Rekommendationer

Translations proofread by EDPB Members.
This language version has not yet been proofread.

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

Antagna den 10 november 2020

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 överförs och behandlas i tredjelandet.

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

dataskyddsförordningen för överföringar som är regelbundna och återkommande. Endast i vissa fall med tillfälliga och icke återkommande överföringar kan du åberopa ett av de undantag som anges i artikel 49 i den allmänna dataskyddsförordningen, under förutsättning att du uppfyller villkoren.

Ett **tredje steg** är att **bedöma** om det finns något i **det tredje landets lagstiftning eller praxis** som kan påverka effektiviteten hos de lämpliga skyddsåtgärderna i de överföringsverktyg som du använder i samband med din överföring. Din bedömning bör i första hand vara inriktad på den lagstiftning i det tredje landet som är relevant för din överföring och som eventuellt kan undergräva skyddet för de överföringsverktyg i artikel 46 i den allmänna dataskyddsförordningen som du förlitar dig på. 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. Detta bör i synnerhet övervägas noggrant om den lagstiftning som reglerar de offentliga myndigheternas tillgång till uppgifter är tvetydig eller otillgänglig för allmänheten. Om det inte finns någon lagstiftning som reglerar de omständigheter under vilka de offentliga myndigheterna kan komma åt personuppgifter, och om du fortfarande vill genomföra överföringen, bör du ta hänsyn till andra relevanta och objektiva faktorer och inte förlita dig på subjektiva faktorer, som sannolikheten att de offentliga myndigheterna kommer åt dina uppgifter på ett sätt som inte uppfyller EU:s normer. Du bör utföra denna bedömning med tillbörlig aktsamhet och dokumentera den noggrant, eftersom du kommer att hållas 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 lagstiftningen i tredjelandet 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 lagstiftningen i tredjelandet och det överföringsverktyg du förlitar dig på, och du kommer att hållas ansvarig för alla beslut som du fattar. 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. 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 du med lämpliga mellanrum bör omvärdera den skyddsnivå som har uppnåtts för de uppgifter 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. Som domstolen erinrar om kommer tillsynsmyndigheterna att avbryta eller förbjuda överföringar av uppgifter om de, efter en utredning eller ett klagomål, konstaterar att en väsentligen likvärdig skyddsnivå inte kan säkerställas.

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*),

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 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 EU. 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.

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, allmänheten 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 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

[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.
[16] C-311/18 (Schrems II), punkterna 134, 135, 139, 140, 141, 142.

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 personuppgiftsansvariga eller det personuppgiftsbiträde som agerar som uppgiftsutförare och som behandlar personuppgifter inom dataskyddsförordningens tillämpningsområde – inbegripet behandling som utförs av privata enheter och offentliga organ vid överföring av uppgifter till privata organ.[19] 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.*[20]

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.[21]

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[22] är det första steget att säkerställa att du är fullt medveten om dina överföringar. Registrering och kartläggning av alla överföringar kan vara en 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.

[17] C-311/18 (Schrems II), punkt 134.
[18] Artikel 5.2 och artikel 28.3 h i den allmänna dataskyddsförordningen.
[19] 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
[20] 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
[21] Artikel 5.2 i den allmänna dataskyddsförordningen och artikel 24.1 i den allmänna dataskyddsförordningen.
[22] Observera att fjärråtkomst av en enhet i ett tredjeland till uppgifter som finns inom EES också betraktas som en överföring.

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.[23] 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.[24]

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[25].

11. I linje med dataskyddsförordningens princip om ”uppgiftsminimering”[26] måste du kontrollera att de uppgifter du överför är adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de överförs till och behandlas i det tredjelandet.

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 också betraktas som överföringar.[27] Mer specifikt, om du använder en internationell molninfrastruktur måste du bedöma om och när dina uppgifter kommer att överföras till tredjeländer, såvida inte molnleverantören tydligt uppger i sitt avtal att uppgifterna inte kommer att behandlas alls i tredjeländer.

[23] 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).

[24] 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.

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

[26] Artikel 5.1 c i den allmänna dataskyddsförordningen.

[27] 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, 23 juli 2020.

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.[28]

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).[29]

18. EU-kommissionen offentliggör en förteckning över sina beslut om adekvat skyddsnivå på sin webbplats.[30]

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.**[31] Du måste emellertid fortfarande övervaka om de beslut om adekvat skyddsnivå som är relevanta för dina överföringar återkallas eller ogiltigförklaras.[32]

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.[33]

---

[28] 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.

[29] Artikel 45.1 i den allmänna dataskyddsförordningen.

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

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

[32] 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)).

[33] 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 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.

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).[34]

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 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.[35]

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.

[34] Mål C-362/14 (Schrems I).
[35] C-311/18 (Schrems II), punkterna 130 och 133. Se även punkt 2.3 nedan.

25. Artikel 49 i den allmänna dataskyddsförordningen har en undantagskaraktär. Undantagen måste tolkas restriktivt och huvudsakligen avse behandling som är tillfällig och inte återkommande. EDPB har utfärdat sina riktlinjer 2/2018 om undantagen i artikel 49 enligt förordning 2016/679. [36]

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 räcker inte alltid att välja ett av överföringsverktygen i artikel 46 i den allmänna dataskyddsförordningen. Överföringsverktyget måste säkerställa att den skyddsnivå som garanteras genom dataskyddsförordningen inte undergrävs av överföringen.[37] Med andra ord måste ditt överföringsverktyg vara effektivt i praktiken.

29. Med *effektivt* avses att de överförda personuppgifterna har en skyddsnivå i tredjelandet som är väsentligen likvärdig med den nivå som garanteras inom EES.[38] 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.

30. Därför måste du bedöma, i tillämpliga fall tillsammans med uppgiftsinföraren, om det finns något i tredjelandets lagstiftning eller praxis som kan påverka effektiviteten hos de lämpliga skyddsåtgärderna i det överföringsverktyg i artikel 46 i den allmänna dataskyddsförordningen som du förlitar dig på i samband med din specifika överföring. I tillämpliga fall bör din uppgiftsinförare ge dig relevanta källor och information om det tredjeland där uppgiftsinföraren är etablerad och vilka lagar som är tillämpliga för överföringen. Du kan även använda andra informationskällor, till exempel de som ingår i den icke uttömmande förteckningen i bilaga 3.[39]

31. 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 vidareöverföringar i din bedömning.

32. För detta ändamål måste du undersöka egenskaperna hos var och en av dina överföringar och avgöra hur den nationella rättsordningen i det land som uppgifterna överförs (eller vidareförs) till är tillämplig på dessa överföringar.

---

[36] Ytterligare vägledning om detta finns på webbadressen https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation_sv.
[37] Artikel 44 i den allmänna dataskyddsförordningen.
[38] C-311/18 (Schrems II), punkt 105 och den andra slutsatsen.
[39] Se även punkt 43 nedan.

33. Den tillämpliga rättsliga ramen beror på omständigheterna kring överföringen, 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, finans etc),
- kategorierna av personuppgifter som överförs (personuppgifter som rör barn kan t.ex. omfattas av särskild lagstiftning i tredjelandet),
- möjligheten att uppgifterna kan lagras i tredjelandet eller om tredjelandet endast kommer att ha fjärråtkomst till uppgifter som lagras inom EU/EES,
- formatet på de uppgifter som ska överföras (dvs. i klartext, pseudonymiserade eller krypterade[40]),
- möjligheten att uppgifterna kan överföras vidare från tredjelandet till ett annat tredjeland.[41]

34. Du måste även bedöma om någon av de tillämpliga lagarna kan påverka åtagandena för de överföringsverktyg i artikel 46 i den allmänna dataskyddsförordningen som du har valt. Du bör kontrollera om åtaganden som gör att registrerade personer kan utöva sina rättigheter i samband med internationella överföringar (däribland att komma åt, korrigera och radera överförda uppgifter) kan tillämpas på ett effektivt sätt i praktiken och att de inte motverkas av lagstiftningen i tredjelandet.

35. Du kommer att behöva bedöma relevanta regler av allmän karaktär i den mån de påverkar den effektiva tillämpningen av de skyddsåtgärder som ingår i överföringsverktyget i artikel 46 i den allmänna dataskyddsförordningen och enskilda personers grundläggande rättigheter (i synnerhet den registrerades rätt till domstolsprövning om de offentliga myndigheterna i tredjelandet kommer åt de överförda uppgifterna).

36. 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 och nationella säkerhetssyften). Om dessa krav eller befogenheter är begränsade till vad som är nödvändigt och proportionerligt i ett demokratiskt samhälle[42] kan det hända att de inte påverkar åtagandena för de överföringsverktyg i artikel 46 i den allmänna dataskyddsförordningen som du förlitar dig på.

37. EU:s normer, däribland artiklarna 47 och 52 i EU-stadgan om de grundläggande rättigheterna, måste användas som referens 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.

[40] Vissa tredjeländer tillåter inte att krypterade uppgifter förs in.
[41] Om den personuppgiftsansvariga har gett ett särskilt eller allmänt skriftligt förhandsgodkännande i enlighet med artikel 28.2 i den allmänna dataskyddsförordningen.
[42] 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. 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.[43] 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.[44]

***

39. I EDPB:s rekommendationer för europeiska väsentliga garantier (EEG) beskrivs 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 (och att den därmed inte inkräktar på åtagandena för överföringsverktyget i artikel 46 i den allmänna dataskyddsförordningen) 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.

40. Om EDPB:s rekommendationer för europeiska väsentliga garantier tillämpas på situationen för överföringar av uppgifter med överföringsverktygen i artikel 46 kan de hjälpa uppgiftsutföraren och uppgiftsinföraren att bedöma om sådana befogenheter innebär en omotiverad inblandning i uppgiftsinförarens skyldigheter att säkerställa en väsentlig likvärdighet.

41. Bristen på en väsentligen likvärdig skyddsnivå kommer att vara särskilt uppenbar om den lagstiftning eller praxis i tredjelandet som är relevant för din överföring inte uppfyller kraven för de europeiska väsentliga garantierna.

42. Din bedömning måste först och främst utgå från den lagstiftning som finns tillgänglig offentligt. I vissa situationer är detta emellertid inte tillräckligt, eftersom lagstiftningen i tredjelandet kan vara bristfällig. I sådana fall, om du fortfarande vill genomföra överföringen, bör du ta hänsyn till andra relevanta och objektiva faktorer[45] och inte förlita dig på subjektiva faktorer, som sannolikheten att de offentliga myndigheterna kommer åt dina uppgifter på ett sätt som inte uppfyller EU:s normer. Du bör utföra denna bedömning med tillbörlig aktsamhet och dokumentera den noggrant, eftersom du kommer att hållas ansvarig för alla beslut som du fattar på denna grund.[46]

43. Du kan komplettera din bedömning med information från andra källor[47], däribland

- upplysningar som visar att en myndighet i tredjelandet kommer att försöka komma åt uppgifterna med eller utan uppgiftsinförarens kännedom, mot bakgrund av rapporterade prejudikat, lagstiftning och praxis,
- upplysningar som visar att en myndighet i tredjelandet kommer att kunna få åtkomst till uppgifterna via uppgiftsinföraren eller genom direkt inblandning i kommunikationskanalen

[43] C-311/18 (Schrems II), punkt 104.

[44] Några exempel: Konvention 108 (Europarådets konvention om skydd för enskilda vid automatisk databehandling av personuppgifter, ETS nr 108) eller konvention 108+ (Moderniserad konvention om skydd för enskilda vid automatisk databehandling av personuppgifter, CETS nr 223) ger tillgång till verkställbara internationella rättsmedel vid överträdelser av bestämmelserna om dataskydd och bidrar till en miniminivå av skydd för personuppgifter och respekt för privatlivet.

[45] Se punkt 43 nedan samt bilaga 3.

[46] Artikel 5.2 i den allmänna dataskyddsförordningen.

[47] Se även bilaga 3.

mot bakgrund av rapporterade prejudikat, rättsliga befogenheter samt tillgängliga tekniska, finansiella och mänskliga resurser.

44. Din slutgiltiga bedömning av det överföringsverktyg i artikel 46 i den allmänna dataskyddsförordningen som du förlitar dig på och de ingående lämpliga skyddsåtgärderna kan visa följande:

- Överföringsverktyget säkerställer effektivt att de överförda personuppgifterna har en skyddsnivå i tredjelandet som väsentligen är likvärdig med den nivå som garanteras inom EES. Tredjelandets tillämpliga lagstiftning och praxis för överföringen innebär att uppgiftsinföraren kan 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 fullgöra sina skyldigheter på grund av tredjelandets tillämpliga lagstiftning och/eller praxis för överföringen. 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.[48]

EU-domstolen framhöll till exempel 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. Som en följd av detta, om uppgiftsinföraren eller någon annan mottagare som uppgiftsinföraren kan lämna ut uppgifterna till omfattas av avsnitt 702 i Fisa[49], kan standardavtalsklausuler eller andra överföringsverktyg i artikel 46 i den allmänna dataskyddsförordningen endast användas för sådana överföringar om ytterligare kompletterande tekniska åtgärder gör att åtkomsten till de överförda uppgifterna blir omöjlig eller ineffektiv.

2.4 Steg 4: Inför kompletterande åtgärder

45. 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.[50] Med *kompletterande åtgärder* avses åtgärder som per definition kompletterar de skyddsåtgärder som överföringsverktyget enligt artikel 46 i dataskyddsförordningen redan tillhandahåller.[51]

[48] EU-domstolens dom i mål C-311/18 (Schrems II), punkterna 134–135.
[49] Avsnitt 702 i Fisa är tillämpligt om uppgifterna hämtas från eller med stöd av en leverantör av elektroniska kommunikationstjänster (avsnitt 702 i Fisa = 50 USC, 1881a §, enligt led h 2 A vi), vilken i sin tur definieras i 50 USC, 1881 b 4 § som
”A) en teleoperatör enligt definitionen i avsnitt 153 i avdelning 47,
B) en leverantör av elektroniska kommunikationstjänster enligt definitionen i avsnitt 2510 i avdelning 18,
C) en leverantör av fjärrbearbetningstjänster enligt definitionen i avsnitt 2711 i avdelning 18,
D) en annan leverantör av kommunikationstjänster som har tillgång till trådbunden eller elektronisk kommunikation antingen genom att kommunikationen överförs eller att kommunikationen lagras, eller
E) en tjänsteman, anställd eller agent hos en enhet som beskrivs i led A, B, C eller D.”.
[50] C-311/18 (Schrems II), punkt 96.
[51] Skäl 109 i den allmänna dataskyddsförordningen och C-311/18 (Schrems II), punkt 133.

46. 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 kommer att kunna bygga vidare på dina bedömningar 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.

47. 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.

48. Avtalsrättsliga och organisatoriska åtgärder räcker i regel inte för att hindra de offentliga myndigheterna i tredjelandet från att komma åt personuppgifter (i de fall där detta påverkar uppgiftsinförarens skyldigheter att säkerställa en väsentlig likvärdighet på ett omotiverat sätt). Det kommer att finnas situationer där endast tekniska åtgärder kan hindra eller begränsa de offentliga myndigheternas åtkomst till personuppgifter i tredjelandet, i synnerhet för övervakningsändamål.[52] I sådana situationer kan avtalsrättsliga eller organisatoriska åtgärder komplettera de tekniska åtgärderna och förstärka uppgifternas övergripande skyddsnivå, t.ex. genom att skapa hinder om de offentliga myndigheterna försöker komma åt uppgifter på ett sätt som inte är förenligt med EU:s normer.

49. 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:

- Formatet på de uppgifter som ska överföras (dvs. i klartext, pseudonymiserade eller krypterade).
- Typen av uppgifter.
- 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)).[53]
- Möjligheten att uppgifterna kan överföras vidare, inom samma tredjeland eller till och med till andra tredjeländer (t.ex. genom uppgiftsinförarens underentreprenörer[54]).

[52] 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.

[53] 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.

[54] Se fotnot 25.

Exempel på kompletterande åtgärder

50. Några exempel på tekniska, avtalsrättsliga och organisatoriska åtgärder som kan övervägas finns i den icke uttömmande förteckningen i bilaga 2.

***

51. 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 gå vidare med dina överföringar.

52. Om du inte kan hitta eller genomföra effektiva kompletterande åtgärder som säkerställer att de överförda uppgifterna har en väsentligen likvärdig skyddsnivå[55] 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.[56] 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.[57]

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.

53. Om du beslutar att fortsätta med överföringen trots att uppgiftsinföraren inte kan uppfylla de åtaganden som gjorts enligt överföringsverktyget i artikel 46 i den allmänna dataskyddsförordningen bör du meddela den behöriga tillsynsmyndigheten i enlighet med de särskilda bestämmelserna för det relevanta överföringsverktyget.[58] Den behöriga tillsynsmyndigheten kommer att avbryta eller förbjuda överföringar av uppgifter i de fall där den konstaterar att en väsentligen likvärdig skyddsnivå inte kan säkerställas.[59]

54. 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.

[55] 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.

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

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

[58] Se EDPB:s vanliga frågor om EU-domstolens dom i mål C-311/18 – Data Protection Commissioner mot Facebook Ireland Ltd och Maximillian Schrems, som antogs den 23 juli 2020, i synnerhet frågorna 5, 6 och 9. Se även klausul 4 g i kommissionens beslut 2010/87/EU, klausul 5 a i kommissionens beslut 2001/497/EG samt klausul II c om standardavtal II i bilagan till kommissionens beslut 2004/915/EG.

[59] C-311/18 (Schrems II), punkterna 113 och 121.

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

55. 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.

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

56. 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.[60] 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).

57. 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[61] 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)

58. 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

---

[60] 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.

[61] 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_sv.pdf.

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.[62]

59. 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. Schrems II-domens exakta konsekvenser för bindande företagsbestämmelser diskuteras fortfarande. EDPB kommer att lämna mer information så fort som möjligt när det gäller huruvida ytterligare åtaganden måste införas i de bindande företagsbestämmelser som hänvisas till i dokumenten WP 256/257.[63]

60. 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)

61. 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.[64] 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. Schrems II-domens exakta konsekvenser för avtalsklausuler diskuteras fortfarande. EDPB kommer att lämna mer information så fort som möjligt.

2.6 Steg 6: Omvärdera med lämpliga mellanrum

62. 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).

63. 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
- de kompletterande åtgärderna inte längre är effektiva i det berörda tredjelandet.

[62] EU-domstolen, C-311/18 (Schrems II), punkt 132.
[63] 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 ingår i bindande företagsbestämmelser, senast reviderat och antaget den 6 februari 2018, WP 257 rev.01.
[64] EU-domstolen, C-311/18 (Schrems II), punkt 132.

3 SLUTSATS

64. 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.[65]

65. 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 överförs och behandlas i tredjelandet.

66. 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.

67. 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.

68. 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)

[65] 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, EUR 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

69. 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. 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.

70. 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 är inriktad på de specifika brister som du identifierade i din bedömning av den rättsliga situationen i tredjelandet. Om du inte kan säkerställa en väsentligen likvärdig skyddsnivå får du inte överföra personuppgifterna.

71. Som personuppgiftsansvarig eller personuppgiftsbiträde kanske du redan är tvungen att genomföra vissa av de åtgärder som beskrivs i denna bilaga, även om din uppgiftsinförare omfattas av ett beslut om adekvat skyddsnivå, eller tvungen att genomföra dem när du behandlar uppgifter inom EES.[66]

Tekniska åtgärder

72. 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[67].

73. För att förtydliga ytterligare inleds detta avsnitt med de tekniska åtgärder som kan vara effektiva i vissa scenarier/användningsfall för att säkerställa en väsentligen likvärdig skyddsnivå. Avsnittet fortsätter sedan med scenarier/användningsfall där inga tekniska åtgärder finns tillgängliga för att uppnå denna skyddsnivå.

Scenarier där *effektiva* åtgärder finns tillgängliga

74. 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 dataskyddsförordningen. Dessa åtgärder gäller även om de offentliga myndigheternas åtkomst är förenlig med lagstiftningen i uppgiftsinförarens hemland om åtkomsten går längre än vad som är nödvändigt och proportionerligt i ett demokratiskt samhälle[68]. 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

[66] Artikel 5.2 och artikel 32 i den allmänna dataskyddsförordningen.
[67] C-311/18 (Schrems II), punkt 135.
[68] Se artiklarna 47 och 52 i Europeiska unionens stadga om de grundläggande rättigheterna, artikel 23.1 i den allmänna dataskyddsförordningen och EDPB:s rekommendationer om europeiska väsentliga garantier för övervakningsåtgärder.

ett annat sammanhang eller koppla de överförda uppgifterna till andra datauppsättningar som de kan ha tillgång till, däribland nätidentifierare genom anordningar, program, verktyg och protokoll som används av de registrerade i andra sammanhang.

75. 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.

76. 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.

77. I scenarierna beskrivs de särskilda omständigheterna och vilka åtgärder som vidtagits. Eventuella ändringar av scenarierna kan ge upphov till olika slutsatser.

78. 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 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

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

Om

1. personuppgifterna behandlas med användning av stark kryptering före överföringen,
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,
3. styrkan i krypteringen har fastställts med beaktande av den specifika tidsperiod under vilken de krypterade personuppgifternas konfidentialitet måste upprätthållas,
4. krypteringsalgoritmen har genomförts felfritt med hjälp av korrekt underhållen programvara 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), och
6. nycklarna helt och hållet förvaras under kontroll av uppgiftsutföraren eller någon annan aktör som anförtrotts denna uppgift och som är verksam inom EES eller i ett tredjeland, ett territorium eller en eller flera angivna sektorer i ett tredjeland, eller vid en internationell organisation för vilken kommissionen i enlighet med artikel 45 i den allmänna dataskyddsförordningen har fastställt att en adekvat skyddsnivå säkerställs,

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

Användningsfall 2: Överföring av pseudonymiserade uppgifter

80. 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[69],
2. dessa ytterligare uppgifter helt och hållet innehas av uppgiftsutföraren och förvaras separat i en medlemsstat eller i ett tredjeland, ett territorium eller en eller flera angivna sektorer i ett tredjeland, eller vid en internationell organisation för vilken kommissionen i enlighet med artikel 45 i den allmänna dataskyddsförordningen har fastställt att en adekvat skyddsnivå säkerställs,
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 personuppgiftsansvariga genom en noggrann analys av uppgifterna i ärendet, och med beaktande av alla uppgifter som de offentliga myndigheterna i det mottagande landet kan ha tillgång till, 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.

[69] I linje med artikel 4.5 i den allmänna dataskyddsförordningen avses med *pseudonymisering* en ”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”.

81. 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[70], i många situationer kan möjliggöra en identifiering av den berörda personen även om namn, adress eller andra identitetsbeteckningar har utelämnats.

82. 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.

83. 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.

Användningsfall 3: Krypterade uppgifter som endast transiteras via tredjeländer

84. En uppgiftsutförare vill överföra uppgifter till ett land som bedöms erbjuda adekvat skydd i enlighet med artikel 45 i den allmänna dataskyddsförordningen. Uppgifterna överförs via ett tredjeland.

Om

1. en uppgiftsutförare överför personuppgifter till en uppgiftsinförare i en jurisdiktion som säkerställer en adekvat skyddsnivå, om uppgifterna transporteras över internet och om uppgifterna kan styras geografiskt genom ett tredjeland som inte tillhandahåller en väsentligen likvärdig skyddsnivå,
2. uppgiftsutföraren använder transportkryptering med krypteringsprotokoll som uppfyller kraven för den senaste tekniska nivån och ger ett effektivt skydd mot aktiva och passiva attacker med resurser som enligt uppgift finns tillgängliga för de offentliga myndigheterna i tredjelandet,
3. dekryptering endast är möjlig utanför det berörda tredjelandet,
4. de parter som deltar i kommunikationen kommer överens om en pålitlig myndighet eller infrastruktur för certifiering av öppna nycklar,
5. särskilda skyddsåtgärder som uppfyller kraven för den senaste tekniska nivån används mot aktiva och passiva attacker mot transportkrypterade uppgifter,
6. personuppgifterna även krypteras genomgående i applikationsskiktet med krypteringsmetoder som uppfyller kraven för den senaste tekniska nivån, på grund av att transportkrypteringen i sig inte uppnår en lämplig skyddsnivå till följd av sårbarheter i den infrastruktur eller programvara som används,
7. 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

[70] 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 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”.

kryptoanalys som utförs av de offentliga myndigheterna i det transiterande landet med beaktande av de resurser och den tekniska kapacitet (t.ex. datorkapacitet för uttömmande attacker) som de har tillgång till,
8. styrkan i krypteringen har fastställts med beaktande av den specifika tidsperiod under vilken de krypterade personuppgifternas konfidentialitet måste upprätthållas,
9. krypteringsalgoritmen har genomförts felfritt med hjälp av korrekt underhållen programvara vars överensstämmelse med den valda algoritmens specifikation har verifierats, t.ex. genom certifiering,
10. förekomsten av bakdörrar (i maskinvaran eller programvaran) har uteslutits,
11. 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

85. 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 endast finns i den skyddade uppgiftsinförarens ägo och har ett lämpligt skydd mot obehörig 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

86. 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. 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,
6. den personuppgiftsansvariga genom en noggrann analys av uppgifterna i ärendet, och med beaktande av alla uppgifter som de offentliga myndigheterna i de mottagande länderna kan ha tillgång till, 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,

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

Scenarier där *inga effektiva* åtgärder finns tillgängliga

87. 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 kompletterande åtgärder.

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

88. En uppgiftsutförare använder en leverantör av en molntjänst eller ett annat personuppgiftsbiträde som behandlar personuppgifter enligt uppgiftsutförarens anvisningar i ett tredjeland.

Om

1. en personuppgiftsansvarig överför uppgifter 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 de offentliga myndigheterna i det mottagande landet för att komma åt de överförda uppgifterna går längre än vad som är nödvändigt och proportionerligt i ett demokratiskt samhälle,[71]

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 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.

89. 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: Fjärråtkomst till uppgifter för affärsändamål

90. En uppgiftsutförare gör personuppgifter tillgängliga för aktörer i ett tredjeland så att de kan användas för delade affärsändamål. 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 gemensamt 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 använder uppgifterna i klartext för sina egna syften,
3. den befogenhet som tilldelats de offentliga myndigheterna i det mottagande landet för att komma åt de överförda uppgifterna går längre än vad som är nödvändigt och proportionerligt i ett demokratiskt samhälle,

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

[71] Se artiklarna 47 och 52 i Europeiska unionens stadga om de grundläggande rättigheterna, artikel 23.1 i den allmänna dataskyddsförordningen och EDPB:s rekommendationer om europeiska väsentliga garantier för övervakningsåtgärder.

91. 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.

Ytterligare avtalsrättsliga åtgärder

92. Dessa åtgärder består i allmänhet av unilaterala, bilaterala eller multilaterala[72] avtalsrättsliga åtaganden.[73] 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.[74]

93. 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 EU. 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[75], bör dessa åtgärder 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.

94. 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.

95. 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.[76]

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

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

[73] 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.

[74] 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).

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

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

Uppfyllande av avtalsförpliktelsen att använda särskilda tekniska åtgärder

97. ***Beroende på överföringarnas särskilda omständigheter kan avtalet behöva innehålla föreskrifter om att särskilda tekniska åtgärder måste vidtas för att överföringarna ska kunna äga rum (se de tekniska åtgärder som föreslås ovan).***

98. ***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

99. ***Uppgiftsutföraren kan lägga till bilagor till avtalet med information om åtkomst till uppgifterna som uppgiftsinföraren, efter bästa förmåga, kan ge de offentliga myndigheterna, 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.***

100. 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,[77] 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,[78]

[77] 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.
[78] 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.

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

101. 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.

102. ***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.[79]
- 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 EU. Denna skyldighet kan emellertid varken motivera att uppgiftsinföraren lämnar ut personuppgifter eller skapa en förväntning om det inte kommer fler begäranden om åtkomst.

***

103. ***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.***[80]

104. ***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 vara tvungen att meddela uppgiftsutföraren om att han eller hon inte längre kan uppfylla sina åtaganden enligt avtalet.[81]
- 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

[79] Se punkt 32.5 ovan.
[80] Denna klausul är viktig för att garantera en adekvat nivå av skydd för de personuppgifter som överförs och bör krävas i vanliga fall.
[81] Se punkt 32.5 ovan.

program, manipulerade affärsprocesser, eller krav på att genomföra något av dessa alternativ, eller underlåter att informera uppgiftsutföraren när förekomsten blir känd.

***

105. ***Uppgiftsutföraren skulle kunna utöka sin befogenhet att utföra revisioner[82] 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.***

106. ***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 bör vara manipuleringssäkra så att revisorerna kan hitta bevis för 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.

***

107. ***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 informera uppgiftsutföraren om han eller hon inte kan uppfylla de avtalsenliga åtagandena och därmed inte heller den ”väsentligen likvärdiga skyddsnivå” som krävs.[83].***

108. Denna oförmåga att uppfylla kraven kan vara ett resultat av förändringar i tredjelandets lagstiftning eller praxis.[84] Klausulerna kan innehålla specifika och strikta tidsfrister och förfaranden 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.

---

[82] 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.

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

[84] 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.”.*

109. ***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 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.

***

110. ***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.***

111. ***Villkor för effektivitet:***

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

112. ***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.***

113. ***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.

***

114. ***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[85] och att 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.***

[85] 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 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.

115. ***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

116. ***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 samtycke av uppgiftsutföraren och/eller den registrerade personen.***

117. ***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)[86].
- 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.

***

118. ***Avtalet skulle kunna omfatta en skyldighet för uppgiftsinföraren och/eller uppgiftsutföraren att omedelbart underrätta den registrerade personen om 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).***

[86] Artikel 4.11 i den allmänna dataskyddsförordningen.

119. ***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 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.

***

120. ***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.***

121. ***Villkor för effektivitet***

- 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 EU. 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. Under alla omständigheter skulle detta inte vara en effektiv kompletterande åtgärd mot övervakningsåtgärder om det inte fanns någon prövningsmekanism.

Organisatoriska åtgärder

122. 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 EU.

123. 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

124. ***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 dolda eller officiella 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, som bör vara baserad inom EES och bestå av experter inom it, dataskydd och integritetslagstiftning, för att hantera begäranden som inbegriper personuppgifter som överförts från EU, 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.***

125. 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.

126. ***Villkor för effektivitet:***

- Dessa regler kan endast övervägas för de fall där begäran från de offentliga myndigheterna i tredjelandet är förenlig med unionsrätten.[87] 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.

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

Åtgärder för öppenhet och ansvarsskyldighet

127. ***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 vid behov.***

128. ***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 försämrad skyddsnivå.

***

129. ***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.***

130. ***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

131. ***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 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).***

132. ***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.

***

133. ***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.***

134. ***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

135. ***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 och sannolikheten för att offentliga myndigheter ska försöka komma åt dem.***

Övriga

136. ***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 likvärdig med den som garanteras inom EU upprätthålls för de överförda personuppgifterna.***

***

137. ***Åtaganden från uppgiftsinförarens sida att inte vidareöverföra personuppgifterna inom samma eller till ett annat tredjeland eller avbryta pågående överföringar om en skyddsnivå som är likvärdig med den som garanteras inom EU inte kan garanteras i tredjelandet.***[88]

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

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

138. Din uppgiftsinförare bör kunna tillhandahålla relevanta källor och uppgifter om det tredjeland där uppgiftsinföraren är etablerad och vilken lagstiftning som är tillämplig i tredjelandet. Du kan även använda andra informationskällor, till exempel de som ingår i följande icke uttömmande förteckning:

- Rättspraxis från Europeiska unionens domstol och Europeiska domstolen för de mänskliga rättigheterna[89] i enlighet med rekommendationerna för europeiska väsentliga garantier.[90]
- Beslut om adekvat skyddsnivå i det mottagande landet om överföringen bygger på en annan rättslig grund.[91]
- Resolutioner och rapporter från mellanstatliga organisationer, t.ex. Europarådet[92], andra regionala organ[93] och FN:s organ och byråer (t.ex. FN:s råd för mänskliga rättigheter[94], kommittén för de mänskliga rättigheterna[95]).
- Nationell rättspraxis eller beslut som fattats av oberoende rättsliga eller administrativa myndigheter med behörighet inom området för dataskydds- och integritetsfrågor i tredjeländer.
- Rapporter från akademiska institutioner och organisationer i det civila samhället (t.ex. icke-statliga organisationer och branschorganisationer).

[89] Se faktabladet om rättspraxis från Europeiska domstolen för de mänskliga rättigheterna angående massövervakning: https://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf
[90] https://www.coe.int/en/web/data-protection/reports-studies-and-opinions
[91] 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
[92] https://www.coe.int/en/web/data-protection/reports-studies-and-opinions
[93] Se till exempel landsrapporterna från den interamerikanska kommissionen för de mänskliga rättigheterna (IACHR), https://www.oas.org/en/iachr/reports/country.asp.
[94] Se https://www.ohchr.org/EN/HRBodies/UPR/Pages/Documentation.aspx
[95] Se https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/TBSearch.aspx?Lang=en&TreatyID=8&DocTypeID=5