EUROPEISKA
KOMMISSIONEN

Bryssel den 6.11.2015
COM(2015) 566 final

MEDDELANDE FRÅN KOMMISSIONEN TILL EUROPAPARLAMENTET OCH RÅDET

om överföring av personuppgifter från EU till Amerikas förenta stater enligt direktiv 95/46/EG med anledning av domstolens dom i mål C-362/14 (Schrems)

MEDDELANDE FRÅN KOMMISSIONEN TILL EUROPAPARLAMENTET OCH RÅDET

om överföring av personuppgifter från EU till Amerikas förenta stater enligt direktiv 95/46/EG med anledning av domstolens dom i mål C-362/14 (Schrems)

1. INLEDNING: OGILTIGFÖRKLARINGEN AV SAFE HARBOUR-BESLUTET

Europeiska unionens domstol, nedan kallad *domstolen*, bekräftar i sin dom av den 6 oktober 2015 i mål C-362/14 (Schrems)[1] på nytt betydelsen av den grundläggande rätten till skydd av personuppgifter, vilken är stadfäst i Europeiska unionens stadga om de mänskliga rättigheterna, inklusive när sådana uppgifter överförs utanför EU.

Överföringar av personuppgifter är en väsentlig del av de transatlantiska förbindelserna. EU och Förenta staterna är varandras viktigaste handelspartner och dataöverföringar utgör en allt viktigare del av deras handelsutbyte.

För att underlätta dessa dataflöden, och samtidigt garantera en hög skyddsnivå för personuppgifter, erkände kommissionen safe harbour-principerna som adekvata genom att anta kommissionens beslut 2000/520/EG av den 20 juli 2000, nedan kallat *safe harbour-beslutet*. I detta beslut, baserat på artikel 25.6 i direktiv 95/46/EG[2], erkänner kommissionen att safe harbour-principerna om integritetsskydd och de tillhörande frågor och svar som Förenta staternas handelsministerium utfärdat säkerställer ett adekvat skydd vid överföringar av personuppgifter från EU[3]. Som ett resultat därav kunde personuppgifter överföras fritt från EU-medlemsstater till företag i Förenta staterna som har anslutit sig till principerna, trots att det saknas en allmän dataskyddslagstiftning i Förenta staterna. Safe harbour-systemet byggde på åtaganden och självcertifiering från de medverkande företagens sida. Medan det är frivilligt att ansluta sig till safe harbour-principerna om integritetsskydd och de tillhörande frågorna och svaren, är reglerna bindande enligt amerikansk lag för de enheter som ansluter sig till dem och reglerna verkställs av Förenta staternas konkurrensmyndighet (Federal Trade Commission)[4].

I sin dom av den 6 oktober 2015 ogiltigförklarade domstolen safe harbour-beslutet. Det är mot denna bakgrund som det aktuella meddelandet syftar till att ge en översikt av de alternativa verktygen för transatlantiska dataöverföringar enligt direktiv 95/46/EG i frånvaron av ett beslut om adekvat skyddsnivå. I meddelandet beskrivs även kortfattat domens konsekvenser

---

1 Domstolens dom av den 6 oktober 2015 i mål C-362/14, Maximilian Schrems mot dataskyddskommissionären, EU:C:2015:650 (nedan kallad *domen* eller *Schrems-domen*).

2 Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter, EGT L 281, 23.11.1995, s. 31, (nedan kallat *direktiv 95/46/EG*, eller *direktivet*).

3 I detta meddelande avses med EU även EES. Med ”medlemsstater” avses därmed även EES-medlemsstater.

4 För en mer djupgående översikt av safe harbour-systemet, se meddelandet från kommissionen till Europaparlamentet och rådet om hur principerna om integritetsskydd (safe harbour) fungerar när det gäller EU:s medborgare och företag som är etablerade i EU, COM/2013/847 final.

för andra av kommissionens beslut om adekvat skyddsnivå. I domen klargjorde domstolen att ett beslut om adekvat skyddsnivå enligt artikel 25.6 i direktiv 95/46/EG förutsätter att kommissionen har fastställt att det i det aktuella tredjelandet finns en nivå för skydd av personuppgifter som inte nödvändigtvis är identisk, men ”väsentligen likvärdig” med den nivå som garanteras inom EU genom direktivet jämfört med stadgan om de grundläggande rättigheterna. Gällande safe harbour-beslutet ansåg domstolen att det inte innehöll tillräckliga konstateranden från kommissionen rörande begränsningarna av amerikanska myndigheters åtkomst till data som överförs i enlighet med beslutet och existensen av effektivt rättsligt skydd mot sådana ingrepp. I synnerhet fastslog domstolen att den lagstiftning som tillåter myndigheterna generell åtkomst till innehållet i elektroniska kommunikationer måste anses kränka det väsentliga innehållet i den grundläggande rätten till respekt för privatlivet. Dessutom bekräftade domstolen att även där det finns ett beslut om adekvat skyddsnivå enligt artikel 25.6 i direktiv 95/46/EG behåller medlemsstaternas dataskyddsmyndigheter sin befogenhet och skyldighet att fullständigt oberoende utreda huruvida dataöverföringar till ett tredjeland är i enlighet med kraven i direktiv 95/46/EG, jämförda med artiklarna 7, 8 och 47 i stadgan om de grundläggande rättigheterna. Domstolen konstaterade även att endast domstolen kan förklara en unionsrättsakt, såsom ett kommissionsbeslut om adekvat skyddsnivå, ogiltigt.

I domen använder sig domstolen använder sig av kommissionens meddelande från 2013 om hur principerna om integritetsskydd (safe harbour) fungerar när det gäller EU:s medborgare och företag som är etablerade i EU[5], där kommissionen identifierade ett antal tillkortakommanden och formulerade 13 rekommendationer. Utifrån dessa rekommendationer har kommissionen hållit samtal med de amerikanska myndigheterna sedan januari 2014 i syfte att införa ett förnyat och starkare system för transatlantiskt datautbyte.

Efter domen håller kommissionen fast vid målet att upprätta ett förnyat och sunt system för transatlantiska överföringar av personuppgifter. På denna punkt har den omedelbart återupptagit och intensifierat sina samtal med Förenta staternas regering för att se till att ett nytt system för transatlantiska överföringar av personuppgifter helt och hållet uppfyller de normer som fastlagts av domstolen. Varje sådant system måste därför ha tillräckliga begränsningar, skyddsåtgärder och rättsliga kontrollmekanismer på plats för att säkerställa fortsatt skydd av EU-medborgares personuppgifter, även när det gäller myndigheters åtkomst i syften som rör brottsbekämpning och nationell säkerhet. Under tiden har näringslivet gett uttryck för farhågor rörande möjligheterna för fortsatta dataöverföringar[6]. Det finns därför ett

---

5 Meddelande från kommissionen till Europaparlamentet och rådet om hur principerna om integritetsskydd (safe harbour) fungerar när det gäller EU:s medborgare och företag som är etablerade i EU, COM(2013) 847 final, 27.11.2013. Se även kommissionens meddelande till Europaparlamentet och rådet, *Återskapande av förtroendet för dataflöden mellan EU och Förenta staterna*, COM(2013) 846 final, 27.11.2013, och tillhörande memorandum *Restoring Trust in EU-US data flows – Frequently Asked Questions* (ej översatt till svenska), MEMO/13/1059, 27.11.2013.

6 Representanter från näringslivsorganisationer uttryckte bland annat dessa farhågor vid ett möte som anordnades kort efter Schrems-domen av vice ordförande Ansip och kommissionärerna Jourová och Oettinger den 14 oktober. Se kommissionens dagliga nyheter (Daily News) den 14.10.2015 (MEX/15/5840). Se även *Open letter on the implementation of the CJEU Judgement on Case C-362/14 Maximillian Schrems v Data Protection Commissioner* (ej översatt till svenska) av den 13 oktober 2015 till kommissionens ordförande Jean-Claude Juncker och undertecknat av många näringslivsorganisationer och företag i EU och

behov att klargöra under vilka förhållanden som sådana överföringar fortfarande kan ske. Detta föranledde artikel 29-gruppen – det oberoende rådgivande organ som samlar företrädare för alla dataskyddsmyndigheter i medlemsstaterna samt Europeiska datatillsynsmannen – att den 16 oktober göra ett uttalande[7] om de första slutsatser som kan dras från domen. Uttalandet innehöll bland annat följande vägledning för dataöverföringar:

- Dataöverföringar kan inte längre baseras på kommissionens ogiltigförklarade safe harbour-beslut.

- Standardavtalsklausuler och bindande företagsregler kan under tiden användas som grundval för dataöverföringar, men artikel 29-gruppen kommer att fortsätta att analysera domens betydelse för dessa alternativa verktyg.

I uttalandet uppmanades medlemsstater och EU-institutioner att inleda samtal med amerikanska myndigheter i syfte att finna rättsliga och tekniska lösningar för dataöverföringar. Förhandlingarna för att nå fram till ett nytt safe harbour kunde enligt artikel 29-gruppen vara en del av denna lösning.

Artikel 29-gruppen meddelade att om man vid slutet av januari 2016 inte nått fram till en lösning tillsammans med de amerikanska myndigheterna, samt beroende på bedömningen av alternativa verktyg för dataöverföringar, kommer dataskyddsmyndigheterna att vidta alla nödvändiga och lämpliga åtgärder, inklusive koordinerade verkställighetsåtgärder.

Slutligen betonade artikel 29-gruppen att dataskyddsmyndigheterna, EU:s institutioner, medlemsstaterna och företagen har ett gemensamt ansvar för att hitta hållbara lösningar för att tillämpa domstolens dom. I synnerhet uppmanade gruppen företag att överväga att införa juridiska och tekniska lösningar för att minimera möjliga risker som de står inför vid överföring av data.

Detta meddelande påverkar inte dataskyddsmyndigheternas befogenheter och skyldigheter att fullständigt oberoende utreda huruvida sådana överföringar är lagenliga[8]. Det fastställer inte några bindande regler och erkänner till fullo de nationella domstolarnas befogenheter att tolka den tillämpliga lagstiftningen och, där så krävs, framställa en begäran om förhandsavgörande till EU-domstolen. Meddelandet kan inte heller ligga till grund för individuella eller kollektiva lagliga rättigheter eller anspråk.

Förenta staterna: http://www.digitaleurope.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&EntryId=1045&PortalId=0&TabId=353.

7 Uttalande från artikel 29-gruppen, tillgängligt på internet på följande adress: http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf.

8 Se artikel 8.3 i stadgan om de grundläggande rättigheterna och artikel 16.2 i EUF-fördraget. Detta oberoende betonas även av domstolen i Schrems-domen.

2. ALTERNATIVA GRUNDVALAR FÖR ÖVERFÖRING AV PERSONUPPGIFTER TILL FÖRENTA STATERNA

Reglerna om internationella dataöverföringar i direktiv 95/46/EG baseras på en tydlig åtskillnad mellan å ena sidan överföringar till tredjeländer som garanterar en adekvat skyddsnivå (artikel 25 i direktivet) och å andra sidan överföringar till tredjeländer som inte har funnits garantera en adekvat skyddsnivå (artikel 26 i direktivet).

Schrems-domen tar upp de villkor under vilka kommissionen enligt artikel 25.6 i direktiv 95/46/EG kan fastställa att ett tredjeland erbjuder en adekvat skyddsnivå.

Om det tredjeland till vilket personuppgifterna ska överföras från EU inte har funnits garantera denna adekvata skyddsnivå, anger artikel 26 i direktiv 95/46/EG ett antal alternativa grundvalar på vilka överföringar likväl kan ske. I synnerhet får överföringar ske då den som är ansvarig för att bestämma ändamålen och medlen för behandlingen av personuppgifter, nedan kallad *den registeransvariga*:

– ställer tillräckliga garantier, enligt artikel 26.2 i direktiv 95/46/EG, för att privatliv och enskilda personers grundläggande fri- och rättigheter skyddas samt för utövningen av de rättigheterna. Sådana garantier kan ges genom avtalsklausuler som är bindande för exportören och importören av data (se avsnitt 2.1 och 2.2 nedan). Dessa innefattar standardavtalsklausuler som utfärdats av kommissionen och, för överföringar mellan de olika enheterna i en multinationell koncern, bindande företagsregler som har godkänts av dataskyddsmyndigheter; eller

– grundar sig på något av undantagen som uttryckligen anges under bokstäverna a) till f) i artikel 26.1 i direktiv 95/46/EG (se avsnitt 2.3 nedan).

Jämfört med beslut om adekvat skyddsnivå, som vilar på en sammantagen bedömning av ett givet tredjelands system och i princip kan omfatta alla överföringar till det systemet, kan dessa alternativa grundvalar för överföringar ha såväl ett mer begränsat tillämpningsområde (eftersom de bara gäller för specifika dataflöden) som ett bredare tillämpningsområde (eftersom de inte nödvändigtvis är begränsade till ett specifikt land). De är tillämpliga för dataflöden som sker från specifika enheter som har valt att använda sig av någon av möjligheterna som erbjuds i artikel 26 i direktiv 95/46/EG. Vid överföringar som sker på sådana grundvalar saknar dataexportörer och dataimportörer möjligheten att vila sig på en konstaterat adekvat skyddsnivå för ett tredjeland i form av ett kommissionsbeslut. De bär därför själva ansvaret för att garantera att överföringarna sker i enlighet med kraven i direktivet.

2.1. Avtalslösningar

Såsom framhävs av artikel 29-gruppen måste avtalsklausulerna, för att erbjuda tillräckliga garantier enligt artikel 26.2 i direktiv 95/46/EG, ”på ett tillfredsställande sätt kompensera att det generellt saknas en adekvat skyddsnivå genom att omfatta sådana viktiga delar i skyddet

som saknas i varje enskilt fall”[9]. För att underlätta användningen av sådana verktyg vid internationella överföringar har kommissionen i enlighet med artikel 26.4 i direktivet godkänt fyra uppsättningar av standardavtalsklausuler som anses uppfylla kraven i artikel 26.2 i direktivet. Två av uppsättningarna rör överföring mellan registeransvariga[10], medan de andra två rör överföringar mellan en registeransvarig och en registerförare som agerar enligt dennas anvisningar[11]. Var och en av dessa uppsättningar av avtalsklausuler föreskriver de respektive skyldigheterna för dataexportörer och dataimportörer. Till dessa hör skyldigheter som bland annat rör säkerhetsåtgärder, information till den registrerade vid överföring av känsliga uppgifter, underrättande av dataexportören om begäran om åtkomst från tredjeländernas brottsbekämpande myndigheter eller vid oavsiktlig eller obehörig åtkomst, liksom de registrerades rätt till åtkomst, rättelse och radering av sina personuppgifter, såväl som regler om kompensering för den registrerade vid skada som beror på att någon av parterna har brutit mot standardavtalsklausulerna. Modellerna för avtalsklausuler kräver även att registrerade i EU ska ha möjligheten att inför en dataskyddsmyndighet eller en domstol i den medlemsstat där dataexportören är etablerad åberopa de rättigheter som de enligt avtalsklausulerna har som en berättigad tredje part[12]. Dessa rättigheter och skyldigheter är nödvändiga i avtalsklausuler eftersom man, till skillnad från när kommissionen har konstaterat en adekvat skyddsnivå, inte kan utgå från att dataimportören i tredjelandet är föremål för ett adekvat system för övervakning och verkställighet av dataskyddsregler.

Eftersom kommissionens beslut är bindande i sin helhet i medlemsstaterna innebär införlivandet av standardavtalsklausulerna i avtal att nationella myndigheter i princip är skyldiga att acceptera de klausulerna. Av det skälet får de inte vägra överföringen av data till ett tredjeland enbart på grund av att dessa standardavtalsklausuler inte ger tillräckliga garantier. Detta påverkar inte deras befogenhet att utreda dessa klausuler mot bakgrund av de krav som domstolen angett i Schrems-domen. Vid tvivel bör de ta ett fall till en nationell domstol som i sin tur kan framställa en begäran om förhandsavgörande till EU-domstolen. Medan det inte finns något krav på nationellt förhandsgodkännande för att fullfölja överföringen i de flesta medlemsstaters lagstiftning som genomför direktiv 95/45/EG, har vissa medlemsstater ett system för anmälan och/eller förhandsgodkännande av användningen av standardavtalsklausulerna. I dessa fall måste den nationella dataskyddsmyndigheten jämföra de klausuler som ett avtal faktiskt innehåller med standardavtalsklausulerna och

---

9 Se artikel 29-gruppen, *Överföring av personuppgifter till tredje land: tillämpning av artiklarna 25 och 26 i EU:s dataskyddsdirektiv*, arbetsdokument 12, den 24 juli 1998, s. 15.

10 Kommissionens beslut 2001/497/EG av den 15 juni 2001 om standardavtalsklausuler för överföring av personuppgifter till tredje land enligt direktiv 95/46/EG, EGT L 181, 4.7.2001, s. 19, och kommissionens beslut 2004/915/EG av den 27 december 2004 om ändring av beslut 2001/497/EG om standardavtalsklausuler för överföring av personuppgifter till tredje land, EUT L 385, 29.12.2004, s. 74.

11 Kommissionens beslut 2002/16/EG av den 27 december 2001 om standardavtalsklausuler för överföring av personuppgifter till registerförare etablerade i tredje land i enlighet med direktiv 95/46/EG, EGT L 6, 10.1.2002, s. 52, och kommissionens beslut 2010/87/EU av den 5 februari 2010 om standardavtalsklausuler för överföring av personuppgifter till registerförare etablerade i tredjeland i enlighet med Europaparlamentets och rådets direktiv 95/46/EG, EUT L 39, 12.2.2010, s. 5. Det tidigare beslutet, som upphävdes genom det senare, gäller bara för avtal som ingicks före den 15 maj 2010.

12 Se t.ex. skäl 6 i kommissionens beslut 2004/915/EG och klausul 7 i bilagan till kommissionens beslut 2010/87/EU.

kontrollera att det inte har gjorts några ändringar[13]. Om klausulerna har använts utan ändringar[14] kommer ett godkännande i princip[15] att ges automatiskt[16]. Som förklaras närmare nedan (se avsnitt 2.4) påverkar detta inte ytterligare åtgärder som dataexportören kan behöva vidta, i synnerhet om information emottas från dataimportören om ändringar i tredjelandets rättssystem som kan förhindra dataimportören från att fullgöra sina förpliktelser enligt avtalet. Vid tillämpningen av standardavtalsklausulerna är såväl dataexportörer som – i och med att de ingår avtalet – dataimportörer under dataskyddsmyndigheters tillsyn.

Antagandet av standardavtalsklausuler hindrar inte företag från att använda sig av andra verktyg, såsom avtalsvillkor för särskilda ändamål, för att visa att deras överföringar sker med tillräckliga garantier enligt artikel 26.2 i direktiv 95/46/EG. I enlighet med artikel 26.2 i direktivet måste dessa godkännas av nationella myndigheter i det enskilda fallet. Vissa dataskyddsmyndigheter har tagit fram vägledning på detta fält, däribland i form av standardiserade avtal och detaljerade regler som ska följas vid formuleringen av dataöverföringsklausuler. De flesta avtal som för närvarande används av företag för utförandet av internationella dataöverföringar är emellertid baserade på standardavtalsklausuler som kommissionen godkänt[17].

2.2. Överföringar inom en koncern

För att överföra personuppgifter från EU till andra företag i koncernen utanför EU i enlighet med kraven i artikel 26.2 i direktiv 95/46/EG kan ett multinationellt företag anta bindande företagsregler. Denna typ av förfarande ger en grundval bara för överföringar inom koncernen.

Bindande företagsregler gör det möjligt att överföra personuppgifter fritt mellan de olika enheterna i en koncern globalt – utan att det krävs ett avtal mellan varje koncernenhet –

---

13 I förslaget till en allmän uppgiftsskyddsförordning (COM(2012) 11 final) föreskrivs det att överföringar som grundar sig på standardavtalsklausuler eller bindande företagsregler, i den utsträckning som dessa har antagits av kommissionen eller i enlighet med den planerade mekanismen för enhetlighet, inte ska kräva något ytterligare godkännande.

14 Användningen av standardavtalsklausuler hindrar emellertid inte parterna från att komma överens om ytterligare klausuler, så länge som de inte står i direkt eller indirekt motsättning till de klausuler som godkänts av kommissionen eller inskränker de registrerades grundläggande fri- och rättigheter. Se Europeiska kommissionen, *Frequently Asked Questions Relating to Transfers of Personal Data from the EU/EEA to Third Countries* (ej översatt till svenska), FAQ B.1.9, s. 28, tillgängligt på internet på följande adress: http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf.

15 Om en dataskyddsmyndighet hyser tvivel rörande standardavtalsklausulers förenlighet med kraven i direktivet, bör den ta upp frågan i en nationell domstol som då kan framställa en begäran om förhandsavgörande till EU-domstolen (jfr punkterna 51, 52, 64 och 65 i Schrems-domen).

16 Artikel 29-gruppen har etablerat ett specifikt samarbetsförfarande mellan dataskyddsmyndigheter för godkännandet av avtalsklausuler som ett företag vill tillämpa i olika medlemsstater. Se artikel 29-gruppen, *Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on "Contractual clauses" Considered as compliant with the EC Model Clause*, arbetsdokument 226, 26 november 2014. Se även klausul 7 i bilagan till kommissionens beslut 2004/915/EG och klausul 10 i bilagan till kommissionens beslut 2010/87/EU.

17 Se artikel 29-gruppen, *Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on "Contractual clauses" Considered as compliant with the EC Model Clause*, arbetsdokument 226, 26 november 2014, s. 2.

samtidigt som man kan garantera att samma höga skyddsnivå för personuppgifter iakttas i hela koncernen genom en enda uppsättning bindande och verkställbara regler. En enda uppsättning regler medför ett enklare och effektivare system, som är enklare att tillämpa för personalen och lättare att förstå för de registrerade. För att hjälpa företag att utforma bindande företagsregler har artikel 29-gruppen har formulerat de materiella kraven (t.ex. begränsning av syfte, säkerhet vid behandling, transparent information till registrerade, restriktioner för vidare överföring utanför koncernen, individuell rätt till åtkomst, rättelse och motsättning) och förfarandekrav (t.ex. revisioner, övervakning av efterlevnad, hantering av klagomål, samarbete med dataskyddsmyndigheter, skadeståndsansvar och jurisdiktion) för bindande företagsregler baserade på EU:s normer för uppgiftsskydd[18]. Dessa regler är inte bara bindande för företag som ingår i koncernen, utan i likhet med standardavtalsklausulerna är de även verkställbara inom EU: individer vilkas uppgifter behandlas av en enhet i koncernen ska i egenskap av berättigade tredje parter kunna se till att de bindande företagsreglerna efterlevs genom att lämna in ett klagomål till en dataskyddsmyndighet och väcka talan vid en domstol i en medlemsstat. Därutöver måste de bindande företagsreglerna ange någon enhet inom EU som tar på sig ansvar för regelöverträdelser från alla andra medlemmar i koncernen utanför EU som är bundna av dessa regler.

Enligt de flesta av de lagar i medlemsstaterna som genomför direktivet måste dataöverföringar som sker på grundval av bindande företagsregler godkännas av dataskyddsmyndigheten i varje medlemsstat från vilken det multinationella företaget avser att överföra data. För att förenkla processen och göra den snabbare, och samtidigt minska bördan på sökande, har artikel 29-gruppen tagit fram ett standardiserat ansökningsformulär[19] och ett specifikt samarbetsförfarande mellan de berörda dataskyddsmyndigheterna[20] som innefattar att en ”ledande myndighet” utses som ska vara ansvarig för godkännandeförfarandet.

2.3. Undantag

I frånvaron av ett beslut om adekvat skyddsnivå enligt artikel 25.6 i direktiv 95/46/EG och oberoende av användningen av standardavtalsklausuler eller bindande företagsregler kan personuppgifter fortfarande överföras till enheter som är etablerade i ett tredjeland i den mån som något av undantagen i artikel 26.1 i direktiv 95/46/EG är tillämpligt:[21]

---

[18] Se artikel 29-gruppen, *Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules* (ej översatt till svenska), arbetsdokument 153, 24 juni 2008; *Working Document setting up a framework for the structure of Binding Corporate Rules* (ej översatt till svenska), arbetsdokument 154, 24 juni 2008; samt *Working Document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules* (ej översatt till svenska), arbetsdokument 155, 24 juni 2008.

[19] Artikel 29-gruppen, *Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data* (ej översatt till svenska), arbetsdokument 133, 10 januari 2007.

[20] Se artikel 29-gruppen, *Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on Adequate Safeguards Resulting From ”Binding Corporate Rules”* (ej översatt till svenska), arbetsdokument 107, 14 april 2005.

[21] I den utsträckning som andra bestämmelser i direktiv 95/46/EG innehåller ytterligare krav som är relevanta för tillämpningen av dessa undantag (till exempel begränsningarna i artikel 8 för behandlingen av känsliga uppgifter) måste dessa respekteras, något som artikel 29-gruppen har betonat. Se artikel 29-gruppen, *Arbetsdokument om en gemensam tolkning av artikel 26.1 i direktiv 95/46/EG av den 24 oktober 1995*, arbetsdokument 114, 25 november 2005, s. 8. Se även Europeiska kommissionen, *Frequently Asked*

– den registrerade har otvetydigt samtyckt till den planerade överföringen,

– överföringen är nödvändig för att fullgöra ett avtal mellan den registrerade och den registeransvariga eller för att genomföra åtgärder som föregår ett sådant avtal på den registrerades begäran,

– överföringen är nödvändig för att ingå eller fullgöra ett avtal mellan den registeransvariga och tredje man som ingås i den registrerades intresse,

– överföringen är nödvändig eller följer av lag på grund av viktiga allmänna intressen[22], eller för att kunna fastställa, göra gällande eller försvara rättsliga anspråk,

– överföringen är nödvändig för att skydda intressen som är av avgörande betydelse för den registrerade,

– överföringen görs från ett offentligt register som enligt lagar eller andra författningar är avsett att ge allmänheten information och som är tillgängligt antingen för allmänheten eller för var och en som kan styrka ett berättigat intresse, i den utsträckning som de i lagstiftningen angivna villkoren för tillgänglighet uppfylls i det enskilda fallet.

På dessa grundvalar möjliggörs undantag från det allmänna förbudet mot att överföra personuppgifter till enheter som är etablerade i ett tredjeland utan en adekvat skyddsnivå. I själva verket behöver dataexportören inte se till att dataimportören säkerställer adekvat skydd, och behöver i allmänhet inte inhämta något förhandsgodkännande för överföringen från de berörda nationella myndigheterna. Likväl anser artikel 29-gruppen att dessa undantag måste tolkas restriktivt på grund av deras undantagskaraktär[23].

Artikel 29-gruppen har utfärdat flera icke-bindande riktlinjer för tillämpningen av artikel 26.1 i direktiv 95/46/EG[24]. Till dem hör ett antal regler för ”bästa praxis” i syfte att vägleda dataskyddsmyndigheterna vid verkställighetsåtgärder[25]. I synnerhet rekommenderar gruppen

---

Questions Relating to Transfers of Personal Data from the EU/EEA to Third Countries (ej översatt till svenska), FAQ D.2, s. 50.

22 Detta kan till exempel innefatta överföringar av uppgifter mellan skattemyndigheter eller tullmyndigheter eller mellan socialförsäkringsmyndigheter (se skäl 58 i direktiv 95/46/EG). Överföringar mellan tillsynsmyndigheter på finansområdet kan även dra fördel av undantaget. Se artikel 29-gruppen, *Arbetsdokument: Överföring av personuppgifter till tredje land: tillämpning av artiklarna 25 och 26 i EU:s dataskyddsdirektiv*, arbetsdokument 12, 24 juli 1998, s. 23.

23 Se artikel 29-gruppen, *Arbetsdokument om en gemensam tolkning av artikel 26.1 i direktiv 95/46/EG av den 24 oktober 1995*, arbetsdokument 114, 25 november 2005, s. 6, 17.

24 Se artikel 29-gruppen, *Arbetsdokument: Överföring av personuppgifter till tredje land: tillämpning av artiklarna 25 och 26 i EU:s dataskyddsdirektiv*, arbetsdokument 12, 24 juli 1998; *Arbetsdokument om en gemensam tolkning av artikel 26.1 i direktiv 95/46/EG av den 24 oktober 1995*, arbetsdokument 114, 25 november 2005. Se även Europeiska kommissionen, *Frequently Asked Questions Relating to Transfers of Personal Data from the EU/EEA to Third Countries* (ej översatt till svenska), FAQ D.1 till D.9, s. 48–54.

25 Se artikel 29-gruppen, *Arbetsdokument om en gemensam tolkning av artikel 26.1 i direktiv 95/46/EG av den 24 oktober 1995*, arbetsdokument 114, 25 november 2005, s. 8–10.

att överföring av personuppgifter som kan anses vara av återkommande, omfångsrik eller strukturell natur ska utföras med tillräckliga garantier och i möjligaste mån inom en särskild rättslig ram såsom standardavtalsklausuler eller bindande företagsregler[26].

I det här meddelandet kommer kommissionen bara att ta upp de undantag som framstår som särskilt relevanta för överföringar i ett kommersiellt sammanhang efter ogiltigförklaringen av safe harbour-beslutet.

2.3.1. Överföringar som är nödvändiga för att fullgöra ett avtal eller för att genomföra åtgärder som föregår ett avtal på den registrerades begäran (artikel 26.1 b)

Detta undantag kan till exempel vara tillämpligt vid en hotellbokning eller när betalningsinformation överförs till ett tredjeland för att genomföra en banköverföring. I vart och ett av dessa fall anser artikel 29-gruppen emellertid att det måste finnas en ”nära och väsentlig förbindelse”, en ”direkt och objektiv förbindelse” mellan den registrerade och avtalets ändamål eller åtgärderna som föregår ett avtal (”nödvändighetstest”)[27]. Undantaget får inte heller tillämpas på överföringar av ytterligare information som inte är nödvändig för överföringens syfte, eller överföringar i ett annat syfte än att fullgöra avtalet (till exempel uppföljande marknadsföring)[28]. Gällande åtgärder som föregår ett avtal företrädde artikel 29-gruppen uppfattningen att dessa bara skulle omfatta situationer där den registrerade tar kontaktinitiativet (till exempel en begäran om information om en viss tjänst), och inte sådana som följer av den registeransvarigas marknadsföring[29].

2.3.2. Överföringar som är nödvändiga för att ingå eller fullgöra ett avtal mellan den registeransvariga och tredje man som ingås i den registrerades intresse (artikel 26.1 c)

Detta undantag kan till exempel vara tillämpligt när den registrerade är mottagare av en internationell banköverföring, eller när en resebyrå vidarebefordrar uppgifterna för en flygbokning till ett flygbolag. Även här ska nödvändighetstestet tillämpas och i detta fall krävs en nära och väsentlig förbindelse mellan den registrerades intresse och avtalets ändamål.

---

[26] Se artikel 29-gruppen, *Arbetsdokument om en gemensam tolkning av artikel 26.1 i direktiv 95/46/EG av den 24 oktober 1995*, arbetsdokument 114, 25 november 2005, s. 9. Enligt gruppen kan omfattande eller återkommande överföringar utföras på grundval av ett undantag bara när det i praktiken är omöjligt att använda sig av standardavtalsklausuler eller bindande företagsregler och där riskerna för de registrerade är små (t.ex. vid internationella penningöverföringar). Se även Europeiska kommissionen, *Frequently Asked Questions Relating to Transfers of Personal Data from the EU/EEA to Third Countries* (ej översatt till svenska), FAQ D.1, s. 49.

[27] Se artikel 29-gruppen, *Arbetsdokument om en gemensam tolkning av artikel 26.1 i direktiv 95/46/EG av den 24 oktober 1995*, arbetsdokument 114, 25 november 2005, s. 13. Se även *Yttrande 6/2002 om överlämnande av information ur flygbolagens passagerarlistor och övriga upplysningar till USA*, arbetsdokument 66, 24 oktober 2002.

[28] Se artikel 29-gruppen, *Arbetsdokument: Överföring av personuppgifter till tredje land: tillämpning av artiklarna 25 och 26 i EU:s dataskyddsdirektiv*, arbetsdokument 12, 24 juli 1998, s. 22; *Arbetsdokument om en gemensam tolkning av artikel 26.1 i direktiv 95/46/EG av den 24 oktober 1995*, arbetsdokument 114, 25 november 2005, s. 13.

[29] Se artikel 29-gruppen, *Arbetsdokument: Överföring av personuppgifter till tredje land: tillämpning av artiklarna 25 och 26 i EU:s dataskyddsdirektiv*, arbetsdokument 12, 24 juli 1998, s. 22.

2.3.3. Överföringar som är nödvändiga eller bindande enligt författning för att fastslå, göra gällande eller försvara rättsliga anspråk (artikel 26.1 d)

Detta undantag kan till exempel vara tillämpligt när ett företag behöver överföra uppgifter för att försvara sig mot ett rättsligt anspråk, eller för att göra gällande sådana anspråk inför domstol eller inför en myndighet. Liksom för de två föregående undantagen är detta föremål för nödvändighetstestet:[30] det ska finnas en nära förbindelse med rättssaker (inklusive administrativa ärenden).

Enligt artikel 29-gruppen kan undantaget bara tillämpas om internationella regler som styr samarbete i straffrättsliga eller civilrättsliga förfaranden som reglerar denna typ av överföring har följts, i synnerhet då de har sitt ursprung i bestämmelserna i Haagkonventionen av den 18 mars 1970 (”bevisupptagning”)[31].

2.3.4. Otvetydigt förhandssamtycke till den planerade överföringen (artikel 26.1 a)

Samtycke kan användas som grundval för dataöverföringar men ett antal överväganden bör beaktas. Eftersom samtycke måste ges till den ”planerade” överföringen fordras samtycke på förhand till den specifika överföringen (eller en specifik kategori av överföringar). Om den registrerade tillfrågas på internet har artikel 29-gruppen rekommenderat användning av rutor som den registrerade ska kryssa i (i stället för rutor som redan är ikryssade)[32]. Eftersom samtycket måste vara otvetydigt, skulle undantaget bli otillämpligt vid tvivel om huruvida det faktiskt har givits. Detta kommer sannolikt att innebära att många situationer där samtycke som mest är implicit (till exempel där någon har informerats om en överföring och inte invänt mot den) inte skulle omfattas. Undantaget kan däremot användas i fall där överföraren har direkt kontakt med den registrerade, den nödvändiga informationen kan ges på ett enkelt sätt och otvetydigt samtycke kan erhållas[33].

Därutöver måste enligt artikel 2 h i direktiv 95/46/EG samtycket vara frivilligt, specifikt och informerat. Enligt artikel 29-gruppen innebär det första kravet att varje form av ”påtryckning” kan göra samtycket ogiltigt. Detta är särskilt relevant i anställningssammanhang, där anställdas underordnade ställning och beroendeförhållande i normalfallet kommer att väcka

---

30 Se artikel 29-gruppen, *Arbetsdokument om en gemensam tolkning av artikel 26.1 i direktiv 95/46/EG av den 24 oktober 1995*, arbetsdokument 114, 25 november 2005, s. 15. Till exempel kan undantaget i anställningssammanhang inte användas för att överföra alla handlingar om anställda till koncernens moderbolag i ett tredjeland med motiveringen att rättsliga förfaranden kan bli möjliga i framtiden.

31 Haagkonventionen av den 18 mars 1970 om bevisupptagning i utlandet i mål och ärenden av civil och kommersiell natur, *öppnades för undertecknande* den 18 mars 1970, 23 U.S.T. 2555, 847 U.N.T.S. 241. Konventionen omfattar bland annat utlämnande av bevis före rättegång och begäran från den rättsliga myndigheten i en stat till den behöriga myndigheten i en annan stat om att erhålla bevis som ska användas i rättsliga förfaranden i den begärande staten.

32 Artikel 29-gruppen, *Arbetsdokument om en gemensam tolkning av artikel 26.1 i direktiv 95/46/EG av den 24 oktober 1995*, arbetsdokument 114, den 25 november 2005, s. 10–11, med hänvisning till *Yttrande 5/2004 om icke begärd kommunikation i marknadsföringssyfte enligt artikel 13 i direktiv 2002/58/EG*, arbetsdokument 90, den 27 februari 2004, punkt 3.2.

33 Se artikel 29-gruppen, *Arbetsdokument: Överföring av personuppgifter till tredje land: tillämpning av artiklarna 25 och 26 i EU:s dataskyddsdirektiv*, arbetsdokument 12, den 24 juli 1998, s. 22.

tvivel om samtycket[34]. Mer allmänt kan samtycke som ges av en registrerad som inte har haft möjlighet att göra ett verkligt val eller som har ställts inför ett fullbordat faktum inte anses vara giltigt[35].

Det är av stor vikt att de registrerade är tillräckligt informerade i förväg om att uppgifterna kan överföras utanför EU, till vilket tredjeland överföringen kan ske och under vilka villkor (dess syfte, mottagarens identitet samt uppgifter om denna osv.). Denna information ska ta upp den särskilda risken för att uppgifterna överförs till ett tredjeland där det inte finns adekvat skydd[36]. Som artikel 29-gruppen påpekar bör ett återtagande av den registrerades samtycke, om än det inte är retroaktivt, i princip omöjliggöra all vidare behandling av personuppgifterna[37]. Mot bakgrund av dessa begränsningar företräder artikel 29-gruppen ståndpunkten att det är osannolikt att samtycke kan ligga till grund för en adekvat ram på lång sikt för registeransvariga vid strukturerade överföringar[38].

2.4. Sammanfattning av alternativa grundvalar för överföringar av personuppgifter

Det framgår av det ovanstående att företag kan använda ett antal olika alternativa verktyg för att utföra sina internationella dataöverföringar till tredjeländer som inte bedöms garantera en adekvat skyddsnivå i den mening som avses i artikel 25.2 i direktiv 95/46/EG. Efter Schrems-domen har artikel 29-gruppen i synnerhet klargjort att standardavtalsklausuler och bindande företagsregler kan användas för att överföra uppgifter till Förenta staterna medan gruppen fortsätter sin bedömning och utan att det påverkar dataskyddsmyndigheters befogenhet att utreda enskilda fall[39]. Näringslivet har å sin sida reagerat på olika sätt på domen, bland annat genom att använda dessa alternativa verktyg som grundval för sina dataöverföringar[40].

---

[34] Artikel 29-gruppen, *Opinion 8/2001 on the processing of personal data in the employment context*, arbetsdokument 48, 13 september 2001, s. 3, 23 och 26. Arbetsgruppen anser att användningen av samtycke som grundval bör begränsas till de fall där arbetaren har ett verkligt fritt val och kan dra tillbaka sitt samtycke utan negativa konsekvenser. Se även artikel 29-gruppen, *Arbetsdokument om en gemensam tolkning av artikel 26.1 i direktiv 95/46/EG av den 24 oktober 1995*, arbetsdokument 114, 25 november 2005, s. 11.

[35] Se artikel 29-gruppen, *Arbetsdokument om en gemensam tolkning av artikel 26.1 i direktiv 95/46/EG av den 24 oktober 1995*, arbetsdokument 114, 25 november 2005, s. 11. Se även *Yttrande 6/2002 om överlämnande av information ur flygbolagens passagerarlistor och övriga upplysningar till USA*, arbetsdokument 66, 24 oktober 2002.

[36] Se artikel 29-gruppen, *Arbetsdokument: Överföring av personuppgifter till tredje land: tillämpning av artiklarna 25 och 26 i EU:s dataskyddsdirektiv*, arbetsdokument 12, 24 juli 1998, s. 22.

[37] Artikel 29-gruppen, *Yttrande 15/2011 om definitionen av begreppet "samtycke"*, arbetsdokument 187, 13 juli 2011, s. 9.

[38] Se artikel 29-gruppen, *Arbetsdokument om en gemensam tolkning av artikel 26.1 i direktiv 95/46/EG av den 24 oktober 1995*, arbetsdokument 114, 25 november 2005, s. 11.

[39] Se artikel 29-gruppens uttalande av den 16 oktober 2015 (ovanför fotnot 8).

[40] Ett antal multinationella företag har förklarat att de använder sig av alternativa verktyg som grundval för sina dataöverföringar till Förenta staterna. Se t.ex. uttalandena av Microsoft (http://blogs.microsoft.com/on-the-issues/2015/10/06/a-message-to-our-customers-about-eu-us-safe-harbor/) och Salesforce (http://www.salesforce.com/company/privacy/data-processing-addendum-faq.jsp). Andra amerikanska företag såsom Oracle har sagt att de erbjuder molnkunder möjligheten att spara sina uppgifter i Europa så att de inte överförs för att sparas någon annanstans: http://www.irishtimes.com/business/technology/oracle-keeps-european-data-within-its-eu-based-data-centres-1.2408505?mode=print&ot=example.AjaxPageLayout.ot

Det finns dock två viktiga villkor som behöver påpekas. För det första måste man komma ihåg att överföringar till ett tredjeland, oavsett den specifika rättsliga grund man vilar sig på, bara kan utföras lagenligt om uppgifterna ursprungligen har inhämtats och senare behandlats av den registeransvariga som är etablerad i EU i enlighet med de tillämpliga nationella lagar som genomför direktiv 95/46/EG. I direktivet står det uttryckligen att den behandling som sker före överföringen, liksom överföringen själv, helt och hållet måste ske i enlighet med de regler som medlemsstaterna har antagit för genomförande av direktivet[41]. För det andra är det när kommissionen inte har konstaterat en adekvat skyddsnivå den registeransvariga som ansvarar för att se till att de egna dataöverföringarna sker med tillräckliga garantier i enlighet med artikel 26.2 i direktivet. Denna bedömning måste göras på grundval av alla de förhållanden som har samband med överföringen i fråga. I synnerhet föreskriver både standardavtalsklausulerna och de bindande företagsreglerna att om dataimportören har skäl att tro att den tillämpliga lagstiftningen i mottagarlandet kan hindra den från att fullgöra sina förpliktelser ska den utan dröjsmål underrätta dataexportören i EU. I ett sådant läge är det upp till exportören att överväga att vidta lämpliga åtgärder för att säkerställa skyddet av personuppgifter[42]. Det kan därvid röra sig om allt från tekniska, organisatoriska, affärsmodellrelaterade och rättsliga åtgärder[43], till möjligheten att avbryta dataöverföringar eller häva avtalet. Under beaktande av alla omständigheter kring överföringen kan dataexportörer därför behöva tillämpa ytterligare garantier för att komplettera dem som redan ges enligt den tillämpliga rättsliga grunden för överföringen för att uppfylla kraven i artikel 26.2 i direktivet.

Efterlevnaden av sådana krav ska i sista hand bedömas av dataskyddsmyndigheter i det enskilda fallet som en del av deras tillsynsfunktioner, inklusive i samband med godkännandet av avtalsvillkor och bindande företagsregler eller på grundval av enskilda klagomål. Medan vissa dataskyddsmyndigheter har uttryckt tvivel om möjligheten att använda överföringsverktyg såsom standardavtalsklausuler och bindande företagsregler för transatlantiska dataflöden[44], har artikel 29-gruppen i sitt uttalande efter Schrems-domen meddelat att den kommer att fortsätta att analysera domens betydelse för andra

---

41 Se skäl 60 och artikel 25.1 i direktiv 95/46/EG.

42 Se t.ex. klausul 5 i bilagan till kommissionens beslut 2010/87/EU och artikel 29-gruppen, *Working Document setting up a framework for the structure of Binding Corporate Rules*, arbetsdokument 154, 24 juni 2008, s. 8.

43 Se t.ex. den vägledning som utfärdats av Europeiska unionens byrå för nät- och informationssäkerhet (Enisa): https://resilience.enisa.europa.eu/article-13/guideline-for-minimum-security-measures/Article_13a_ENISA_Technical_Guideline_On_Security_Measures_v2_0.pdf.

44 Se t.ex. det ståndpunktsdokument som utfärdats av de tyska dataskyddsmyndigheterna på federal och delstatlig nivå den 26.10.2015 i samband med en dataskyddskonferens: https://www.datenschutz.hessen.de/ft-europa.htm#entry4521. Man framhåller där att Schrems-domen innehåller ”stränga materiella krav” som såväl kommissionen som dataskyddsmyndigheterna måste respektera, och anger att de tyska dataskyddsmyndigheterna kommer att utvärdera lagenligheten hos dataöverföringar som sker på grundval av alternativa verktyg (standardavtalsklausuler, bindande företagsregler) och att de inte längre kommer att utfärda nya godkännanden för användningen av dessa verktyg. Samtidigt har enskilda tyska dataskyddsmyndigheter utfärdat tydliga varningar om att de alternativa verktygen för överföring genomgår juridisk granskning. Se t.ex. de ståndpunktsdokument som utfärdats av dataskyddsmyndigheterna i Schleswig-Holstein: https://www.datenschutzzentrum.de/artikel/981-ULD-Position-Paper-on-the-Judgment-of-the-Court-of-Justice-of-the-European-Union-of-6-October-2015,-C-36214.html och Rheinland-Pfalz: https://www.datenschutz.rlp.de/de/aktuell/2015/images/20151026_Folgerungen_des_LfDI_RLP_zum_EuGH-Urteil_Safe_Harbor.pdf.

överföringsverktyg[45]. Detta påverkar inte dataskyddsmyndigheters befogenheter att utreda enskilda fall och utöva sina befogenheter för att skydda individer.

3. SCHREMS-DOMENS KONSEKVENSER FÖR BESLUT OM ADEKVAT SKYDDSNIVÅ

I sin dom ifrågasätter domstolen inte kommissionens befogenhet enligt artikel 25.6 i direktiv 95/46/EG att konstatera att ett tredjeland garanterar en adekvat skyddsnivå, så länge de krav som domstolen fastställt respekteras. I enlighet med dessa krav förtydligas och redogörs i förslaget till en allmän uppgiftsskyddsförordning[46] från 2012, som ska ersätta direktiv 95/46/EG, de villkor enligt vilka beslut om adekvat skyddsnivå kan antas. I Schrems-domen klargjorde domstolen även att när kommissionen antar ett beslut om adekvat skyddsnivå är det bindande för alla medlemsstater och deras organ, inklusive dataskyddsmyndigheterna, ända tills det återtas, upphävs eller ogiltigförklaras av domstolen, som har exklusiv behörighet i detta avseende. Dataskyddsmyndigheterna förblir behöriga att enligt artikel 28.4 i direktiv 95/46/EG utreda om dataöverföringen uppfyller kraven i direktivet (såsom det tolkas av domstolen), men kan inte nå fram till en definitiv slutsats. Medlemsstaterna måste i stället se till att det är möjligt att föra ärendet till en nationell domstol, som i sin tur kan aktivera EU-domstolens behörighet genom att begära ett förhandsavgörande i enlighet med artikel 267 i EUF-fördraget.

Vidare har domstolen uttryckligen bekräftat att den omständigheten att ett tredjeland tillämpar ett system med självcertifiering (såsom är fallet med safe harbour-principerna om integritetsskydd) inte utesluter att en adekvat skyddsnivå kan konstateras enligt artikel 25.6 i direktiv 95/46/EG, så länge det finns effektiva spårnings- och kontrollmekanismer som gör det praktiskt möjligt att upptäcka och beivra eventuella överträdelser av dataskyddsreglerna.

Då safe harbour-beslutet inte innehöll tillräckliga resultat i detta avseende ogiltigförklarade domstolen beslutet. Det är därför tydligt att dataöverföringar mellan EU och Förenta staterna inte längre kan utföras på grundval av det beslutet, dvs. enbart genom att åberopa iakttagande av safe harbour-principerna om integritetsskydd. Eftersom dataöverföringar till ett tredjeland som inte garanterar en adekvat skyddsnivå (eller åtminstone där detta inte har fastställts i ett kommissionsbeslut enligt artikel 25.6 i direktiv 95/46/EG) i princip är förbjudna[47], kommer de bara att vara lagenliga i de fall då dataexportören kan förlita sig på något av de alternativa verktyg som beskrivs ovan i avsnitt 2. I avsaknad av ett beslut om adekvat skyddsnivå är det

---

45 Se artikel 29-gruppens uttalande av den 16 oktober 2015 (ovanför fotnot 8).

46 Europeiska kommissionen, förslag till Europaparlamentets och rådets förordning om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (allmän uppgiftsskyddsförordning). Se även Europaparlamentet, lagstiftningsresolution av den 12 mars 2014 om förslaget till Europaparlamentets och rådets förordning om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (allmän uppgiftsskyddsförordning), COM(2012)0011 – C7-0025/2012 – 2012/0011(COD); rådet, förslag till Europaparlamentets och rådets förordning om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (allmän uppgiftsskyddsförordning), utarbetande av allmänna riktlinjer, 9565/15. Förslaget är för närvarande i lagstiftningsprocessens sista stadium.

47 Se skäl 57 i direktiv 95/46/EG.

dataexportörens ansvar – under dataskyddsmyndigheternas tillsyn – att se till att villkoren för att förlita sig på (något av) dessa verktyg är uppfyllda för den specifika dataöverföringen.

Domens räckvidd är begränsad till kommissionens safe harbour-beslut. Emellertid innehåller alla de andra besluten om adekvat skyddsnivå[48] en begränsning av dataskyddsmyndigheternas befogenheter som är identisk med den i artikel 3 i safe harbour-beslutet som domstolen ansåg vara ogiltig[49]. Kommissionen kommer nu att dra de nödvändiga slutsatserna av domen, genom att inom kort förbereda ett beslut som ska antas i enlighet med det tillämpliga kommittéförfarandet och som ska ersätta den bestämmelsen i alla befintliga beslut om adekvat skyddsnivå. Kommissionen ska även utföra en regelbunden utvärdering av befintliga och framtida beslut om adekvat skyddsnivå, vilket innefattar en återkommande gemensam översyn av hur de fungerar tillsammans med de behöriga myndigheterna i det aktuella tredjelandet.

4. SLUTSATS

Såsom bekräftats av artikel 29-gruppen kan alternativa verktyg som tillåter dataflöden fortfarande användas av företag för lagenliga dataöverföringar till tredjeländer som Förenta staterna. Kommissionen anser dock att ett förnyat och sunt system för överföring av personuppgifter till Förenta staterna förblir en huvudprioritering. Ett sådant system är den mest omfattande lösningen för att garantera effektiv kontinuitet i skyddet av EU-medborgares personuppgifter när de överförs till Förenta staterna. Det är även den bästa lösningen för transatlantisk handel eftersom den erbjuder en överföringsmekanism som är enklare, kräver mindre arbete och därmed är billigare, i synnerhet för små och medelstora företag.

Redan 2013 inledde kommissionen förhandlingar med Förenta staternas regering rörande ett nytt system för transatlantiska dataöverföringar baserat på kommissionens 13 rekommendationer[50]. Det har skett betydande framsteg i att sammanföra de båda sidornas synsätt, till exempel gällande stärkt övervakning och tillsyn av safe harbour-principerna från Förenta staternas handelsministeriums (*Department of Commerce*) respektive den federala konkurrensmyndighetens (*Federal Trade Commission*) sida, ökad transparens för konsumenter när det gäller deras rätt till dataskydd, förenklad och billigare tillgång till rättslig prövning vid klagomål samt tydligare regler om vidare överföring från safe harbour-företag till företag som inte är anslutna till safe harbour (t.ex. för behandlingsändamål eller för behandling utförd av underentreprenörer). När safe harbour-beslutet nu har förklarats ogiltigt har kommissionen intensifierat samtalen med Förenta staternas regering för att se till att de rättsliga krav som formulerats av domstolen beaktas. Kommissionens mål är att nå fram till en slutsats i dessa diskussioner och uppnå detta inom tre månader.

---

48 I nuläget har beslut om adekvat skyddsnivå antagits för följande länder: Andorra, Argentina, Kanada, Färöarna, Guernsey, Isle of Man, Israel, Jersey, Nya Zeeland, Schweiz och Uruguay. Se: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm.

49 Se punkterna 99–104 i Schrems-domen.

50 Se fotnot 4.

Fram till dess att den förnyade transatlantiska ramen är på plats måste företagen förlita sig på de alternativa verktyg för överföring som är tillgängliga. Detta alternativ medför emellertid ansvarsområden för dataexportörer, under dataskyddsmyndigheternas tillsyn.

Till skillnad från en situation där kommissionen har funnit att ett tredjeland garanterar en adekvat skyddsnivå som dataexportörer kan förlita sig på vid dataöverföringar från EU, förblir de senare ansvariga för att bekräfta att personuppgifterna skyddas effektivt när alternativa verktyg används. Detta kan innebära att man måste vidta lämpliga åtgärder där så krävs.

I detta avseende får dataskyddsmyndigheterna en central roll. Som de primära tillsynsmyndigheterna för de registrerades grundläggande rättigheter har dataskyddsmyndigheterna både ansvar för och befogenhet att övervaka dataöverföringar från EU till tredjeländer på ett fullständigt oberoende sätt. Kommissionen uppmanar de registeransvariga att samarbeta med dataskyddsmyndigheterna, vilket hjälper dem att utföra sina tillsynsuppgifter på ett effektivt sätt. Kommissionen kommer att fortsätta att samarbeta nära med artikel 29-gruppen för att säkerställa en enhetlig tillämpning av EU:s dataskyddslagstiftning.