Rekommendationer 01/2020 om åtgärder som komplement till överföringsverktyg för att säkerställa överensstämmelsen med EU-nivån för skydd av personuppgifter

Version 2.0

Antagna den 18 juni 2021

Versionshistorik

Version 2.0	18 juni 2021	Antagande av rekommendationerna efter offentligt samråd
Version 1.0	10 november 2020	Antagande av rekommendationerna inför offentligt samråd

Sammanfattning

EU:s allmänna dataskyddsförordning antogs för att tjäna två olika syften: att underlätta det fria flödet av personuppgifter inom Europeiska unionen och samtidigt bevara enskilda personers grundläggande rättigheter och friheter, i synnerhet deras rätt till skydd av sina personuppgifter.

I sin nyligen meddelade dom C-311/18 (Schrems II) påminner Europeiska unionens domstol (nedan kallad *domstolen*) oss om att det skydd som ges till personuppgifter inom Europeiska ekonomiska samarbetsområdet (EES) alltid måste följa med uppgifterna. Överföring av personuppgifter till tredjeländer får inte vara ett sätt att undergräva eller urvattna det skydd som uppgifterna har inom EES. Domstolen betonar även detta genom att förtydliga att nivån av skydd i tredjeländer inte behöver vara identisk med den som garanteras inom EES, men väsentligen likvärdig. Domstolen framhåller även användningen av standardavtalsklausuler som ett överföringsverktyg som genom ett avtal kan tjäna till att säkerställa en väsentligen likvärdig skyddsnivå för uppgifter som överförs till tredjeländer.

Standardavtalsklausuler och andra överföringsverktyg som anges i artikel 46 i den allmänna dataskyddsförordningen fungerar inte i ett vakuum. Domstolen fastslår att personuppgiftsansvariga eller personuppgiftsbiträden, i deras roller som uppgiftsutförare, är ansvariga för att verifiera, från fall till fall och där det är lämpligt i samarbete med uppgiftsinföraren i tredjelandet, om landets lag eller praxis inkräktar på effektiviteten hos de lämpliga skyddsåtgärder som ingår i överföringsverktygen i artikel 46 i den allmänna dataskyddsförordningen. I dessa fall lämnar domstolen fortfarande utrymme för uppgiftsutförarna att genomföra kompletterande åtgärder som fyller dessa luckor i skyddet och höja det till den nivå som krävs enligt unionsrätten. Domstolen specificerar inte vilka åtgärder det kan röra sig om, men understryker att uppgiftsutförarna kommer att behöva identifiera dem från fall till fall. Detta är i linje med principen om ansvarsskyldighet i artikel 5.2 i den allmänna dataskyddsförordningen, som innebär att personuppgiftsansvariga ska vara ansvariga för och kunna visa att principerna i dataskyddsförordningen efterlevs när det gäller behandling av personuppgifter.

För att hjälpa uppgiftsutförarna (oavsett om de är personuppgiftsansvariga eller personuppgiftsbiträden, privata enheter eller offentliga organ som behandlar personuppgifter inom den allmänna dataskyddsförordningens tillämpningsområde) med den komplicerade uppgiften att bedöma tredjeländer och identifiera lämpliga kompletterande åtgärder vid behov har Europeiska dataskyddsstyrelsen (EDPB) antagit dessa rekommendationer. Rekommendationerna omfattar ett antal steg som uppgiftsutförarna bör följa, möjliga informationskällor och ett antal exempel på kompletterande åtgärder som kan vidtas.

Som ett **första steg** rekommenderar EDPB att du, som uppgiftsutförare, ska se till att du har **kunskap om dina överföringar**. Att kartlägga alla överföringar av personuppgifter till tredjeländer kan vara en svår uppgift. Det är emellertid nödvändigt att vara medveten om var personuppgifterna hamnar för att säkerställa att de får ett väsentligen likvärdigt skydd var de än behandlas. Du måste även verifiera att de uppgifter du överför är adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka uppgifterna behandlas.

Ett **andra steg** är att **verifiera det överföringsverktyg som används för överföringen**, bland de som förtecknas i kapitel V i den allmänna dataskyddsförordningen. Om EU-kommissionen redan har förklarat att det land, den region eller den sektor som du överför uppgifterna till har en adekvat skyddsnivå, genom ett beslut enligt artikel 45 i dataskyddsförordningen eller enligt det föregående direktivet 95/46 så länge beslutet fortfarande är i kraft, behöver du inte vidta några ytterligare åtgärder förutom att övervaka att beslutet om adekvat skyddsnivå är giltigt. Om det inte finns något beslut om adekvat skyddsnivå måste du förlita dig på ett av de överföringsverktyg som förtecknas i artikel 46 i den allmänna dataskyddsförordningen. Endast i vissa fall kan du åberopa ett av de undantag som anges i artikel 49 i den allmänna dataskyddsförordningen, under förutsättning att du uppfyller villkoren. Undantag kan inte bli en ”regel” i praktiken, utan måste begränsas till specifika situationer.

Ett **tredje steg** är att **bedöma** om det finns något i rättsläget och/eller gällande praxis i tredjelandet som kan påverka effektiviteten hos de lämpliga skyddsåtgärderna i de överföringsverktyg som du använder i samband med din överföring. Din bedömning bör först och främst vara inriktad på den lagstiftning i tredjelandet som är relevant för din överföring och de överföringsverktyg i artikel 46 i den allmänna dataskyddsförordningen som du förlitar dig på. Genom att också undersöka praxis för tredjelandets offentliga myndigheter kan du kontrollera om skyddsåtgärderna i överföringsverktyget i praktiken säkerställer ett effektivt skydd av de överförda personuppgifterna. Att undersöka sådan praxis blir särskilt relevant för din bedömning när

(i.) lagstiftningen i tredjelandet som formellt uppfyller EU:s normer uppenbart inte tillämpas/uppfylls i praktiken,

(ii.) det finns praxis som inte är förenlig med åtagandena för överföringsverktyget där relevant lagstiftning saknas i tredjelandet,

(iii.) dina överförda uppgifter och/eller din uppgiftsinförare omfattas eller skulle kunna omfattas av problematisk lagstiftning (dvs. påverkar överföringsverktygets avtalsrättsliga garanti av en väsentligen likvärdig skyddsnivå och uppfyller inte EU:s normer om grundläggande rättigheter, nödvändighet och proportionalitet).

I de två första situationerna måste du avbryta överföringen eller genomföra lämpliga kompletterande åtgärder om du vill fortsätta med den.

På grund av osäkerhet kring den potentiella tillämpningen av problematisk lagstiftning för din överföring kan du i den tredje situationen besluta att avbryta överföringen, genomföra kompletterande åtgärder för att fortsätta med den eller alternativt besluta att fortsätta med överföringen utan att genomföra kompletterande åtgärder om du anser och förmår påvisa och dokumentera att du inte har några skäl att tro att relevant och problematisk lagstiftning i praktiken kommer att tolkas och/eller tillämpas för att omfatta dina överförda uppgifter och uppgiftsinföraren.

EDPB:s rekommendationer för europeiska väsentliga garantier innehåller information om utvärderingen av de faktorer som måste beaktas vid bedömningen av ett tredjelands lagstiftning som reglerar de offentliga myndigheternas tillgång till uppgifter för övervakningssyfte.

Du bör utföra denna bedömning med tillbörlig aktsamhet och dokumentera den noga. Din behöriga tillsynsmyndighet och/eller rättsliga myndighet kan kräva in den och hålla dig ansvarig för alla beslut som du fattar på denna grund.

Ett **fjärde steg** är att **identifiera och anta kompletterande åtgärder** som är nödvändiga för att höja skyddsnivån för de överförda uppgifterna till EU:s normer för väsentlig likvärdighet. Detta steg är endast nödvändigt om din bedömning visar att tredjelandets lagstiftning och/eller praxis påverkar effektiviteten i det överföringsverktyg i artikel 46 i den allmänna dataskyddsförordningen som du förlitar dig på eller har för avsikt att förlita dig på i samband med överföringen. Dessa rekommendationer innehåller (i bilaga 2) en icke uttömmande förteckning med exempel på kompletterande åtgärder med vissa av de villkor som krävs för att de ska vara effektiva. Som fallet är med de lämpliga skyddsåtgärderna i de överföringsverktyg som ingår i artikel 46 kan vissa kompletterande åtgärder vara effektiva i vissa länder, men inte nödvändigtvis i andra. Du kommer att vara ansvarig för att bedöma deras effektivitet i samband med överföringen, mot bakgrund av tredjelandets lagstiftning och praxis och det överföringsverktyg du förlitar dig på, eftersom du kommer att hållas ansvarig för alla beslut som du fattar på denna grund. Du kan även behöva kombinera flera olika kompletterande åtgärder. Till sist kanske du konstaterar att det inte finns några kompletterande åtgärder som kan säkerställa en väsentligen likvärdig skyddsnivå för din överföring. I de fall där det inte finns några lämpliga kompletterande åtgärder måste du undvika, avbryta eller avsluta överföringen för att undvika att försämra personuppgifternas skyddsnivå. Du bör även utföra denna bedömning av kompletterande åtgärder med tillbörlig aktsamhet och dokumentera den.

Ett **femte steg** är att **vidta** de **formella förfarandeåtgärder** som kan krävas för antagandet av din kompletterande åtgärd, beroende på vilket överföringsverktyg enligt artikel 46 i den allmänna dataskyddsförordningen du förlitar dig på. Vissa av dessa formaliteter specificeras i dessa rekommendationer. Du kan behöva rådgöra med dina behöriga tillsynsmyndigheter i vissa av fallen.

Det **sjätte och sista steget** är att med lämpliga mellanrum **omvärdera** den skyddsnivå som har uppnåtts för de personuppgifter du överför till tredjeländer och övervaka om de har eller kommer att påverkas av några utvecklingstrender. Principen om ansvarsskyldighet kräver en kontinuerlig vaksamhet när det gäller personuppgifternas skyddsnivå.

Tillsynsmyndigheterna kommer att fortsätta att utöva sitt mandat för att övervaka tillämpningen av den allmänna dataskyddsförordningen och verkställa den. Tillsynsmyndigheterna kommer att ta vederbörlig hänsyn till de åtgärder som uppgiftsutförarna vidtar för att säkerställa att de uppgifter som överförs har en väsentligen likvärdig skyddsnivå. Domstolen påminner om att behöriga tillsynsmyndigheter kommer att avbryta eller förbjuda överföringar av uppgifter i de fall där de konstaterar att en väsentligen likvärdig skyddsnivå inte kan säkerställas, efter en utredning eller ett klagomål.

Tillsynsmyndigheterna kommer att fortsätta att utarbeta riktlinjer för uppgiftsutförare och samordna deras åtgärder i EDPB för att säkerställa en enhetlig tillämpning av EU:s dataskyddslagstiftning.

INNEHÅLLSFÖRTECKNING

Europeiska dataskyddsstyrelsen har antagit detta yttrande

med beaktande av artikel 70.1 e i Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (nedan kallad *den allmänna dataskyddsförordningen* eller *dataskyddsförordningen*),

med beaktande av EES-avtalet, särskilt bilaga XI och protokoll 37 till detta, ändrat genom gemensamma EES-kommitténs beslut nr 154/2018 av den 6 juli 2018[1],

med beaktande av artikel 12 och artikel 22 i arbetsordningen, och

av följande skäl:

(1) I sin dom av den 16 juli 2020 i mål C-311/18, *Data Protection Commissioner mot Facebook Ireland LTD, Maximillian Schrems*, drar Europeiska unionens domstol slutsatsen att artikel 46.1 och 46.2 c i den allmänna dataskyddsförordningen ska tolkas som att de lämpliga skyddsåtgärder, lagstadgade rättigheter och effektiva rättsmedel som krävs enligt de bestämmelserna måste säkerställa att registrerade personer vars personuppgifter överförs till ett tredjeland i enlighet med standardiserade dataskyddsbestämmelser har en skyddsnivå som är väsentligen likvärdig med den nivå som garanteras inom Europeiska unionen genom den förordningen, tolkad mot bakgrund av Europeiska unionens stadga om de grundläggande rättigheterna.[2]

(2) Domstolen betonar att en skyddsnivå för fysiska personer som är väsentligen likvärdig med den som garanteras inom Europeiska unionen genom allmänna dataskyddsförordningen, tolkad mot bakgrund av stadgan, måste garanteras oberoende av vilken bestämmelse i kapitel V som utgör grunden för överföringen av personuppgifter till ett tredjeland. Bestämmelserna i kapitel V är avsedda att säkerställa att den höga skyddsnivån fortsätter att gälla vid överföring av personuppgifter till ett tredjeland.[3]

(3) I skäl 108 och artikel 46.1 i allmänna dataskyddsförordningen föreskrivs att en personuppgiftsansvarig eller ett personuppgiftsbiträde bör vidta åtgärder för att kompensera för det bristande dataskyddet i ett tredjeland med hjälp av lämpliga skyddsåtgärder för den registrerade om beslut om adekvat skyddsnivå saknas. En personuppgiftsansvarig eller ett personuppgiftsbiträde får tillhandahålla lämpliga garantier, utan att ett särskilt tillstånd krävs från en tillsynsmyndighet, genom att använda ett av de överföringsverktyg som ingår i förteckningen i artikel 46.2 i den allmänna dataskyddsförordningen, däribland standardiserade dataskyddsbestämmelser.

[1] Hänvisningar till ”medlemsstater” som görs i alla delar av detta dokument ska förstås som hänvisningar till ”EES-medlemsstater”.
[2] EU-domstolens dom av den 16 juli 2020, Data Protection Commissioner mot Facebook Ireland Ltd, Maximillian Schrems, (nedan kallad C-311/18 (Schrems II)), andra slutsatsen.
[3] C-311/18 (Schrems II), punkterna 92 och 93.

(4) Domstolen klargör att de standardiserade dataskyddsbestämmelser som antagits av kommissionen endast är avsedda att ge avtalsrättsliga garantier som tillämpas på ett likvärdigt sätt i alla tredjeländer till personuppgiftsansvariga och personuppgiftsbiträden som är etablerade i Europeiska unionen. På grund av deras avtalsrättsliga natur kan standardiserade dataskyddsbestämmelser inte vara bindande för de offentliga myndigheterna i tredjeländer, eftersom de inte är parter i avtalet. Följaktligen kan uppgiftsutförare behöva komplettera de garantier som ingår i de standardiserade dataskyddsbestämmelserna med kompletterande åtgärder för att säkerställa överensstämmelsen med den skyddsnivå som enligt unionsrätten krävs i ett visst tredjeland. Domstolen hänvisar till skäl 109 i den allmänna dataskyddsförordningen, där denna möjlighet nämns och där personuppgiftsansvariga och personuppgiftsbiträden uppmuntras att använda den.[4]

(5) Domstolen påpekade att det i första hand är uppgiftsutföraren som i varje enskilt fall och, i förekommande fall, i samarbete med mottagaren av överföringen, ska kontrollera huruvida lagstiftningen i mottagarlandet säkerställer ett lämpligt skydd med hänsyn till unionsrätten för personuppgifter som överförts med stöd av standardiserade dataskyddsbestämmelser och vid behov tillhandahålla ytterligare skyddsåtgärder utöver dem som erbjuds genom dessa bestämmelser.[5]

(6) Om en personuppgiftsansvarig eller ett personuppgiftsbiträde som har etablerat sig i unionen inte kan vidta lämpliga kompletterande åtgärder för att säkerställa en skyddsnivå som är väsentligen likvärdig med unionsrätten är dessa, eller i andra hand den behöriga tillsynsmyndigheten, skyldiga att avbryta eller upphöra med överföringen av personuppgifter till det berörda tredjelandet.[6]

(7) Varken dataskyddsförordningen eller domstolen ger någon definition eller specifikation av ”ytterligare skyddsåtgärder”, ”ytterligare åtgärder” eller ”kompletterande åtgärder” till skyddsåtgärderna för de överföringsverktyg som förtecknas i artikel 46.2 i den allmänna dataskyddsförordningen och som personuppgiftsansvariga eller personuppgiftsbiträden kan vidta för att säkerställa överensstämmelsen med den skyddsnivå som enligt unionsrätten krävs i ett visst tredjeland.

(8) EDPB har på eget initiativ beslutat att undersöka denna fråga och ge personuppgiftsansvariga och personuppgiftsbiträden, som agerar som uppgiftsutförare, rekommendationer om den process de kan följa för att identifiera och anta kompletterande åtgärder. I dessa rekommendationer beskrivs metoder som uppgiftsutförarna kan använda för att fastställa om kompletterande åtgärder måste vidtas för deras överföringar, och i så fall vilka. Det är uppgiftsutförarnas primära ansvar att säkerställa att de uppgifter som överförs har en skyddsnivå i tredjelandet som är väsentligen likvärdig med den nivå som garanteras inom EES. Med dessa rekommendationer vill EDPB uppmuntra en enhetlig tillämpning av den allmänna dataskyddsförordningen och domstolens domar, i enlighet med EDPB:s mandat[7].

HÄRIGENOM REKOMMENDERAS FÖLJANDE.

[4] C-311/18 (Schrems II), punkterna 132 och 133.
[5] C-311/18 (Schrems II), punkt 134.
[6] C-311/18 (Schrems II), punkt 135.
[7] Artikel 70.1 e i den allmänna dataskyddsförordningen.

1 ANSVARSSKYLDIGHET VID ÖVERFÖRING AV UPPGIFTER

1. Enligt EU:s primärrätt är rätten till dataskydd en grundläggande rättighet.[8] Följaktligen ges rätten till dataskydd en hög skyddsnivå, och begränsningar får endast göras om de är föreskrivna i lag, förenliga med det väsentliga innehållet i rättigheterna, proportionerliga, nödvändiga och faktiskt svarar mot mål av allmänt samhällsintresse som erkänns av EU eller behovet att skydda andra människors rättigheter och friheter.[9] Rätten till skydd av personuppgifter är inte en absolut rättighet, utan den måste förstås utifrån dess uppgift i samhället och vägas mot andra grundläggande rättigheter i enlighet med proportionalitetsprincipen.[10]

2. En skyddsnivå som är väsentligen likvärdig med den som garanteras inom EU måste åtföljа uppgifterna när de överförs till tredjeländer utanför EES för att säkerställa att den skyddsnivå som garanteras genom den allmänna dataskyddsförordningen inte undergrävs, både under och efter överföringen.

3. Rätten till dataskydd är en aktiv rättighet. Den kräver att uppgiftsutförare och uppgiftsinförare (oavsett om de är personuppgiftsansvariga och/eller personuppgiftsbiträden) går längre än att bara erkänna eller passivt efterleva denna rättighet.[11] Personuppgiftsansvariga och personuppgiftsbiträden måste försöka uppfylla rätten till dataskydd på ett aktivt och fortlöpande sätt genom att vidta rättsliga, tekniska och organisatoriska åtgärder som säkerställer skyddets effektivitet. Personuppgiftsansvariga och personuppgiftsbiträden måste även kunna visa dessa ansträngningar för de registrerade och tillsynsmyndigheterna för dataskydd. Detta är den så kallade principen om ansvarsskyldighet.[12]

4. Principen om ansvarsskyldighet, som är nödvändig för att säkerställa en effektiv tillämpning av den skyddsnivå som följer av dataskyddsförordningen, gäller även överföringar av uppgifter till tredjeländer[13], eftersom de är en form av databehandling i sig.[14] Som domstolen underströk i sin dom måste en skyddsnivå som är väsentligen likvärdig med den nivå som garanteras inom unionen genom dataskyddsförordningen, tolkad mot bakgrund av stadgan, garanteras oberoende av bestämmelsen i det kapitel som ligger till grund för överföringen av personuppgifter till ett tredjeland.[15]

5. I Schrems II-domen betonar domstolen uppgiftsutförarnas och uppgiftsinförarnas ansvar att säkerställa att behandlingen av personuppgifter har utförts och kommer fortsätta att utföras i överensstämmelse med den skyddsnivå som fastställs genom EU:s dataskyddslagstiftning och att

---

[8] Artikel 8.1 i stadgan om de grundläggande rättigheterna, artikel 16.1 i EUF-fördraget samt skäl 1 och artikel 1.2 i den allmänna dataskyddsförordningen.
[9] Artikel 52.1 i EU-stadgan om de grundläggande rättigheterna.
[10] Skäl 4 i den allmänna dataskyddsförordningen och mål C-507/17, Google LLC mot Commission nationale de l'informatique et des libertés (CNIL), punkt 60.
[11] C-92/09 och C-93/02, Volker und Markus Schecke GbR mot Land Hessen, förslag till avgörande av generaladvokat Eleanor Sharpston, 17 juni 2010, punkt 71.
[12] Artikel 5.2 och artikel 28.3 h i den allmänna dataskyddsförordningen.
[13] Artikel 44 och skäl 101 i den allmänna dataskyddsförordningen, samt artikel 47.2 d i den allmänna dataskyddsförordningen.
[14] EU-domstolens dom av den 6 oktober 2015, *Maximillian Schrems mot Data Protection Commissioner (*nedan kallad C-362/14 (Schrems I)), punkt 45.
[15] C-311/18 (Schrems II), punkterna 92 och 93.

avbryta överföringen och/eller häva avtalet om uppgiftsinföraren inte längre kan uppfylla de standardiserade dataskyddsbestämmelser som ingår i det relevanta avtalet mellan uppgiftsutföraren och uppgiftsinföraren.[16] Den personuppgiftsansvariga eller det personuppgiftsbiträde som agerar som uppgiftsutförare måste säkerställa att uppgiftsinförarna, i tillämpliga fall, samarbetar med uppgiftsutföraren för att fullgöra dessa ansvarsområden, till exempel genom att informera om eventuella utvecklingar som påverkar skyddsnivån för de personuppgifter som tagits emot i uppgiftsinförarens land.[17] Dessa ansvarsområden är en tillämpning av principen om ansvarsskyldighet i dataskyddsförordningen när det gäller överföring av uppgifter.[18]

2 FÄRDPLAN: TILLÄMPNING AV PRINCIPEN OM ANSVARSSKYLDIGHET VID ÖVERFÖRING AV UPPGIFTER I PRAKTIKEN

6. Nedan följer en färdplan över de steg som du bör gå igenom för att ta reda på om du (uppgiftsutföraren) måste vidta kompletterande åtgärder för att kunna överföra uppgifter utanför EES i enlighet med lagen. I detta dokument avses med du eller dig den personuppgiftsansvarige eller det personuppgiftsbiträde som agerar som uppgiftsutförare[19], och som behandlar personuppgifter inom dataskyddsförordningens tillämpningsområde – inbegripet behandling som utförs av privata enheter och offentliga organ vid överföring av uppgifter till privata organ.[20] När det gäller överföringar av personuppgifter som utförs mellan offentliga organ finns det särskilda riktlinjer i *Riktlinjer 2/2020 om artiklarna 46.2 a och 46.3 b i förordning 2016/679 för överföring av personuppgifter mellan offentliga myndigheter och organ inom och utanför EES.*[21]

7. Du måste dokumentera denna bedömning och de kompletterande åtgärder du väljer på ett lämpligt sätt och genomföra och tillgängliggöra dokumentationen för den behöriga tillsynsmyndigheten på begäran.[22]

2.1 Steg 1: Lär känna dina överföringar

8. För att ta reda på vad som kan krävas av dig (uppgiftsutföraren) för att kunna fortsätta med eller utföra nya överföringar av personuppgifter[23] är det första steget att säkerställa att du är fullt medveten om dina överföringar. Registrering och kartläggning av alla överföringar kan vara en

[16] C-311/18 (Schrems II), punkterna 134, 135, 139, 140, 141, 142.
[17] C-311/18 (Schrems II), punkt 134.
[18] Artikel 5.2 och artikel 28.3 h i den allmänna dataskyddsförordningen.
[19] Därför kommer du till exempel inte att betraktas som en uppgiftsutförare om du är en registrerad person som lämnar in dina personuppgifter via ett frågeformulär på nätet till en personuppgiftsansvarig som är etablerad i ett tredjeland.
[20] Se EDPB:s riktlinjer 3/2018 om den allmänna dataskyddsförordningens territoriella tillämpningsområde (artikel 3) https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_en
[21] EDPB:s riktlinjer 2/2020 om artiklarna 46.2 a och 46.3 b i förordning 2016/679 för överföring av personuppgifter mellan offentliga myndigheter och organ inom och utanför EES, se https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-22020-articles-46-2-and-46-3-b_en
[22] Artikel 5.2 i den allmänna dataskyddsförordningen och artikel 24.1 i den allmänna dataskyddsförordningen.
[23] Observera att fjärråtkomst av en enhet i ett tredjeland till uppgifter som finns inom EES också betraktas som en överföring.

komplicerad uppgift för enheter som utför ett stort antal skiftande och regelbundna överföringar till tredjeländer och som använder flera olika personuppgiftsansvariga på olika nivåer. Att lära känna dina överföringar är ett viktigt första steg mot att fullgöra dina skyldigheter enligt principen om ansvarsskyldighet.

9. För att se till att du är fullt medveten om dina överföringar kan du bygga vidare på det register över behandlingen som du kan vara skyldig att upprätthålla som personuppgiftsansvarig eller personuppgiftsbiträde enligt artikel 30 i den allmänna dataskyddsförordningen.[24] Du kan även ha nytta av tidigare åtgärder för att uppfylla skyldigheten att informera de registrerade om dina överföringar av deras personuppgifter till tredjeländer enligt artiklarna 13.1 f och 14.1 f i den allmänna dataskyddsförordningen.[25]

10. När du kartlägger överföringarna får du inte glömma att även ta hänsyn till vidareöverföringar, till exempel om dina personuppgiftsbiträden utanför EES överför personuppgifter som du har anförtrott dem till en underentreprenör i ett annat tredjeland eller samma tredjeland[26].

11. I linje med dataskyddsförordningens princip om ”uppgiftsminimering”[27] måste du kontrollera att de uppgifter du överför är adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas.

12. Detta måste utföras innan någon överföring görs och uppdateras innan överföringarna av uppgifter återupptas efter ett avbrott. Du måste känna till var de personuppgifter du förde ut sparas eller bearbetas av uppgiftsinförarna (karta över mottagare).

13. Tänk på att fjärråtkomst från ett tredjeland (till exempel i stödsituationer) och/eller lagring i en molntjänst utanför EES som erbjuds av en tjänsteleverantör, också betraktas som överföringar.[28] Mer specifikt, om du använder en internationell molninfrastruktur måste du bedöma om och när

---

[24] Se artikel 30 i den allmänna dataskyddsförordningen, särskilt punkterna 1 e och 2 c. Ditt register över behandlingen bör dessutom innehålla en beskrivning av dina behandlingar (inbegripet, men inte begränsat till, kategorierna av registrerade, kategorierna av personuppgifter, syftet med behandlingen och särskild information om överföringarna av uppgifter. Vissa personuppgiftsansvariga och personuppgiftsbiträden är undantagna från skyldigheten att föra ett register över behandlingen (artikel 30.5 i den allmänna dataskyddsförordningen). Riktlinjer för detta undantag finns i artikel 29 i arbetsgruppens ståndpunktsdokument om undantag från skyldigheten att upprätthålla register över behandling enligt artikel 30.5 i den allmänna dataskyddsförordningen (som godkändes av EDPB den 25 maj 2018).

[25] Enligt den allmänna dataskyddsförordningens öppenhetsregler måste du informera de registrerade om överföringar av personuppgifter till tredjeländer (artiklarna 13.1 f och 14.1 f i dataskyddsförordningen). I synnerhet måste du informera dem om huruvida kommissionen har fattat ett beslut om adekvat skyddsnivå eller, när det gäller sådana överföringar som avses i artikel 46 eller 47 i den allmänna dataskyddsförordningen, eller det andra stycket i artikel 49.1 i den förordningen, hänvisa till lämpliga eller passande skyddsåtgärder och förklara hur en kopia av dem kan erhållas eller var de har gjorts tillgängliga. Den information som lämnas till den registrerade måste vara korrekt och aktuell, särskilt mot bakgrund av domstolens rättspraxis för överföringar.

[26] Om den personuppgiftsansvariga har gett ett särskilt eller allmänt skriftligt förhandsgodkännande i enlighet med artikel 28.2 i den allmänna dataskyddsförordningen.

[27] Artikel 5.1 c i den allmänna dataskyddsförordningen.

[28] Se fråga nr 11: ”man bör komma ihåg att även utlämning av uppgifter från ett tredjeland, till exempel för administrationsändamål, utgör en överföring”, EDPB:s Vanliga frågor om EU-domstolens dom i mål C-311/18 – Data Protection Commissioner mot Facebook Ireland Ltd och Maximillian Schrems, den 23 juli 2020.

dina uppgifter kommer att överföras till tredjeländer, såvida inte molnleverantören är etablerad i EES och tydligt uppger i sitt avtal att uppgifterna inte kommer att behandlas alls i tredjeländer.

2.2 Steg 2: Identifiera vilka överföringsverktyg du förlitar dig på

14. Ett andra steg som du måste gå igenom är att identifiera vilka överföringsverktyg du förlitar dig på bland de som ingår i förteckningen i kapitel V i den allmänna dataskyddsförordningen.

Beslut om adekvat skyddsnivå

15. EU-kommissionen kan genom sina **beslut om adekvat skyddsnivå** för vissa eller alla av de tredjeländer du överför personuppgifter till fastställa att de erbjuder en adekvat skyddsnivå för personuppgifter.[29]

16. Följden av ett sådant beslut om adekvat skyddsnivå är att personuppgifter kan flöda från EES till det berörda tredjelandet utan att ett överföringsverktyg enligt artikel 46 i den allmänna dataskyddsförordningen måste användas.

17. Beslut om adekvat skyddsnivå kan omfatta ett helt land eller vara begränsade till en del av det. Beslut om adekvat skyddsnivå kan omfatta alla överföringar av uppgifter till ett land eller vara begränsade till vissa typer av överföringar (t.ex. inom en sektor).[30]

18. EU-kommissionen offentliggör en förteckning över sina beslut om adekvat skyddsnivå på sin webbplats.[31]

19. Om du överför personuppgifter till tredjeländer, regioner eller sektorer som omfattas av ett beslut om adekvat skyddsnivå (i tillämpliga fall), **behöver du inte vidta några ytterligare av de steg som beskrivs i dessa rekommendationer**.[32] Du måste emellertid fortfarande övervaka om de beslut om adekvat skyddsnivå som är relevanta för dina överföringar återkallas eller ogiltigförklaras.[33]

20. Beslut om adekvat skyddsnivå hindrar emellertid inte att registrerade personer lämnar in klagomål. De hindrar inte heller tillsynsmyndigheterna från att väcka talan i en nationell domstol om de hyser tvivel om beslutets giltighet, så att en nationell domstol kan begära ett förhandsavgörande av EU-domstolen för att undersöka beslutets giltighet.[34]

---

[29] EU-kommissionen har enligt artikel 45 i den allmänna dataskyddsförordningen befogenhet att fastställa huruvida ett land utanför EU erbjuder en adekvat nivå av dataskydd. Likaså har EU-kommissionen befogenhet att fastställa att en internationell organisation erbjuder en adekvat skyddsnivå.

[30] Artikel 45.1 i den allmänna dataskyddsförordningen.

[31] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

[32] Under förutsättning att du och uppgiftsinföraren har genomfört åtgärder för att fullgöra skyldigheterna i den allmänna dataskyddsförordningen, annars måste dessa åtgärder genomföras.

[33] EU-kommissionen ska granska alla beslut om adekvat skyddsnivå med jämna mellanrum och kontrollera att de tredjeländer som omfattas av besluten upprätthåller en adekvat skyddsnivå (se artikel 45.3 och 45.4 i den allmänna dataskyddsförordningen). Dessutom kan EU-domstolen ogiltigförklara beslut om adekvat skyddsnivå (se domarna i målen C-362/14 (Schrems I) och C-311/18 (Schrems II)).

[34] C-311/18 (Schrems II), punkterna 118–120. Tillsynsmyndigheterna får inte åsidosätta beslut om adekvat skyddsnivå och avbryta eller förbjuda överföringar av personuppgifter till sådana länder om de endast hänvisar till den otillräckliga skyddsnivån. De får endast utöva sina befogenheter att avbryta eller förbjuda överföringar

Exempel:

En EU-medborgare, Max Schrems, lämnade i juni 2013 in ett klagomål till den irländska dataskyddskommissionen (DPC) och bad denna tillsynsmyndighet att förbjuda eller avbryta överföringen av hans personuppgifter från Facebook Ireland till USA, eftersom han ansåg att USA:s lagstiftning och praxis inte gav tillräckligt skydd mot de offentliga myndigheternas övervakning av de personuppgifter som lagras inom landets territorium. DPC avslog klagomålet, framför allt med hänvisning till att EU-kommissionen i sitt beslut 2000/520/EG ansåg att USA enligt ”safe harbour-principen” säkerställde en adekvat skyddsnivå för överförda personuppgifter (Safe Harbour-beslutet). Max Schrems invände mot DPC:s beslut, och Irlands högsta domstol lämnade in en fråga om giltigheten av beslut 2000/520/EG till Europeiska unionens domstol. EU-domstolen beslutade därefter att ogiltigförklara kommissionens beslut 2000/520/EG om huruvida ett adekvat skydd säkerställs genom principerna om integritetsskydd (Safe Harbor Privacy Principles).[35]

Överföringsverktyg i artikel 46 i den allmänna dataskyddsförordningen

21. Artikel 46 i den allmänna dataskyddsförordningen innehåller en förteckning över ett antal överföringsverktyg med ”lämpliga skyddsåtgärder” som uppgiftsutförare kan använda för att överföra personuppgifter till tredjeländer i avsaknad av ett beslut om adekvat skyddsnivå. De viktigaste typerna av överföringsverktyg i artikel 46 är

    - standardiserade dataskyddsbestämmelser,
    - bindande företagsbestämmelser,
    - uppförandekoder,
    - certifieringsmekanismer, och
    - avtalsklausuler.

22. Vilket överföringsverktyg i artikel 46 i den allmänna dataskyddsförordningen du än väljer måste du säkerställa att de överförda personuppgifterna kommer att omfattas av en väsentligen likvärdig skyddsnivå.

23. Överföringsverktygen i artikel 46 i dataskyddsförordningen innehåller huvudsakligen lämpliga skyddsåtgärder med avtalsrättslig karaktär som kan tillämpas på överföringar till alla tredjeländer. Situationen i det tredjeland som du överför uppgifter till kan kräva att du kompletterar dessa överföringsverktyg och deras skyddsåtgärder med ytterligare åtgärder (”kompletterande åtgärder”) för att säkerställa en väsentligen likvärdig skyddsnivå.[36]

av personuppgifter till det berörda tredjelandet på andra grunder (t.ex. otillräckliga skyddsåtgärder i strid med artikel 32 i dataskyddsförordningen eller avsaknad av en rättslig grund som stöd till databehandlingen som sådan i strid med artikel 6 i den allmänna dataskyddsförordningen). Tillsynsmyndigheterna får helt oberoende undersöka om överföringen av uppgifter uppfyller de krav som fastställs i den allmänna dataskyddsförordningen och, i relevanta fall, väcka talan i en nationell domstol för att de, om de hyser tvivel om giltigheten av kommissionens beslut om adekvat skyddsnivå, ska kunna begära ett förhandsavgörande av EU-domstolen för att undersöka dess giltighet.

[35] Mål C-362/14 (Schrems I).

[36] C-311/18 (Schrems II), punkterna 130 och 133. Se även underavsnitt 2.3 nedan.

Undantag

24. Vid sidan av besluten om adekvat skyddsnivå och överföringsverktygen i artikel 46 i den allmänna dataskyddsförordningen omfattar förordningen ett tredje alternativ för att möjliggöra överföringar av personuppgifter i särskilda situationer. Under särskilda omständigheter kan du överföra personuppgifter genom ett av de undantag som anges i artikel 49 i den allmänna dataskyddsförordningen.

25. Artikel 49 i den allmänna dataskyddsförordningen har en undantagskaraktär. De undantag den innehåller måste tolkas på ett sätt som inte står i strid med undantagens själva beskaffenhet som undantag från regeln att personuppgifter inte får överföras till ett tredjeland såvida inte landet garanterar en adekvat skyddsnivå för uppgifter eller, alternativt, lämpliga skyddsåtgärder sätts in. Undantag kan inte bli en ”regel” i praktiken, utan måste begränsas till specifika situationer. EDPB har utfärdat sina riktlinjer 2/2018 om undantagen i artikel 49 enligt förordning 2016/679. [37]

26. Innan du åberopar ett undantag enligt artikel 49 i den allmänna dataskyddsförordningen måste du kontrollera om din överföring uppfyller de stränga villkor som fastställts för vart och ett av undantagen.

***

27. Om din överföring inte har någon rättslig grund i ett beslut om adekvat skyddsnivå eller ett undantag enligt artikel 49 måste du fortsätta med steg 3.

2.3 Steg 3: Bedöm om överföringsverktyget i artikel 46 i den allmänna dataskyddsförordningen är effektivt mot bakgrund av alla omständigheter kring överföringen

28. Det valda överföringsverktyget i artikel 46 i den allmänna dataskyddsförordningen måste effektivt säkerställa att den skyddsnivå som garanteras genom dataskyddsförordningen i praktiken inte undergrävs av överföringen.[38]

29. Framför allt måste det skydd som tilldelas de överförda personuppgifterna i tredjelandet vara väsentligen likvärdigt med det som garanteras inom EES i den allmänna dataskyddsförordningen, mot bakgrund av EU-stadgan om de grundläggande rättigheterna.[39] Detta är inte fallet om uppgiftsinföraren hindras från att fullgöra sina skyldigheter enligt det valda överföringsverktyget i artikel 46 i den allmänna dataskyddsförordningen på grund av den lagstiftning och praxis som gäller för överföringen i tredjelandet, inräknat under överföringen av uppgifterna från uppgiftsutförarens till uppgiftsinförarens land[40].

30. Du måste först bedöma, i tillämpliga fall tillsammans med uppgiftsinföraren, om det finns något i rättsläget och/eller gällande praxis i tredjelandet[41] som kan påverka effektiviteten hos de lämpliga

---

[37] Ytterligare vägledning om detta finns på webbadressen https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation_en.
[38] Artikel 44 i den allmänna dataskyddsförordningen och punkterna 126, 137 och 148 i C-311/18 (Schrems II).
[39] C-311/18 (Schrems II), punkt 105 och den andra slutsatsen.
[40] Se C-311/18 (Schrems II), punkt 183 tillsammans med punkt 184.
[41] Se punkt 126 i domen i målet C-311/18 (Schrems II) där domstolen uttryckligen hänvisar till ”rättsläget och gällande praxis i det berörda tredjelandet” och kräver att ”i praktiken säkerställa ett effektivt skydd av de personuppgifter som överförs till det berörda tredjelandet.” (betoning tillagd), och punkt 158.

skyddsåtgärderna i det överföringsverktyg i artikel 46 i den allmänna dataskyddsförordningen som du förlitar dig på i samband med din specifika överföring. Detta innebär att fastställa huruvida din överföring omfattas av lagstiftning och/eller praxis som kan påverka effektiviteten hos ditt överföringsverktyg i artikel 46 i den allmänna dataskyddsförordningen. Den bedömning som krävs måste först och främst utgå från den lagstiftning som finns tillgänglig offentligt.

31. Denna bedömning måste innehålla aspekter avseende offentliga myndigheters tillgång till uppgifter i din uppgiftsinförares tredjeland såsom följande:

    - Aspekter av huruvida offentliga myndigheter i din uppgiftsinförares tredjeland kan söka tillgå uppgifterna med eller utan uppgiftsinförarens kännedom, mot bakgrund av lagstiftning, praxis och rapporterade prejudikat.
    - Aspekter av huruvida offentliga myndigheter i din uppgiftsinförares tredjeland kan tillgå uppgifterna genom uppgiftsinföraren eller genom telekomleverantörer eller kommunikationskanaler mot bakgrund av lagstiftning, rättsliga befogenheter, tekniska och finansiella resurser och personalresurser som de förfogar över och av rapporterade prejudikat.

Att identifiera relevanta lagar och praxis mot bakgrund av alla omständigheter kring överföringen

32. Du måste undersöka egenskaperna hos var och en av dina överföringar och avgöra om den nationella rättsordningen och/eller gällande praxis i det land till vilket uppgifterna överförs (eller vidareförs) påverkar dina överföringar. Din bedömning begränsas därmed till lagstiftning och praxis som är relevant för skyddet av de specifika uppgifter du överför, till skillnad från de allmänna och breda tillräcklighetsbedömningar som EU-kommissionen utför i enlighet med artikel 45 i den allmänna dataskyddsförordningen.

33. Den tillämpliga rättsliga ramen och/eller praxisen beror på de specifika omständigheterna kring din överföring, framför allt

    - syftet med överföringen och behandlingen av uppgifterna (t.ex. marknadsföring, HR, lagring, it-support, kliniska prövningar),
    - typerna av enheter som deltar i behandlingen (offentliga/privata, personuppgiftsansvariga/personuppgiftsbiträden),
    - sektorn där överföringen äger rum (t.ex. adtech, telekommunikation och finans),
    - kategorierna av personuppgifter som överförs (personuppgifter som rör barn kan t.ex. omfattas av särskild lagstiftning i tredjelandet),[42]

[42] En överföring av personuppgifter är en behandlingsåtgärd (artikel 4.2 i den allmänna dataskyddsförordningen). Om du vill överföra känsliga uppgifter som omfattas av artiklarna 9 och 10 i den allmänna dataskyddsförordningen får du bara utföra en överföring om den omfattas av ett av de undantag och villkor som fastställs i artiklarna 9 och 10 i den allmänna dataskyddsförordningen och lagstiftningen i EU:s medlemsstater. I enlighet med artikel 32 i den allmänna dataskyddsförordningen måste du även genomföra, där uppgiftsinföraren agerar som personuppgiftsansvarig eller personuppgiftsbiträde, lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till riskerna för de registrerades rättigheter och friheter av en potentiell personuppgiftsincident för de överförda uppgifterna (artikel 4.12 i den allmänna

- möjligheten att uppgifterna kan lagras i tredjelandet eller om tredjelandet kommer att ha fjärråtkomst till uppgifter som lagras inom EU/EES,
- formatet på de uppgifter som ska överföras (dvs. i klartext, pseudonymiserade eller krypterade[43]),
- möjligheten att uppgifterna kan överföras vidare från tredjelandet till ett annat tredjeland.[44]

34. I din bedömning bör du ta hänsyn till alla aktörer som deltar i överföringen (t.ex. personuppgiftsansvariga och personuppgiftsbiträden på olika nivåer som behandlar uppgifterna i tredjelandet) enligt kartläggningen av överföringarna. Ju fler personuppgiftsansvariga, personuppgiftsbiträden eller uppgiftsinförare som är inblandade, desto mer omfattande kommer din bedömning att bli. Du kommer även att behöva ta hänsyn till eventuella planerade vidareöverföringar i din bedömning.

35. Under alla omständigheter bör du vara särskilt uppmärksam på relevanta lagar, i synnerhet lagar som utfärdats för att fastställa krav om att personuppgifter ska lämnas ut till offentliga myndigheter eller för att ge offentliga myndigheter befogenhet att komma åt personuppgifter (t.ex. för brottsbekämpning, myndighetstillsyn eller nationella säkerhetssyften). Om dessa krav eller befogenheter begränsar de registrerades grundläggande rättigheter samtidigt som de är förenliga med deras väsentliga innehåll och är nödvändiga och proportionerliga åtgärder i ett demokratiskt samhälle för att viktiga målsättningar ska skyddas som även erkänns i unionsrätten eller i medlemsstaternas nationella rätt,[45] inkräktar de inte på åtagandena för det överföringsverktyg i artikel 46 i den allmänna dataskyddsförordningen som du förlitar dig på.

36. Du kommer att behöva bedöma relevant lagstiftning och praxis av allmän art i den mån detta påverkar den effektiva tillämpningen av skyddsåtgärder i artikel 46 i den allmänna dataskyddsförordningen.

37. När denna bedömning utförs är olika aspekter av tredjelandets rättsliga system också relevanta, däribland de faktorer som förtecknas i artikel 45.2 i den allmänna dataskyddsförordningen. Exempelvis kan rättsstatsprincipen i ett tredjeland vara relevant för bedömningen av effektiviteten hos tillgängliga mekanismer som gör att enskilda personer kan få upprättelse om myndigheterna har kommit åt personuppgifter på ett olagligt sätt. Förekomsten av en omfattande dataskyddslagstiftning eller en oberoende dataskyddsmyndighet, såväl som användningen av internationella instrument för dataskyddsåtgärder, kan bidra till att säkerställa om den offentliga inblandningen är proportionerlig.

---

dataskyddsförordningen). Kategorierna av överförda uppgifter och deras känslighet kommer att vara relevanta för bedömningen av risken och för åtgärdernas lämplighet.

[43] Vissa tredjeländer tillåter inte att krypterade uppgifter förs in.

[44] Om den personuppgiftsansvariga har gett ett särskilt eller allmänt skriftligt förhandsgodkännande i enlighet med artikel 28.2 i den allmänna dataskyddsförordningen.

[45] Se artiklarna 47 och 52 i Europeiska unionens stadga om de grundläggande rättigheterna, artikel 23.1 i den allmänna dataskyddsförordningen och EDPB:s rekommendationer 02/2020 om europeiska väsentliga garantier för övervakningsåtgärder av den 10 november 2020, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en.

38. De skyldigheter eller befogenheter som följer av sådan lagstiftning och praxis ska anses inkräkta på/vara oförenliga med åtagandena för överföringsverktyget i artikel 46 i den allmänna dataskyddsförordningen om de[46]

   - inte är förenliga med det väsentliga innehållet i de grundläggande rättigheterna och friheterna i Europeiska unionens stadga om de grundläggande rättigheterna, eller

   - överskrider vad som är nödvändigt och proportionerligt i ett demokratiskt samhälle för att skydda en av de viktiga målsättningarna som även erkänns i unionsrätten eller i medlemsstaternas nationella rätt såsom de som förtecknas i artikel 23.1 i den allmänna dataskyddsförordningen.

39. Du bör kontrollera om uppgiftsinförarens åtaganden som gör att registrerade personer kan utöva sina rättigheter såsom dessa fastställs i överföringsverktyget i artikel 46 i den allmänna dataskyddsförordningen (däribland att komma åt, korrigera och radera överförda uppgifter, liksom domstolsprövning) kan tillämpas på ett effektivt sätt i praktiken och att de inte motverkas av lagarna och/eller praxis i det mottagande tredjelandet

40. EU:s normer, däribland artiklarna 47 och 52 i EU-stadgan om de grundläggande rättigheterna, måste användas som referens, särskilt för att bedöma om de offentliga myndigheternas åtkomst är begränsad till vad som är nödvändigt och proportionerligt i ett demokratiskt samhälle och om de registrerade har rätt till effektiv domstolsprövning.

41. I EDPB:s rekommendationer för europeiska väsentliga garantier[47] lämnas förtydliganden om de faktorer som måste bedömas för att fastställa huruvida den rättsliga ram som styr de offentliga myndigheternas åtkomst till personuppgifter i ett tredjeland, vare sig om det rör sig om nationella säkerhetsorgan eller brottsbekämpande myndigheter, kan anses vara en motiverad inblandning[48] eller ej. Detta bör i synnerhet övervägas noggrant om den lagstiftning som reglerar de offentliga myndigheternas tillgång till uppgifter är tvetydig eller otillgänglig för allmänheten. Det första kravet i europeiska väsentliga garantier är att det ska finnas en rättslig ram för att ge en sådan åtkomst, när den är planerad, som är offentligt tillgänglig och tillräckligt tydlig.

42. Om EDPB:s rekommendationer för europeiska väsentliga garantier tillämpas på situationen för överföringar av uppgifter med överföringsverktygen i artikel 46 kan de hjälpa uppgiftsutföraren att bedöma om sådana befogenheter innebär en omotiverad inblandning i uppgiftsutförarens och uppgiftsinförarens skyldigheter att säkerställa en väsentlig likvärdighet i enlighet med dataskyddsförordningen eller åtagandena för överföringsverktyget. Bristen på en väsentligen likvärdig skyddsnivå kommer att vara särskilt uppenbar om den lagstiftning och/eller praxis i tredjelandet som är relevant för din överföring inte uppfyller kraven för de europeiska väsentliga garantierna. Europeiska dataskyddsstyrelsen framhåller att de europeiska väsentliga garantierna

---

[46] Se artiklarna 47 och 52 i Europeiska unionens stadga om de grundläggande rättigheterna, artikel 23.1 i den allmänna dataskyddsförordningen, C-311/18 (Schrems II), punkterna 174 och 187, och EDPB:s rekommendationer 02/2020 om europeiska väsentliga garantier för övervakningsåtgärder av den 10 november 2020.

[47] EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, 10 November 2020.

[48] Och att den därmed inte inkräktar på åtagandena för överföringsverktyget i artikel 46 i den allmänna dataskyddsförordningen.

är en referensstandard vid bedömning av ingrepp som följer av övervakningsåtgärder i ett tredjeland i samband med internationella uppgiftsöverföringar. Denna standard grundar sig på EU-lagstiftningen och på rättspraxis från EU-domstolen och Europadomstolen, som är bindande för EU:s medlemsstater.

43. Din bedömning måste först och främst utgå från den lagstiftning som finns tillgänglig offentligt. Genom att också undersöka praxis för tredjelandets offentliga myndigheter kan du kontrollera om skyddsåtgärderna i överföringsverktyget i artikel 46 i den allmänna dataskyddsförordningen är tillräckliga för att i praktiken säkerställa ett effektivt skydd av de överförda personuppgifterna.[49] Att undersöka gällande praxis i tredjelandet kommer att vara särskilt viktigt för din bedömning av de nedan beskrivna situationerna.

43.1 **Relevant lagstiftning i tredjelandet kan formellt uppfylla EU:s normer om grundläggande rättigheter och friheter samt nödvändigheten och proportionaliteten av begränsningar av dessa.** Emellertid kan den praxis som tillämpas vid dess offentliga myndigheter (t.ex. för att komma åt personuppgifter som innehas av den privata sektorn eller när de verkställer – eller inte verkställer – lagstiftning i egenskap av tillsynsorgan eller rättsliga myndigheter) tydligt visa att de inte normalt tillämpar/uppfyller den lagstiftning som i princip styr deras verksamhet. I detta fall måste du ta hänsyn till denna praxis i din bedömning och beakta att verktyget i artikel 46 i den allmänna dataskyddsförordningen inte, på egen hand (dvs. utan kompletterande åtgärder), effektivt kan säkerställa en väsentligen likvärdig skyddsnivå. I ett sådant fall kommer du att behöva genomföra lämpliga kompletterande åtgärder om du vill fortsätta med överföringen.

43.2 **Relevant lagstiftning i tredjelandet (t.ex. om åtkomst till personuppgifter som innehas av den privata sektorn) kan saknas**. I detta fall medför inte denna avsaknad av relevant lagstiftning att du automatiskt kan dra slutsatsen att ditt överföringsverktyg i artikel 46 i den allmänna dataskyddsförordningen kan tillämpas på ett effektivt sätt. Du måste kontrollera om det finns tecken på gällande praxis i landet som är oförenlig med EU:s lagstiftning och åtagandena för överföringsverktyget i artikel 46 i den allmänna dataskyddsförordningen. Om det förekommer oförenlig praxis kan inte överföringsverktyget i artikel 46 i den allmänna dataskyddsförordningen, på egen hand (dvs. utan lämpliga kompletterande åtgärder), effektivt säkerställa en väsentligen likvärdig skyddsnivå. I ett sådant fall kommer du att behöva genomföra lämpliga kompletterande åtgärder om du vill fortsätta med överföringen.

[49] C-311/18 (Schrems II), punkt 126.

43.3 **Bedömningen kan avslöja att relevant lagstiftning i tredjelandet kan vara problematisk[50] och att de överförda uppgifterna och/eller den befintliga uppgiftsinföraren omfattas eller skulle kunna omfattas av denna problematiska lagstiftning[51].**

Med tanke på osäkerheten kring den potentiella tillämpningen av problematisk lagstiftning på din överföring kan du sedan besluta att göra följande:

- Avbryta överföringen.
- Genomföra kompletterande åtgärder[52] för att förebygga risken för att lagstiftning och/eller praxis från uppgiftsinförarens tredjeland potentiellt tillämpas på din uppgiftsinförare och/eller på dina överförda uppgifter, som kan påverka överföringsverktygets avtalsrättsliga garanti av en väsentligen likvärdig skyddsnivå med den som garanteras inom EES.
- Alternativt kan du besluta att fortsätta med överföringen utan att behöva genomföra kompletterande åtgärder, om du anser att du inte har något skäl att tro att relevant och problematisk lagstiftning i praktiken kommer att tillämpas på dina överförda uppgifter och/eller din uppgiftsinförare. Genom din bedömning måste du ha påvisat och dokumenterat, i tillämpliga fall i samarbete med uppgiftsinföraren, att lagstiftningen i praktiken inte tolkas och/eller tillämpas för att omfatta dina överförda uppgifter och uppgiftsinföraren, även med beaktande av erfarenheten av andra aktörer som verkar inom samma sektor och/eller i samband med liknande överförda personuppgifter samt de ytterligare informationskällor som beskrivs längre ner[53].

  Du kommer därför att behöva ha påvisat och dokumenterat med en utförlig rapport[54] att problematisk lagstiftning i praktiken inte kommer att tillämpas på dina överförda uppgifter och/eller uppgiftsinföraren, och att den följaktligen inte kommer att hindra uppgiftsinföraren från att uppfylla sina skyldigheter enligt överföringsverktyget i artikel 46 i den allmänna dataskyddsförordningen[55].

---

[50] ”Problematisk lagstiftning” förstås som lagstiftning som 1) inför skyldigheter för mottagaren av personuppgifter från EU och/eller påverkar de uppgifter som överförts på ett sätt som kan påverka överföringsverktygets avtalsrättsliga garanti av en väsentligen likvärdig skyddsnivå och 2) inte är förenlig med det väsentliga innehållet i de grundläggande rättigheter och friheter som erkänns i EU-stadgan om de grundläggande rättigheterna eller överskrider vad som är nödvändigt och proportionerligt i ett demokratiskt samhälle för att skydda en av de viktiga målsättningarna, såsom de i artikel 23.1 i den allmänna dataskyddsförordningen.

[51] Det kan vara oklart huruvida uppgiftsinföraren och/eller de överförda uppgifterna omfattas av de allmänna villkor som ofta används i nationell säkerhetslagstiftning för att begränsa deras tillämpningsområde, såsom ”leverantör av elektroniska kommunikationstjänster” och ”utländska underrättelseuppgifter”.

[52] Se skäl 109 i den allmänna dataskyddsförordningen och C-311/18 (Schrems II), punkt 132.

[53] Se punkterna 45–47.

[54] Dina rapporter ska innehålla omfattande information om den rättsliga bedömningen av lagstiftning och praxis, samt deras tillämpning på de specifika överföringarna, det interna förfarandet för att producera bedömningen (inräknat information om aktörer involverade i bedömningen, t.ex. advokatbyråer, konsulter eller interna avdelningar) och datum för kontrollerna. Rapporter ska tillstyrkas av uppgiftsutförarens rättsliga företrädare.

[55] Att du påvisar att problematisk lagstiftning i praktiken inte tillämpas på dina överförda uppgifter och uppgiftsinföraren, även med beaktande av erfarenheten av andra aktörer som verkar inom samma sektor och/eller i samband med liknande överförda personuppgifter, innebär inte att du inte behöver tillhandahålla de

Möjliga informationskällor

44. Din uppgiftsinförare bör ge dig relevanta källor och relevant information om det tredjeland där uppgiftsinföraren är etablerad och vilka lagar och gällande praxis som är tillämpliga för överföringen.

45. Du och din uppgiftsinförare kan utföra din bedömning med information som hämtats från källor, såsom de som förtecknas som exempel i bilaga 3.

46. Utöver den rättsliga ramen i det gällande tredjelandet för överföringen ska källan och informationen vara relevant, objektiv, tillförlitlig, verifierbar och offentligt tillgänglig eller på annat sätt åtkomlig för att avgöra huruvida ditt överföringsverktyg i artikel 46 kan tillämpas på ett effektivt sätt[56], vilket du måste bedöma och dokumentera.

Relevant: informationen måste vara relevant för den specifika överföringen och/eller uppgiftsinförare och dennes överensstämmelse med kraven i EU:s lagstiftning och överföringsinstrument enligt artikel 46 i den allmänna dataskyddsförordningen, och inte alltför allmän eller abstrakt.

Objektiv information: information som understöds av empiriska belägg som grundar sig på tidigare vunnen kunskap, inte på antaganden om potentiella händelser och risker.

Tillförlitlig: uppgiftsutföraren och uppgiftsinföraren måste objektivt bedöma tillförlitligheten hos informationskällan och själva informationen, och utvärdera dem separat.

Verifierbar: information och slutsatser ska kunna verifieras eller jämföras med andra typer av information eller källor, som del av en övergripande bedömning, också för att det behöriga tillsynsorganet eller den rättsliga myndigheten vid behov ska kunna kontrollera objektiviteten och tillförlitligheten hos denna information.

Offentligt tillgänglig eller på annat sätt åtkomlig information: information bör helst vara offentlig eller åtminstone tillgänglig för att göra det lättare att verifiera de ovan angivna kriterierna och säkerställa dess möjliga delning med tillsynsmyndigheter, rättsliga myndigheter och i slutändan de registrerade personerna.

47. Du kan också överväga uppgiftsinförarens dokumenterade praktiska erfarenhet av relevanta tidigare inlämnade begäranden om åtkomst från offentliga myndigheter i tredjelandet. Du kommer bara att kunna använda uppgiftsinförarens erfarenhet som en ytterligare informationskälla om den rättsliga ramen i tredjelandet inte förbjuder uppgiftsinföraren att

ytterligare skyddsåtgärder som behövs för att skydda personuppgifterna medan de överförs och behandlas i det mottagande tredjelandet (t.ex. genomgående kryptering av data – se exempel på tekniska kompletterande åtgärder i bilaga 2) om din analys av den tillämpliga lagstiftningen i det mottagande tredjelandet visar att åtkomst till uppgifter även kan förekomma, också utan intervention från uppgiftsinföraren, vid denna tidpunkt av överföringen. Du kanske redan har förutsett sådana åtgärder där uppgiftsinföraren agerar som personuppgiftsansvarig eller personuppgiftsbiträde i enlighet med artikel 32 i den allmänna dataskyddsförordningen.

[56] Se bilaga 3 för en icke uttömmande förteckning över informationskällor som du och uppgiftsinföraren kan använda.

tillhandahålla information om begäranden om utlämning från offentliga myndigheter eller om frånvaron av sådana begäranden (och du bör även dokumentera en sådan bedömning). Lägg dock märke till att frånvaron av tidigare inlämnade begäranden som mottagits av uppgiftsinföraren aldrig i sig kan betraktas som ett avgörande inflytande på effektiviteten hos överföringsverktyget i artikel 46 i den allmänna dataskyddsförordningen som låter överföringen fortskrida utan kompletterande åtgärder. Du kommer att kunna överväga denna information, tillsammans med andra typer av information som inhämtats från andra källor, som en del av din övergripande bedömning av lagar och praxis i tredjelandet i förhållande till din överföring. Uppgiftsinförarens relevanta och dokumenterade erfarenhet ska bekräftas och inte motsägas av relevant, objektiv, tillförlitlig, verifierbar och offentligt tillgänglig eller på annat sätt åtkomlig information om den praktiska tillämpningen av den relevanta lagen (t.ex. förekomsten eller frånvaron av begäranden om åtkomst som mottagits av andra aktörer som verkar inom samma sektor och/eller i samband med liknande överförda personuppgifter[57] och/eller lagstiftningens tillämpning i praktiken, såsom rättspraxis och rapporter från oberoende tillsynsorgan).

Resultat av din bedömning

48. Du bör utföra denna övergripande bedömning av lagar och praxis i din uppgiftsinförares tredjeland som är tillämplig på din överföring med tillbörlig aktsamhet och dokumentera den noga. Din behöriga tillsynsmyndighet och/eller rättsliga myndighet kan kräva in den och hålla dig ansvarig för alla beslut som du fattar på denna grund[58].

49. Din slutgiltiga bedömning av det överföringsverktyg i artikel 46 i den allmänna dataskyddsförordningen som du förlitar dig på kan visa något av följande:

    - Överföringsverktyget säkerställer effektivt att de överförda personuppgifterna har en skyddsnivå i tredjelandet som väsentligen är likvärdig med den nivå som garanteras i EES. Tredjelandets tillämpliga lagstiftning och praxis för överföringen låter uppgiftsinföraren fullgöra sina skyldigheter enligt det valda överföringsverktyget. Du bör göra en ny utvärdering med jämna mellanrum eller när betydande ändringar konstateras (se steg 6).

    - Överföringsverktyget säkerställer inte en väsentligen likvärdig skyddsnivå. Uppgiftsinföraren kan inte uppfylla sina skyldigheter eftersom tredjelandets tillämpliga lagstiftning och/eller praxis för överföringen inte uppfyller EU:s normer om grundläggande rättigheter och friheter och på grund av nödvändigheten och proportionaliteten av begränsningar av dessa för att skydda legitima mål av allmänintresse. I de fall där överföringsverktygen i artikel 46 i dataskyddsförordningen inte är tillräckliga fastslog EU-domstolen att det är uppgiftsutförarens ansvar att antingen införa effektiva kompletterande åtgärder eller avstå från att överföra personuppgifterna.[59]

[57] Erfarenheten kan vara den av andra enheter som du direkt känner till på grund av tidigare överföringar av samma typ som du sätter in, eller som rapporteras i relevant rättspraxis, icke-statliga organisationers rapporter osv. (se bilaga 3).
[58] Artikel 5.2 i den allmänna dataskyddsförordningen.
[59] EU-domstolen C-311/18 (Schrems II), punkterna 134 och 135.

Exempel:

Bakgrund:
EU-domstolen framhöll att avsnitt 702 i den amerikanska lagen om underrättelseverksamhet och övervakning utomlands (Fisa) inte motsvarar de minimikrav som gäller enligt proportionalitetsprincipen enligt unionsrätten och att övervakningsprogram som grundar sig på dessa bestämmelser inte är begränsade till vad som är strikt nödvändigt. Detta innebär att skyddsnivån för de program som godkänns enligt avsnitt 702 i Fisa inte är väsentligen likvärdig med de skyddsåtgärder som krävs enligt unionsrätten.

Bedömning:
Om din bedömning av den relevanta amerikanska lagstiftningen får dig att anse att din överföring kan omfattas av avsnitt 702 i Fisa, men du är osäker på om den ingår i dess praktiska tillämpningsområde, kan du besluta något av följande:

1. Avbryta överföringen.
2. Anta lämpliga kompletterande åtgärder som effektivt säkerställer en skyddsnivå för de överförda uppgifterna som är väsentligen likvärdig med den nivå som garanteras i EES.
3. Undersöka annan objektiv, tillförlitlig, relevant, verifierbar och helst offentligt tillgänglig information (som kan innefatta information från din uppgiftsinförare) för att i praktiken tydliggöra tillämpningsområdet för avsnitt 702 i Fisa för dina särskilda överföring. Denna information bör besvara vissa relevanta frågor, såsom följande:

- Visar offentligt tillgänglig information att det finns ett lagstadgat förbud mot att informera om en mottagen specifik begäran om åtkomst till uppgifter och omfattande begränsningar av tillhandahållandet av allmän information om mottagna begäranden om åtkomst till uppgifter eller frånvaro av mottagna begäranden?

- Har din uppgiftsinförare bekräftat att den tidigare har mottagit begäranden om åtkomst till uppgifter från amerikanska offentliga myndigheter? Eller har din uppgiftsinförare bekräftat att den inte tidigare har mottagit begäranden om åtkomst till uppgifter från amerikanska offentliga myndigheter och att den inte är förbjuden att tillhandahålla information om sådana begäranden eller deras frånvaro?

- Avslöjar offentligt tillgänglig information som du har mottagit om amerikansk rättspraxis och rapporter från tillsynsorgan, organisationer i det civila samhället samt akademiska institutioner[60] att uppgiftsinförare i samma sektor som din uppgiftsinförare tidigare har mottagit begäranden om åtkomst till uppgifter för liknande överförda uppgifter?

De svar du får på dessa frågor genom din övergripande bedömning leder dig till följande slutsats:

- Avsnitt 702 i Fisa gäller i praktiken för din särskilda överföring och påverkar därför effektiviteten hos ditt överföringsverktyg i artikel 46 i den allmänna dataskyddsförordningen. Om du vill fortsätta med överföringen måste du följaktligen överväga, i tillämpliga fall i samarbete med uppgiftsinföraren, om du kan införa kompletterande åtgärder som effektivt säkerställer en skyddsnivå för de överförda

[60] T.ex. bestämmelser i avsnitt 702 i Fisa; arbetsordningen för Foreign Intelligence Surveillance Court (FISC), FISC-yttranden och beslut för vilka sekretessen har hävts, rättspraxis vid domstolar i Förenta staterna; rapporter och utfrågningsprotokoll från styrelsen för tillsyn av personlig integritet och medborgerliga friheter (Privacy and Civil Liberties Oversight Board, PCLOB); rapporter från Office of the Inspector General – Förenta staternas justitieministerium; rapporter från NSA Director of Civil Liberties and Privacy Office; rapporter utarbetade av Congressional Research Service; rapporter från American Civil Liberties Union Foundation (ACLU).

uppgifterna som är väsentligen likvärdig med den som garanteras i EES. Du får inte överföra personuppgifterna om du inte kan hitta effektiva kompletterande åtgärder.
eller
- Avsnitt 702 i Fisa gäller inte i praktiken för din särskilda överföring och påverkar därför inte effektiviteten hos ditt överföringsverktyg i artikel 46 i den allmänna dataskyddsförordningen. Du kan då fortsätta med överföringen utan några kompletterande åtgärder.

2.4 Steg 4: Inför kompletterande åtgärder

50. Om din bedömning enligt steg 3 har visat att ditt överföringsverktyg enligt artikel 46 i dataskyddsförordningen inte är effektivt måste du överväga, i tillämpliga fall i samarbete med uppgiftsinföraren, om det finns några kompletterande åtgärder som, i kombination med de skyddsåtgärder som ingår i överföringsverktygen, skulle kunna säkerställa att de överförda uppgifterna får en skyddsnivå i tredjelandet som är väsentligen likvärdig med den nivå som garanteras inom EU.[61] ”Kompletterande åtgärder” är per definition kompletterande till de skyddsåtgärder som överföringsverktyget i artikel 46 i den allmänna dataskyddsförordningen redan tillhandahåller och till alla andra tillämpliga säkerhetskrav (t.ex. tekniska skyddsåtgärder) i den allmänna dataskyddsförordningen.[62]

51. Du måste i varje enskilt fall identifiera vilka kompletterande åtgärder som kan vara effektiva för överföringar till ett visst tredjeland vid användning av ett visst överföringsverktyg i artikel 46 i den allmänna dataskyddsförordningen. Du behöver inte göra om bedömningen varje gång du utför samma överföring av en specifik typ av uppgifter till samma tredjeland. Vissa av de uppgifter som planeras att överföras kan kräva kompletterande åtgärder, medan andra kanske inte gör det (med tanke på formell och/eller praktisk tillämpning av tredjelandets lagstiftning). Du kommer att kunna bygga vidare på dina bedömningar och slutsatser i tidigare steg 1, 2 och 3 ovan och använda deras resultat för att kontrollera om de kompletterande åtgärderna kan garantera den skyddsnivå som krävs.

52. I princip kan kompletterande åtgärder ha en avtalsrättslig, teknisk eller organisatorisk karaktär. Att kombinera olika åtgärder på ett sätt som gör att de stöder och bygger på varandra kan förstärka nivån av skydd och därmed bidra till att uppnå EU:s normer.

53. Enbart avtalsrättsliga och organisatoriska åtgärder kommer i allmänhet inte att övervinna de offentliga myndigheternas åtkomst till personuppgifter i tredjelandet baserat på problematisk lagstiftning och/eller praxis[63]. Det kommer att finnas situationer där endast tekniska åtgärder som

[61] C-311/18 (Schrems II), punkt 96.
[62] Skäl 109 i den allmänna dataskyddsförordningen och C-311/18 (Schrems II), punkt 133.
[63] ”Problematisk lagstiftning” förstås som lagstiftning som 1) inför skyldigheter för mottagaren av personuppgifter från EU och/eller påverkar de uppgifter som överförts på ett sätt som kan påverka överföringsverktygets avtalsrättsliga garanti av en väsentligen likvärdig skyddsnivå och 2) inte är förenlig med det väsentliga innehållet i de grundläggande rättigheter och friheter som erkänns i EU-stadgan om de

genomförs på rätt sätt kan hindra eller begränsa de offentliga myndigheternas åtkomst till personuppgifter i tredjelandet, i synnerhet för övervakningsändamål.[64] I sådana situationer kan avtalsrättsliga eller organisatoriska åtgärder komplettera de tekniska åtgärderna och förstärka uppgifternas övergripande skyddsnivå (t.ex. genom att införa kontroller och undanröja automatismer om de offentliga myndigheterna försöker komma åt uppgifter på ett sätt som inte är förenligt med EU:s normer).

54. Du kan, i tillämpliga fall i samarbete med uppgiftsinföraren, gå igenom följande (icke uttömmande) förteckning över faktorer för att identifiera vilka kompletterande åtgärder som hade varit mest effektiva för att skydda de överförda uppgifterna mot offentliga myndigheters begäranden om åtkomst till uppgifter baserat på problematisk lagstiftning tillämpad i praktiken:

    - Formatet på de uppgifter som ska överföras (dvs. i klartext, pseudonymiserade eller krypterade).
    - Arten av uppgifter (t.ex. en högre skyddsnivå medges i EES för kategorier av uppgifter i artiklarna 9 och 10 i den allmänna dataskyddsförordningen)[65].
    - Varaktigheten och komplexiteten i databehandlingens arbetsflöden, antalet aktörer som deltar i behandlingen och deras inbördes relationer (t.ex. om överföringarna inbegriper flera personuppgiftsansvariga eller både personuppgiftsansvariga och personuppgiftsbiträden, eller om personuppgiftsansvariga deltar för att överföra uppgifterna från dig till din uppgiftsinförare – i enlighet med de relevanta bestämmelser som är tillämpliga enligt lagstiftningen i det mottagande tredjelandet).[66]
    - Teknik eller parametrar för praktisk tillämpning av tredjelandets lagstiftning som genomförts i steg 3.
    - Möjligheten att uppgifterna kan överföras vidare, inom samma tredjeland eller till och med till andra tredjeländer (t.ex. genom uppgiftsinförarens underentreprenörer[67]).

Exempel på kompletterande åtgärder

grundläggande rättigheterna eller överskrider vad som är nödvändigt och proportionerligt i ett demokratiskt samhälle för att skydda en av de viktiga målsättningarna, såsom de i artikel 23.1 i den allmänna dataskyddsförordningen.

[64] Om sådan åtkomst går längre än vad som är nödvändigt och proportionerligt i ett demokratiskt samhälle, se artiklarna 47 och 52 i Europeiska unionens stadga om de grundläggande rättigheterna, artikel 23.1 i den allmänna dataskyddsförordningen och EDPB:s rekommendationer 02/2020 om europeiska väsentliga garantier för övervakningsåtgärder av den 10 november 2020 https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en.

[65] Se fotnot 42.

[66] Enligt den allmänna dataskyddsförordningen har personuppgiftsansvariga och personuppgiftsbiträden särskilda skyldigheter. Överföringar kan ske mellan personuppgiftsansvariga, mellan gemensamma personuppgiftsansvariga, från personuppgiftsansvarig till personuppgiftsbiträde och, med tillstånd av den personuppgiftsansvarige, från personuppgiftsbiträde till personuppgiftsansvarig eller mellan personuppgiftsbiträden.

[67] Se fotnot 26.

55. Några exempel på tekniska, avtalsrättsliga och organisatoriska åtgärder som kan övervägas, om de inte redan ingår i det använda överföringsverktyget i artikel 46 i den allmänna dataskyddsförordningen, finns i den icke uttömmande förteckningen i bilaga 2.

***

56. Om du har infört effektiva kompletterande åtgärder som, i kombination med det överföringsverktyg i artikel 46 i dataskyddsförordningen som du har valt, uppnår en skyddsnivå som är väsentligen likvärdig med den nivå som garanteras inom EES kan du fortsätta med dina överföringar.

57. Om du inte kan hitta eller genomföra effektiva kompletterande åtgärder som säkerställer att de överförda uppgifterna har en väsentligen likvärdig skyddsnivå[68] får du inte börja överföra personuppgifter till det berörda tredjelandet på grundval av det överföringsverktyg i artikel 46 i dataskyddsförordningen som du förlitar dig på. Om du redan genomför överföringar måste du avbryta eller avsluta överföringen av personuppgifter.[69] I enlighet med de skyddsåtgärder som ingår i de överföringsverktyg i artikel 46 i dataskyddsförordningen som du förlitar dig på bör de uppgifter som du redan har överfört till tredjelandet och deras kopior återlämnas till dig eller makuleras i sin helhet av uppgiftsinföraren.[70]

Exempel:

Tredjelandets lagstiftning innebär att de kompletterande åtgärder som du har valt är förbjudna (t.ex. förbud mot kryptering) eller att deras effektivitet begränsas på något annat sätt. Du får inte börja överföra personuppgifter till det berörda landet, och du måste avbryta alla pågående befintliga överföringar.

58. Den behöriga tillsynsmyndigheten kan införa andra korrigerande åtgärder (t.ex. böter) om du påbörjar eller fortsätter överföringen trots att du inte kan påvisa en väsentligen likvärdig skyddsnivå i tredjelandet.

2.5 Steg 5: Förfaranden om du har identifierat effektiva kompletterande åtgärder

59. De förfaranden som du kan behöva följa om du har identifierat vilka effektiva kompletterande åtgärder som ska vidtas kan variera beroende på vilket överföringsverktyg i artikel 46 i den allmänna dataskyddsförordningen du använder eller planerar att använda.

[68] Om sådan åtkomst går längre än vad som är nödvändigt och proportionerligt i ett demokratiskt samhälle, se artiklarna 47 och 52 i Europeiska unionens stadga om de grundläggande rättigheterna, artikel 23.1 i den allmänna dataskyddsförordningen och EDPB:s rekommendationer 02/2020 om europeiska väsentliga garantier för övervakningsåtgärder av den 10 november 2020 https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en.

[69] C-311/18 (Schrems II), punkt 135.

[70] Se t.ex. klausul 12 i bilagan till beslut 2010/87/EU om standardavtalsklausuler samt den (valfria) extra uppsägningsklausulen i bilaga B till beslut 2004/915/EG.

2.5.1 Standardiserade dataskyddsbestämmelser (artikel 46.2 c och d i den allmänna dataskyddsförordningen)

60. Om du har för avsikt att införa kompletterande åtgärder som tillägg till standardavtalsklausuler behöver du inte begära tillstånd från den behöriga tillsynsmyndigheten för att lägga till dessa typer av klausuler eller ytterligare skyddsåtgärder, under förutsättning att de identifierade kompletterande åtgärderna inte, direkt eller indirekt, står i strid med standardavtalsklausulerna och att de är tillräckliga för att säkerställa att den skyddsnivå som garanteras genom dataskyddsförordningen inte undergrävs.[71] Uppgiftsutföraren och uppgiftsinföraren måste säkerställa att ytterligare klausuler inte kan tolkas så att de begränsar rättigheterna och skyldigheterna i standardavtalsklausulerna eller på något annat sätt försämrar nivån av dataskydd. Du bör kunna påvisa detta, liksom att alla klausuler är otvetydiga, enligt principen om ansvarsskyldighet och skyldigheten att tillhandahålla en tillräcklig nivå av dataskydd. De behöriga tillsynsmyndigheterna har befogenhet att granska dessa kompletterande klausuler vid behov (t.ex. i samband med klagomål eller frågor på eget initiativ).

61. Om du har för avsikt att ändra de standardiserade dataskyddsbestämmelserna i sig, eller om de kompletterade åtgärderna direkt eller indirekt står i strid med standardavtalsklausulerna, anses du inte längre förlita dig på standardavtalsklausuler[72] och måste ansöka om tillstånd från den behöriga tillsynsmyndigheten i enlighet med artikel 46.3 a i den allmänna dataskyddsförordningen.

2.5.2 Bindande företagsbestämmelser (artikel 46.2 b i den allmänna dataskyddsförordningen)

62. Det resonemang som förs i Schrems II-domen gäller även andra överföringsinstrument enligt artikel 46.2 i den allmänna dataskyddsförordningen, eftersom alla dessa instrument i grund och botten har en avtalsrättslig karaktär, vilket innebär att de garantier som föreskrivs och de

---

[71] I skäl 109 i dataskyddsförordningen fastställs följande: ”Personuppgiftsansvarigas eller personuppgiftsbiträdens möjlighet att använda standardiserade dataskyddsbestämmelser som antagits av kommissionen eller av en tillsynsmyndighet bör inte hindra att de infogar standardiserade dataskyddsbestämmelser i ett vidare avtal, såsom ett avtal mellan personuppgiftsbiträdet och ett annat personuppgiftsbiträde, eller lägger till andra bestämmelser eller ytterligare skyddsåtgärder, under förutsättning att de inte direkt eller indirekt står i strid med standardavtalsklausuler som antagits av kommissionen eller av en tillsynsmyndighet eller påverkar de registrerades grundläggande rättigheter eller friheter.” Liknande bestämmelser ingår i de uppsättningar av standardiserade dataskyddsbestämmelser som antagits av EU-kommissionen enligt direktiv 95/45/EG.

[72] Jämför med EDPB:s yttrande 17/2020 om det utkast till standardavtalsklausuler som lämnades in av den slovenska tillsynsmyndigheten (artikel 28.8 i den allmänna dataskyddsförordningen) om en redan antagen standardavtalsklausul enligt artikel 28 som innehåller en liknande bestämmelse (”Därutöver påminner styrelsen om att möjligheten att använda standardavtalsklausuler som antagits av en tillsynsmyndighet inte hindrar parterna från att lägga till andra klausuler eller ytterligare skyddsmekanismer under förutsättning att de inte, direkt eller indirekt, motsäger de antagna standardavtalsklausulerna eller kränker de registrerades grundläggande rättigheter och friheter. Om standarddataskyddsklausulerna ändras kan parterna dessutom inte längre anses ha tillämpat de antagna standardavtalsklausulerna.”), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinion_202017_art28sccs_si_en.pdf.

åtaganden som vidtas av de berörda parterna inte kan vara bindande för offentliga myndigheter i tredjeland.[73]

63. Schrems II-domen är relevant för överföringar av personuppgifter på grundval av bindande företagsbestämmelser, eftersom lagstiftningen i tredjelandet kan påverka det skydd som ges av sådana instrument.

64. Hänvisning kommer att göras till alla åtaganden som måste inkluderas i de uppdaterade WP256/257-referenserna[74] till vilka alla grupper som åberopar bindande företagsbestämmelser som överföringsverktyg måste anpassa sina befintliga och framtida bindande företagsbestämmelser.

65. EU-domstolen har betonat att det är uppgiftsutförarens och uppgiftsinförarens ansvar att bedöma om den skyddsnivå som krävs enligt unionsrätten följs i det berörda tredjelandet för att avgöra om de garantier som ges genom standardavtalsklausulerna eller de bindande företagsbestämmelserna kan uppfyllas i praktiken. Om så inte är fallet bör du bedöma om du kan vidta kompletterande åtgärder för att säkerställa en skyddsnivå som är väsentligen likvärdig med den som tillhandahålls i EES, och om lagstiftningen eller praxis i tredjelandet inte inkräktar på dessa kompletterande åtgärder så att deras effektivitet försämras.

2.5.3 Avtalsklausuler (artikel 46.3 a i den allmänna dataskyddsförordningen)

66. Det resonemang som förs i Schrems II-domen gäller även andra överföringsinstrument enligt artikel 46.2 i den allmänna dataskyddsförordningen, eftersom alla dessa instrument i grund och botten har en avtalsrättslig karaktär, vilket innebär att de garantier som föreskrivs och de åtaganden som vidtas av de berörda parterna inte kan vara bindande för offentliga myndigheter i tredjeland.[75] Schrems II-domen är därför relevant för överföringar av personuppgifter på grundval av avtalsklausuler, eftersom lagstiftningen i tredjelandet kan påverka det skydd som ges av sådana instrument.

2.6 Steg 6: Omvärdera med lämpliga mellanrum

67. Du måste hela tiden, i tillämpliga fall i samarbete med uppgiftsinföraren, övervaka utvecklingstrender som kan påverka din ursprungliga bedömning av skyddsnivån i det tredjeland som du har överfört personuppgifter till och de beslut som du har fattat i enlighet med bedömningen. Ansvarsskyldigheten är en pågående skyldighet (artikel 5.2 i den allmänna dataskyddsförordningen).

68. Du bör inrätta väl fungerande mekanismer för att säkerställa att du utan dröjsmål avbryter eller avslutar överföringarna om

    - uppgiftsinföraren har brutit mot eller inte kan efterleva de åtaganden som han eller hon har vidtagit enligt överföringsverktyget i artikel 46 i den allmänna dataskyddsförordningen, eller

[73] EU-domstolen, C-311/18 (Schrems II), punkt 132.
[74] Artikel 29 i arbetsgruppens arbetsdokument om inrättande av en tabell med de beståndsdelar och principer som ska ingå i bindande företagsbestämmelser, senast reviderat och antaget den 6 februari 2018, WP 256 rev.01 samt artikel 29 i arbetsgruppens arbetsdokument om inrättande av en tabell med de beståndsdelar och principer som ska ingå i bindande företagsbestämmelser, senast reviderat och antaget den 6 februari 2018, WP 257 rev.01.
[75] EU-domstolen, C-311/18 (Schrems II), punkt 132.

- de kompletterande åtgärderna inte längre är effektiva i det berörda tredjelandet.

3 SLUTSATS

69. I den allmänna dataskyddsförordningen fastställs regler för behandling av personuppgifter inom EES i syfte att möjliggöra en fri rörlighet för personuppgifter inom EES. Genom kapitel V i den allmänna dataskyddsförordningen regleras överföringarna av personuppgifter till tredjeländer med ett högt mål: överföringen får inte undergräva den skyddsnivå för fysiska personer som garanteras genom dataskyddsförordningen (artikel 44). I EU-domstolens dom i mål C-311/18 (Schrems II) betonas behovet av att säkerställa en kontinuitet i den skyddsnivå som föreskrivs i den allmänna dataskyddsförordningen för personuppgifter som överförs till ett tredjeland.[76]

70. För att säkerställa en väsentligen likvärdig skyddsnivå för dina uppgifter måste du först och främst ha en ingående kunskap om dina överföringar. Du måste även kontrollera att de uppgifter du överför är adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka uppgifterna behandlas.

71. Du måste även identifiera vilka överföringsverktyg du förlitar dig på för dina överföringar. Om överföringsverktyget inte är ett beslut om adekvat skyddsnivå måste du kontrollera från fall till fall om det mottagande tredjelandets lagstiftning eller praxis undergräver de skyddsåtgärder som ingår i överföringsverktyget enligt artikel 46 i den allmänna dataskyddsförordningen i samband med dina överföringar. Om överföringsverktyget i artikel 46 i den allmänna dataskyddsförordningen inte är tillräckligt för att uppnå en väsentligen likvärdig skyddsnivå för de personuppgifter du överför kan kompletterande åtgärder fylla ut luckorna.

72. Om du inte kan hitta eller genomföra effektiva kompletterande åtgärder som säkerställer att de överförda uppgifterna har en väsentligen likvärdig skyddsnivå får du inte börja överföra personuppgifter till det berörda tredjelandet på grundval av det överföringsverktyg du har valt. Om du redan genomför överföringar måste du omedelbart avbryta eller avsluta överföringen av personuppgifter.

73. Den behöriga tillsynsmyndigheten har befogenhet att avbryta eller avsluta överföringar av personuppgifter till ett tredjeland om det skydd för de överförda uppgifterna som krävs enligt unionsrätten, i synnerhet artiklarna 45 och 46 i den allmänna dataskyddsförordningen och EU-stadgan om de grundläggande rättigheterna, inte säkerställs.

För Europeiska dataskyddsstyrelsen
Ordförande
(Andrea Jelinek)

[76] C-311/18 (Schrems II), punkt 93.

BILAGA 1: DEFINITIONER

- tredjeland: alla länder som inte är medlemmar i EES.
- EES: Europeiska ekonomiska samarbetsområdet, vilket omfattar medlemsstaterna i Europeiska unionen samt Island, Norge och Liechtenstein. Den allmänna dataskyddsförordningen gäller för de sistnämnda länderna i kraft av EES-avtalet, i synnerhet bilaga XI och protokoll 37.
- den allmänna dataskyddsförordningen: Europaparlamentets och rådets förordning (EU) nr 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).
- stadgan: Europeiska unionens stadga om de grundläggande rättigheterna, EUT C 326, 26.10.2012, s. 391–407.
- domstolen eller EU-domstolen: Europeiska unionens domstol. Den utgör Europeiska unionens rättsliga myndighet och säkerställer, i samarbete med medlemsstaternas domstolar, att unionsrätten tillämpas och tolkas på ett enhetligt sätt.
- uppgiftsutförare: den personuppgiftsansvariga eller det personuppgiftsbiträde inom EES som överför personuppgifter till en personuppgiftsansvarig eller ett personuppgiftsbiträde i ett tredjeland.
- uppgiftsinförare: den personuppgiftsansvariga eller det personuppgiftsbiträde i ett tredjeland som tar emot eller ges åtkomst till personuppgifter som överförts från EES.
- överföringsverktyg i artikel 46 i den allmänna dataskyddsförordningen: de lämpliga skyddsåtgärder som förtecknas i artikel 46 i dataskyddsförordningen och som uppgiftsutförare ska använda när de överför personuppgifter till ett tredjeland i avsaknad av ett beslut om adekvat skyddsnivå enligt artikel 45.3 i den allmänna dataskyddsförordningen. Artikel 46.2 och 46.3 i dataskyddsförordningen innehåller en förteckning över de överföringsverktyg som personuppgiftsansvariga eller personuppgiftsbiträden får använda.
- standardavtalsklausuler: standardiserade dataskyddsbestämmelser som EU-kommissionen har antagit för överföringar av personuppgifter mellan personuppgiftsansvariga eller personuppgiftsbiträden inom EES och personuppgiftsansvariga eller personuppgiftsbiträden utanför EES. Standardavtalsklausuler som antagits av EU-kommissionen är överföringsverktyg i enlighet med artikel 46.2 c och 46.5 i dataskyddsförordningen.

BILAGA 2: EXEMPEL PÅ KOMPLETTERANDE ÅTGÄRDER

74. Följande åtgärder är exempel på kompletterande åtgärder som du kan överväga när du kommit till steg 4, ”Inför kompletterande åtgärder”. Denna förteckning är inte uttömmande. Du kan utforska andra kompletterande åtgärder. Framtida tekniska, rättsliga eller organisatoriska framsteg kan leda till uppkomsten av nya kompletterande åtgärder som du kan överväga. Om du väljer och genomför en eller flera av dessa åtgärder säkerställer du inte nödvändigtvis och systematiskt att dina överföringar uppfyller den väsentligen likvärdiga standard som krävs enligt unionsrätten. Du bör välja de kompletterande åtgärder som kan garantera en effektiv skyddsnivå för dina överföringar.

75. En kompletterande åtgärd kan endast anses vara effektiv i den mening som avses i EU-domstolens dom i målet ”Schrems II” om och i den utsträckning den – i sig eller i kombination med andra åtgärder – är inriktad på de specifika brister som du identifierade i din bedömning av den rättsliga situationen i tredjelandet vad gäller dess lagar och praxis som är tillämpliga på din överföring. Om du inte kan säkerställa en väsentligen likvärdig skyddsnivå får du inte överföra personuppgifterna.

76. I egenskap av personuppgiftsansvarig eller personuppgiftsbiträde kan du redan behöva genomföra vissa av de åtgärder som beskrivs i denna bilaga för att uppfylla kraven i den allmänna dataskyddsförordningen. Detta innebär att liknande åtgärder eventuellt måste införas för personuppgifter som behandlas i EES, och överföras till en uppgiftsinförare som omfattas av ett beslut om adekvat skyddsnivå, eller till andra tredjeländer.[77]

2.1 Tekniska åtgärder

77. Detta avsnitt innehåller en icke uttömmande beskrivning av ett antal exempel på tekniska åtgärder som kan komplettera de skyddsåtgärder som ingår i överföringsverktygen i artikel 46 i den allmänna dataskyddsförordningen för att säkerställa efterlevnaden av den skyddsnivå som krävs enligt unionsrätten i samband med överföring av personuppgifter till ett tredjeland. Åtgärderna behövs i synnerhet om uppgiftsinföraren enligt landets lagstiftning har skyldigheter som strider mot skyddsåtgärderna i överföringsverktygen i artikel 46 i dataskyddsförordningen och som riskerar att inkräkta på den avtalsrättsliga garantin för en väsentligen likvärdig skyddsnivå som gör att de offentliga myndigheterna i tredjelandet inte kan komma åt uppgifterna[78].

78. Som förtydligande beskriver detta avsnitt först vissa exempel på scenarier där en del tekniska åtgärder skulle kunna vara effektiva för att säkerställa en väsentligen likvärdig skyddsnivå. Avsnittet fortsätter sedan med vissa scenarier där de tekniska åtgärderna för att säkerställa denna skyddsnivå inte har identifierats.

Exempel på scenarier med ärenden där *effektiva* åtgärder identifieras

79. Åtgärderna i förteckningen syftar till att säkerställa att de offentliga myndigheternas åtkomst till de överförda uppgifterna i tredjeländer inte begränsar effektiviteten hos de lämpliga skyddsåtgärder som ingår i överföringsverktygen i artikel 46 i den allmänna

[77] Artikel 5.2 och artikel 32 i den allmänna dataskyddsförordningen.
[78] C-311/18 (Schrems II), punkt 135.

dataskyddsförordningen. Dessa åtgärder skulle behövas för att garantera en väsentligen likvärdig skyddsnivå med den som garanteras inom EES, också om de offentliga myndigheternas åtkomst uppfyller lagstiftningen i uppgiftsinförarens land, där en sådan åtkomst i praktiken går längre än vad som är nödvändigt och proportionerligt i ett demokratiskt samhälle[79]. Åtgärderna syftar till att förebygga eventuell inkräktade åtkomst genom att hindra myndigheterna från att identifiera registrerade personer, inhämta uppgifter om dem, skilja ut dem i ett annat sammanhang eller koppla de överförda uppgifterna till andra datauppsättningar, däribland nätidentifierare genom anordningar, program, verktyg och protokoll som används av de registrerade i andra sammanhang.

80. De offentliga myndigheterna i tredjeländer kan försöka komma åt överförda uppgifter vid följande tillfällen:

    a) I samband med överföringen genom att försöka komma åt de kommunikationsvägar som används för att överföra uppgifterna till det mottagande landet. Denna åtkomst kan vara passiv, vilket innebär att det innehåll som överförs helt enkelt kopieras, eventuellt efter en urvalsprocess. Åtkomsten kan emellertid även vara aktiv i den bemärkelsen att de offentliga myndigheterna ingriper i kommunikationsprocessen genom att inte bara läsa innehållet utan även manipulera eller dölja vissa delar.

    b) Medan uppgifterna är i den avsedda mottagarens förvar, antingen genom att försöka komma åt själva behandlingsanläggningen eller genom att kräva att mottagaren lokaliserar och hämtar intressanta uppgifter för att överlämna dem till myndigheterna.

81. I detta avsnitt behandlas scenarier där de tillämpade åtgärderna är effektiva i båda fallen. Olika kompletterande åtgärder kan tillämpas med tillräckliga resultat under vissa omständigheter i samband med en konkret överföring om endast en typ av åtkomst föreskrivs i det mottagande landets lagstiftning. Uppgiftsutföraren måste därför, med stöd av uppgiftsinföraren, noggrant analysera vilka skyldigheter som gäller för den sistnämnda.

Som exempel kan nämnas att uppgiftsinförare i USA som omfattas av USC 50 1881a § (Fisa 702) har en direkt skyldighet att bevilja åtkomst till eller överlämna införda personuppgifter i deras ägo, förvar eller kontroll. Denna skyldighet kan utökas till eventuella krypteringsnycklar som behövs för att göra uppgifterna läsbara.

82. Scenarierna beskriver specifika förhållanden samt vidtagna åtgärder som tjänar som exempel. Eventuella ändringar av scenarierna kan ge upphov till olika slutsatser. Scenarierna avser situationer där slutsatsen dragits att det är nödvändigt med kompletterande åtgärder i första hand, dvs. där problematisk lagstiftning i tredjelandet i praktiken tillämpas på överföringen i ärendet.

83. Personuppgiftsansvariga kan behöva vidta några eller alla av de åtgärder som beskrivs här oavsett vilken skyddsnivå som föreskrivs genom de lagar som är tillämpliga för uppgiftsinföraren, eftersom de måste uppfylla kraven i artiklarna 25 och 32 i dataskyddsförordningen under de konkreta omständigheterna vid överföringen. Med andra ord kan uppgiftsutförare vara tvungna

[79] Se artiklarna 47 och 52 i Europeiska unionens stadga om de grundläggande rättigheterna, artikel 23.1 i den allmänna dataskyddsförordningen och EDPB:s rekommendationer 02/2020 om europeiska väsentliga garantier för övervakningsåtgärder av den 10 november 2020.

att genomföra de åtgärder som beskrivs i denna bilaga även om deras uppgiftsinförare omfattas av ett beslut om adekvat skyddsnivå, precis som personuppgiftsansvariga och personuppgiftsbiträden kan vara tvungna att genomföra dem när uppgifter behandlas inom EES.

Användningsfall 1: Datalagring för säkerhetskopiering och andra ändamål som inte kräver åtkomst till uppgifter i klartext

84. En uppgiftsutförare använder en värdtjänstleverantör i ett tredjeland för att lagra personuppgifter, t.ex. för säkerhetskopiering.

Om

1. personuppgifterna behandlas med stark kryptering före överföringen, och uppgiftsinförarens identitet verifieras,
2. krypteringsalgoritmen och dess sättning av parametrar (t.ex. nyckellängd, driftläge, i tillämpliga fall) uppfyller kraven för den senaste tekniska nivån och kan anses vara skyddade mot en kryptoanalys som utförs av de offentliga myndigheterna i det mottagande landet med beaktande av de resurser och den tekniska kapacitet (t.ex. datorkapacitet för uttömmande attacker) som de har tillgång till[80],
3. styrkan i krypteringen och nyckellängd har fastställts med beaktande av den specifika tidsperiod under vilken de krypterade personuppgifternas konfidentialitet måste upprätthållas[81],
4. krypteringsalgoritmen har genomförts på rätt sätt med hjälp av korrekt underhållen programvara utan kända sårbarheter vars överensstämmelse med den valda algoritmens specifikation har verifierats, t.ex. genom certifiering,
5. nycklarna hanteras på ett tillförlitligt sätt (genereras, förvaltas, lagras, i relevanta fall, kopplas till den avsedda mottagarens identitet och upphävs) [82], och

---

[80] För att bedöma styrkan i krypteringsalgoritmerna, hur de uppfyller kraven för den senaste tekniska nivån, och hur de är skyddade mot kryptoanalys över tid kan uppgiftsutförare förlita sig till den tekniska vägledning som ges ut av officiella cybersäkerhetsmyndigheter i EU och dess medlemsstater. Se t.ex. Enisas rapport *What is "state of the art" in IT security?* , 2019, https://www.enisa.europa.eu/news/enisa-news/what-is-state-of-the-art-in-it-security; vägledning från det tyska förbundsorganet för informationssäkerhet i dess tekniska vägledningar i TR-02102-serien och *Algorithms, Key Size and Protocols Report* (2018), H2020-ICT-2014 – Project 645421, D5.4, ECRYPT-CSA, 02/2018" på https://www.ecrypt.eu.org/csa/documents/D5.4-FinalAlgKeySizeProt.pdf.

[81] Krypteringsalgoritmernas skyddande förmåga minskar med tiden i takt med upptäckten av nya kryptanalytiska tekniker, tillkomsten av nya dataparadigmer såsom kvantdatorteknik och den allmänna ökningen av tillgänglig datorkraft, om inte de tillämpade algoritmerna visas vara en teoretiskt säker information. Detta gäller framför allt för offentliga nyckelalgoritmer som är i allmänt bruk när detta skrivs. Uppgiftsutföraren måste därför beakta att offentliga myndigheter kan söka tillgå krypterade uppgifter under de förhållanden som beskrivs i punkt nr 80, samt lagra dem tills de har tillräckliga resurser för dekryptering. Den kompletterande åtgärden kan bara anses effektiv om en sådan dekryptering och efterföljande ytterligare behandling vid denna tid inte längre utgör någon kränkning av registrerade personers rättigheter, t.ex. eftersom uppgifterna inte längre kan användas för att direkt eller indirekt identifiera dem.

[82] NIST Special Publication 800-57, Recommendation for Key Management https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-5/final

6. nycklarna kvarhålls enbart under den personuppgiftsansvariges kontroll, eller av en enhet som anförtrotts av uppgiftsutföraren i EES eller under en jurisdiktion som erbjuder en väsentligen likvärdig skyddsnivå med den som garanteras inom EES,

anser EDPB att den kryptering som utförts utgör en effektiv kompletterande åtgärd.

Användningsfall 2: Överföring av pseudonymiserade uppgifter

85. En uppgiftsutförare pseudonymiserar först alla uppgifter och överför dem därefter till ett tredjeland för analys, t.ex. för forskningsändamål.

Om

1. en uppgiftsutförare överför personuppgifter som har behandlats på ett sådant sätt att personuppgifterna inte längre kan tillskrivas en viss registrerad person eller användas för att skilja ut den registrerade från en större grupp utan användning av ytterligare uppgifter[83],
2. de ytterligare uppgifterna innehas enbart av uppgiftsutföraren och förvaras separat i en medlemsstat eller i ett tredjeland, av en enhet som anförtrotts av uppgiftsutföraren i EES eller under en jurisdiktion som erbjuder en väsentligen likvärdig skyddsnivå med den som garanteras inom EES,
3. utlämning eller otillåten användning av dessa ytterligare uppgifter förhindras med lämpliga tekniska och organisatoriska skyddsåtgärder som säkerställer att uppgiftsutföraren behåller egen kontroll över den algoritm eller datakatalog som möjliggör en ny identifiering med användning av de ytterligare uppgifterna, och
4. den personuppgiftsansvarige genom en noggrann analys av uppgifterna i ärendet, och med beaktande av alla uppgifter som de offentliga myndigheterna i det mottagande landet kan förväntas ha tillgång till och använda, har fastställt att de pseudonymiserade personuppgifterna inte kan tillskrivas en identifierad eller identifierbar fysisk person även om korshänvisningar görs till sådana uppgifter,

anser EDPB att den pseudonymisering som utförts utgör en effektiv kompletterande åtgärd.

86. Observera att faktorer som är specifika för en fysisk persons fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet, såväl som personens fysiska hemvist eller samverkan med en internetbaserad tjänst vid särskilda tidpunkter[84], i många situationer kan

[83] I linje med artikel 4.5 i den allmänna dataskyddsförordningen: ”pseudonymisering: behandling av personuppgifter på ett sätt som innebär att personuppgifterna inte längre kan tillskrivas en specifik registrerad utan att kompletterande uppgifter används, under förutsättning att dessa kompletterande uppgifter förvaras separat och är föremål för tekniska och organisatoriska åtgärder som säkerställer att personuppgifterna inte tillskrivs en identifierad eller identifierbar fysisk person”. Ytterligare uppgifter kan bestå av tabeller som kombinerar pseudonymer med de beskrivande attribut som de ersätter, krypteringsnycklar eller andra parametrar för omvandling av attribut, eller andra uppgifter som gör att de pseudonymiserade uppgifterna kan tillskrivas identifierade eller identifierbara fysiska personer.

[84] Artikel 4.1 i den allmänna dataskyddsförordningen: ”personuppgifter: varje upplysning som avser en identifierad eller identifierbar fysisk person (nedan kallad en registrerad), varvid en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett

möjliggöra en identifiering av den berörda personen även om namn, adress eller andra identitetsbeteckningar har utelämnats.

87. Detta gäller särskilt i de fall då uppgifterna avser användningen av informationstjänster (tidpunkt för åtkomsten, ordningsföljd för de funktioner som använts, egenskaperna hos den anordning som använts etc.). Dessa tjänster kan mycket väl, precis som uppgiftsinföraren, omfattas av skyldigheten att bevilja åtkomst till samma offentliga myndigheter inom deras jurisdiktion, vilka i sådana fall sannolikt kommer att ha tillgång till uppgifter om den berörda personens användning av dessa informationstjänster.

88. Med tanke på att användningen av vissa informationstjänster är offentlig i sig, eller kan utnyttjas av aktörer med betydande resurser, måste personuppgiftsansvariga dessutom vara extra försiktiga, eftersom de offentliga myndigheterna inom deras jurisdiktion sannolikt har tillgång till uppgifter om den berörda personens användning av dessa informationstjänster.

89. Om en krypteringsalgoritm används för att omvandla attribut som ingår i personuppgifterna under utförandet av pseudonymiseringen gäller vägledningen i fotnoterna 80 och 81. Fortsättningsvis rekommenderas det att man avstår från att enbart använda kryptografi, och tillämpar omvandlingar som bygger på mekanismer för referenstabeller.

Användningsfall 3: Kryptering av uppgifter för att skydda dem från offentliga myndigheters åtkomst i uppgiftsinförarens tredjeland när de övergår mellan uppgiftsutföraren och dennes uppgiftsinförare

90. En uppgiftsutförare vill överföra uppgifter till en plats där lagstiftning och/eller praxis medger offentliga myndigheters åtkomst till uppgifter medan de övergår mellan uppgiftsutförarens land och det mottagande landet.

Om

1. en uppgiftsutförare överför personuppgifter till en uppgiftsinförare i en jurisdiktion där lagstiftning och/eller praxis medför att de offentliga myndigheterna tillåts komma åt uppgifter medan de transporteras via internet till detta tredjeland utan europeiska väsentliga garantier om denna åtkomst; transportkryptering används som tillser att de tillämpade krypteringsprotokollen är på senaste tekniska nivå och ger effektivt skydd mot aktiva och passiva angrepp med resurser som är kända för att vara tillgängliga för de offentliga myndigheterna i detta tredjeland,
2. de parter som deltar i kommunikationen kommer överens om en pålitlig myndighet eller infrastruktur för certifiering av öppna nycklar,
3. specifikt skydd och åtgärder på senaste tekniska nivå används mot aktiva och passiva angrepp mot system för sändning och mottagande som tillhandahåller transportkryptering, inräknat tester av programsårbarheter och möjliga bakdörrar,
4. personuppgifterna även krypteras genomgående i applikationsskiktet med krypteringsmetoder som uppfyller kraven för den senaste tekniska nivån, på grund av att

identifikationsnummer, en lokaliseringsuppgift eller onlineidentifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet".

transportkrypteringen i sig inte uppnår en lämplig skyddsnivå till följd av sårbarheter i den infrastruktur eller programvara som används,

5. krypteringsalgoritmen och dess sättning av parametrar (t.ex. nyckellängd, driftläge, i tillämpliga fall) uppfyller kraven för den senaste tekniska nivån och kan anses vara skyddade mot en kryptoanalys som utförs av de offentliga myndigheterna när uppgifter överförs till detta tredjeland med beaktande av de resurser och den tekniska kapacitet (t.ex. datorkapacitet för uttömmande attacker) som de har tillgång till (se fotnot 80 ovan), [85]
6. styrkan i krypteringen har fastställts med beaktande av den specifika tidsperiod under vilken de krypterade personuppgifternas konfidentialitet måste upprätthållas,
7. krypteringsalgoritmen har genomförts på rätt sätt med hjälp av korrekt underhållen programvara utan kända sårbarheter vars överensstämmelse med den valda algoritmens specifikation har verifierats, t.ex. genom certifiering,
8. nycklarna hanteras på ett tillförlitligt sätt (genereras, förvaltas, lagras och, i relevanta fall, kopplas till den avsedda mottagarens identitet och upphävs) av uppgiftsutföraren eller en aktör som anförtrotts av uppgiftsutföraren inom en jurisdiktion som erbjuder en väsentligen likvärdig skyddsnivå,

anser EDPB att transportkryptering, vid behov i kombination med genomgående kryptering av innehållet, utgör en effektiv kompletterande åtgärd.

Användningsfall 4: Skyddad mottagare

91. En uppgiftsutförare överför personuppgifter till en uppgiftsinförare i ett tredjeland med särskilt skydd av det landets lagstiftning, t.ex. för att gemensamt tillhandahålla medicinsk behandling till en patient eller juridiska tjänster till en klient.

Om

1. lagstiftningen i ett tredjeland ger en uppgiftsinförare som är bosatt i landet undantag för potentiellt inkräktande åtkomst till uppgifter som innehas av mottagaren för det avsedda syftet, t.ex. om uppgiftsinföraren omfattas av tystnadsplikt,
2. undantaget omfattar alla uppgifter i uppgiftsinförarens ägo som kan användas för att kringgå skyddet av konfidentiell information (krypteringsnycklar, lösenord, andra behörighetsuppgifter etc.),
3. uppgiftsinföraren inte har anlitat ett personuppgiftsbiträde på ett sätt som gör det möjligt för de offentliga myndigheterna att komma åt uppgifterna medan de innehas av personuppgiftsbiträdet, och om uppgiftsinföraren inte vidarebefordrar uppgifterna till en annan enhet som inte är skyddad, på grundval av överföringsverktygen i artikel 46 i den allmänna dataskyddsförordningen,
4. personuppgifterna krypteras innan de överförs med en metod som uppfyller kraven för den senaste tekniska nivån och som garanterar att dekryptering inte är möjlig utan kännedom om dekrypteringsnyckeln (genomgående kryptering) under hela den tid då uppgifterna måste skyddas,
5. dekrypteringsnyckeln innehas endast av den skyddade uppgiftsinföraren, och, möjligen, uppgiftsutföraren själv eller en annan enhet som anförtrotts av uppgiftsutföraren som finns i

[85] Se fotnot 80 avseende vissa hänvisningar till teknisk vägledning som ges ut av officiella cybersäkerhetsmyndigheter i EU och dess medlemsstater.

EES eller en jurisdiktion som erbjuder en väsentligen likvärdig skyddsnivå med den som garanteras inom EES, och skyddas på lämpligt sätt mot otillåten användning eller utlämning genom tekniska och organisatoriska åtgärder som uppfyller kraven för den senaste tekniska nivån, och

6. uppgiftsutföraren har fastställt på ett tillförlitligt sätt att den krypteringsnyckel som han eller hon har för avsikt att använda motsvarar den dekrypteringsnyckel som innehas av mottagaren,

anser EDPB att den transportkryptering som utförts utgör en effektiv kompletterande åtgärd.

Användningsfall 5: Delad behandling eller behandling av flera aktörer

92. Uppgiftsutföraren vill att personuppgifterna ska behandlas gemensamt av två eller fler oberoende personuppgiftsbiträden i olika jurisdiktioner utan att lämna ut uppgifternas innehåll till dem. Före överföringen delas uppgifterna upp så att ingen del som tas emot av ett enskilt personuppgiftsbiträde räcker för att rekonstruera personuppgifterna helt eller delvis. Uppgiftsutföraren tar emot resultatet av behandlingen oberoende från vart och ett av personuppgiftsbiträdena och sammanställer de olika delarna till ett slutgiltigt resultat som kan utgöra personliga eller aggregerade uppgifter.

Om

1. en uppgiftsutförare behandlar personuppgifter på ett sådant sätt att de delas upp i två eller fler delar som var för sig inte längre kan tolkas eller tillskrivas en viss registrerad person utan användning av ytterligare uppgifter,
2. var och en av delarna överförs till enskilda personuppgiftsbiträden i olika jurisdiktioner,
3. personuppgiftsbiträdena har möjlighet att behandla uppgifterna gemensamt, t.ex. med användning av säker databehandling på ett sätt som gör att de inte kan ta del av några uppgifter som de inte hade tillgång till före behandlingen,
4. den algoritm som används vid den gemensamma behandlingen är skyddad mot aktiva angrepp,
5. den personuppgiftsansvarige genom en noggrann analys av uppgifterna i ärendet, och med beaktande av ofullständig information som de offentliga myndigheterna i de mottagande länderna kan förväntas ha tillgång till och använda, har fastställt att de personuppgifter som överförs till personuppgiftsbiträdena inte kan tillskrivas en identifierad eller identifierbar fysisk person även om korshänvisningar görs till sådana uppgifter,
6. det inte finns några belägg för ett samarbete mellan de offentliga myndigheterna i personuppgiftsbiträdenas respektive jurisdiktion som hade gett dem tillgång till alla uppsättningar av personuppgifter som innehas av personuppgiftsbiträdena och gett dem möjlighet att återskapa och utnyttja personuppgifternas innehåll i en tydligt läsbar form under omständigheter där ett sådant utnyttjande inte hade varit förenligt med de registrerades grundläggande rättigheter och friheter, och om de offentliga myndigheterna i de olika länderna inte har befogenhet att komma åt personuppgifter som innehas av personuppgiftsbiträden i alla de berörda jurisdiktionerna,

anser EDPB att den delade behandling som utförts utgör en effektiv kompletterande åtgärd.

Exempel på scenarier med ärenden där *effektiva* åtgärder inte identifieras

93. De åtgärder som beskrivs nedan under vissa scenarier skulle inte vara effektiva för att säkerställa en väsentligen likvärdig skyddsnivå för de uppgifter som överförs till tredjelandet. De skulle därför inte betraktas som lämpliga kompletterande åtgärder.

Användningsfall 6: Överföring till leverantörer av molntjänster eller andra personuppgiftsbiträden som behöver komma åt uppgifter i klartext

94. En uppgiftsutförare överför personuppgifter, antingen elektroniskt eller genom att göra uppgifterna tillgängliga för en leverantör av en molntjänst eller ett annat personuppgiftsbiträde för att få personuppgifterna behandlade enligt sina anvisningar i ett tredjeland (t.ex. för att ge tekniskt stöd eller någon annan typ av molnbehandling), och dessa uppgifter pseudonymiseras inte – eller kan inte pseudonymiseras – såsom beskrivs i användningsfall 2, eller krypteras såsom beskrivs i användningsfall 1, eftersom behandlingen kräver att uppgifterna tillgås i klartext,

Om

1. en personuppgiftsansvarig överför personuppgifter till en leverantör av en molntjänst eller ett annat personuppgiftsbiträde,
2. leverantören av molntjänsten eller personuppgiftsbiträdet behöver komma åt uppgifterna i klartext för att kunna utföra de avtalade uppgifterna, och
3. den befogenhet som tilldelats offentliga myndigheter i det mottagande landet för att tillgå de överförda uppgifterna i ärendet går längre än vad som är nödvändigt och proportionerligt i ett demokratiskt samhälle, där problematisk lagstiftning i tredjelandet i praktiken tillämpas på överföringen i ärendet (se steg 3),[86]

kan EDPB, med tanke på den rådande tekniska nivån, inte föreställa sig en effektiv teknisk åtgärd som skulle förhindra att åtkomsten inkräktar på de registrerades grundläggande rättigheter. EDPB utesluter inte möjligheten att den framtida tekniska utvecklingen kan leda till åtgärder som uppnår de avsedda affärsändamålen utan att parterna behöver komma åt uppgifterna i klartext.

95. I scenarier där okrypterade personuppgifter är tekniskt nödvändiga för att personuppgiftsbiträdet ska kunna tillhandahålla tjänsten utgör transportkryptering och kryptering av data i vila, även om de kombineras, inte någon kompletterande åtgärd som säkerställer en väsentligen likvärdig skyddsnivå om uppgiftsinföraren innehar krypteringsnycklarna.

Användningsfall 7: Överföring av personuppgifter för yrkesändamål, inräknat genom fjärråtkomst

96. En uppgiftsutförare överför personuppgifter till enheter i ett tredjeland för att användas för delade yrkesändamål – antingen elektroniskt eller genom att göra uppgifterna tillgängliga för

[86] Se artiklarna 47 och 52 i Europeiska unionens stadga om de grundläggande rättigheterna, artikel 23.1 i den allmänna dataskyddsförordningen och EDPB:s rekommendationer 02/2020 om europeiska väsentliga garantier för övervakningsåtgärder av den 10 november 2020.

fjärråtkomst av uppgiftsinföraren – och dessa uppgifter pseudonymiseras inte – eller kan inte pseudonymiseras – såsom beskrivs i användarfall 2, eller krypteras såsom beskrivs i användarfall 1, eftersom behandlingen kräver att uppgifterna tillgås i klartext. En typisk konstellation kan bestå av en personuppgiftsansvarig eller ett personuppgiftsbiträde i en medlemsstat som överför personuppgifter till en personuppgiftsansvarig eller ett personuppgiftsbiträde i ett tredjeland som tillhör samma företagsgrupp eller koncern och som deltar i en gemensam ekonomisk verksamhet. Uppgiftsinföraren kan till exempel använda de mottagna uppgifterna för att tillhandahålla personaluppgifter till uppgiftsutföraren eller för att kommunicera med uppgiftsutförarens kunder som är bosatta i Europeiska unionen via telefon eller e-post.

Om

1. en uppgiftsutförare överför personuppgifter till en uppgiftsinförare i ett tredjeland genom att göra uppgifterna tillgängliga i ett informationssystem på ett sätt som gör att uppgiftsinföraren kan komma åt uppgifterna direkt, eller genom att överföra dem direkt, enskilt eller i bulk, med användning av en kommunikationstjänst,
2. uppgiftsinföraren[87] behandlar uppgifterna i klartext i tredjelandet (även för egna syften om uppgiftsinföraren är en personuppgiftsansvarig),
3. den befogenhet som tilldelats offentliga myndigheter i det mottagande landet för att tillgå de överförda uppgifterna går längre än vad som är nödvändigt och proportionerligt i ett demokratiskt samhälle, där problematisk lagstiftning i tredjelandet i praktiken tillämpas på överföringen i ärendet (se steg 3),

kan EDPB inte föreställa sig en effektiv teknisk åtgärd som skulle förhindra att åtkomsten inkräktar på den registrerades grundläggande rättigheter.

97. I scenarier där okrypterade personuppgifter är tekniskt nödvändiga för att personuppgiftsbiträdet ska kunna tillhandahålla tjänsten utgör transportkryptering och kryptering av data i vila, även om de kombineras, inte någon kompletterande åtgärd som säkerställer en väsentligen likvärdig skyddsnivå om uppgiftsinföraren innehar krypteringsnycklarna.

[87] Huruvida det är en personuppgiftsansvarig eller ett personuppgiftsbiträde i ett tredjeland som tar emot eller ges åtkomst till personuppgifter som överförts från EES.

2.2 Ytterligare avtalsrättsliga åtgärder

98. Dessa åtgärder består i allmänhet av unilaterala, bilaterala eller multilaterala[88] avtalsrättsliga åtaganden.[89] Om ett överföringsverktyg enligt artikel 46 i den allmänna dataskyddsförordningen används omfattar det i de flesta fall redan ett antal åtaganden (i första hand avtalsrättsliga) av uppgiftsutföraren och uppgiftsinföraren som ska fungera som skyddsåtgärder för personuppgifterna.[90]

99. I vissa situationer kan dessa åtgärder komplettera och förstärka de skyddsåtgärder som ingår i överföringsverktyget och den relevanta lagstiftningen i tredjelandet om dessa, med hänsyn till omständigheterna för överföringen, inte uppfyller alla villkor som krävs för att säkerställa en skyddsnivå som är väsentligen likvärdig med den som garanteras inom EES. På grund av de avtalsrättsliga åtgärdernas karaktär, som gör att de i regel inte kan vara bindande för myndigheterna i tredjelandet om de inte är parter i avtalet[91], kan dessa åtgärder ofta behöva kombineras med andra tekniska och organisatoriska åtgärder för att tillhandahålla den nivå av dataskydd som krävs. Om du väljer och genomför en eller flera av dessa åtgärder säkerställer du inte nödvändigtvis och systematiskt att dina överföringar uppfyller den väsentligen likvärdiga standard som krävs enligt unionsrätten.

100. Beroende på vilka avtalsrättsliga åtgärder som redan ingår i det verktyg som används enligt artikel 46 i den allmänna dataskyddsförordningen kan ytterligare avtalsrättsliga åtgärder också vara till hjälp för att EES-baserade uppgiftsutförare ska kunna få reda på nya utvecklingstrender som påverkar skyddet av de uppgifter som överförs till tredjeländer.

101. Som tidigare nämnts kommer avtalsrättsliga åtgärder inte att kunna utesluta tillämpningen av lagstiftningen i ett tredjeland som inte uppfyller EDPB:s standard för europeiska väsentliga garantier i de fall då uppgiftsinförare enligt lagstiftningen är skyldiga att på begäran lämna ut uppgifter till offentliga myndigheter.[92]

102. Här nedan följer några exempel på dessa möjliga avtalsrättsliga åtgärder indelade efter deras karaktär.

Uppfyllande av avtalsförpliktelsen att använda särskilda tekniska åtgärder

103. Beroende på överföringarnas särskilda omständigheter (inräknat den praktiska tillämpningen av tredjelandets lagstiftning) kan avtalet behöva innehålla föreskrifter om att särskilda tekniska åtgärder måste vidtas för att överföringarna ska kunna genomföras (se de tekniska åtgärder som föreslås ovan).

---

[88] T.ex. inom ramen för bindande företagsbestämmelser som under alla omständigheter hade reglerat några av de åtgärder som förtecknas nedan.

[89] De kommer att ha en privat karaktär och kommer inte att betraktas som internationella avtal enligt offentlig internationell rätt. Följaktligen kommer de i normala fall inte att vara bindande för tredjelandets offentliga myndigheter eftersom dessa inte är parter i avtalet om det ingås med privata organ i tredjeländer, vilket domstolen underströk i sin dom i mål C-311/18 (Schrems II), punkt 125.

[90] Se domen i mål C-311/18 (Schrems II), punkt 137, där domstolen konstaterade att standardavtalsklausulen innehåller ”effektiva mekanismer som i praktiken gör det möjligt att säkerställa att den skyddsnivå som krävs enligt unionsrätten iakttas och att överföringar av personuppgifter med stöd av sådana dataskyddsbestämmelser avbryts eller förbjuds om dessa bestämmelser åsidosätts eller är omöjliga att iaktta”. Se även punkt 148).

[91] C-311/18 (Schrems II), punkt 125.

[92] EU-domstolens dom i mål C-311/18 (Schrems II), punkt 132.

104. Villkor för effektivitet:

- Denna klausul kan vara effektiv i de situationer där behovet av tekniska åtgärder har identifierats av uppgiftsutföraren. I sådana fall måste detta föreskrivas i en rättslig form för att säkerställa att uppgiftsinföraren också åtar sig att införa nödvändiga tekniska åtgärder vid behov.

Skyldighet att säkerställa öppenhet

105. Uppgiftsutföraren kan lägga till bilagor till avtalet med information som uppgiftsinföraren, efter bästa förmåga, skulle ha tillhandahållit innan avtalet ingicks, om offentliga myndigheters åtkomst till uppgifterna, däribland inom underrättelseområdet, under förutsättning att lagstiftningen uppfyller EDPB:s europeiska väsentliga garantier i det mottagande landet. Detta kan hjälpa uppgiftsutföraren att uppfylla sin skyldighet att dokumentera bedömningen av skyddsnivån i tredjelandet. Den kan även betona uppgiftsinförarens skyldighet att bistå uppgiftsutföraren i sin bedömning och ådra sig ansvar att ge information som är objektiv, tillförlitlig, relevant, verifierbar och offentligt tillgänglig eller på annat sätt åtkomlig information

106. Det skulle till exempel kunna finnas krav på att uppgiftsinföraren ska

(1) ange vilka lagar och förordningar i det mottagande landet som är tillämpliga för uppgiftsinföraren eller dennes personuppgiftsbiträden och som ger de offentliga myndigheterna åtkomst till de personuppgifter som ingår i överföringen, särskilt inom de områden för underrättelseverksamhet, brottsbekämpning, administrativ tillsyn och myndighetstillsyn som är tillämpliga för de överförda uppgifterna,

(2) om det inte finns några lagar som reglerar de offentliga myndigheternas åtkomst till uppgifter, tillhandahålla information och statistik baserat på uppgiftsinförarens erfarenheter eller rapporter från olika källor (t.ex. partner, öppna källor, nationell rättspraxis och beslut av tillsynsorgan) om offentliga myndigheters åtkomst till personuppgifter i situationer som motsvarar den aktuella överföringen (dvs. inom det specifika regleringsområdet för den typ av enhet som uppgiftsinföraren tillhör…),

(3) ange vilka åtgärder som har vidtagits för att förhindra åtkomst till överförda uppgifter (i förekommande fall),

(4) ge tillräckligt detaljerad information om alla begäranden från offentliga myndigheter om åtkomst till personuppgifter som uppgiftsinföraren har tagit emot under en viss tidsperiod,[93] i synnerhet inom de områden som avses i punkt 1 ovan, däribland information om vilka begäranden som tagits emot, vilka uppgifter som har begärts, vilket organ som har begärt uppgifterna, den rättsliga grunden för utlämningen samt i vilken utsträckning uppgiftsinföraren har lämnat ut de begärda uppgifterna,[94]

[93] Tidsperiodens längd bör anpassas till riskerna avseende rättigheterna och friheterna för de registrerade personer vars uppgifter omfattas av den aktuella överföringen – t.ex. det senaste året innan överföringsinstrumentet avslutades med uppgiftsutföraren.

[94] Efterlevnad av denna skyldighet innebär inte i sig att en lämplig skyddsnivå tillhandahålls. Samtidigt leder eventuella olämpliga utlämningar som faktiskt har inträffat till att kompletterande åtgärder måste genomföras.

ange om och i vilken utsträckning uppgiftsinföraren enligt lag är förbjuden att lämna ut de uppgifter som avses i punkterna 1–5 ovan.

107. Denna information kan lämnas med hjälp av strukturerade frågeformulär som uppgiftsinföraren ska fylla i och underteckna i förening med uppgiftsinförarens avtalsenliga skyldighet att inom en fastställd tidsperiod meddela möjliga ändringar av denna information, vilket är gällande praxis för tillbörlig aktsamhet.

108. Villkor för effektivitet:

- Uppgiftsinföraren måste kunna ge uppgiftsutföraren dessa typer av information efter bästa kunskap och efter att ha gjort sitt bästa för att erhålla den.
- Denna skyldighet som åligger uppgiftsinföraren är ett sätt att säkerställa att uppgiftsutföraren blir och förblir medveten om riskerna med överföringen av uppgifter till ett tredjeland. Den kommer således att ge uppgiftsutföraren möjlighet att avstå från att ingå avtalet eller, om informationen ändras efter ingåendet, att fullgöra sin skyldighet att avbryta överföringen och/eller häva avtalet om lagstiftningen i tredjelandet, skyddsåtgärderna i det överföringsverktyg i artikel 46 i den allmänna dataskyddsförordningen som används och eventuella ytterliga skyddsåtgärder som uppgiftsutföraren kan ha vidtagit inte längre säkerställer en skyddsnivå som är väsentligen likvärdig med den som garanteras inom EES. Denna skyldighet kan emellertid varken motivera att uppgiftsinföraren lämnar ut personuppgifter eller skapa en förväntning om det inte kommer fler begäranden om åtkomst.

***

109. Uppgiftsutföraren skulle även kunna lägga till klausuler genom vilka uppgiftsinföraren intygar 1) att han eller hon inte medvetet har skapat bakdörrar eller liknande program som skulle kunna användas för att komma åt systemet och/eller personuppgifterna, 2) att han eller hon inte medvetet har skapat eller ändrat några affärsprocesser på ett sätt som underlättar åtkomsten till personuppgifterna eller systemet och 3) att den nationella lagstiftningen eller den offentliga politiken inte kräver att uppgiftsinföraren skapar eller upprätthåller bakdörrar eller underlättar åtkomsten till personuppgifter eller system eller att uppgiftsinföraren innehar eller lämnar över krypteringsnyckeln.[95]

110. Villkor för effektivitet:

- Om lagstiftningen eller den offentliga politiken hindrar uppgiftsinförare från att lämna ut denna information kan denna klausul bli ineffektiv. Uppgiftsinföraren kommer därmed inte att kunna ingå avtalet eller kommer att behöva meddela uppgiftsutföraren om att han eller hon inte längre kan uppfylla sina åtaganden enligt avtalet.
- Avtalet måste omfatta påföljder och/eller ge uppgiftsutföraren möjlighet att häva avtalet med kort varsel i de fall då uppgiftsinföraren inte uppger att det finns en bakdörr eller liknande program, manipulerade affärsprocesser, eller krav på att genomföra något av dessa alternativ, eller underlåter att omedelbart informera uppgiftsutföraren när förekomsten blir känd.

[95] Denna klausul är viktig för att garantera en adekvat nivå av skydd för de personuppgifter som överförs och bör krävas i vanliga fall.

- Under omständigheter där uppgiftsinföraren har lämnat ut personuppgifter som överförts i strid med de ingående åtagandena enligt det valda överföringsverktyget, kan avtalet även omfatta ersättning från uppgiftsinföraren till en registrerad för all liden ekonomisk och ideell skada.

***

111. Uppgiftsutföraren skulle kunna utöka sin befogenhet att utföra revisioner[96] eller inspektioner av uppgiftsinförarens databehandlingsanläggningar, på plats och/eller på distans, för att kontrollera om uppgifterna lämnats ut till de offentliga myndigheterna och på vilka villkor (åtkomst som inte går längre än vad som är nödvändigt och proportionerligt i ett demokratiskt samhälle), till exempel genom kontroller på kort varsel eller mekanismer som säkerställer ett snabbt ingripande av kontrollorganen och förstärker uppgiftsutförarens självständighet när det gäller att välja kontrollorgan.

112. Villkor för effektivitet:

- För att ha full effekt bör revisionens tillämpningsområde juridiskt och tekniskt sett omfatta all behandling av de personuppgifter som överförts till tredjelandet som utförs av uppgiftsinförarens personuppgiftsbiträden.
- Åtkomstloggar och andra liknande verifieringskedjor ska vara säkra mot förfalskning (de ska t.ex. göras säkra mot ändring med hjälp av de senaste krypteringsteknikerna, såsom hashning, och även systematiskt överföras till uppgiftsutföraren) så att revisorer kan finna belägg på utlämning. Åtkomstloggar och andra liknande verifieringskedjor bör även göra åtskillnad mellan åtkomst på grund av regelmässig affärsverksamhet och åtkomst på grund av order eller begäranden om åtkomst.

***

113. Om lagstiftning och praxis i det tredjeland där uppgiftsinföraren är etablerad ursprungligen ansågs uppfylla en skyddsnivå som var väsentligen likvärdig med den nivå som garanteras i EU för de uppgifter som överförs av uppgiftsutföraren skulle uppgiftsutföraren ändå kunna förstärka uppgiftsinförarens skyldighet att omedelbart, om situationen ändras, informera uppgiftsutföraren om han eller hon inte kan uppfylla de avtalsenliga åtagandena och därmed inte heller den ”väsentligen likvärdiga skyddsnivå” som krävs.[97]

114. Denna oförmåga att uppfylla kraven kan vara ett resultat av förändringar i tredjelandets lagstiftning eller praxis.[98] Klausulerna kan innehålla specifika och strikta tidsfrister och förfaranden

---

[96] Se till exempel klausul 5 f mellan personuppgiftsansvariga och personuppgiftsbiträden i beslut 2010/87/EU om standardavtalsklausuler. Revisionerna skulle även kunna genomföras inom ramen för en uppförandekod eller genom certifiering.

[97] Klausul 5 a och d (i) i beslut 2010/87/EU om standardavtalsklausuler.

[98] Se mål C-311/18 (Schrems II), punkt 139, där domstolen hävdar följande: ”Enligt klausul 5 d punkt i är det tillåtet för mottagaren av en överföring av personuppgifter att underlåta att underrätta den personuppgiftsansvarige som är etablerad i unionen om en bindande begäran från rättsliga myndigheter om utlämnande av personuppgifter, om det föreligger lagstiftning som förhindrar det, såsom ett straffrättsligt förbud som syftar till att skydda sekretess vid brottsutredningar, men vederbörande är emellertid, enligt klausul 5 a i bilagan till beslutet om standardavtalsklausuler, skyldig att informera den personuppgiftsansvarige om att denne inte kan iaktta de standardiserade dataskyddsbestämmelserna.”

för att omedelbart avbryta överföringen av uppgifter och/eller häva avtalet och för att uppgiftsinföraren ska återlämna eller makulera de mottagna uppgifterna. Bevakningen av de begäranden som tagits emot, deras syfte och effektiviteten i de åtgärder som vidtagits för att motverka dem bör ge uppgiftsutföraren tillräckliga indikationer för att kunna utöva sin plikt att avbryta eller avsluta överföringen och/eller häva avtalet.

115. Villkor för effektivitet:

- Underrättelsen måste ske innan åtkomst till uppgifterna kan beviljas. Om begäran grundas på lagstiftning i tredjelandet som överstiger den nivå av dataskydd som unionsrätten medger kan den enskilda personens rättigheter annars redan ha kränkts när uppgiftsutföraren får ta del av underrättelsen. Underrättelsen kan fortfarande förhindra framtida överträdelser och göra det möjligt för uppgiftsutföraren att fullgöra sin plikt att avbryta överföringen av personuppgifter till tredjelandet och/eller häva avtalet.
- Uppgiftsinföraren måste övervaka alla rättsliga och politiska utvecklingar som kan leda till att han eller hon inte kan fullgöra sina skyldigheter och omedelbart informera uppgiftsutföraren om sådana ändringar och utvecklingar, om möjligt innan de genomförs, för att göra det möjligt för uppgiftsutföraren att hämta tillbaka uppgifterna från uppgiftsinföraren.
- Klausulerna bör innehålla föreskrifter om en snabb mekanism som uppgiftsutföraren kan använda för att godkänna att uppgiftsinföraren omedelbart säkrar eller återlämnar uppgifterna till uppgiftsutföraren eller, om detta inte är möjligt, raderar eller krypterar uppgifterna på ett säkert sätt utan att behöva vänta på uppgiftsutförarens anvisningar om ett särskilt tröskelvärde[99] i avtalet mellan uppgiftsutföraren och uppgiftsinföraren har uppfyllts. Uppgiftsinföraren bör genomföra denna mekanism när överföringen av uppgifter påbörjas och prova den regelbundet för att säkerställa att den kan tillämpas på kort varsel.
- Andra klausuler kan göra det möjligt för uppgiftsutföraren att övervaka uppgiftsinförarens efterlevnad av dessa skyldigheter genom revisioner, inspektioner och andra kontrollåtgärder och verkställa dem med påföljder för uppgiftsinföraren och/eller uppgiftsutförarens möjligheter att avbryta överföringen och/eller omedelbart häva avtalet.

***

116. Om lagstiftningen i tredjelandet tillåter det skulle avtalet kunna förstärka uppgiftsinförarens skyldighet att säkerställa öppenhet genom att föreskriva en ”Warrant Canary”-metod, varigenom uppgiftsinföraren åtar sig att regelbundet (t.ex. minst var 24:e timme) offentliggöra ett kryptografiskt undertecknat meddelande för att informera uppgiftsutföraren om att inget föreläggande att lämna ut personuppgifter eller liknande har tagits emot. Om detta meddelande inte uppdateras indikerar det för uppgiftsutföraren att uppgiftsinföraren kan ha tagit emot ett föreläggande.

117. Villkor för effektivitet:

- Föreskrifterna i tredjelandet måste tillåta att uppgiftsinföraren utfärdar denna format passivt meddelande till uppgiftsutföraren.
- Uppgiftsutföraren måste övervaka meddelandena automatiskt.

[99] Detta tröskelvärde ska säkerställa att registrerade personer fortsätter att ha en skyddsnivå som är likvärdig med den nivå som garanteras inom EES.

- Uppgiftsinföraren måste säkerställa att den privata nyckeln för undertecknande av Warrant Canary-meddelanden hålls i säkert förvar och att den inte kan tvingas att utfärda falska meddelanden genom föreskrifterna i tredjelandet. Därför kan det vara lämpligt om flera signaturer av olika personer behövs och/eller att Warrant Canary-meddelandet utfärdas av en person utanför tredjelandets jurisdiktion.

Skyldigheter att vidta särskilda åtgärder

118. Uppgiftsinföraren skulle, enligt lagstiftningen i det mottagande landet, kunna åta sig att granska om ett föreläggande att lämna ut uppgifter är laglig, framför allt om den omfattas av den befogenhet som tilldelats den begärande offentliga myndigheten, och invända mot föreläggandet om han eller hon, efter en ingående bedömning, drar slutsatsen att detta är möjligt enligt lagstiftningen i det mottagande landet. Om uppgiftsinföraren invänder mot ett föreläggande bör han eller hon vidta provisoriska åtgärder för att skjuta upp föreläggandets verkan tills domstolen har prövat sakfrågan. Uppgiftsinföraren är i sådana fall skyldig att inte lämna ut de begärda personuppgifterna förrän detta krävs enligt de tillämpliga förfarandereglerna. Uppgiftsinföraren skulle även åta sig att endast lämna ut den minsta föreskrivna mängden av uppgifter vid ett föreläggande, baserat på en rimlig tolkning av föreläggandet.

119. Villkor för effektivitet:

- Tredjelandets rättsordning måste erbjuda effektiva rättsliga möjligheter att invända mot förelägganden att lämna ut uppgifter.
- Denna klausul kommer alltid att erbjuda ett mycket begränsat extra skydd, eftersom ett föreläggande att lämna ut uppgifter kan vara lagligt enligt tredjelandets rättsordning även om denna rättsordning inte uppfyller EU:s normer. Denna avtalsrättsliga åtgärd kan endast vara ett komplement till andra kompletterande åtgärder.
- Invändningarna mot föreläggandena måste ha en uppskjutande verkan enligt tredjelandets lagstiftning, annars kommer de offentliga myndigheterna ändå att ha tillgång till de enskilda personernas uppgifter. En åtgärd till förmån för en enskild person skulle därmed endast ha den begränsade effekten att ge den berörda personen möjlighet att kräva skadestånd för de negativa konsekvenserna av utlämningen av uppgifter.
- Uppgiftsinföraren måste kunna dokumentera och visa för uppgiftsutföraren vilka åtgärder som har vidtagits för att uppfylla detta åtagande.

***

120. I samma situation som beskrivs ovan skulle uppgiftsinföraren kunna åta sig att informera den begärande offentliga myndigheten om att föreläggandet inte är förenligt med de skyddsåtgärder som ingår överföringsverktyget i artikel 46 i den allmänna dataskyddsförordningen[100] och att

[100] Exempelvis föreskrivs i standardavtalsklausulerna att behandlingen av uppgifter, däribland överföringen, ska utföras och fortsätta att utföras i enlighet med ”den tillämpliga dataskyddslagstiftningen”. Denna lagstiftning definieras som ”sådan lagstiftning som avser att skydda personers grundläggande fri- och rättigheter, särskilt deras personliga integritet i samband med behandling av personuppgifter, och som är tillämplig på

detta strider mot uppgiftsinförarens skyldigheter. Uppgiftsinföraren skulle samtidigt och så fort som möjligt meddela uppgiftsutföraren och/eller den behöriga tillsynsmyndigheten inom EES om detta är möjligt enligt tredjelandets rättsordning.

121. Villkor för effektivitet:

- Sådan information om det skydd som följer av unionsrätten och skyldigheternas motstridighet bör ha viss rättslig verkan i tredjelandets rättsordning, till exempel en rättslig eller administrativ granskning av föreläggandet eller begäran om åtkomst, ett krav på ett domstolsbeslut och/eller ett tillfälligt upphävande av föreläggandet för att ge uppgifterna ett visst skydd.
- Landets rättsliga system får inte hindra uppgiftsinföraren från att meddela uppgiftsutföraren eller åtminstone den behöriga tillsynsmyndigheten inom EES om det föreläggande eller den begäran som tagits emot.
- Uppgiftsinföraren måste kunna dokumentera och visa för uppgiftsutföraren vilka åtgärder som har vidtagits för att uppfylla detta åtagande.

Möjligheter för registrerade personer att utöva sina rättigheter

122. Avtalet skulle kunna innehålla föreskrifter om att personuppgifter som överförs i klartext vid normal verksamhet (däribland i stödärenden) endast får göras tillgängliga efter uttryckligt eller underförstått avtal av uppgiftsutföraren och/eller den registrerade personen om en särskild åtkomst till uppgifter.

123. Villkor för effektivitet:

- Denna klausul skulle kunna vara effektiv i situationer där uppgiftsinföraren får en begäran av de offentliga myndigheterna att samarbeta på frivillig grund istället för att de offentliga myndigheterna har åtkomst till uppgifter utan uppgiftsinförarens vetskap eller mot dennes vilja.
- I vissa situationer kan det hända att den registrerade personen inte kan motsätta sig åtkomsten eller ge ett samtycke som uppfyller alla villkor som fastställs i unionsrätten (frivillig, specifik, informerad och otvetydig) (t.ex. när det gäller anställda)[101].
- Nationella föreskrifter eller riktlinjer som tvingar uppgiftsinföraren att inte lämna ut föreläggandet om åtkomst kan göra att denna klausul blir ineffektiv om den inte stöds av tekniska metoder som kräver ett ingripande av uppgiftsutföraren eller den registrerade för att uppgifterna ska finnas tillgängliga i klartext. Sådana tekniska åtgärder för att begränsa åtkomsten bör främst övervägas om åtkomst endast beviljas i särskilda stöd- eller tjänsteärenden, men där uppgifterna i sig lagras inom EES.

***

registeransvariga i den medlemsstat där uppgiftsutföraren är etablerad". EU-domstolen bekräftar att bestämmelserna i den allmänna dataskyddsförordningen, tolkade mot bakgrund av EU-stadgan om de grundläggande rättigheterna, utgör en del av denna lagstiftning, se EU-domstolens dom i mål C-311/18 (Schrems II), punkt 138.

[101] Artikel 4.11 i den allmänna dataskyddsförordningen.

124. Avtalet skulle kunna omfatta en skyldighet för uppgiftsinföraren och/eller uppgiftsutföraren att omedelbart underrätta den registrerade personen om att en begäran eller ett föreläggande inkommit från de offentliga myndigheterna i tredjelandet, eller om uppgiftsinföraren inte kan fullgöra sina avtalsrättsliga skyldigheter, så att den registrerade kan söka information och få en effektiv domstolsprövning (t.ex. genom att anmäla ärendet till sin behöriga tillsynsmyndighet och/eller rättsliga myndighet och uppvisa sin ställning i tredjelandets domstolar), inräknat ersättning från uppgiftsinföraren för all liden ekonomisk och ideell skada på grund av utlämnandet av hans/hennes personuppgifter som överförts enligt det valda överföringsverktyget i strid med de åtaganden det innehåller.

125. Villkor för effektivitet:

- Denna underrättelse skulle kunna varna den registrerade om de offentliga myndigheterna i tredjelandet försöker komma åt hans/hennes uppgifter. Den registrerade skulle därmed få möjlighet att söka ytterligare information av uppgiftsutföraren och anmäla ärendet till sin behöriga tillsynsmyndighet. Denna klausul skulle även kunna avhjälpa och kompensera några av den enskilda personens svårigheter att uppvisa sin ställning (talerätt) inför en domstol i tredjelandet för att kunna motsätta sig de offentliga myndigheternas åtkomst till hans/hennes uppgifter.
- Nationella föreskrifter och riktlinjer kan förhindra att denna underrättelse lämnas till den registrerade. Uppgiftsutföraren och uppgiftsinföraren skulle trots detta kunna åta sig att informera den registrerade så fort restriktionerna avseende utlämning av uppgifter hävs och göra sitt bästa för att få undantag från förbudet att lämna ut uppgifter. Uppgiftsutföraren eller den behöriga tillsynsmyndigheten skulle åtminstone kunna underrätta den registrerade om det tillfälliga eller slutgiltiga upphörandet av överföringen av hans/hennes personuppgifter på grund av uppgiftsinförarens oförmåga att fullgöra sina avtalsrättsliga åtaganden till följd av mottagandet av en begäran om åtkomst.

***

126. Avtalet skulle kunna omfatta en skyldighet för uppgiftsutföraren och uppgiftsinföraren att hjälpa den registrerade att utöva sina rättigheter inom tredjelandets jurisdiktion genom särskilda prövningsmekanismer och juridisk rådgivning.

127. Villkor för effektivitet

- Vissa nationella föreskrifter kan förbjuda att uppgiftsinföraren ger denna typ av bistånd direkt till registrerade personer, även om de kan tillåta att uppgiftsinföraren upphandlar detta bistånd åt de registrerade.
- Nationella föreskrifter och riktlinjer kan innehålla villkor som undergräver effektiviteten hos de särskilda prövningsmekanismer som föreskrivs.
- Juridisk rådgivning skulle kunna hjälpa den registrerade, särskilt med tanke på hur komplicerat och dyrt det kan vara för en registrerad person att förstå ett tredjelands rättsliga system och vidta rättsliga åtgärder från ett annat land, i vissa fall i ett annat språk. Denna klausul kommer emellertid alltid att erbjuda ett begränsat skydd, eftersom stöd och juridisk rådgivning till registrerade personer inte i sig kan avhjälpa brister i den rättsliga ordningen som gör att ett tredjeland inte kan säkerställa en skyddsnivå som är väsentligen likvärdig med den som

garanteras inom EES. Denna avtalsrättsliga åtgärd kan endast vara ett komplement till andra kompletterande åtgärder.

- Denna kompletterande åtgärd skulle endast vara effektiv om lagstiftningen i tredjelandet ger möjlighet till prövning i de nationella domstolarna eller om det finns en särskild prövningsmekanism, även mot övervakningsåtgärder.

2.3 Organisatoriska åtgärder

128. Ytterligare organisatoriska åtgärder kan bestå av interna regler, organisatoriska metoder och standarder som personuppgiftsansvariga och personuppgiftsbiträden skulle kunna tillämpa på sig själva och ålägga uppgiftsinförare i tredjeländer. De kan bidra till att säkerställa ett enhetligt skydd av personuppgifterna under hela behandlingscykeln. Organisatoriska åtgärder kan även öka uppgiftsutförarnas medvetenhet om riskerna med försök att komma åt uppgifterna i tredjeländer och öka deras förmåga att bekämpa dem. Om du väljer och genomför en eller flera av dessa åtgärder säkerställer du inte nödvändigtvis och systematiskt att dina överföringar uppfyller den väsentligen likvärdiga standard som krävs enligt unionsrätten. Beroende på de särskilda omständigheterna kring överföringen och den bedömning av tredjelandets lagstiftning som utförts kan organisatoriska åtgärder vara nödvändiga som komplement till avtalsrättsliga och/eller tekniska åtgärder för att säkerställa att personuppgifterna har en nivå av skydd som är väsentligen likvärdig med den som garanteras inom EES.

129. Vilka åtgärder som är lämpligast måste bedömas från fall till fall eftersom de personuppgiftsansvariga och personuppgiftsbiträdena måste följa principen om ansvarsskyldighet. I nedanstående förteckning ger EDPB några exempel på organisatoriska åtgärder som uppgiftsutförare kan genomföra. Förteckningen är inte uttömmande och andra åtgärder kan också vara lämpliga.

Interna regler för styrning av överföringar mellan grupper av företag

130. Antagande av adekvata interna regler med tydlig ansvarsfördelning för överföringar av uppgifter, rapporteringskanaler och standardiserade operativa förfaranden i de fall då offentliga myndigheter lämnar in formella eller informella begäranden om att komma åt uppgifterna. När det gäller överföringar bland grupper av företag kan dessa regler bland annat omfatta utnämningen av en särskild grupp, bestående av experter inom it, dataskydd och integritetslagstiftning, för att hantera begäranden som inbegriper personuppgifter som överförts från EES, underrättelser till företagsledningen och uppgiftsutföraren vid mottagande av sådana begäranden, förfarandet för att invända mot oproportionerliga eller olagliga begäranden samt tillhandahållandet av öppen information till registrerade personer.

131. Utarbetande av särskilda utbildningsförfaranden för personal som är ansvarig för hanteringen av begäranden om åtkomst till personuppgifter från offentliga myndigheter, vilka bör uppdateras regelbundet för att återspegla nya utvecklingar inom lagstiftning och rättspraxis i tredjelandet och EES. Utbildningen bör omfatta kraven i unionsrätten när det gäller offentliga myndigheters åtkomst till personuppgifter, i synnerhet de krav som följer av artikel 52.1 i stadgan om de grundläggande rättigheterna. Personalens medvetenhet bör främst stärkas genom bedömning av praktiska exempel på offentliga myndigheters begäranden om åtkomst till uppgifter och genom tillämpning av den standard som följer av artikel 52.1 i stadgan om de grundläggande rättigheterna för sådana praktiska exempel. Utbildningen bör säkerställa att hänsyn tas till uppgiftsinförarens situation, t.ex. de lagar och förordningar i tredjelandet som uppgiftsinföraren omfattas av, och om möjligt utarbetas i samarbete med uppgiftsutföraren.

132. Villkor för effektivitet:

- Dessa regler kan endast övervägas för de fall där begäran från de offentliga myndigheterna i tredjelandet är förenlig med unionsrätten.[102] Om begäran inte är förenlig med unionsrätten är dessa regler inte tillräckliga för att säkerställa en likvärdig skyddsnivå för personaluppgifterna. Som nämns ovan måste överföringarna avbrytas eller lämpliga kompletterande åtgärder införas för att förhindra åtkomsten.

Åtgärder för öppenhet och ansvarsskyldighet

133. Dokumentera och registrera de begäranden om åtkomst som tagits emot från offentliga myndigheter och de svar som lämnats, tillsammans med det rättsliga resonemanget och de medverkande aktörerna (t.ex. om uppgiftsutföraren har underrättats och dennes svar, bedömningen av den grupp som har ansvar för att hantera sådana begäranden etc.). Dessa register bör finnas tillgängliga för uppgiftsutföraren, som i sin tur bör överlämna dem till de berörda registrerade personerna.

134. Villkor för effektivitet:

- Den nationella lagstiftningen i tredjelandet kan förhindra att begärandena eller viktig information om dem lämnas ut och därmed göra denna metod ineffektiv. Uppgiftsinföraren bör informera uppgiftsutföraren om han eller hon inte kan tillhandahålla sådana dokument och register och därmed ge uppgiftsutföraren möjlighet att avbryta överföringarna om detta skulle leda till en underlåtenhet att tillhandahålla en adekvat skyddsnivå.

***

135. Regelbundet offentliggörande av öppenhetsrapporter eller sammanfattningar av offentliga begäranden om åtkomst till uppgifter och vilken typ av svar som lämnats, om ett sådant offentliggörande är tillåtet enligt den lokala lagstiftningen.

136. Villkor för effektivitet:

- Den information som tillhandahålls bör vara relevant, tydlig och så detaljerad som möjligt. Den nationella lagstiftningen i tredjelandet kan förhindra att detaljerad information lämnas ut. I sådana fall bör uppgiftsinföraren efter bästa förmåga offentliggöra statistisk information eller liknande aggregerade uppgifter.

Organisationsmetoder och åtgärder för uppgiftsminimering

137. Befintliga organisatoriska krav enligt principen om ansvarsskyldighet, däribland antagandet av strikta och detaljerade regler och metoder för uppgiftsåtkomst och konfidentialitet, baserade på en strikt princip om behov av uppgifter, övervakade genom regelbundna revisioner och verkställda genom disciplinära åtgärder kan också vara användbara åtgärder i samband med överföringar. Uppgiftsminimering bör övervägas i detta avseende för att begränsa personuppgifternas exponering för obehörig åtkomst. I vissa fall är det till exempel inte alltid

[102] Se mål C-362/14 (Schrems I), punkt 94 och mål C-311/18 (Schrems II), punkterna 168, 174, 175 och 176.

nödvändigt att överföra vissa uppgifter (t.ex. vid fjärråtkomst till uppgifter i EES, däribland i stödärenden, om begränsad åtkomst har beviljats istället för full åtkomst, eller om tillhandahållandet av en tjänst endast kräver överföring av en begränsad datauppsättning och inte en hel databas).

138. Villkor för effektivitet:

- Regelbundna revisioner och stränga disciplinära åtgärder bör införas för att övervaka och säkerställa efterlevnaden av åtgärderna för uppgiftsminimering, även i samband med överföringar.
- Uppgiftsutföraren ska utföra en bedömning av personuppgifterna innan överföringen äger rum för att identifiera vilka uppsättningar av uppgifter som inte måste överföras och som därmed inte kommer att delas med uppgiftsinföraren.
- Åtgärder för uppgiftsminimering bör kompletteras med tekniska åtgärder för att säkerställa att uppgifterna inte utsätts för obehörig åtkomst. Exempelvis kan genomförandet av säkra behandlingsmekanismer med flera aktörer och spridningen av krypterade datauppsättningar bland betrodda enheter genom sin utformning förhindra att ensidig åtkomst leder till utlämning av identifierbara uppgifter.

***

139. Utarbetande av bästa praxis för att på ett lämpligt sätt och vid rätt tillfälle involvera och ge åtkomst till information till den dataskyddsansvarige, i förekommande fall, och till de rättsliga och interna revisionstjänsterna i frågor som rör internationella överföringar av personuppgifter.

140. Villkor för effektivitet:

- Den dataskyddsansvarige, om en sådan finns, och den rättsliga och interna revisionsgruppen ska ges tillgång till all relevant information före överföringen och rådfrågas om behovet av överföringen och de extra skyddsåtgärderna i förekommande fall.
- Relevant information bör till exempel omfatta bedömningen av behovet att överföra de berörda personuppgifterna, en översikt över tredjelandets tillämpliga lagstiftning och de skyddsåtgärder som uppgiftsinföraren har åtagit sig att genomföra.

Antagande av standarder och bästa praxis

141. Antagande av strikta regler för datasäkerhet och integritet baserade på EU:s certifiering eller uppförandekoder eller på internationella standarder (t.ex. ISO-normerna) och bästa praxis (t.ex. Enisa) med vederbörlig hänsyn till den senaste tekniska nivån, i enlighet med riskerna för de kategorier av uppgifter som behandlas.

Övriga

142. Antagande och regelbunden granskning av interna regler för att bedöma de genomförda kompletterande åtgärdernas lämplighet och för att identifiera och genomföra ytterligare eller alternativa lösningar vid behov för att säkerställa att en skyddsnivå som är väsentligen likvärdig med den som garanteras inom EES upprätthålls för de överförda personuppgifterna.

***

143. Åtaganden från uppgiftsinförarens sida att inte vidareöverföra personuppgifterna inom samma eller till ett annat tredjeland eller avbryta pågående överföringar om en skyddsnivå som är väsentligen likvärdig med den som garanteras inom EES inte kan garanteras i tredjelandet.[103]

[103] C-311/18 (Schrems II), punkterna 135 och 137.

BILAGA 3: MÖJLIGA KÄLLOR TILL INFORMATION FÖR BEDÖMNING AV ETT TREDJELAND

144. Din uppgiftsinförare bör kunna tillhandahålla relevanta källor och uppgifter om det tredjeland där uppgiftsinföraren är etablerad, inräknat vilken lagstiftning och praxis som är tillämplig för uppgiftsinföraren och de överförda uppgifterna. Du och uppgiftsinföraren kan hänvisa till flera informationskällor, såsom de som upptas i prioritetsordning i den icke uttömmande förteckningen nedan:

- Rättspraxis från Europeiska unionens domstol och Europeiska domstolen för de mänskliga rättigheterna[104] i enlighet med rekommendationerna för europeiska väsentliga garantier.[105]
- Beslut om adekvat skyddsnivå i det mottagande landet om överföringen bygger på en annan rättslig grund.[106]
- Resolutioner och rapporter från mellanstatliga organisationer, t.ex. Europarådet[107], andra regionala organ[108] och FN:s organ och byråer (t.ex. FN:s råd för mänskliga rättigheter[109], kommittén för de mänskliga rättigheterna[110]).
- Rapporter och analys från behöriga tillsynsnätverk, såsom Global Privacy Assembly (GPA).[111]
- Nationell rättspraxis eller beslut som fattats av oberoende rättsliga eller administrativa myndigheter med behörighet inom området för dataskydds- och integritetsfrågor i tredjeländer.
- Rapporter från oberoende tillsynsorgan eller parlamentariska organ.
- Rapporter baserade på praktisk erfarenhet av tidigare inlämnade begäranden om utlämning från offentliga myndigheter, eller frånvaron av sådana begäranden, från enheter som är verksamma inom samma sektor som uppgiftsinföraren.
- Warrant Canary-meddelanden från andra enheter som behandlar uppgifter inom samma område som uppgiftsinföraren.
- Rapporter som tagits fram eller beställts av uppgiftsutförarens eller andra tredjeländers handelskamrar, företags-, yrkes- och branschorganisationer, statliga diplomatiska organ, handels- och investeringsorgan som exporterar till det tredjeland till vilket överföringen görs.

---

[104] Se faktabladet om rättspraxis från Europeiska domstolen för de mänskliga rättigheterna angående massövervakning: https://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf

[105] Dataskyddsstyrelsens dokument *Rekommendationer 02/2020 om europeiska nödvändiga garantier för övervakningsåtgärder*, av den 10 november 2020, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en

[106] C-311/18 (Schrems II), punkt 141, se beslut om adekvat skyddsnivå i https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

[107] https://www.coe.int/en/web/data-protection/reports-studies-and-opinions

[108] Se till exempel landsrapporterna från den interamerikanska kommissionen för de mänskliga rättigheterna (IACHR), https://www.oas.org/en/iachr/reports/country.asp.

[109] Se https://www.ohchr.org/EN/HRBodies/UPR/Pages/Documentation.aspx

[110] Se: https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/TBSearch.aspx?Lang=en&TreatyID=8&DocTypeID=5

[111] Se t.ex. https://globalprivacyassembly.org/wp-content/uploads/2020/10/Day-1-1_2a-Day-3-3_2b-v1_0-Policy-Strategy-Working-Group-WS1-Global-frameworks-and-standards-Report-Final.pdf

- Rapporter från akademiska institutioner och organisationer i det civila samhället (t.ex. icke-statliga organisationer).
- Rapporter från privata leverantörer av information för beslutsstöd om företags finansiella, regulatoriska och anseenderelaterade risker.
- Warrant Canary-meddelanden från uppgiftsinföraren själv. [112]
- Öppenhetsrapporter, under förutsättning att de uttryckligen nämner att inga begäranden om åtkomst har mottagits. Öppenhetsrapporter som förbigår denna fråga skulle inte betraktas som tillräckliga belägg eftersom dessa rapporter oftast fokuserar på begäranden om åtkomst som mottagits från brottsbekämpande myndigheter och endast ger statistik för denna aspekt medan de förbigår mottagna begäranden om åtkomst för nationella säkerhetssyften. Detta innebär inte att inga begäranden om åtkomst har mottagits, utan snarare att denna information inte kan delas. [113]
- Interna yttranden eller register tillhörande uppgiftsinföraren i vilka det uttryckligen anges att inga begäranden om åtkomst har mottagits under en tillräckligt lång tid, och företrädesvis yttranden eller register som ligger till grund för uppgiftsinförarens ansvar och/eller utfärdas av interna positioner med viss självständighet såsom internrevisorer och dataskyddsombud. [114]

[112] Se villkor för att överväga uppgiftsinförarens dokumenterade praktiska erfarenhet av relevanta tidigare inlämnade begäranden om åtkomst från offentliga myndigheter i tredjelandet i punkt 47.
[113] *Ibid.*
[114] *Ibid.*