DATA DRIVEN MARKETING ASSOCIATION

DATA DELEN BUITEN DE EU

JULI 2020

1. Intro

Op 16 juli 2020 deed het Europese Hof van Justitie een uitspraak met enorme consequenties voor het internationale dataverkeer. Privacy Shield, het certificeringsmechanisme dat de juridische basis vormt voor doorgifte van data aan ruim 5500 Amerikaanse organisaties is onrechtmatig verklaard. Denk daarbij aan de bekendste cloud aanbieders, sociale netwerken, advertentienerwerken, hostingpartijen en tools. Iedere doorgifte van persoonsgegevens die gebaseerd werd op Privacy Shield is daarmee per direct een overtreding van de AVG. Aan het alternatief worden door het Hof strenge eisen gesteld. Reden voor iedere organisatie om in kaart te brengen of je organisatie hierdoor geraakt wordt en wat je nu al kunt doen.

1.1 De wereld vóór de Schrems II-uitspraak

De AVG[1] stelt eisen aan de doorgifte van persoonsgegevens door een verwerkingsverantwoordelijke (hierna verantwoordelijke) naar buiten de EU. Vooraf een belangrijke definitie: wanneer kun je spreken van 'doorgifte'? In de AVG Handleiding van de Rijksoverheid wordt dit als volgt omschreven: *"Op het moment dat u persoonsgegevens naar landen buiten de Europese Unie stuurt, of vanuit deze landen toegang biedt tot uw gegevens, dan is er sprake van een doorgifte van persoonsgegevens"* [2]

Je kunt dus spreken van doorgifte zodra je ervoor zorgt dat persoonsgegevens verwerkt worden door iemand buiten de Europese Unie (EU)[3]. Verwerken heeft in de AVG een zeer brede definitie[4]. Je moet er dus van uitgaan dat er bijvoorbeeld sprake is van doorgifte wanneer:

- Je een e-mail met persoonsgegevens stuurt naar een ontvanger buiten de EU
- Wanneer je persoonsgegevens door een verwerker buiten de EU laat verwerken, ook al staan de persoonsgegevens binnen de EU opgeslagen. Dit kan al het geval zijn wanneer men van buiten de EU leesrechten heeft
- Wanneer je persoonsgegevens opslaat in een clouddienst buiten de EU
- Wanneer je persoonsgegevens opslaat op een server buiten de EU

Als er sprake is van doorgifte buiten de EU moet de verantwoordelijke die de gegevens doorgeeft (hierna 'exporteur'), of de ontvanger nou een verwerker of een verantwoordelijke is, zorgen dat

[1] Het gaat hier om hoofdstuk 5 van de AVG: Doorgiften van persoonsgegevens aan derde landen of internationale organisaties
[2] Handleiding Algemene verordening gegevensbescherming en Uitvoeringswet Algemene verordening gegevensbescherming, Ministerie van Justitie en Veiligheid.
[3] Waar we in dit document spreken over de EU gaat het feitelijk om de Europese Economische Ruimte (EER). Dat zijn de 27 EU-landen plus Liechtenstein, Noorwegen en IJsland.
[4] : Een niet-limitatieve lijst van handelingen met persoonsgegevens die volgens de AVG gelden als 'verwerken': het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens;

de gegevens buiten de EU gelijkwaardig beschermd worden. De AVG biedt daarvoor een aantal instrumenten, waarvan er in het kader van de Schrems II-uitspraak twee relevant zijn:

1. Het adequaatheidsbesluit

De EU bepaalt hiervoor in een besluit dat het ontvangende land "een passend beschermingsniveau waarborgt". Dat gebeurde recent betreffende Japan. Andere landen die op de 'veilige lijst' staan zijn onder andere Argentinië, Canada (alleen commerciële organisaties), Nieuw Zeeland, Zwitserland en Uruguay. De verwachting is dat binnenkort ook Zuid-Korea aan deze lijst toegevoegd zal worden.

Voor de Verenigde Staten werd niet besloten dat het een passend beschermingsniveau waarborgt. Voor het waarborgen van een passend beschermingsniveau in de Verenigde Staten is er een aanvullend certificeringsmechanisme opgezet, waar Amerikaanse organisaties zich bij konden aansluiten. Dit heet het Privacy Shield. Met de aanvullende waarborgen van dit programma mochten Europese exporteurs aannemen dat, als de ontvangende partij op de lijst van het Privacy Shield stond, de bescherming adequaat was.

2. Standard Contractual Clauses (SCC's)

Voor het doorgeven van persoonsgegevens naar landen die van de EU nog geen adequate status hebben gekregen moet de exporteur zelf zorgen voor 'passende waarborgen'. De AVG biedt daarvoor zeven opties. Voor deze handleiding is er één met name relevant: *"standaardbepalingen inzake gegevensbescherming die door de Commissie volgens de in artikel 93, lid 2, bedoelde onderzoeksprocedure zijn vastgesteld".* Deze worden ook wel Standard Contractual Clauses (SCC's) genoemd. Een door de Europese Commissie aangeboden modelcontract dat je als addendum bij een verwerkersovereenkomst kunt afsluiten met de ontvangende partij uit het buitenland.

1.2 Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems 1.3 (Case C-311/18, "Schrems II")

Max Schrems, een Oostenrijkse privacy-activist, is inmiddels een bekende in privacyland. Hij slaagde er in 2015 in om via het Europese Hof van Justitie de voorganger van het Privacy Shield, genaamd 'Safe Harbor', ongeldig te laten verklaren.

In 2020 stond hij opnieuw tegenover Facebook. Hij beargumenteerde dat ook het Privacy Shield onvoldoende waarborgen biedt. Met name de toegenomen bevoegdheden van Amerikaanse inlichtingendiensten zouden ervoor zorgen dat er in de VS niet gesproken kan worden van een passend beschermingsniveau voor de gegevens van Europese burgers. Op 16 juli 2020 deed het Hof uitspraak. Het zette een streep door het Privacy Shield, en deed ook een aantal verrijkende uitspraken over de SCC's. Vooraf werd ervoor gevreesd dat deze contracten, die voor veel organisaties het enige realistische alternatief zijn voor doorgifte op basis van het Privacy Shield, ook ongeldig verklaard zouden worden. Het zou de 'perfect storm' zijn waar een aantal privacy-experts vooraf voor waarschuwden. De uitspraak van het hof komt er aardig bij in de buurt. De SCC's worden niet ongeldig verklaard, maar er wordt wel een kanttekening bij gemaakt. Exporteurs mogen er niet langer van uitgaan dat deze contracten zorgen voor passende waarborgen. Naast het sluiten van de SCC's waarin de ontvangende partij buiten de EU ervoor tekent dat het een beschermingsniveau gelijkwaardig aan de AVG zal garanderen, moet de exporteur nagaan of het ontvangende land wel adequate bescherming biedt. Ofwel: kan de ontvangende partij de beloftes wel waarmaken?

Dat geldt niet alleen voor de VS, maar voor alle landen buiten de EU zonder 'adequate' status. Het is vooralsnog een raadsel hoe zo'n beoordeling plaats moet vinden. Privacy-experts spreken van een onmogelijke opgave, die SCC's in de praktijk ook onwerkbaar maakt.

2. Vijf acties om compliant te worden

De situatie lijkt op die in 2015 na Schrems I, waarbij het Transatlantische dataverkeer per direct onrechtmatig werd verklaard. Alleen is nu het alternatief, de SCC's, ook sterk ingeperkt. Hieronder leggen we je uit wat je op dit moment kunt doen om de impact van deze uitspraak in kaart te brengen, en de acties die je nu al kunt nemen om (zo veel mogelijk) compliant te zijn.

1. Breng ontvangers van data in kaart

Dit kun je terugvinden in je verwerkingenregister. Sinds de AVG is het bijhouden van een dergelijk register verplicht. In dat register moet vermeld staan welke (categorieën van) ontvangers van persoonsgegevens er zijn. Controleer wanneer dit register voor het laatst is bijgewerkt. Kijk of er sinds die datum nieuwe ontvangers van persoonsgegevens bijgekomen zijn. Werk het register bij indien nodig.

2. Controleer welke ontvangende partijen gegevens verwerken buiten de EU

Ook dit zou in het verwerkingenregister terug moeten te vinden zijn. De AVG verplicht het vermelden van doorgifte van persoonsgegevens buiten de EU en de bijbehorende waarborgen in dit register. Begin met partijen die afkomstig zijn van buiten de EU, bij die groep is de kans logischerwijs het grootst dat gegevens buiten de EU belanden.

Kijk vervolgens naar de Europese ontvangers, en ga er niet vanuit dat deze hun gegevens enkel in de EU opslaan. Controleer ook voor Europese partijen of de gegevens naar buiten de EU gebracht worden. Bijvoorbeeld doordat gebruik wordt gemaakt van cloudopslag buiten de EU. Als het gaat om verwerkers (bijvoorbeeld tool-aanbieders) zou dit in de verwerkersovereenkomst opgenomen moeten zijn. Verwerkers mogen namelijk niet zonder goedkeuring van de verantwoordelijke de gegevens buiten de EU brengen.

Ook mag een verwerker niet zonder de goedkeuring van de verantwoordelijke een andere verwerker (ook wel 'sub-verwerker') inschakelen. Op die manier hou je als verantwoordelijke regie over de keten. Zorg ervoor dat je niet enkel vaart op de afspraken die op papier zijn gemaakt. Doe wat mogelijk is om voor de keten die onder de verantwoordelijkheid van jouw organisatie staat inzichtelijk te maken waar data de EU verlaten. Kijk daarvoor ook naar eventuele sub-verwerkers van je verwerkers. Bijvoorbeeld de hostingpartij van je webbouwer, of de analysetools van je marketingbureau. Je bent als opdrachtgever verantwoordelijk voor alle verwerkingen die - direct of indirect - in opdracht van jouw organisatie plaatsvinden.

We raden je aan om in ieder geval naar de volgende tools te kijken:

- Cloudproviders (check ook waar de back-ups opgeslagen worden)
- Webhosting
- E-maildiensten
- Socialmediaplatformen
- Cookietools
- CRM-systemen
- Socialmediamonitoring
- Videobelapplicaties

In de verwerkersovereenkomst met deze organisaties moet vermeld staan of de gegevens doorgegeven worden buiten de EU.

3. Kies waar mogelijk voor gegevensopslag binnen de EU

Veel dienstverleners van buiten de EU hebben de afgelopen jaren de mogelijkheid toegevoegd om te kiezen voor gegevensopslag binnen de EU. Als dat gebeurt op een manier waarbij er daadwerkelijk geen verwerking is buiten de EU, hoeven er geen extra maatregelen getroffen te worden. Let op: er kan alsnog sprake zijn van doorgifte wanneer een supportafdeling van buiten de EU op verzoek kan meekijken in het systeem.

Vindt de doorgifte plaats bij subverwerkers van de verwerkers die je inschakelt? Dring er dan bij die verwerkers op aan dat zij ervoor zorgen dat de gegevens bij hun onderaannemers in Europa blijven.

4. Informeer de betrokkenen

Ook het informeren over doorgifte is al een wettelijke verplichting. De betrokkene moet er (bijvoorbeeld in het privacy statement van de verantwoordelijke organisatie) over geïnformeerd worden dat zijn of haar gegevens worden doorgegeven buiten de EU. Er moet ook geïnformeerd worden over de manier waarop er voor die doorgifte een passend beschermingsniveau gerealiseerd wordt in het land van bestemming. We raden aan om die informatie aan te passen op een manier waarop duidelijk wordt dat je organisatie op de hoogte is van de Schrems II-uitspraak. Zeker wanneer nog niet helemaal duidelijk is of je organisatie voldoet aan de AVG op dit punt is het aanbevolen om helder te informeren dat hier aan gewerkt wordt. Wanneer je regelmatig contact hebt met de doelgroep zou je er bijvoorbeeld ook aandacht aan kunnen besteden in een nieuwsbrief.

5. Houd de toezichthouder in de gaten

Nu een groot deel van het bedrijfsleven per direct in overtreding van de AVG is, ligt de bal bij de toezichthouder. Starten zij direct met handhaven of verlenen ze een coulanceperiode waarin de doorgifte 'gedoogd' wordt? Formeel heeft de AP de mogelijkheid om boetes op te leggen tot 4% van de wereldwijde omzet. Toen de voorloper van het Privacy Shield ongeldig werd verklaard verleenden de toezichthouders in Europa een gedoogperiode van 9 maanden waarbinnen de Europese Commissie en de Amerikaanse regering de tijd hadden om de Safe Harbor-constructie te aan te passen. Het is nu afwachten of de toezichthouders opnieuw bereid zijn om een dergelijk gedoogperiode te hanteren. In de reacties op de Schrems II-uitspraak spreekt de Autoriteit Persoonsgegevens niet over een gedoogperiode. In een Frequently Asked Questions-document maakt de EDBP, de Europese koepel van privacytoezichthouders, duidelijk dat er wat hen betreft geen sprake van gedogen zal zijn. Het lijkt een kwestie van tijd voordat er in heel Europa klachten van privacy-activisten worden ingediend bij toezichthouders.

3. Frequently Asked Questions

3.1 Is deze uitspraak definitief?

Ja, het Europees Hof van Justitie is de hoogste rechter van Europa. De uitspraak heeft direct effect in de hele Europese Unie en er is geen mogelijkheid om in beroep te gaan. In theorie zou het Hof zich in een latere zaak kunnen bedenken, maar deze uitspraak past volledig in de lijn die het Hof met de Schrems I-uitspraak heeft ingezet. We moeten er daarom van uitgaan dat dit de nieuwe realiteit is.

3.2 Waarom is Privacy Shield ongeldig verklaard?

De zorgen omtrent het delen van data met de Verenigde Staten dateren uit de periode waarin Edward Snowden onthullingen deed over het spionageprogramma van de inlichtingendiensten in de VS. De vergaande bevoegdheden van diensten t.a.v. buitenlanders vormen een belangrijk punt van zorg wanneer gegevens van Europeanen in de VS worden opgeslagen. Het Privacy Shield is het resultaat van afspraken tussen de Europese Commissie en de Amerikaanse regering, waarbij gecertificeerde Amerikaanse organisaties als 'veilig' beschouwd mogen worden. Er geldt dan formeel een beschermingsniveau dat in essentie gelijkwaardig is aan dat in de EU. Volgens het Hof kwam dat niet (meer) overeen met de realiteit. De bevoegdheden van inlichtingendiensten vormen een beperking op het recht op gegevensbescherming van Europese burgers. Bovendien kunnen Europese burgers in de VS onvoldoende hun rechten uitoefenen. Dit was voor het Hof voldoende aanleiding om het besluit dat aan het Privacy Shield ten grondslag ligt onrechtmatig te verklaren. Net zoals het dat in 2015 deed met voorloper Safe Harbor.

3.3 Kan ik wel nog SCC's afsluiten?

Het Europese Hof liet zich naast het ongeldig verklaren van het Privacy Shield ook uit over de

modelcontracten van de Europese Commissie. Deze contracten zijn een middel om burgers in Europa een niveau van bescherming te bieden voor hun gegevens dat onafhankelijk is van waar hun gegevens zich in de wereld bevinden. In de AVG is bepaald dat de exporteur moet zorgen voor:

1. passende waarborgen
2. afdwingbare rechten
3. doeltreffende rechtsmiddelen

Het Hof wijst er in haar uitspraak nadrukkelijk op dat het aan de exporteur is om na te gaan of dat waargemaakt kan worden in het land van bestemming. Het afsluiten van SCC's als maatregel om data te kunnen doorgeven aan een ontvanger in een niet-EU-land is op zichzelf dus niet onrechtmatig. De verantwoordelijke moet kunnen beargumenteren dat het voor de ontvanger van de data in het land van bestemming mogelijk is om de afspraken uit de SCC's na te komen. Wie dat niet kan onderbouwen kan daarvoor beboet worden door de toezichthouder.

3.4 Zijn mijn bestaande SCC's nog geldig?

Officieel is er geen besluit dat deze overeenkomsten ongeldig zijn. Het is door het Hof echter wel duidelijk gemaakt dat er een onderzoeksplicht bij hoort. Wanneer je afspraken hebt gemaakt met ontvangers die in hun lokale rechtssysteem niet in staat zijn om een passend beschermingsniveau te bieden zit je met dilemma. Formeel gezien zou je nog kunnen stellen dat je aan de AVG-verplichting hebt voldaan, tot je van de ontvanger te horen krijgt dat ze hun verplichtingen niet kunnen nakomen. In de praktijk lijkt dit een onhoudbare situatie. Als het land van bestemming niet voldoende waarborgen biedt, kan er geen sprake zijn van doorgifte van gegevens, tenzij je op een of andere manier extra waarborgen weet te treffen. Bijvoorbeeld door de gegevens volledig versleuteld op te slaan, waardoor veiligheidsdiensten niets met de data kunnen doen. Voor de Verenigde Staten lijken deze extra waarborgen (wat deze ook mogen zijn) onmisbaar, het Hof kwam immers in haar besluit over het Privacy Shield zelf tot de conclusie dat het rechtssysteem in de VS onvoldoende waarborgen biedt.

3.5 Wat betekent dit in het kader van de Brexit?

Met het naderende uittreden van het Verenigd Koninkrijk (VK) zal het land daarmee vanzelfsprekend een niet-EU-land worden. Doorgifte van persoonsgegevens naar het VK zal volgens hetzelfde mechanisme moeten gewaarborgd worden als andere landen buiten de EU. Uit de gesprekken over het uittreden van het VK is duidelijk dat het de voorkeur heeft om zo snel mogelijk te beslissen over een adequaatheidsbesluit, waardoor het land de facto alsnog als 'veilig' wordt bestempeld. Privacy-experts achten de kans daarop gering doordat het Verenigd Koninkrijk net als de VS over omvangrijke spionagebevoegdheden voor inlichtingendiensten beschikt. Met name de Investigatory Powers Act uit 2016 verleent een brede bevoegdheid om communicatie te onderscheppen en toegang te verkrijgen tot gegevens. Nu in de Schrems II-uitspraak duidelijk wordt wat de consequenties van dergelijk bevoegdheden zijn is zo'n adequaatheidsbesluit wellicht verder weg dan ooit. Ook het oordeel over de SCC's heeft een impact op data doorgifte naar het VK na Brexit.
Exporteurs zullen bij het afsluiten van SCC's als middel voor het zorgen voor een passend beschermingsniveau moeten beoordelen of het rechtssysteem van het Verenigd Koningkrijk genoeg waarborgen biedt. Dat lijkt vrijwel een onmogelijke opgave. Daardoor is het een risico om je op SCC's te beroepen, een toezichthouder kan alsnog besluiten een boete uit te delen als het onderzoek van de exporteur niet degelijk onderbouwt waarom het land voldoende waarborgen biedt.
Het tekenen van SCC's met organisaties in de VS lijkt op dit moment niet meer mogelijk. Als exporteur weet je door de Schrems II-uitspraak dat er door organisaties die vallen onder de Amerikaanse inlichtingenwetgeving geen passend beschermingsniveau gerealiseerd kan worden. Ook de Amerikaanse partij kan deze overeenkomst niet tekenen, omdat ze weten dat ze de verplichtingen die erin staan niet kunnen nakomen.

3.6 Wat moet ik doen als ik tot de conclusie kom dat mijn SCC's onvoldoende waarborgen bieden?

Wanneer uit je analyse van de omstandigheden van de doorgifte van de gegevens en eventuele aanvullende maatregelen blijkt dat er geen passende waarborgen zijn, dan moet je de doorgifte van persoonsgegevens naar dat land opschorten. Is dat niet mogelijk en moet de doorgifte plaatsvinden? Dan ben je volgens de

SCC's verplicht om dat te melden aan de bevoegde toezichthouder (in Nederland de Autoriteit Persoonsgegevens). De toezichthouder heeft vervolgens de mogelijkheid om een controle te verrichten bij de ontvangen van de gegevens.

3.7 Wat zijn aanvullende waarborgen?

Het Hof legt in de Schrems II uitspraak uit dat exporterende organisaties er met aanvullende maatregelen voor kunnen zorgen dat de gegevens in landen buiten de EU alsnog voldoende beschermd zijn. Dit zou zelfs het geval kunnen zijn bij organisaties die vallen onder de Amerikaanse inlichtingenwetgeving. Het Hof specificeert niet om welke maatregelen het gaat, maar te denken valt dat encryptie hier een uitkomst kan bieden. Wanneer de gegevens zowel versleuteld worden verzonden als opgeslagen, zonder dat de Amerikaanse organisatie over de sleutel beschikt, zou het risico van toegang door een inlichtingendienst ingeperkt kunnen worden.

3.8 Kan toestemming van de betrokkene een oplossing bieden?

De AVG biedt de mogelijkheid om toestemming te hanteren als middel om de doorgifte rechtmatig te maken. Dit maakt het mogelijk om als betrokkene voor je eigen persoonsgegevens te beslissen dat de gegevens doorgegeven mogen worden buiten de EU, bijvoorbeeld door het plaatsen van een bericht op Twitter. Toestemming vragen aan derden kan problematisch zijn, omdat deze toestemming aan alle eisen van de AVG moet voldoen. De toestemming moet vrij, specifiek, ondubbelzinnig en op informatie berust zijn. Bovendien moet de betrokkene die toestemming ook op ieder moment zonder nadelige gevolgen kunnen intrekken.

3.9 Hoe weet ik of mijn verwerker data doorgeeft buiten de EU?

Dat moet beschreven staan in de verwerkersovereenkomst. Daarin hoort te staan of doorgifte toegestaan is. Dat geldt ook voor sub-verwerkers. (Sub-)verwerkers mogen niet zelfstandig beslissen om persoonsgegevens buiten de EU te delen. Daarbij maakt het niet uit of het gaat om de opslag van back-ups, toegang voor onderhoud of service, of een tijdelijke doorgifte.

3.10 Wat als ik in de verwerkersovereenkomst doorgifte heb toegestaan?

Als doorgifte door de (sub-) verwerker contractueel is toegestaan door de verantwoordelijke organisatie, maar er in het land van bestemming geen sprake is van beschermingsniveau dat gelijkwaardig is aan dat in de EU, dan is de enige optie om de doorgifte te staken. Met de (sub-) verwerker zal een amendement of een nieuwe overeenkomst gesloten moeten worden die hun bevoegdheid om data buiten de EU door te geven in te perken. De doorgifte is op dit moment weliswaar geen contractbreuk van de (sub-)verwerker, maar je bent dan als verantwoordelijke zelf wel in overtreding. Het is daarom van belang om dit zo snel mogelijk te beëindigen.

3.11 Hoe zit het met dochter/zuster/moederondernemingen buiten de EU?

Er kan evengoed sprake zijn van doorgifte buiten de EU wanneer dit plaatsvindt binnen de eigen organisatie(structuur). Daarvoor geldt hetzelfde als wanneer de gegevens naar een andere organisatie gestuurd worden. De AVG biedt echter het middel van Binding Corporate Rules (BCR) als maatregel om doorgifte te waarborgen. De Schrems II-uitspraak lijkt ook BCR's te bemoeilijken omdat de lokale context in de landen van bestemming geanalyseerd zal moeten worden.

3.12 Is het voldoende als een Amerikaanse dienstverlener de data in de EU opslaat?

De AVG-bepalingen over doorgifte buiten de EU zijn vanzelfsprekend enkel van toepassing wanneer er daadwerkelijk sprake is van doorgifte. Amerikaanse organisaties moeten naast de AVG ook voldoen aan Amerikaanse wetgeving. Zo is er sinds enkele jaren de CLOUD Act, die bepaalde Amerikaanse organisaties verplicht om gegevens die buiten de VS worden verwerkt te bewaren en verstrekken op verzoek van Amerikaanse veiligheidsdiensten. Deze verplichte achterdeur zorgt ervoor dat gegevensopslag door Amerikaanse aanbieders binnen Europa alsnog kan zorgen voor toegang door Amerikaanse veiligheidsdiensten. De Amerikaanse organisatie komt dan in een juridische spagaat: negeer het verzoek van de veiligheidsdienst, of overtreed artikel 48 AVG.
Voor de verantwoordelijke organisatie lijkt het mogelijk om zelfs in dat geval nog AVG-compliant

te blijven doordat je zelf geen data doorgeeft buiten de EU. De overtreding zou dan begaan worden door de Amerikaanse organisatie. Deze organisatie treedt dan op als verantwoordelijke. Formeel zou jouw organisatie dan geen persoonsgegevens doorgeven buiten de EU. Dat is uiteraard de juridische werkelijkheid, je kunt je afvragen of het niet raadzaam is om te kijken naar een Europees alternatief.

Bovendien geldt dat opslag niet het enige criterium is voor doorgifte. Wanneer de gegevens opgeslagen zijn in de EU, maar er is toegang vanuit de VS, dan is er alsnog sprake van doorgifte buiten de EU. In de praktijk zal er vaak sprake zijn van toegang, bijvoorbeeld voor het verlenen van klantenservice of het onderhouden van de techniek.

3.13 Kan mijn organisatie een boete krijgen als we op dezelfde manier verder werken?

Ja dat kan. De uitspraak is direct van toepassing. Een overtreding kan door de Autoriteit Persoonsgegevens beboet worden met maximaal 20 miljoen Euro of 4% van de wereldwijde omzet. Uiteraard zal de AP bij het opleggen van een boete aan de hand van haar boetebeleidsregels moeten kijken wat de werkelijke boete wordt. Daarbij spelen onder andere de aard, de ernst en de duur van de inbreuk een rol. Ook opzet en nalatigheid, het aantal getroffen betrokkenen en de geleden schade worden meegenomen bij het bepalen van de boete. Het is daarom aan te raden om zo snel mogelijk maatregelen te nemen. Wanneer het niet mogelijk is om op korte termijn compliant te worden is het aanbevolen om daar transparant over te zijn richting de betrokkenen, en een planning te maken met de te nemen stappen. Zo kan, mocht dat nodig zijn, aan de toezichthouder aangetoond worden dat je organisatie ervan bewust is, en de vereiste maatregelen op de planning staan.