA bedriver arbete inom ramen för G20 att utveckla OECD:s ramverk.

Bindande överenskommelser:

- Privacy Shield för EU och Schweiz. Gäller ej längre för vare sig EU eller Schweiz, även om USA ensidigt tillämpar det fortfarande.
- USA har avtal med Asien och Stillahavsområdet. APEC Cross-Border Privacy Rules (CBPR) System.

3 Väsentligen likvärdig skyddsnivå

Detta kapitel avser klargöra om en väsentligen likvärdig skyddsnivå för överföringen kan garanteras i det specifika fallet.

Enligt EU-domstolsbeslutet för Schrems II beskrivs att personer vars personuppgifter överförs till ett tredjeland med stöd av standardiserade dataskyddsbestämmelser ska åtnjuta en skyddsnivå som är *väsentligen likvärdig* med den som garanteras inom unionen genom denna förordning, jämförd med stadgan.[10]

EDPB har skapat en frågebank med vanliga frågor gällande Schrems II[11] om när personuppgifter överförs till ett tredjeland enligt bindande företagsregler. Kort sagt måste man göra en analys från fall till fall av omständigheterna för överföringen om man avser överföra personuppgifter baserat på standardavtalsklausuler (SCC) eller Bindande företagsregler (BCR). Dessutom ska man analysera om tredjelandet tillhandahåller en tillräcklig skyddsnivå och om kompletterande åtgärder är nödvändiga. Se GDPR Artikel 45.2 eller beskrivningen i kapitel *2 Tredjelandets generella skyddsnivå* om nödvändiga kriterier.

3.1 Respekt för integritets- och dataskydd

Respekterar tredjelandets relevanta lagstiftning nivån av dataskydd som EU-lagstiftningen kräver (på ett sätt som överensstämmer med SCC:s eller BCR:s garantier)?

☐ Ja
☒ Nej

Förklaring:

Enligt The World Justice Project Rule of Law Index 2020 placeras USA på plats 21, av 128. Flera EU-länder ligger lägre. Sverige placeras på plats 4.

Enligt Freedom in the World report ligger USA på 86 av 100 poäng (enbart Sverige, Norge och Finland har 100 poäng).

Oberoende tillsynsmyndigheter avseende dataskydd saknas emellertid i USA. De övervakningsprogram som är möjliga genom FISA avsnitt 702, EO 12,333, PPD-28 innebär enligt EU-domstolens dom i mål nr C 311-18 (Schrems II) att Förenta Staternas lagstiftning inte kan anses respektera nivån av dataskydd på det sätt som EU-lagstiftningen kräver.

[10] Se Press Release No 91/20: The Court of Justice invalidates Decision 2016/1250 on the adequacy of the protection provided by the EU-US Data Protection Shield).

[11] Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems

3.2 SCCs/BCRs efterlevnad

Motverkar tredjelandets relevanta lagstiftning efterlevnaden av SCC:s eller BCR:s? Med andra ord, motverkar eller hindrar landets lagstiftning efterlevnaden SCC:s eller BCR:s.

Om leverantören använder SCC:s

- Klausul 5(b) i Annex of Decision 2010/87 kräver att säljaren godkänner och garanterar "att han inte har anledning att förmoda att den lagstiftning som är tillämplig på honom hindrar honom från att fullfölja uppdragsutförarens instruktioner och sina skyldigheter enligt detta avtal; om lagstiftningen ändras på ett sätt som sannolikt har en avsevärt skadlig inverkan på de garantier som klausulerna innebär, ska han anmäla ändringen till uppgiftsutföraren, varvid uppgiftsutföraren har rätt att avbryta överföringen av uppgifter och/eller häva avtalet."

Om leverantören använder BCR:s

- De bindande företagsreglerna måste bland annat specificera "rutinerna för att till den behöriga tillsynsmyndigheten rapportera alla rättsliga krav som en medlem i koncernen eller gruppen av företag som deltar i gemensam ekonomisk verksamhet är underkastad i ett tredjeland och som sannolikt kommer att ha en avsevärd negativ inverkan på de garantier som ges genom de bindande företagsbestämmelserna." Art. 47(2)(m), GDPR.

☒ Ja
☐ Nej

Förklaring:

Cloud Act ger USA:s brottsbekämpande myndigheter omfattande befogenheter att beordra vissa typer av tjänsteleverantörer (inklusive molntjänstleverantörer) att bland annat lämna ut data om användare. Tjänsteleverantören måste lämna ut denna data oavsett om den lagras i eller utanför USA.
FISA reglerar insamling av ”foreign intelligence information” för ändamål som är relaterade till nationell säkerhet. Metoderna som får användas av amerikanska myndigheter i detta syfte är bland annat avlyssning av kommunikation och tillgång till data som lagras i molntjänster. Exempel på sådana metoder är övervakningsprogrammen PRISM och Upstream.
Åtgärder som vidtas med stöd av FISA är begränsade till USA:s territorium medan Cloud Act gör det möjligt för amerikanska myndigheter att begära ut data som lagras utanför USA:s territorium. Båda dessa lagar motverkar eller hindrar efterlevnaden av SCC:s, framförallt FISA.

3.3 Offentliga myndigheters begäran om uppgifter

Har leverantören (Microsoft) någonsin fått en begäran om tillgång till personuppgifter av tredjelandets myndigheter för ändamål som gäller brottsbekämpning eller nationell säkerhet?

Beskriv omständigheterna kring denna/dessa förfrågningar eller begäran, inkluderat den rättsliga grunden, etc.

☒ Ja
☐ Nej

Förklaring:

Microsoft skriver att det inte finns någon direkt teknisk koppling från USA:s myndigheter till e-post eller annan lagrad information hos Microsoft, utan alla utlämningar sker efter begäran och eventuell överlämning av dokument sker utan direkt access.[12]

Begäran gällande brottsbekämpning

Begäranden från polis och rättsväsende redovisas halvårsvis och per land i Microsoft Trust Center. Redovisningen sker med sex månaders fördröjning. Detta inkluderar bägaranden enligt Cloud Act.

Under perioden jan-jun 2020 gällande Sverige:

- 210 förfrågningar gällande 275 konton/användare.

Utlämnanden:

- 76,19% icke-innehållsdata
- 17,14% ingen data funnen
- 6,67% avvisade begäran
- 0% innehållsdata

Begäran gällande nationell säkerhet

Begäranden till Microsoft från FISA-domstolar (FISA) Order) redovisas i tusental före 2015 och femhundratal efter och specificeras inte var i världen kontona finns. Redovisningen sker med sex månaders fördröjning efter avslutad period och finns i Microsoft Trust Center. Omfattningen är nationella säkerhetsintressen gällande terrorism, massförstörelsevapen eller militära hot mot USA.

Under perioden jul - dec 2019 hela världen:

- Innehållsdata: 0–499 förfrågningar gällande 14 500–14 999 konton
- Metadata: 0–499 förfrågningar gällande 0–499 konton

Det är likartad omfattning på begäranden under tidigare perioder med variation på något tusental.

Sannolikhet för utlämning enligt FISA

En beräkning av sannolikheten av risken för att uppgifter begärs ut kan göras. Det fanns cirka 200 miljoner aktiva Office 365 konton i september 2019. FISA:s order omfattar alla olika typer av Microsofttjänster.

Med förfrågningar gällande max 15 000 konton motsvarar det 0,0075% samma tid räknat på 2019 års information. Det motsvarar att 1 konto per 13 333 konton kan ha fått en förfrågan. Microsoft skriver också att antalet personer som omfattas kan vara färre, eftersom personer som eftersöks ofta har flera konton.

Vidare ska man beakta sannolikheten enligt USA:s prioriterade länder för övervakning gällande terrorism, massförstörelsevapen eller militära hot mot USA eller dess intressen. USA är tydliga med var de anser att hoten finns och listar främst Nordkorea, Kina, Ryssland och Iran. Se bedömning av hot världen av USAs underrättelsetjänster från 2019.

[12] Mer information om Microsofts hantering av begäran från USA:s myndigheter ang. Cloud Act och FISA order

3.4 Tillhandahåller tredjelandet en väsentligen likvärdig skyddsnivå

Tillhandahåller tredjelandet en väsentligen likvärdig nivå av dataskydd som garanteras av GDPR, förenligt med EU:s stadga om de grundläggande rättigheterna?

Enligt EU-domstolsbeslutet för Schrems II beskrivs att personer vars personuppgifter överförs till ett tredjeland med stöd av standardiserade dataskyddsbestämmelser ska åtnjuta en skyddsnivå som är *väsentligen likvärdig* med den som garanteras inom unionen genom denna förordning, jämförd med stadgan.[13]

Enligt EDPB:s frågebank FAQs om Schrems II, ska standarden för lämpliga skyddsåtgärder enligt Artikel 46 i GDPR vara *väsentligen likvärdiga*. Därför måste tredjelandet respektera den skyddsnivån som EU-lagstiftningen kräver så att "de garantier som ges genom standardavtalsklausulerna eller de bindande företagsbestämmelserna kan uppfyllas i praktiken".

Se även GDPR Artikel 45.2 eller beskrivningen i kapitel *2 Tredjelandets generella skyddsnivå* om nödvändiga kriterier sant GDPR Skäl 104 står att "Tredjelandet bör erbjuda garantier som säkerställer en tillfredsställande skyddsnivå som i huvudsak motsvarar den som säkerställs i unionen...".

☐ Ja
☒ Nej

Förklaring:

Klicka eller tryck här för att ange text.

3.5 Kompletterande åtgärder

Om landet inte kan erbjuda likvärdigt skydd och SCC:s eller BCR:s inte själva uppnår en tillräcklig garantinivå, finns det kompletterande åtgärder för att säkerställa en likvärdig skyddsnivå som erbjuds i EU/EES för överföring av personuppgifter?

Enligt EDPB's FAQs on Schrems II, utöver SCC och BCR, "[d]e kompletterande åtgärder [antingen rättsliga, tekniska eller organisatoriska åtgärder] som kan komma i fråga vid behov måste vidtas från fall till fall med hänsyn till alla omständigheter kring överföringen och efter bedömning av tredjelandets lagstiftning för att kontrollera om den säkerställer en adekvat skyddsnivå".

☒ Ja
☐ Nej

Förklara:

[13] Se Press Release No 91/20: The Court of Justice invalidates Decision 2016/1250 on the adequacy of the protection provided by the EU-US Data Protection Shield).

Klicka eller tryck här för att ange text.

3.6 Kompletterande åtgärder - omfattning

Europeiska dataskyddsstyrelsen (EDPB) föreslår kompletterande åtgärder i Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data och delar in dessa i tekniska, organisatoriska och avtalsmässiga.

Beskriv inom vilka områden de kompletterande åtgärderna är:

☐ Tekniska åtgärder för toppmodern kryptering
☐ Lämplig hantering av kryptografiska nycklar
☐ Pseudonymisering
☒ Separerande av information
☐ Grundlig förberedelse mot kryptoanalys
☐ Avtalsförpliktelser för tekniska åtgärder
☒ Avtalsförpliktelser för transparens
☐ Avtalsförpliktelser för andra särskilda åtgärder
☒ Avtalsförpliktelser för andra registrerade rättigheter
☒ Interna styrande regler som är gemensamma för organisationen
☒ Interna åtgärder för ansvarsskyldighet, såsom transparens
☒ Interna åtgärder för uppgiftsminimering
☐ Antagande av standarder och bästa praxis
☒ Regelbundna granskningar
☒ Dataimportörens egna åtaganden
☒ Annat

Förklara:

1. **Separerande av information**

Lokal lagring finns kvar, såväl gemensamma mappar på kommunens egna servrar och inledningsvis även en personlig nätverksplats på kommunens server. Användarna har att välja på flera olika lagringsalternativ beroende på vilken typ av information det rör sig om. Därtill finns verksamhetssystemen kvar. E-post är lokalt baserad - hybridlösning är införd där enbart kalenderfunktionen är migrerad till O365.

2. **Avtalsförpliktelser för transparens**

Detta finns genom MS transparensrapporter som finns i deras Trust Center: https://www.microsoft.com/sv-se/trust-center

- Begäranden från polis och rättsväsende redovisas halvårsvis och per land. Detta inkluderar bägaranden från Cloud Act.
- Begäranden rörande nationell säkerhet (USA) från de amerikanska myndigheterna rörande nationella säkerhetslagar redovisas halvårsvis med ett halvårs fördröjning i intervaller om tusental för FISA

Foreign Intelligence Surveillance Act (FISA) och intervaller om 500-tal för National Security Letters (NSL).

3. Avtalsförpliktelser för andra registrerade rättigheter

- Microsoft erbjuder stöd för hantering av begäran av information för registrerades rättigheter via deras säkerhetscenter och även ett verktyg som Lunds kommun kan använda för att efterleva registrerades rättigheter i Office 365 med DSR (Data Subject Requests): https://docs.microsoft.com/sv-se/compliance/regulatory/gdpr-data-subject-requests

Omfattningen av de olika delarna som Microsoft enligt nuvarande avtal tillhandahåller genom sitt säkerhetscenter och DSR case tool:

- Sökning – En process för att finna vilka data som behövs för att slutföra en begäran från registrerade.
- Tillgång – Hämtning och potentiell överföring till den registrerade av funnen information.
- Korrigering – Implementera ändringar eller andra begärda ändringar av personuppgifter.
- Begränsa – Ändra åtkomst eller bearbetning av personuppgifter genom att begränsa åtkomst eller ta bort data från Microsoftmolnet.
- Dataportabilitet – Att tillhandahålla ett verktyg för att exportera ett "strukturerat, vanligt använt, maskinläsbart format" av personuppgifter till den registrerade, i enlighet med GDPR: s "rätt till dataportabilitet."
- Radera – Permanent borttagning av personuppgifter från Microsoftmolnet.

4. Interna styrande regler som är gemensamma för organisationen

- Uppgifter som synkas till Azure AD minimeras, personnummer synkas ej.
- Gemensamma regler för vilken information som får hanteras i Teams och bakomliggande tjänster från M365 är framtagna och gäller hela organisationen. I korthet innebär reglerna att sekretessreglerad information och känsliga personuppgifter inte får hanteras i tjänsterna. Riktlinjerna är publicerade på intranätet Inloggad.
- Informationsklassning ska genomföras.

5. Interna åtgärder för ansvarsskyldighet, såsom transparens

- Informationstexter tas fram till interna intranätet och externa webben utifrån målgrupp, för att informera om överföringen till tredjeland.
- Förberedelser för att meddela individer om en begäran rapporteras från MS. Processbeskrivning och rollfördelning ska tas fram.

6. Interna åtgärder för uppgiftsminimering

Inte överföra mer än nödvändigt. Detta är en kombination av olika åtgärder för att minska och undvika att onödiga data förs över, specifikt gällande diagnostiska data:

- Där det är möjligt, ställ in lägsta nivån på diagnostiska data (telemetri).
- Upprätta regler samt information för att förhindra att filnamn och sökvägsnamn innehåller personuppgifter.
- Tillämpa informationshanteringsplan och verkställ gallringsbeslut.

Enligt kommunens juridiska riktlinjer får inte sekretessreglerad information eller känsliga personuppgifter hanteras i tjänsterna. Riktlinjerna gäller samtliga förvaltningar (dvs. personuppgiftsansvariga nämnder) och är publicerade på intranätet Inloggad.

7. **Regelbundna granskningar**

En funktion för löpande uppföljning av tredjelandsöverföringar och förändringar i avtal och lagstiftning behöver finnas för att kontinuerligt bedöma om åtgärder är tillräckliga. Uppföljning ska göras årsvis och vid behov. Granskningar kan ske genom rättsavdelningen med stöd av expertkompetens från dataskyddsombud.

8. **Dataimportörens egna åtaganden**

Microsofts utfästelse "Defending your data" där de lovar att bestrida alla förfrågningar från myndigheter samt ge ekonomisk kompensation om en enskild registrerades rättigheter blir kränkt. Detta åtagande kan delvis likställas med EEGs Garanti D - Effektiva rättsmedel ska finnas tillgängliga för individen.

9. Exitstrategi och möjlighet att avbryta överföring

En ytterligare åtgärd blir även att Lunds kommun behöver förbereda en realistisk exitstrategi, även om den kanske inte behöver realiseras. Ett konkret förslag behöver finnas och därefter behöver bevakning efter lämpliga alternativ eller hybrid-alternativ utvärderas löpande.

3.7 Tillräcklig skyddsnivå

Är de kompletterande åtgärderna kombinerat med SCC:s eller BCR:s tillräckligt för att garantera den tillräckliga (adekvata) skyddsnivån som EU eftersträvar?

☒ Ja
☐ Nej

Förklaring:

EU-kommissionen har vid underkännandet av Privacy Shield konstaterat att den lämpliga metoden för tredjelandsöverföring till USA är SCC. Olika aktörer och utredningar har pekat på att problemen med SCC är desamma som för Privacy Shield. Dock har inte detta blivit prövat av EU-domstolen.

De kompletterande åtgärder som föreslås till SCC minskar riskerna för registrerades fri- och rättigheter för överföringens omfattning genom: separerande av information; interna styrande regler samt åtgärder för uppgiftsminimering och transparens; avtalsförpliktelser för transparens och andra registrerades rättigheter; kontinuerlig bevakning av utvecklingen på området och genomförande av regelbundna granskningar.

Microsofts egen utfästelse "Defending your data" ger den registrerade indirekt en möjlighet att bestrida begäran om utlämnanden samt att ger en möjlighet till gottgörelse genom ekonomisk kompensation om den registrerades rättigheter blir kränkta i enlighet med GDPR. Detta åtagande kan delvis likställas med EEG:s Garanti D - Enskilda personer ska ha tillgång till effektiva rättsmedel.

Security Solution Scandinavia AB
Flöjelbergsgatan 20 C
431 37 Mölndal, Sverige

Office +46 31 98 90 00
www.securitysolution.se

4 Överföring av personuppgifter till tredjeland

Detta kapitel avser själva underlag för överföringen till tredjelandet av personuppgiftsbiträdet inklusive eventuella underbiträden.

Som bakgrund kan *frågorna 11 och 12* i EDPB:s frågebank med vanliga frågor gällande Schrems II användas [14].

Se även underlag i GDPR i följande artiklar:

- Artikel 28 - Personuppgiftsbiträden
- Artikel 29 - Behandling under den personuppgiftsansvariges eller personuppgiftsbiträdets överinseende
- Artikel 30(2) - Register över behandling
- Artikel 44 - Allmän princip för överföring av uppgifter
- Artikel 45 - Överföring på grundval av ett beslut om adekvat skyddsnivå
- Artikel 46 - Överföring som omfattas av lämpliga skyddsåtgärder
- Artikel 47 - Bindande företagsbestämmelser
- Artikel 49 - Undantag i särskilda situationer

samt *skäl 101* I GDPR:s beaktandesatser:

Flöden av personuppgifter till och från länder utanför unionen och till och från internationella organisationer är nödvändiga för utvecklingen av internationell handel och internationellt samarbete. Ökningen av dessa flöden har medfört nya utmaningar och nya farhågor när det gäller skyddet av personuppgifter. Det är viktigt att den skyddsnivå som fysiska personer säkerställs inom unionen genom denna förordning inte undergrävs när personuppgifter överförs från unionen till personuppgiftsansvariga, personuppgiftsbiträden eller andra mottagare i tredjeland eller till internationella organisationer, vilket inbegriper vidarebefordran av personuppgifter från tredjelandet eller den internationella organisationen till personuppgiftsansvariga, personuppgiftsbiträden i samma eller ett annat tredjeland eller en annan internationell organisation. Överföringar till tredjeländer och internationella organisationer får under alla omständigheter endast utföras i full överensstämmelse med denna förordning. En överföring kan endast ske, om de villkor som fastställs i bestämmelserna i denna förordning om överföring av personuppgifter till tredjeländer eller internationella organisationer har uppfyllts av den personuppgiftsansvarige eller personuppgiftsbiträdet, med förbehåll för de övriga bestämmelserna i denna förordning.

4.1 Vidareöverföring

Vidareöverför leverantören (Microsoft) personuppgifter till ett annat tredjeland (dvs. ett land utanför EU/EES och utanför personuppgiftsansvarigs jurisdiktion) för behandling för personuppgiftsansvarigs ändamål?

Enligt EDPB:s fakta om Schrems II som finns i EDPB:s frågebank med vanliga frågor står det att:
"utlämning av uppgifter från ett tredjeland, till exempel för administrationsändamål, utgör en överföring".

[14] Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems

☒ Ja
☐ Nej

4.2 Underbiträden

Utför underbiträden till leverantören (Microsoft) specifika behandlingar för personuppgiftsansvarigs ändamål?

☒ Ja
☐ Nej

Förklaring:

Klicka eller tryck här för att ange text.

4.3 Underbiträden - avtalskrav

Uppnår varje underbiträdesavtal kraven från GDPR?

Article 28 of the GDPR kräver följande:

Avtalet eller annan rättsakt måste binda underbiträdet till samma dataskyddskrav som finns i avtalet mellan den personuppgiftsansvarige och personuppgiftsbiträdet.

Avtalet eller annan rättsakt måste ange

- Behandlingens tillämpningsområde och varaktighet
- Behandlingens karaktär och ändamål
- Kategorier av registrerade och typ av personuppgift
- Personuppgiftsansvariges rättigheter och skyldigheter

Avtalet eller annan rättsakt måste fastställa att underbiträdet:

- endast får behandla personuppgifter på dokumenterade instruktioner från den personuppgiftsansvarige, inbegripet när det gäller överföringar av personuppgifter till ett tredjeland eller en internationell organisation, såvida inte denna behandling krävs enligt unionsrätten eller enligt en medlemsstats nationella rätt som personuppgiftsbiträdet omfattas av, och i så fall ska personuppgiftsbiträdet informera den personuppgiftsansvarige om det rättsliga kravet innan uppgifterna behandlas, såvida sådan information inte är förbjuden med hänvisning till ett viktigt allmänintresse enligt denna rätt
- säkerställer att personer med behörighet att behandla personuppgifterna har åtagit sig att iaktta konfidentialitet eller omfattas av en lämplig lagstadgad tystnadsplikt,
- ska vidta alla åtgärder som krävs enligt artikel 32,
- ska respektera de villkor som avses i punkterna 2 och 4 för anlitandet av ett annat personuppgiftsbiträde,

- med tanke på behandlingens art, ska hjälpa den personuppgiftsansvarige genom lämpliga tekniska och organisatoriska åtgärder, i den mån detta är möjligt, så att den personuppgiftsansvarige kan fullgöra sin skyldighet att svara på begäran om utövande av den registrerades rättigheter i enlighet med kapitel III,
- ska bistå den personuppgiftsansvarige med att se till att skyldigheterna enligt artiklarna 32–36 fullgörs, med beaktande av typen av behandling och den information som personuppgiftsbiträdet har att tillgå,
- beroende på vad den personuppgiftsansvarige väljer, ska radera eller återlämna alla personuppgifter till den personuppgiftsansvarige efter det att tillhandahållandet av behandlingstjänster har avslutats, och radera befintliga kopior såvida inte lagring av personuppgifterna krävs enligt unionsrätten eller medlemsstaternas nationella rätt, och
- ska ge den personuppgiftsansvarige tillgång till all information som krävs för att visa att de skyldigheter som fastställs i denna artikel har fullgjorts samt möjliggöra och bidra till granskningar, inbegripet inspektioner, som genomförs av den personuppgiftsansvarige eller av en annan revisor som bemyndigats av den personuppgiftsansvarige.

☒ Ja
☐ Nej

Förklaring:

Klicka eller tryck här för att ange text.

4.4 Tredjeland

Till vilket land eller till vilka länder överför leverantören (Microsoft) personuppgifter för behandling för personuppgiftsansvarigs ändamål (antingen internt eller till underbiträden)?

USA

4.5 Lagenlig mekanism för överföring av uppgifter mellan länder

Välj den lagliga mekanismen leverantören (Microsoft) förlitar sig på för överföring av personuppgifter (antigen internt eller till ett underbiträde).

För mer information, se Kapitel V - Överföring av personuppgifter till tredjeländer eller internationella organisationer.

☐ Beslut om adekvat skyddsnivå
☐ Skölden för skydd av privatlivet i EU och USA (Privacy Shield)
☒ Lämpliga skyddsåtgärder
☐ Undantag

Förklaring:

EU-kommissionens standardavtalsklausuler.

4.6 Länder med adekvat skyddsnivå

Välj det land eller de länder som leverantören (Microsoft) uteslutande överför personuppgifter till.

En överföring av personuppgifter till ett tredjeland eller internationell organisation kan utföras då Kommissionen beslutat att det tredjeland, territorium eller specifika sektor inom det landet, eller en internationell organisation säkerställer en tillfredsställande skyddsnivå. Art. 45(1), GDPR.

Europeiska kommissionen har utfärdat ett adekvat beslut (adequacy decision) för följande länder och anser att de erbjuder adekvata nivåer av dataskydd.

☐ Andorra
☐ Argentina
☐ Kanada
☐ Schweiz
☐ Färöarna
☐ Guernsey
☐ Israel
☐ Isle of Man
☐ Japan
☐ Jersey
☐ Nya Zeeland
☐ Uruguay
☒ Ej tillämpbar

Förklaring:

Klicka eller tryck här för att ange text.

4.7 Lämpliga skyddsåtgärder

Välj vilken/vilka lämpliga skyddsåtgärder som används av för överföring mellan tredjeländer.

För mer information, se artikel 46 (Överföring som omfattas av lämpliga skyddsåtgärder) och artikel 47 (Bindande företagsbestämmelser) i GDPR.

☐ Bindande företagsregler
☒ Standardavtalsklausuler
☐ Tillstånd från den behöriga
☐ Tillsynsmyndighet

☐ Ej tillämpbar

Förklaring:

Klicka eller tryck här för att ange text.

4.8 EU-US Privacy Shield

Har leverantören (Micorsoft), inklusive eventuella underbiträden, slutat överföra personuppgifter baserat på den ogiltiga EU-US Privacy Shield?

I mål C-311/18 – Data Protection Commissioner mot Facebook Ireland och Maximillian Schrems, den Europeiska unionens domstol ogiltigförklarade EU-US Privacy Shield.

International Trade Administration, U.S. Department of Commerce skriver att: "The EU-U.S. Privacy Shield Framework is no longer a valid mechanism to comply with EU data protection requirements when transferring personal data from the European Union to the United States."

Enligt europeiska dataskyddsstyrelsens (EDPB) vanliga frågor om Schrems II är överföring av personuppgifter ”olagligt” om det baseras på EU-US Privacy Shield Framework

För mer information om EU-US Privacy Shield, se följande:

- Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield
- The European Commission's website - Commercial sector: EU-US Privacy Shield
- The International Trade Administration (ITA), U.S. Department of Commerce's website - Privacy Shield framework in the United States
- The U.S. Federal Trade Commission's website - Privacy Shield

☒ Ja
☐ Nej

Förklaring:

Microsoft uppdaterade sitt DPA den 20 juli 2020 och meddelade i samband med detta att överföring till tredje land enbart baseras på EU-kommissionens standardavtalsklausuler.

4.9 Undantag

Välj det/de undantag som personuppgiftsansvarig och leverantören förlitar sig på, eller kommer förlita sig på.

Se även Europeiska dataskyddsstyrelsen - Riktlinjer 2/2018 för undantagen i artikel 49 enligt förordning 2016/679.

Tänk på:

1) Man kan endast använda ett undantag från artikel 49 i avsaknad av ett adekvat beslut enligt artikel 45(3), eller av lämpliga skyddsåtgärder enligt artikel 46, inkluderat bindande företagsregler.

2) Om man förlitar sig på ett undantag enligt artikel 49 kräver artikel 44 (Article 44) att man efterlever alla bestämmelserna i kapitel V (Chapter V) för att säkerställa att överföringar av personuppgifter inte undergräver den registrerades skyddsnivå som garanteras av GDPR.

3) Enligt dataskyddsstyrelsens riktlinjer för undantag (EDPB's Guidelines on derogations).

4) "utnyttjande av undantagen i artikel 49 aldrig får leda till en situation där grundläggande rättigheter kan komma att kränkas."

5) "undantagen [måste] tolkas restriktivt, så att undantaget inte blir till regel".

6) "När dataexportörer planerar att överföra personuppgifter till tredjeländer eller internationella organisationer bör de därför välja lösningar som ger de registrerade en garanti för att de kommer att fortsätta att dra fördel av de grundläggande rättigheter och skyddsåtgärder som de har rätt till när det gäller behandling av deras uppgifter efter överföringen."

☐ Den registrerade har lämnat ett uttryckligt samtycke
☐ Fullgöra ett avtal mellan den registrerade för att genomföra åtgärder som föregår ett sådant avtal på den registrerades begäran
☐ Fullgöra eller ingå i ett avtal i den registrerades intressen
☐ Viktigt allmänt intresse
☐ Fastställa, göra gällande eller försvara rättsliga anspråk
☐ Skydda någons grundläggande intressen (exempelvis livshotande)
☐ Överföring från offentligt register
☐ Tvingande berättigade intressen
☒ Ej tillämpbar

Förklaring:

Klicka eller tryck här för att ange text.

4.10 Tredjeland – grundläggande likvärdighet

Tillhandahåller varje tredjeland dit personuppgiftsansvarig och leverantören överför personuppgifter en väsentligen likvärdig nivå av dataskydd som garanteras av GDPR, förenligt med EU:s stadga om de grundläggande rättigheterna?

Enligt EDPB's FAQs on Schrems II, när SCC eller BCR används måste kunden och säljaren "bedöma om skyddsnivån som krävs enligt EU-lagstiftningen följs i det berörda tredjelandet i syfte att avgöra om de garantier som ges genom standardavtalsklausulerna eller de bindande företagsbestämmelserna kan uppfyllas i praktiken. Om så inte är fallet ska kunden [och säljaren] bedöma om [ni] kan vidta kompletterande åtgärder för att säkerställa en

väsentligen likvärdig skyddsnivå som den som tillhandahålls i EES, och om lagstiftningen i tredjelandet inte inkräktar på dessa kompletterande åtgärder så att deras effektivitet förhindras".

Enligt EU-domstolsbeslutet för Schrems II beskrivs att personer vars personuppgifter överförs till ett tredjeland med stöd av standardiserade dataskyddsbestämmelser ska åtnjuta en skyddsnivå som är *väsentligen likvärdig* med den som garanteras inom unionen genom denna förordning, jämförd med stadgan[15].

EDPB har skapat en frågebank med vanliga frågor gällande Schrems II[16] om när personuppgifter överförs till ett tredjeland enligt bindande företagsregler. Kort sagt måste man göra en analys från fall till fall av omständigheterna för överföringen om man avser överföra personuppgifter baserat på standardavtalsklausuler (SCC) eller Bindande företagsregler (BCR). Dessutom ska man analysera om tredjelandet tillhandahåller en tillräcklig skyddsnivå och om kompletterande åtgärder är nödvändiga. Se GDPR Artikel 45.2 eller beskrivningen i kapitel *2 Tredjelandets generella skyddsnivå* om nödvändiga kriterier.

Förklara er bedömning och huruvida man behöver, och kan, implementera lämpliga kompletterande åtgärder.

☒ Ja
☐ Nej

Förklaring:

Se kompletterande åtgärder beskrivna under avsnitt *3.5 Kompletterande åtgärder*.

4.11 Upphörande/avbryt av vidareöverföring

Om ett tredjeland inte tillhandahåller väsentligen likvärdigt skydd, även med implementerade kompletterande åtgärder tillgängliga procedurer för att stoppa eller avbryta överföringen?

☒Ja
☐Nej

Förklaring:

Lunds kommun tar fram en realistisk exitstrategi med handlingsplan och skapar därmed möjlighet att avbryta vidareöverföring.

[15] Se Press Release No 91/20: The Court of Justice invalidates Decision 2016/1250 on the adequacy of the protection provided by the EU-US Data Protection Shield).

[16] Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems

4.12 Behandlingen upphör – personuppgifter ska tas tillbaka eller raderas

Om denna bedömning indikerar att man måste stoppa/avbryta överföringen av personuppgifter permanent, har personuppgiftsansvarig då utsett en lämplig roll för att avgöra om personuppgiftsbiträden ska lämna tillbaka de överförda personuppgifterna, inkluderat eventuella kopior, eller förstöra uppgifterna och försäkra att det verkligen har gjorts?

☒ Ja
☐ Nej

Förklaring:

Om personuppgiftsbehandling skall avslutas kommer juridiska avdelningen ansvara för att beslut tas och säkerställa att detta verkställs för att radera eller ta tillbaka personuppgifterna.

4.13 Nytt personuppgiftsbiträde

Om denna bedömning indikerar att man måste stoppa/avbryta överföringen av personuppgifter permanent, har personuppgiftsansvarig utsett en lämplig roll att hitta ett nytt underbiträde lokaliserad i ett land som säkerställer väsentligen likvärdigt skydd som garanteras inom EU av GDPR, förenligt med EU:s stadga om de grundläggande rättigheterna?

Till exempel borde man överväga att hitta ett underbiträde lokaliserad i ett land där europeiska kommissionen har utsett ett adekvat beslut (adequacy decision).

☒ Ja
☐ Nej

Förklaring:

Lunds kommun tar fram en realistisk exitstrategi med handlingsplan som inkluderar val av nytt underbiträde.

4.14 Ändring av avtal

Har man startat diskussioner med personuppgiftsbiträden för att ändra avtalen till att förbjuda överföring av personuppgifter till ett tredjeland utan tillräcklig skyddsnivå och försäkrat att personuppgifter lagras och administreras någon annanstans än i det inadekvata tredjelandet?

Ett land utan tillräcklig skyddsnivå är ett land som inte tillhandahåller väsentligen likvärdigt dataskydd. Enligt dataskyddsstyrelsens (EDPB's FAQs on Schrems II), "Om det inte finns någon lämplig grund för överföring till ett tredjeland ska personuppgifter inte överföras utanför EES och all behandling ska ske inom EES."

☐ Ja
☒ Nej

Förklaring:

Klicka eller tryck här för att ange text.

5 Referenser och information gällande tredjelandsöverföring av personuppgifter

Denna del innehåller länkar till relevant underlag för analysen. Referenser till specifika källor behandlas i den löpandende texten samt i fotnoter.

5.1 Bakgrundinformation för mål C-311/18 – Schrems II

- EU-domstolens dom i mål C-311/18 – Data Protection Commissioner mot Facebook Ireland och Maximillian Schrems Case C-311/18 - *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems*
- Europeiska unionens domstol – pressmeddelande nr 91/20: Domstolen ogiltigförklarar beslut 2016/1250 om huruvida ett adekvat skydd säkerställs genom skölden för skydd av privatlivet i EU-Förenta staterna Press Release No 91/20: The Court of Justice invalidates Decision 2016/1250 on the adequacy of the protection provided by the EU-US Data Protection Shield
- Europeiska dataskyddsstyrelsen - Vanliga frågor om EU-domstolens dom i mål C-311/18 – Data Protection Commissioner mot Facebook Ireland och Maximillian Schrems (Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems ("EDPB's FAQs on Schrems II")).
- Europeiska datatillsynsmannen - "Statement following the Court of Justice ruling in Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems ("Schrems II")"

5.2 Relevanta europeiska lagstiftningar och riktlinjer

- Dataskyddsförordningen - Chapter V - Transfers of personal data to third countries or international organisations
- Europeiska datatillsynsmannen (EDPS) - Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit
- Europeiska datatillsynsmannen (EDPS) - EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data
- Europeiska unionens byrå för grundläggande rättigheter - Handbook on European data protection law (2018 edition)
- Europeiska domstolen för mänskliga rättigheter (ECHR) - Guide on Article 8 of the European Convention on Human Rights (31 December 2019)

- Europeiska dataskyddsstyrelsen (EDPB) Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data
- Europeiska dataskyddsstyrelsen (EDPB): Recommendations 02/2020 on the European Essential Guarantees for surveillance measures

5.3 Standardavtalsklausuler (SCC) för överföring mellan EU och icke-EU länder

- Europeiska kommissionens webbsida om standardavtalsklausuler **(Standard Contractual Clauses)** [endast på engelska]:

  The European Commission can decide that standard contractual clauses offer sufficient safeguards on data protection for the data to be transferred internationally.

  It has so far issued two sets of standard contractual clauses for data transfers from data controllers in the EU to data controllers established outside the EU or European Economic Area (EEA).

  It has also issued one set of contractual clauses for data transfers from controllers in the EU to processors established outside the EU or EEA.

- **EU controller to non-EU or EEA controller**

  decision 2001/497/EC

  decision 2004/915/EC

- **EU controller to non-EU or EEA processor**

  decision 2010/87/EU

5.4 Bindande företagsregler (BCR) om överföring inom internationella organisationer

- Europeiska kommissionens webbsida om bindande företagsregler (Binding Corporate Rules (BCRs)) [endast på engelska]:

  What are binding corporate rules?
  Binding corporate rules (BCR) are data protection policies adhered to by

companies established in the EU for transfers of personal data outside the EU within a group of undertakings or enterprises. Such rules must include all general data protection principles and enforceable rights to ensure appropriate safeguards for data transfers. They must be legally binding and enforced by every member concerned of the group.

Approval of binding corporate rules
Companies must submit binding corporate rules for approval to the competent data protection authority in the EU. The authority will approve the BCRs in accordance with the consistency mechanism set out in Article 63 of the GDPR. This procedure may involve several supervisory authorities since the group applying for approval of its BCRs may have entities in more than one Member State. The competent authority communicates its draft decision to the European Data Protection Board, which will issue its opinion on the binding corporate rules. When the BCRs have been finalised in accordance with the EDPB opinion, the competent authority will approve the BCRs.

Authorisations of supervisory authorities on the basis of Directive 95/46/EC remain valid until amended, replaced or repealed, if necessary, by that supervisory authorities.

Relevant documentation
The Article 29 Working Party adopted the following documents, which have been endorsed by the EDPB. These documents describe the procedure of approval and provide guidance on the structure and requirements of binding corporate rules.

1. Working Document on the approval procedure of the Binding Corporate Rules for controllers and processors (wp263rev.01)
2. Recommendation on the approval of the Controller Binding Corporate Rules form (wp264)
3. Recommendation on the approval of the Processor Binding Corporate Rules form (wp265)
4. Working Document on Binding Corporate Rules for Controllers (wp256rev.01)

5. Working Document on Binding Corporate Rules for Processors (wp257rev.01)