



18/SV

WP254 rev. 01

Artikel 29-arbetsgruppen

Referensram för adekvat skyddsnivå

Antagen den 28 november 2017

Senast reviderad och antagen den 6 februari 2018

Denna arbetsgrupp inrättades genom artikel 29 i direktiv 95/46/EG. Den är ett oberoende rådgivande EU-organ i frågor som rör uppgiftsskydd och integritetsskydd. Arbetsuppgifterna finns beskrivna i artikel 30 i direktiv 95/46/EG och artikel 15 i direktiv 2002/58/EG.

Arbetsgruppens sekretariat finns hos direktorat C (Grundläggande rättigheter och unionsmedborgarskap) vid Europeiska kommissionen, Generaldirektoratet för rättsliga frågor, B-1049 Bryssel, Belgien, Kontor MO-59 02/013.

Webbplats:

http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358&tpa_id=6936http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358&tpa_id=6936

Inledning

Arbetsgruppen för EU:s dataskyddsmyndigheter¹ (artikel 29-arbetsgruppen) har tidigare publicerat ett arbetsdokument om överföring av personuppgifter till tredje land (WP12)². I och med att direktivet ersätts av EU:s allmänna dataskyddsförordning (GDPR)³ väljer artikel 29-arbetsgruppen att se över WP12, gruppens tidigare vägledning, för att uppdatera den utifrån den nya lagstiftningen och ny rättspraxis hos Europeiska unionens domstol⁴.

Syftet med det här arbetsdokumentet är att uppdatera kapitel ett i WP12 som gäller den centrala frågan om adekvat skyddsnivå för personuppgifter i ett tredjeland, ett territorium eller en eller flera specificerade sektorer i tredjelandet eller i en internationell organisation (nedan kallat tredjeländer eller internationella organisationer). Det här dokumentet kommer kontinuerligt att ses över och vid behov uppdateras under de kommande åren, baserat på den praktiska erfarenhet som erhållits genom tillämpningen av den allmänna dataskyddsförordningen. Kapitel 2 (Att tillämpa tillvägagångssättet på de länder som ratificerat Europarådets konvention 108) och kapitel 3 (Att tillämpa tillvägagångssättet på branschens självreglering) i WP12 bör uppdateras i ett senare skede.

Det här arbetsdokumentet är helt och hållet inriktat på beslut om adekvat skyddsnivå, som utgörs av genomförandeakter⁵ från kommissionen enligt artikel 45 i den allmänna dataskyddsförordningen. Andra aspekter av överföringar av personuppgifter till tredjeländer och internationella organisationer kommer att undersökas i senare arbetsdokument som kommer att publiceras separat (bindande företagsbestämmelser och undantag).

Syftet med detta dokument är att ge vägledning åt kommissionen och artikel 29-arbetsgruppen, inom ramen för den allmänna dataskyddsförordningen, kring bedömning av skyddsnivåer för personuppgifter i tredjeländer och internationella organisationer genom att fastställa de grundprinciper för dataskydd som måste finnas i den rättsliga ramen för ett tredjeland eller en internationell organisation för att säkerställa väsentlig likvärdighet med EU:s rättsliga ramar. Därutöver kan dokumentet fungera som vägledning för tredjeländer och internationella organisationer som är intresserade av att uppnå en adekvat skyddsnivå. Principerna som anges i detta arbetsdokument vänder sig dock inte direkt till personuppgiftsansvariga eller personuppgiftsbiträden.

Detta dokument består av fyra kapitel:

Kapitel 1: Generell information om begreppet adekvat skyddsnivå

Kapitel 2: Förfaranden gällande bedömningar om adekvat skyddsnivå inom ramen för den allmänna dataskyddsförordningen

Kapitel 3: Allmänna principer för dataskydd. I detta kapitel finns grundläggande allmänna principer för dataskydd, som används för att säkerställa att skyddsnivån för personuppgifter i ett tredjeland eller en internationell organisation väsentligen är likvärdig med den som fastställs genom EU-lagstiftningen.

Kapitel 4: Grundläggande garantier för åtkomst i samband med brottsbekämpning och nationell säkerhet för att begränsa ingreppen i de grundläggande rättigheterna. I detta kapitel anges de grundläggande garantierna för åtkomst gällande brottsbekämpning och nationell säkerhet, i enlighet med domen från Europeiska unionens domstol i Schrems-målet 2015 och baserat på artikel 29-arbetsgruppens arbetsdokument om grundläggande garantier som antogs 2016.

¹Som inrättades genom artikel 29 i EU:s dataskyddsdirektiv 95/46/EG.

²WP12, Arbetsdokument – Överföring av personuppgifter till tredje land: tillämpning av artiklarna 25 och 26 i EU:s dataskyddsdirektiv, som antogs av arbetsgruppen den 24 juli 1998.

³Europaparlamentets 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 (allmän dataskyddsförordning) (Text av betydelse för EES).

⁴Däribland domstolens dom av den 6 oktober 2015, Maximilian Schrems/Data Protection Commissioner, C-362/14, ECLI:EU:C:2015:650.

⁵Se de relevanta artiklarna 45.3 och 93.2 i den allmänna dataskyddsförordningen för närmare information om genomförandeakterna.

Kapitel 1: Generell information om begreppet adekvat skyddsnivå

I artikel 45.1 i den allmänna dataskyddsförordningen anges principen att överföringar av personuppgifter till ett tredjeland eller en internationell organisation endast får äga rum om tredjelandet, territoriet eller en eller flera specificerade sektorer i tredjelandet eller den internationella organisationen i fråga säkerställer en adekvat skyddsnivå.

Begreppet "adekvat skyddsnivå" som fanns med redan i direktiv 95/46/EG har vidareutvecklats av Europeiska unionens domstol. Det är i detta sammanhang viktigt att påminna om den princip som fastställdes av domstolen i Schrems-målet, närmare bestämt att medan skyddsnivån i tredjelandet måste vara väsentligen likvärdig med den som garanteras inom EU gäller att "de medel som detta tredjeland använder för att säkerställa en sådan skyddsnivå kan skilja sig från dem som används inom [EU]"⁶. Därför är målet inte att punkt för punkt efterlikna EU-lagstiftningen utan att fastställa de grundläggande och avgörande kraven i denna lagstiftning.

Syftet med kommissionens beslut om adekvat skyddsnivå är att formellt bekräfta, med bindande verkan för medlemsstaterna⁷, att skyddsnivån för personuppgifter i ett tredjeland eller en internationell organisation är väsentligen likvärdig med skyddsnivån för personuppgifter i EU⁸. Adekvat skyddsnivå kan uppnås genom en kombination av rättigheter för de registrerade och skyldigheter för de som behandlar personuppgifter, eller som utövar kontroll över sådan behandling, och övervakning av oberoende organ. Bestämmelser om skydd av personuppgifter är dock endast effektiva om de är verkställbara och följs i praktiken. Det är därför nödvändigt att inte bara se till innehållet i bestämmelserna för överföring av personuppgifter till ett tredjeland eller en internationell organisation utan också till de mekanismer som har inrättats för att säkerställa att dessa bestämmelser är verkningfulla. Effektiva verkställighetsmekanismer är av avgörande betydelse för att få effektiva bestämmelser om skydd av personuppgifter.

I artikel 45.2 i den allmänna dataskyddsförordningen fastställs de element som kommissionen ska beakta vid bedömningen av om en adekvat skyddsnivå föreligger i ett tredjeland eller en internationell organisation.

Till exempel ska kommissionen beakta rättsstatsprincipen, respekten för de mänskliga rättigheterna och de grundläggande friheterna, relevant lagstiftning, huruvida det finns en eller flera effektivt fungerande oberoende tillsynsmyndigheter i tredjelandet och vilka internationella åtaganden tredjelandet eller den internationella organisationen har gjort.

Det är därför uppenbart att en analys av vad som är en adekvat skyddsnivå endast blir meningsfull om den beaktar följande två grundläggande element: innehållet i de gällande bestämmelserna och instrumenten för att säkerställa att dessa tillämpas på ett effektivt sätt. Det ligger på kommissionens ansvar att regelbundet kontrollera att de bestämmelser som finns är effektiva i praktiken.

Själva kärnan av innehållsmässiga principer för skydd av personuppgifter och av krav i fråga om förfarande- och verkställandemekanismer, som kan ses som ett minimikrav för att skyddet ska vara adekvat, erhålls från EU-stadgan om de grundläggande rättigheterna och den allmänna dataskyddsförordningen. Dessutom bör hänsyn tas till andra internationella avtal om dataskydd, till exempel konventionen om skydd för enskilda vid automatisk behandling av personuppgifter (konvention 108)⁹.

⁶ Domstolens dom av den 6 oktober 2015, Maximilian Schrems/Data Protection Commissioner, C-362/14, ECLI:EU:C:2015:650, punkterna 73 och 74.

⁷ Artikel 288.2 i fördraget om Europeiska unionens funktionssätt.

⁸ Domstolens dom av den 6 oktober 2015, Maximilian Schrems/Data Protection Commissioner, C-362/14, ECLI:EU:C:2015:650, punkt 52.

⁹ Skäl 105 i den allmänna dataskyddsförordningen.

Hänsyn ska även tas till den rättsliga ramen för offentliga myndigheters tillgång till personuppgifter. Ytterligare vägledning inom detta område finns i arbetsdokumentet WP237 (arbetsdokumentet om grundläggande garantier)¹⁰ som behandlar skyddsåtgärder i samband med övervakning.

Allmänna bestämmelser om uppgiftsskydd och integritetsskydd i tredjelandet är inte tillräckliga. Tvärtom måste specifika bestämmelser som behandlar konkreta behov gällande praktiskt relevanta aspekter av rätten till uppgiftsskydd ingå i tredjelandets eller den internationella organisationens rättsliga ram. Dessa bestämmelser måste vara verkställbara.

Kapitel 2: Förfaranden gällande bedömningar om adekvat skyddsnivå inom ramen för den allmänna dataskyddsförordningen

För att Europeiska dataskyddsstyrelsen ska kunna fullgöra sin uppgift att lämna råd till kommissionen enligt artikel 70.1 s i den allmänna dataskyddsförordningen ska Europeiska dataskyddsstyrelsen få tillgång till relevant dokumentation, inklusive relevant korrespondens och de bedömningar som gjorts av kommissionen. I de fall då den rättsliga ramen är komplex bör eventuella rapporter som tagits fram om skyddsnivån för uppgifter i tredjelandet eller den internationella organisationen innefattas. Under alla omständigheter ska informationen som lämnas av kommissionen vara uttömmande och göra det möjligt för Europeiska dataskyddsstyrelsen att göra en egen bedömning av skyddsnivån för uppgifter i tredjelandet. Europeiska dataskyddsstyrelsen ska avge ett yttrande om kommissionens bedömningar inom utsatt tid och identifiera eventuella brister i den rättsliga ramen för adekvat skyddsnivå. Europeiska dataskyddsstyrelsen ska även sträva efter att föreslå förändringar eller tillägg för att åtgärda eventuella brister.

Enligt artikel 45.4 i den allmänna dataskyddsförordningen ligger det på kommissionens ansvar att fortlöpande övervaka utveckling som kan påverka hur väl beslut om adekvat skyddsnivå fungerar.

I artikel 45.3 i den allmänna dataskyddsförordningen fastställs att en regelbunden översyn måste utföras minst vart fjärde år. Detta ska dock betraktas som en generell tidsram som måste anpassas för varje tredjeland eller internationell organisation som omfattas av ett beslut om adekvat skyddsnivå. Beroende på de specifika omständigheter som råder kan det krävas att översynen utförs med tätare intervall. Dessutom kan incidenter eller annan information om eller ändringar i den rättsliga ramen för tredjelandet eller den internationella organisationen i fråga vara grund för att utföra en översyn tidigare än planerat. Det förefaller även lämpligt att ha en första översyn av ett helt nytt beslut om adekvat skyddsnivå relativt tidigt, och att sedan gradvis justera översynsintervallen utifrån resultatet.

Med tanke på uppdraget att avge ett yttrande till kommissionen huruvida ett tredjeland, ett territorium eller en eller flera specificerade sektorer i tredjelandet eller en internationell organisation inte längre säkerställer en adekvat skyddsnivå, måste Europeiska dataskyddsstyrelsen, inom utsatt tid, erhålla meningsfull information om övervakningen av den relevanta utvecklingen i tredjelandet eller den internationella organisationen från kommissionen. Av den anledningen bör Europeiska dataskyddsstyrelsen hållas underrättad om eventuella översynsprocesser och översynsuppdrag i tredjelandet eller gällande den internationella organisationen. Europeiska dataskyddsstyrelsen skulle uppskatta att bjudas in att delta i dessa översynsprocesser och översynsuppdrag.

Det bör även uppmärksammas att enligt artikel 45.5 i den allmänna dataskyddsförordningen har kommissionen rätt att återkalla, ändra eller upphäva befintliga beslut om adekvat skyddsnivå. Följaktligen bör Europeiska dataskyddsstyrelsen involveras i förfarandet för att återkalla, ändra eller upphäva beslut, genom att dess yttrande inhämtas enligt artikel 70.1 s.

Därutöver måste dataskyddsmyndigheter, vilket fastställs i artikel 58.5 i den allmänna dataskyddsförordningen och i domen från Europeiska unionens domstol i Schrems-målet, kunna delta i rättsliga förfaranden om de finner att en persons anspråk gentemot ett beslut om adekvat skyddsnivå är välgrundat: "Det ankommer härvidlag på den nationella lagstiftaren att föreskriva rättsmedel som gör det möjligt för den nationella tillsynsmyndigheten att vid nationella domstolar göra gällande de invändningar som den anser att det finns fog för, så att nationella domstolar, för det fall att de delar

¹⁰ Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees) (ej översatt till svenska), 16/EN WP237, 13.4.2016.

myndighetens tvivel angående kommissionsbeslutets giltighet, kan hänskjuta en begäran om förhandsavgörande för att pröva detta besluts giltighet.”¹¹

¹¹ Domstolens dom av den 6 oktober 2015, Maximillian Schrems/Data Protection Commissioner, C-362/14, ECLI:EU:C:2015:650, punkt 65.

Kapitel 3: Allmänna principer för dataskydd som används för att säkerställa att skyddsnivån i ett tredjeland, ett territorium eller en eller flera specificerade sektorer i tredjelandet eller en internationell organisation väsentligen är likvärdig med den som garanteras genom EU-lagstiftningen

Ett tredjelands eller en internationell organisations system måste innehålla följande grundläggande innehållsmässiga principer för skydd av personuppgifter och förfarande- och verkställandemekanismer:

A. Innehållsmässiga principer:

1) Begrepp

Grundläggande begrepp och/eller principer rörande skydd av personuppgifter bör vara definierade. Dessa begrepp och principer behöver inte exakt återspegla terminologin i den allmänna dataskyddsförordningen, men de bör avspegla och vara i enlighet med de begrepp som används i EU:s dataskyddslagstiftning. Till exempel innehåller den allmänna dataskyddsförordningen följande viktiga begrepp: "personuppgifter", "behandling av personuppgifter", "personuppgiftsansvarig", "personuppgiftsbiträde", "mottagare" och "känsliga uppgifter".

2) Grunder för laglig och rättvis behandling för berättigade ändamål

Uppgifter måste behandlas på ett lagligt, rättvist och berättigat sätt.

De legitima grunder enligt vilka personuppgifter kan behandlas på ett lagligt, rättvist och berättigat sätt ska anges på ett tillräckligt tydligt sätt. Det finns åtskilliga sådana legitima grunder inom EU:s rättsliga ramar, till exempel bestämmelser i nationell lagstiftning, den registrerades samtycke, fullgörande av ett avtal eller berättigat intresse från den personuppgiftsansvariges eller en tredje parts sida när inte individens intressen väger tyngre.

3) Principen om ändamålsbegränsning

Uppgifter ska behandlas för ett specifikt ändamål och får därefter endast användas i den utsträckning det är förenligt med behandlingens syfte.

4) Principen om uppgifternas kvalitet och proportionalitet

Uppgifterna ska vara korrekta och, när så är nödvändigt, hållas aktuella. Dessutom ska uppgifterna vara adekvata, relevanta och inte mer omfattande än vad som krävs för de ändamål för vilka de behandlas.

5) Principen om lagring av uppgifter

Uppgifter ska, generellt sett, inte bevaras under längre tid än vad som krävs för de ändamål för vilka personuppgifterna behandlas.

6) Principen om säkerhet och konfidentialitet

Varje enhet som behandlar personuppgifter ska se till att uppgifterna behandlas på ett sätt som säkerställer personuppgifternas säkerhet, vilket innefattar skydd mot obehörig eller olaglig behandling och mot förlust, förstörelse eller skada genom olyckshändelse, med användning av lämpliga tekniska

eller organisatoriska åtgärder. Säkerhetsnivån bör fastställas med beaktande av den senaste tekniska utvecklingen och de tillhörande kostnaderna.

7) Öppenhetsprincipen

Varje individ ska informeras om alla huvudelement i behandlingen av hans eller hennes personuppgifter på ett tydligt, lättillgängligt, kortfattat, öppet och begripligt sätt. Informationen ska ange ändamålet med behandlingen, den personuppgiftsansvariges identitet, individens rättigheter och övrig information som krävs för att säkerställa en öppen och rättvis behandling. Under vissa omständigheter kan det finnas undantag från denna rätt till information, till exempel för att skydda brottsutredningar, den nationella säkerheten, rättsväsendets oberoende och rättsliga åtgärder eller andra viktiga mål av generellt allmänt intresse i enlighet med artikel 23 i den allmänna dataskyddsförordningen.

8) Rätt till tillgång, rättelse, radering och invändningar

Den registrerade ska ha rätt att erhålla bekräftelse på om personuppgiftsbehandling som rör honom eller henne äger rum, samt få tillgång till de egna uppgifterna, inklusive en kopia av alla uppgifter avseende honom eller henne som behandlas.

Den registrerade ska ha rätt att vid behov få sina uppgifter rättade av angivna skäl, till exempel om de visar sig vara felaktiga eller ofullständiga, och att få sina uppgifter raderade, till exempel när behandlingen av dem inte längre är nödvändig eller om den är olaglig.

Dessutom ska den registrerade ha rätt att när som helst, av tvingande berättigade skäl gällande hans eller hennes specifika situation, invända mot behandling av hans eller hennes uppgifter som sker baserat på särskilda villkor som anges i tredjelandets rättsliga ramar. I fråga om den allmänna dataskyddsförordningen kan sådana villkor exempelvis vara när behandlingen är nödvändig för att utföra en uppgift av allmänt intresse, när behandlingen är nödvändig som ett led i den personuppgiftsansvariges myndighetsutövning eller när behandlingen är nödvändig för ändamål som rör den personuppgiftsansvariges eller en tredje parts berättigade intressen.

Utövandet av dessa rättigheter ska inte vara alltför betungande för den registrerade. Vissa begränsningar av dessa rättigheter kan finnas, till exempel för att skydda brottsutredningar, den nationella säkerheten, rättsväsendets oberoende och rättsliga åtgärder eller andra viktiga mål av generellt allmänt intresse i enlighet med artikel 23 i den allmänna dataskyddsförordningen.

9) Restriktioner för vidare överföring

Vidare överföring av personuppgifter från den första mottagaren av den ursprungliga överföringen ska endast tillåtas när nästa mottagare (det vill säga mottagaren av den vidare överföringen) också omfattas av bestämmelser (inklusive avtalsbaserade bestämmelser) som ger en adekvat skyddsnivå och följer relevanta instruktioner vid behandling av uppgifter på den personuppgiftsansvariges uppdrag. Skyddsnivån för de fysiska personer vars personuppgifter överförs får inte undergrävas av den vidare överföringen. Den första mottagaren av uppgifter som överförs från EU ska vara skyldig att säkerställa att lämpliga skyddsåtgärder vidtas för vidare överföringar av uppgifter i avsaknad av ett beslut om adekvat skyddsnivå. Sådana vidare överföringar av uppgifter ska endast göras för begränsade och specificerade ändamål och bara så länge det finns en rättslig grund för behandlingen.

B. Exempel på ytterligare innehållsmässiga principer som ska tillämpas för specifika typer av behandlingar:

1) Särskilda kategorier av uppgifter

Specifika skyddsåtgärder bör vidtas när "särskilda kategorier av uppgifter" är inblandade¹². Dessa kategorier bör återspegla dem som anges i artiklarna 9 och 10 i den allmänna dataskyddsförordningen. Det extra skyddet bör införas genom strängare krav för uppgiftsbehandlingen, till exempel i form av att den registrerade ger sitt uttryckliga samtycke till behandlingen eller genom ytterligare säkerhetsåtgärder.

2) Direktmarknadsföring

Om personuppgifter behandlas för direktmarknadsföring ska den registrerade ha möjlighet att när som helst och utan kostnad invända mot att hans eller hennes uppgifter behandlas för detta syfte.

3) Automatiserat beslutsfattande och profilering

Beslut som enbart baseras på automatisk behandling (automatiserat individuellt beslutsfattande), inklusive profilering, som får rättsliga följder för eller i betydande grad påverkar den registrerade, får endast äga rum under vissa villkor som fastställs i tredjelandets rättsliga ramar. Inom EU:s rättsliga ramar räknas till sådana villkor, exempelvis, behovet att erhålla den registrerades uttryckliga samtycke eller nödvändigheten av ett sådant beslut för att ett avtal ska kunna fullgöras. Om beslutet inte sker i enlighet med de villkor som fastställs i tredjelandets rättsliga ramar, ska den registrerade ha rätt att inte underställas det. Tredjelandets lagstiftning ska under alla förhållanden tillhandahålla nödvändiga skyddsåtgärder, inklusive rätten att informeras om de specifika skälen och logiken bakom beslutet, rätten att korrigera felaktig eller ofullständig information och rätten att bestrida beslutet om det har fattats på felaktigt faktaunderlag.

C. Förfarande- och verkställandemekanismer

Även om de medel som tredjelandet använder för att säkerställa en adekvat skyddsnivå kan skilja sig från de som används inom EU¹³, måste följande element finnas med för att ett system ska kunna räknas som förenligt med EU:s:

1) Oberoende behörig tillsynsmyndighet

Det ska finnas en eller flera oberoende tillsynsmyndigheter som har till uppgift att övervaka, säkerställa och kontrollera att bestämmelserna om uppgiftsskydd och integritetsskydd efterlevs i tredjelandet. Tillsynsmyndigheten ska utföra sina uppgifter och utöva sina befogenheter på ett fullständigt oberoende och opartiskt sätt, och varken efterfråga eller ta emot några instruktioner. Tillsynsmyndigheten ska i detta sammanhang ha alla nödvändiga och tillgängliga befogenheter och behörigheter som krävs för att säkerställa att rätten till uppgiftsskydd efterlevs och främja medvetenhet. Tillsynsmyndighetens personal och budget ska även tas under beaktande. Dessutom ska tillsynsmyndigheten ha möjlighet att på eget initiativ utföra utredningar.

2) Systemet för skydd av personuppgifter måste säkerställa en god efterlevnad

Systemet för skydd av personuppgifter i ett tredjeland ska säkerställa att personuppgiftsansvariga och de som behandlar personuppgifter på deras vägnar känner ett stort ansvar för och är medvetna om de

¹² Dessa särskilda kategorier kallas även för "känsliga uppgifter" i skäl 10 i den allmänna dataskyddsförordningen.

¹³ Domstolens dom av den 6 oktober 2015, Maximilian Schrems/Data Protection Commissioner, C-362/14, ECLI:EU:C:2015:650, punkt 74.

skyldigheter, uppgifter och ansvarsområden de omfattas av, samt att de registrerade känner till sina rättigheter och de medel de har för att utöva dem. Tillgång till effektiva och avskräckande sanktioner kan spela en viktig roll för att säkerställa respekten för bestämmelserna, vilket naturligtvis även gäller system för direktkontroll från myndigheters, revisorers eller oberoende dataskyddstjänstemäns sida.

3) Ansvarsskyldighet

De rättsliga ramarna för skydd av personuppgifter i ett tredjeland ska ställa som krav att personuppgiftsansvariga och/eller de som behandlar personuppgifter på deras vägnar efterlever ramarna och att de ska kunna styrka denna efterlevnad, i synnerhet för den behöriga tillsynsmyndigheten. Medlen för att göra detta kan exempelvis inbegripa konsekvensbedömningar avseende dataskydd, förande av register eller loggfiler för personuppgiftsbehandling som sparas under en lämplig tidsperiod, utnämning av ett dataskyddsombud eller inbyggt dataskydd och dataskydd som standard.

4) Systemet för skydd av personuppgifter måste ge stöd och hjälp till enskilda registrerade i deras utövande av sina rättigheter samt tillhandahålla mekanismer för skälig gottgörelse

Den enskilde ska kunna vidta rättsliga åtgärder för att hävda sina rättigheter på ett snabbt och effektivt sätt, och utan orimliga kostnader, liksom för att säkerställa att bestämmelserna efterlevs. För att detta ska bli möjligt måste det finnas kontrollmekanismer som tillåter oberoende utredning av klagomål och gör det möjligt att i praktiken upptäcka och bestraffa eventuella överträdelser av rätten till uppgiftsskydd och respekt för privatlivet.

Om bestämmelserna inte efterlevs ska den registrerade likaså tillförsäkras effektiv administrativ och rättslig prövning, däribland för ersättning för skador som orsakats av den olagliga behandlingen av hans eller hennes personuppgifter. Detta är en nyckelfråga som kräver ett system med oberoende skiljedom så att ersättningar kan betalas ut och sanktioner utkrävas när detta är motiverat.

Kapitel 4: Grundläggande garantier i tredjeländer för åtkomst i samband med brottsbekämpning och nationell säkerhet för att begränsa ingreppen i de grundläggande rättigheterna

Vid bedömning av om skyddsnivån är adekvat ska kommissionen enligt artikel 45.2 a ta hänsyn till "relevant lagstiftning, både allmän lagstiftning och sektorslagstiftning, inklusive avseende allmän säkerhet, försvar, nationell säkerhet och straffrätt och offentliga myndigheters tillgång till personuppgifter samt tillämpningen av sådan lagstiftning ...".

Europeiska unionens domstol anmärkte i Schrems-målet att "begreppet 'adekvat skyddsnivå' ska förstås som att det krävs att detta tredjeland, genom sin interna lagstiftning eller på grund av de internationella förpliktelser som åligger landet, de facto säkerställer en nivå för skyddet av grundläggande fri- och rättigheter som är väsentligen likvärdig med den skyddsnivå som garanteras inom unionen enligt direktiv 95/46 jämfört med stadgan." Även om de medel som detta tredjeland använder sig av i detta sammanhang kan skilja sig från de som används inom EU, måste dessa medel inte desto mindre visa sig vara effektiva i praktiken¹⁴.

I detta sammanhang har domstolen även kritiskt noterat att det tidigare Safe Harbor-beslutet inte innehåller "något konstaterande beträffande förekomsten i Förenta staterna av regler som antagits av staten och som syftar till att begränsa eventuella ingrepp i de grundläggande rättigheterna för personer vilkas personuppgifter överförs från unionen till Förenta staterna, ingrepp som statliga organ kan vara tillåtna att göra när de görs i ett legitimt syfte, såsom nationell säkerhet."

Artikel 29-arbetsgruppen har i yttrandet WP237, som antogs den 13 april 2016, identifierat grundläggande garantier som återspeglar rättspraxisen hos Europeiska unionens domstol och Europeiska domstolen för de mänskliga rättigheterna inom området övervakning. Samtidigt som rekommendationerna som anges i WP237 ska förbli giltiga och tas i beaktande vid bedömning av om ett tredjelands skyddsnivå är adekvat inom området övervakning, kan tillämpningen av dessa garantier variera inom området uppgiftsåtkomst gällande brottsbekämpning och nationell säkerhet. Inte desto mindre ska följande fyra garantier som anges i yttrandet respekteras av alla tredjeländer i fråga om åtkomsten till personuppgifter, oavsett om det gäller den nationella säkerheten eller brottsbekämpning, för att skyddsnivån ska kunna bedömas som adekvat:

- 1) Behandlingen ska baseras på tydliga, exakta och lättillgängliga regler (rättslig grund).**
- 2) Nödvändighet och proportionalitet med avseende på de legitima mål som eftersträvas måste påvisas.**
- 3) Behandlingen måste omfattas av en oberoende tillsyn.**
- 4) Effektiva rättsmedel måste vara tillgängliga för enskilda individer.**

¹⁴ Domstolens dom av den 6 oktober 2015, Maximilian Schrems/Data Protection Commissioner, C-362/14, ECLI:EU:C:2015:650, punkt 74.