



18/NL

WP 254 rev.01

Groep gegevensbescherming artikel 29

Adequaatheidsreferentie

Vastgesteld op 28 november 2017

Laatstelijk gewijzigd en vastgesteld op 6 februari 2018

Deze groep is opgericht op grond van artikel 29 van Richtlijn 95/46/EG. Zij is een onafhankelijk Europees adviesorgaan inzake gegevensbescherming en de persoonlijke levenssfeer, waarvan de taken zijn omschreven in artikel 30 van Richtlijn 95/46/EG en in artikel 15 van Richtlijn 2002/58/EG.

Het secretariaat wordt verzorgd door directoraat C (Grondrechten en burgerschap van de Unie) van de Europese Commissie, directoraat-generaal Justitie en Consumentenzaken, B-1049 Brussel, België, kamer MO-59 02/013.

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

Inleiding

De Groep voor de bescherming van personen in verband met de verwerking van persoonsgegevens¹ (WP29) heeft eerder een werkdocument gepubliceerd inzake de doorgifte van persoonsgegevens naar derde landen (WP12)². Naar aanleiding van de vervanging van de richtlijn door de algemene verordening gegevensbescherming van de EU (AVG)³, buigt de WP29 zich opnieuw over WP12, haar eerdere leidraad, om deze bij te werken in het licht van de nieuwe wetgeving en recente jurisprudentie van het Hof van Justitie van de Europese Unie (HvJ-EU)⁴.

Met dit werkdocument wordt beoogd hoofdstuk 1 van WP12 bij te werken, dat betrekking heeft op het centrale punt van een adequaat niveau van gegevensbescherming in een derde land, een grondgebied of een of meer gespecificeerde sectoren binnen dat derde land of in een internationale organisatie (hierna "derde landen of internationale organisaties" genoemd). Dit document zal de komende jaren voortdurend worden herzien en zo nodig worden bijgewerkt, aan de hand van de praktische ervaring die wordt opgedaan met de toepassing van de AVG. Hoofdstuk 2 (*Toepassing van de aanpak op landen die Verdrag nr. 108 van de Raad van Europa geratificeerd hebben*) en hoofdstuk 3 (*Toepassing van de aanpak op zelfregulering door de industrie*) van het WP12-document worden in een later stadium bijgewerkt.

Dit werkdocument betreft uitsluitend adequaatheidsbesluiten. Dit zijn uitvoeringshandelingen⁵ van de Europese Commissie, in overeenstemming met artikel 45 van de AVG. Andere aspecten van de doorgifte van persoonsgegevens aan derde landen en internationale organisaties worden behandeld in toekomstige werkdocumenten, die afzonderlijk gepubliceerd zullen worden (bindende bedrijfsvoorschriften, afwijkingen).

Dit document is bedoeld als richtsnoer voor de Europese Commissie en de WP29 in het kader van de AVG bij het beoordelen van het gegevensbeschermingsniveau in derde landen en internationale organisaties. Het beschrijft de kernbeginselen voor gegevensbescherming waaraan een internationale organisatie of het rechtskader van een derde land moet voldoen om te waarborgen dat het beschermingsniveau in grote lijnen overeenkomt met dat van het EU-kader. Daarnaast kan het dienen als leidraad voor derde landen en internationale organisaties die aan de eisen voor adequaatheid willen voldoen. De beginselen die in dit werkdocument worden beschreven, zijn echter niet rechtstreeks bedoeld voor verwerkingsverantwoordelijken of gegevensverwerkers.

Dit document bestaat uit vier hoofdstukken:

Hoofdstuk 1: Algemene informatie over het begrip 'adequaatheid'.

Hoofdstuk 2: Procedurele aspecten van adequaatheidsbevindingen in het kader van de AVG.

Hoofdstuk 3: Algemene beginselen inzake gegevensbescherming. Dit hoofdstuk omvat de kernbeginselen voor algemene gegevensbescherming. Doel daarvan is dat het niveau van gegevensbescherming in een derde land of internationale organisatie in grote lijnen overeenkomt met het niveau dat is vastgesteld door EU-wetgeving.

Hoofdstuk 4: Essentiële waarborgen voor de toegang van instanties voor wetshandhaving en nationale veiligheid om aantasting van grondrechten te beperken. Dit hoofdstuk omvat de essentiële waarborgen voor de toegang van instanties voor wetshandhaving en nationale veiligheid naar aanleiding van het arrest-Schrems van het HvJ-EU van 2015. Het werkdocument over essentiële waarborgen dat de WP29 in 2016 heeft goedgekeurd, dient hierbij als basis.

¹ Opgericht op grond van artikel 29 van de EU-gegevensbeschermingsrichtlijn (Richtlijn 95/46/EG).

² WP12, "Doorgifte van persoonsgegevens naar derde landen: toepassing van de artikelen 25 en 26 van de EU-richtlijn betreffende gegevensbescherming" (werkdocument), op 24.7.1998 vastgesteld door de Groep.

³ Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (Voor de EER relevante tekst).

⁴ Waaronder zaak C-362/14, *Maximilian Schrems tegen Data Protection Commissioner*, 6.10.2015.

⁵ Zie artikel 45, lid 3, en artikel 93, lid 2, van de AVG voor verdere informatie over de uitvoeringshandelingen.

Hoofdstuk 1: Algemene informatie over het begrip 'adequaatheid'

Artikel 45, lid 1, van de AVG stipuleert dat doorgiften van gegevens aan een derde land of internationale organisatie uitsluitend kunnen plaatsvinden als dat derde land, een gebied of een of meerdere nader bepaalde sectoren in dat derde land, of de internationale organisatie in kwestie een passend beschermingsniveau waarborgt.

Dit begrip 'passend beschermingsniveau' werd al gehanteerd in Richtlijn 95/46/EG en is verder uitgewerkt door het HvJ-EU. Het is in dit verband belangrijk te herinneren aan de norm die het HvJ-EU heeft gesteld in het arrest-Schrems, namelijk dat het "*beschermingsniveau*" in het derde land "*in grote lijnen*" moet overeenkomen met het niveau dat in de EU wordt gewaarborgd, "*ook al kunnen de middelen waarmee dat derde land voor waarborgen voor een passend beschermingsniveau kan zorgen, anders zijn dan die welke binnen de Unie worden ingezet*"⁶. Het doel is dus niet de Europese wetgeving punt voor punt te kopiëren, maar de grote lijnen van die wetgeving – de kernvereisten – vast te stellen.

Adequaateitsbesluiten van de Europese Commissie hebben tot doel formeel te bevestigen, met bindende rechtsgevolgen voor de lidstaten⁷, dat het niveau van gegevensbescherming in een derde land of internationale organisatie in grote lijnen overeenkomt met het gegevensbeschermingsniveau in de Europese Unie⁸. Adequaatheid kan worden bereikt door een combinatie van rechten voor de betrokkenen, verplichtingen voor gegevensverwerkers of verwerkingsverantwoordelijken en toezicht door onafhankelijke instanties. Regelgeving voor gegevensverwerking is echter alleen doeltreffend als ze afdwingbaar is en in de praktijk wordt nageleefd. Er moet dus niet alleen worden gekeken naar de inhoud van de toepasselijke regelgeving voor de doorgifte van persoonsgegevens aan een derde land of een internationale organisatie, maar ook naar het systeem waarmee de doeltreffendheid van deze regelgeving wordt gewaarborgd. Voor de doeltreffendheid van regelgeving voor gegevensbescherming zijn efficiënte handhavingssystemen van eminent belang.

In artikel 45, lid 2, van de AVG worden de aspecten genoemd waarmee de Commissie rekening moet houden bij haar beoordeling van de vraag of het beschermingsniveau in een derde land of internationale organisatie adequaat is.

Zo moet de Commissie rekening houden met de rechtsstatelijkheid, de eerbiediging van de mensenrechten en de fundamentele vrijheden, de toepasselijke wetgeving, het bestaan en het effectief functioneren van een of meer onafhankelijke toezichthoudende autoriteiten en de internationale toezeggingen die het derde land of de internationale organisatie in kwestie heeft gedaan.

Het is dan ook duidelijk dat een zinvolle analyse van passende bescherming twee basiselementen moet bevatten, namelijk de inhoud van de toepasselijke regelgeving en de middelen om de doeltreffende toepassing daarvan te waarborgen. Het is de taak van de Europese Commissie – periodiek – te verifiëren dat de geldende regelgeving ook daadwerkelijk doeltreffend is.

De inhoudelijke kernbeginselen voor gegevensbescherming en de eisen ten aanzien van procedures en handhaving, die kunnen worden beschouwd als een minimumvereiste voor adequate bescherming, zijn afgeleid van het Handvest van de grondrechten van de Europese Unie en de AVG. Daarnaast moet ook rekening worden gehouden met andere internationale overeenkomsten inzake gegevensbescherming, bijvoorbeeld Verdrag 108⁹.

Ook moet aandacht worden geschonken aan het rechtskader voor de toegang van overheden tot persoonsgegevens. Meer informatie hierover is te vinden in Werkdocument 237 (het document over essentiële waarborgen)¹⁰, dat ingaat op waarborgen in de context van toezichtsactiviteiten.

⁶ Zaak C-362/14, *Maximillian Schrems tegen Data Protection Commissioner*, 6.10.2015 (punten 73 en 74).

⁷ Artikel 288, lid 2, VWEU.

⁸ Zaak C-362/14, *Maximillian Schrems tegen Data Protection Commissioner*, 6.10.2015 (punt 52).

⁹ Overweging 105 van de AVG.

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), 16/EN WP 237, 13.4.2016.

Algemene bepalingen over gegevensbescherming en bescherming van de persoonlijke levenssfeer in het derde land zijn niet voldoende. In het rechtskader van het derde land of de internationale organisatie moeten daarentegen specifieke bepalingen worden opgenomen die concreet invulling geven aan voor de praktijk relevante aspecten van het recht op gegevensbescherming. De naleving van deze bepalingen moet afdwingbaar zijn.

Hoofdstuk 2: Procedurele aspecten van adequaatheidsbevindingen in het kader van de AVG

Het Europees Comité voor gegevensbescherming (European Data Protection Board, EDPB) heeft op grond van artikel 70, lid 1, onder s), van de AVG de taak advies uit te brengen aan de Europese Commissie. Daartoe dient de Commissie het EDPB de nodige documentatie te verstrekken, met inbegrip van relevante correspondentie en de bevindingen van de Europese Commissie. In het geval van een complex rechtskader gaat het daarbij ook om eventuele rapporten over het gegevensbeschermingsniveau in het derde land of de internationale organisatie. De door de Europese Commissie verstrekte informatie moet in elk geval uitputtend zijn en het EDPB in staat stellen zelf het niveau van gegevensbescherming in het derde land te beoordelen. Het EDPB verstrekt te gelegener tijd een advies over de bevindingen van de Europese Commissie en stelt eventuele onvolkomenheden in het adequaatheidskader vast. Het EDPB streeft er ook naar aanpassingen of wijzigingen voor te stellen om mogelijke onvolkomenheden te verhelpen.

Volgens artikel 45, lid 4, van de AVG is het de taak van de Europese Commissie – doorlopend – toezicht te houden op ontwikkelingen in derde landen en internationale organisaties die mogelijk gevolgen hebben voor het functioneren van een adequaatheidsbesluit.

Artikel 45, lid 3, van de AVG voorziet in een periodieke toetsing die minstens om de vier jaar moet plaatsvinden. Dit is echter een algemeen tijdsbestek dat moet worden aangepast aan elk derde land of elke internationale organisatie waarvoor een adequaatheidsbesluit is genomen. Afhankelijk van de specifieke omstandigheden kan een kortere evaluatiecyclus nodig zijn. Ook incidenten of nieuwe informatie over of wijzigingen in het rechtskader van het derde land of de internationale organisatie in kwestie kunnen aanleiding vormen om de toetsing eerder dan gepland uit te voeren. Het is waarschijnlijk een passende werkwijze de eerste toetsing van een volkomen nieuw adequaatheidsbesluit vrij snel uit te voeren en geleidelijk de evaluatiecyclus aan te passen al naargelang de resultaten.

Gezien zijn mandaat een advies uit te brengen aan de Europese Commissie over de vraag of het derde land, een grondgebied of een of meer gespecificeerde sectoren in dat derde land of een internationale organisatie nog wel een passend beschermingsniveau biedt, moet de EDPB tijdig zinvolle informatie ontvangen over het toezicht door de Commissie op de relevante ontwikkelingen in dat derde land of de internationale organisatie. De EDPB moet echter op de hoogte worden gehouden van iedere evaluatieprocedure of -missie in het derde land of bij de internationale organisatie. Het EDPB zou het op prijs stellen te worden uitgenodigd als deelnemer aan deze evaluatieprocedures of -missies.

Verder moet worden opgemerkt dat de Europese Commissie volgens artikel 45, lid 5, van de AVG het recht heeft adequaatheidsbesluiten in te trekken, te wijzigen of te schorsen. Het EDPB zou dan ook bij de procedure tot intrekking, wijziging of schorsing van een adequaatheidsbesluit moeten worden betrokken door het om advies te vragen op grond van artikel 70, lid 1, onder s).

Verder moeten gegevensbeschermingsautoriteiten, conform artikel 58, lid 5, van de AVG en het arrest-Schrems van het HvJ-EU, een rechtsvordering kunnen instellen als naar hun mening een bezwaar dat iemand tegen een adequaatheidsbesluit heeft ingediend, gegrond is: *"In dat verband staat het aan de nationale wetgever om in beroepsgangen te voorzien waarmee bedoelde autoriteit de grieven die zij gegrond acht aan de nationale rechter kan voorleggen, zodat die laatste, wanneer hij de twijfel ten aanzien van de geldigheid van de beschikking van de Commissie deelt, de vraag naar de geldigheid van die beschikking prejudicieel kan verwijzen."*¹¹

¹¹ Zaak C-362/14, *Maximillian Schrems tegen Data Protection Commissioner*, 6.10.2015 (punt 65).

Hoofdstuk 3: Algemene beginselen inzake gegevensbescherming om te waarborgen dat het beschermingsniveau in een derde land, een gebied of een of meerdere nader bepaalde sectoren in dat derde land of de internationale organisatie in grote lijnen overeenkomt met het niveau dat wordt gewaarborgd door de EU-wetgeving

De inhoudelijke elementen en de beginselen en mechanismen voor de procedures/handhaving met betrekking tot gegevensbescherming die het systeem van een derde land of internationale organisatie moet bevatten, zijn als volgt:

A. Inhoudelijke beginselen:

1) Begrippen

Er moet sprake zijn van basisbegrippen en/of -beginselen voor gegevensbescherming. Deze hoeven geen kopie te zijn van de terminologie die in de AVG wordt gehanteerd, maar moeten wel een afspiegeling vormen van de begrippen in de Europese wetgeving inzake gegevensbescherming en daarmee consistent zijn. In de AVG zijn bijvoorbeeld de volgende belangrijke begrippen opgenomen: "persoonsgegevens", "verwerking van persoonsgegevens", "verwerkingsverantwoordelijke", "verwerker", "ontvanger" en "gevoelige gegevens".

2) Gronden voor behoorlijke en rechtmatige verwerking voor legitieme doeleinden

Gegevens moeten worden verwerkt op een behoorlijke, rechtmatige en legitieme wijze.

De gerechtvaardigde grondslagen op basis waarvan persoonsgegevens op behoorlijke, rechtmatige en legitieme wijze worden verwerkt, moeten voldoende duidelijk worden uiteengezet. Het Europees kader erkent verschillende gerechtvaardigde grondslagen, bijvoorbeeld bepalingen in de nationale wetgeving, de toestemming van de betrokkene, de uitvoering van een overeenkomst of de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen van de betrokkene zwaarder wegen.

3) Het beginsel van doelbinding

Gegevens moeten worden verwerkt voor een specifiek doeleinde en mogen vervolgens niet op een met dat doeleinde onverenigbare wijze worden verwerkt.

4) Het beginsel van kwaliteit en evenredigheid van gegevens

De gegevens moeten nauwkeurig zijn en, zo nodig, worden bijgewerkt. De gegevens moeten toereikend, ter zake dienend en niet overmatig zijn uitgaande van de doeleinden waarvoor zij worden verwerkt.

5) Het beginsel van gegevensbewaring

In het algemeen gesproken mogen persoonsgegevens niet langer worden bewaard dan noodzakelijk is voor de doeleinden waarvoor ze worden verwerkt.

6) Het beginsel van beveiliging en vertrouwelijkheid

Iedere entiteit die persoonsgegevens verwerkt, moet ervoor zorgen dat deze op een zodanige wijze worden verwerkt dat een passende beveiliging van de gegevens gewaarborgd is en dat ze onder

meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging. Daartoe moeten passende technische of organisatorische maatregelen worden getroffen. Bij het beveiligingsniveau moet rekening worden gehouden met de stand van de techniek en de bijbehorende kosten.

7) Het transparantiebeginsel

Iedere betrokkene moet in een duidelijke, gemakkelijk toegankelijke, beknopte, transparante en begrijpelijke vorm worden geïnformeerd over alle belangrijke elementen van de verwerking van zijn/haar persoonsgegevens. Deze informatie moet het doel van de verwerking omvatten, de identiteit van de verwerkingsverantwoordelijke, de rechten die hem/haar ter beschikking staan en andere informatie, voor zover noodzakelijk om een behoorlijke verwerking te waarborgen. Onder bepaalde voorwaarden kunnen uitzonderingen op dit informatierecht worden gemaakt, bijvoorbeeld om onderzoeken naar strafbare feiten veilig te stellen of de onafhankelijkheid van de rechter en gerechtelijke procedures te beschermen of om andere gewichtige redenen van openbaar belang, zoals bedoeld in artikel 23 van de AVG.

8) Het recht van toegang, rectificatie, wissing en bezwaar

De betrokkene heeft het recht om uitsluitel te verkrijgen over het al dan niet verwerken van hem/haar betreffende gegevens en om een kopie te verkrijgen van alle gegevens over hem/haar die worden verwerkt.

De betrokkene heeft, waar van toepassing, recht op rectificatie van zijn/haar gegevens om specifieke redenen, bijvoorbeeld wanneer deze gegevens onjuist of onvolledig blijken te zijn. Ook heeft de betrokkene recht op wissing van zijn/haar persoonsgegevens wanneer de verwerking ervan bijvoorbeeld onrechtmatig of niet langer noodzakelijk is.

De betrokkene heeft ook te allen tijde het recht om, op dwingende gerechtvaardigde gronden die verband houden met zijn/haar specifieke situatie, bezwaar te maken tegen de verwerking van zijn/haar gegevens onder bepaalde voorwaarden die zijn vastgelegd in het rechtskader van het derde land. Voorbeelden van deze voorwaarden in de AVG zijn: de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen, of de verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde.

De uitoefening van deze rechten mag voor de betrokkene niet buitensporig omslachtig zijn. Beperking van deze rechten is mogelijk, bijvoorbeeld om onderzoeken naar strafbare feiten veilig te stellen of de onafhankelijkheid van de rechter en gerechtelijke procedures te beschermen of om andere gewichtige redenen van openbaar belang, zoals bedoeld in artikel 23 van de AVG.

9) Beperkingen ten aanzien van verdere doorgifte

Verdere doorgifte van de persoonsgegevens door de eerste ontvanger van de oorspronkelijke gegevensdoorgifte mag alleen worden toegestaan wanneer a) de latere ontvanger – dat wil zeggen de ontvanger van de verdere doorgifte – eveneens is onderworpen aan voorschriften (met inbegrip van contractuele bepalingen) die een passend beschermingsniveau opleveren en b) deze ontvanger de relevante instructies opvolgt wanneer hij/zij namens de verwerkingsverantwoordelijke gegevens verwerkt. Het beschermingsniveau van natuurlijke personen wier gegevens worden doorgegeven, mag niet worden ondermijnd door de verdere doorgifte. De eerste ontvanger van de gegevens die vanuit de EU worden doorgegeven, heeft de verantwoordelijkheid om bij ontstentenis van een adequaatheidsbesluit toe te zien op passende waarborgen voor verdere doorgifte van gegevens. Verdere doorgiften van gegevens mogen alleen plaatsvinden voor beperkte en welbepaalde doeleinden en voor zover er een rechtsgrondslag voor de verwerking is.

B. Voorbeelden van aanvullende beginselen ten aanzien van de inhoud die op bepaalde soorten verwerking moeten worden toegepast:

1) Bijzondere gegevenscategorieën

Wanneer sprake is van 'bijzondere gegevenscategorieën' zijn specifieke waarborgen nodig.¹² Deze categorieën moeten een afspiegeling zijn van de categorieën die worden genoemd in artikelen 9 en 10 van de AVG. Deze bescherming moet de vorm krijgen van strengere eisen voor de gegevensverwerking, bijvoorbeeld de eis dat de betrokkene zijn/haar uitdrukkelijke toestemming voor de verwerking moet geven, of aanvullende beveiligingsmaatregelen.

2) Direct marketing

Wanneer persoonsgegevens ten behoeve van direct marketing worden verwerkt, heeft de betrokkene te allen tijde het recht om kosteloos bezwaar te maken tegen de verwerking van hem/haar betreffende persoonsgegevens voor dergelijke marketing.

3) Geautomatiseerde besluitvorming en profilering

Besluiten die uitsluitend zijn gebaseerd op geautomatiseerde verwerking (geautomatiseerde individuele besluitvorming), waaronder profilering, waaraan voor de betrokkene rechtsgevolgen zijn verbonden of die hem/haar anderszins in aanmerkelijke mate treffen, mogen uitsluitend plaatsvinden onder bepaalde voorwaarden die zijn vastgelegd in het rechtskader van het derde land. Voorbeelden van zulke voorwaarden in het Europees rechtskader zijn dat de uitdrukkelijke toestemming van de betrokkene moet worden verkregen of dat de doorgifte noodzakelijk is voor de sluiting van een overeenkomst. Als het besluit niet voldoet aan de voorwaarden die in het rechtskader van het derde land zijn neergelegd, moet de betrokkene het recht hebben er niet aan te worden onderworpen. De wetgeving van het derde land moet in elk geval voorzien in de noodzakelijke waarborgen, waaronder het recht te worden geïnformeerd over specifieke redenen die ten grondslag liggen aan het besluit en de onderliggende logica, onjuiste of onvolledige informatie te corrigeren en het besluit aan te vechten wanneer dit is goedgekeurd op basis van onjuiste gegevens.

C. Procedurele en handhavingsmechanismen:

Al kunnen de middelen waarmee het derde land voor waarborgen voor een passend beschermingsniveau kan zorgen, anders zijn dan die welke binnen de Unie worden ingezet¹³, een systeem dat verenigbaar is met het Europese systeem moet worden gekenmerkt door de volgende elementen:

1) Bevoegde onafhankelijke toezichthoudende autoriteit

Er moeten in het derde land een of meer onafhankelijke toezichthoudende autoriteiten zijn, die tot taak hebben de naleving van de bepalingen aangaande gegevensbescherming en bescherming van de persoonlijke levenssfeer te controleren, te waarborgen en te handhaven. De toezichthoudende autoriteit is volledig onafhankelijk en onpartijdig in de uitvoering van haar taken en bevoegdheden en zij vraagt noch aanvaardt daarbij instructies. In dit verband moet de toezichthoudende autoriteit beschikken over alle noodzakelijke en beschikbare bevoegdheden en missies om toe te zien op de naleving van de rechten op het gebied van gegevensbescherming en om het bewustzijn hieromtrent te

¹² Deze bijzondere categorieën worden in overweging 10 van de AVG ook "gevoelige gegevens" genoemd.

¹³ Zaak C-362/14, *Maximillian Schrems tegen Data Protection Commissioner*, 6.10.2015, punt 74.

bevorderen. De personeelsbezetting en de begroting van de toezichthoudende autoriteit verdienen eveneens aandacht. De toezichthoudende autoriteit moet ook op eigen initiatief onderzoeken kunnen verrichten.

2) Het gegevensbeschermingssysteem moet een goed nalevingsniveau waarborgen

Het systeem van een derde land moet een hoge mate van verantwoording waarborgen en garanderen dat verwerkingsverantwoordelijken en degenen die namens hen persoonsgegevens verwerken zich bewust zijn van hun verplichtingen, taken en bevoegdheden, en dat betrokkenen zich bewust zijn van hun rechten en de wijze waarop zij deze kunnen uitoefenen. Bij het handhaven van de naleving van de regels kunnen doeltreffende en afschrikkende sancties een belangrijke rol spelen, evenals, uiteraard, systemen voor rechtstreekse controle door autoriteiten, controleurs of onafhankelijke functionarissen voor gegevensbescherming.

3) Verantwoordingsplicht

Het gegevensbeschermingskader van een derde land moet verwerkingsverantwoordelijken en/of degenen die namens hen persoonsgegevens verwerken, verplichten zich aan dit kader te houden en te kunnen aantonen, met name aan de bevoegde toezichthoudende autoriteit, dat zij aan de regels voldoen. Voorbeelden van maatregelen in dit verband zijn: effectbeoordelingen van gegevensbescherming, het gedurende een passende periode registreren van gegevensverwerkingsactiviteiten of het bijhouden van logbestanden daarvan, het aanstellen van een functionaris voor gegevensbescherming, of gegevensbescherming door ontwerp en door standaardinstellingen.

4) Het gegevensbeschermingssysteem moet individuele betrokkenen ondersteunen en bijstaan bij het uitoefenen van hun rechten en het toepassen van passende rechtsmiddelen

Er moeten de betrokkene rechtsmiddelen ter beschikking staan waarmee hij/zij snel en effectief, en zonder kosten die een belemmering zouden kunnen vormen, zijn/haar rechten kan uitoefenen en naleving van de regelgeving kan afdwingen. Daartoe moet een derde land beschikken over toezichtsmechanismen die het mogelijk maken klachten onafhankelijk te onderzoeken en eventuele inbreuken op het recht van gegevensbescherming en eerbiediging van de persoonlijke levenssfeer vast te stellen en daadwerkelijk te bestraffen.

Wanneer de regelgeving niet wordt nageleefd, moet de betrokkene ook beschikken over doeltreffende administratieve en gerechtelijke beroepsmogelijkheden, onder meer voor vergoeding van schade als gevolg van de onrechtmatige verwerking van zijn/haar persoonsgegevens. Dit cruciale element moet een systeem omvatten van onafhankelijke beslechting of arbitrage die schadeloosstelling en het opleggen van sancties, waar van toepassing, mogelijk maakt.

Hoofdstuk 4: Essentiële waarborgen in derde landen voor de toegang van instanties voor wetshandhaving en nationale veiligheid om aantasting van grondrechten te beperken

Bij de beoordeling van de adequaatheid van het beschermingsniveau moet de Commissie, op grond van artikel 45, lid 2, onder a), rekening houden met *"de toepasselijke algemene en sectorale wetgeving, onder meer inzake openbare veiligheid, defensie, nationale veiligheid en strafrecht en de toegang van overheidsinstanties tot persoonsgegevens, evenals de tenuitvoerlegging van die wetgeving ..."*.

Het HvJ-EU merkte in het arrest-Schrems op dat *"de uitdrukking 'passend beschermingsniveau' zo [moet] worden opgevat dat die vereist dat het derde land, op grond van zijn nationale wetgeving of zijn internationale verbintenissen, een niveau van bescherming van de grondrechten en de fundamentele vrijheden biedt dat in grote lijnen overeenkomt met het niveau dat binnen de Unie wordt gewaarborgd op grond van Richtlijn 95/46/EG, gelezen in samenhang met het Handvest."* Ook al kunnen de middelen waarvan dat derde land in dit verband gebruik kan maken, anders zijn dan die welke binnen de Europese Unie worden ingezet, deze middelen moeten in de praktijk niettemin doeltreffend genoeg blijken te zijn.¹⁴

In dit verband merkte het Hof ook kritisch op dat in de eerdere veiligheidsbeschikking *"geen enkele vaststelling [is] gedaan ten aanzien van de vraag of er in de Verenigde Staten overheidsregels bestaan ter beperking van dergelijke inmengingen in de grondrechten van de personen van wie de gegevens vanuit de Unie naar de Verenigde Staten worden doorgegeven, waarbij geldt dat de overheidsinstanties van dat land tot een dergelijke inmenging mogen overgegaan wanneer zij legitieme doelstellingen, zoals de nationale veiligheid, nastreven."*

In haar op 13 april 2016 goedgekeurde advies WP237 heeft de WP29 essentiële waarborgen vastgesteld die op het gebied van toezicht een afspiegeling vormen van de jurisprudentie van het HvJ-EU en het Europees Verdrag tot bescherming van de rechten van de mens. Hoewel de aanbevelingen in dit advies van kracht blijven en in aanmerking moeten worden genomen bij de beoordeling van de adequaatheid van een derde land op toezichtsgebied, kan de toepassing van deze waarborgen variëren als het gaat om de toegang tot gegevens voor doeleinden van rechtshandhaving en nationale veiligheid. Desalniettemin moeten alle derde landen, om als adequaat te worden aangemerkt, de volgende vier waarborgen voor de toegang tot gegevens eerbiedigen, ongeacht of het gaat om nationale veiligheid of rechtshandhaving:

- 1) De verwerking moet gebaseerd zijn op duidelijke, precieze en toegankelijke regels (rechtsgrond);**
- 2) De noodzaak en evenredigheid met betrekking tot de nagestreefde legitieme doelstellingen moeten worden aangetoond;**
- 3) De verwerking moet worden onderworpen aan onafhankelijk toezicht;**
- 4) De betrokken personen moeten beschikken over doeltreffende beroepsmogelijkheden.**

¹⁴ Zaak C 362/14, *Maximillian Schrems tegen Data Protection Commissioner*, 6.10.2015, punt 74..