

De datum is, als volbloed Europeaan, in mijn geheugen gegrift: 6 oktober 2015. Op deze dag werd door het Europese hof van justitie bepaald dat de Safe Harbor Policy de rechten van Europese burgers onvoldoende beschermd. De aanleiding voor deze uitspraak was een Facebook case, waarbij de Oostenrijkse jurist, auteur en privacy activist Max Schreiber facebook voor het gerecht sleepte omdat hij vond dat zijn privacy geschonden werd door de data transfers tussen Europa en de VS door Amerikaanse bedrijven. Het hof gaf hem gelijk en hiermee kwam een streep door overeenkomst 2000/520/EC waarin de safe harbor policy tussen de VS en Europa geregeld werd.

## Safe Harbor Policy?

In oktober 1998 nam de Europese commissie een besluit over data bescherming die regelt dat data overdracht van persoonlijke data naar niet-europese unielanden verboden is als niet voldaan wordt aan de Europese data beschermingsregels (95/46/EC). Nu is de wet in de VS op het gebied van privacy anders geregeld dan in Europa en was er een separate overeenkomst nodig om de verschillen te kunnen overbruggen voor Amerikaanse bedrijven die in Europa zaken wilden doen waarbij persoonlijke data verwerkt wordt op servers die in de VS staan. Voor dit doel ontwikkelden de US Department of Commerce en de Europese Commissie een "Safe Harbor Framework". Dit framework stond al enige jaren onder druk omdat het een framework is dat niet verplicht is en waartegen bedrijven zich door zelf-certificering voor kunnen kwalificeren. In juli 2000 werd bepaald dat bedrijven die zich conform het safe harbor framework gekwalificeerd hebben, persoonlijke data mogen transporteren vanuit de EU naar de VS.

Als Amerikaanse organisatie hoef je maar te voldoen aan 7 basisprincipes en antwoord te kunnen geven op een 15 vragen tellende lijst, de zogenaamde "FAQ". Zodra je daaraan voldoet, krijg je het stempel "Safe Harbor Certified" en mag je binnen en buiten de EU persoonsgegevens transporteren en opslaan. Zonder al te diep op de zeven basisprincipes in te gaan zijn dit de volgende:

1. Notice (verstrek informatie dat data verzameld wordt en wat ermee gebeurt)
2. Choice (Individueel moeten het recht hebben om van een opt-out gebruik te kunnen maken waarbij data naar een 3e partij overgebracht moet kunnen worden)
3. Onward transfer (Data transfer naar 3e partijen mag alleen als die organisaties adequate databeschermingsregels hanteren)
4. Security (Verlies van data moet zoveel mogelijk vermeden worden door "redelijke inspanning")
5. Data Integrity (Data moet relevant en betrouwbaar zijn en het doel dienen waarvoor zij verzameld wordt)

6. Access (Individueen moeten bij hun eigen data kunnen en deze kunnen bewerken of vernietigen als deze data inaccuraat of onjuist is)
7. Enforcement (Bovenstaande regels moeten gewaarborgd kunnen worden).

## **Waar ging het om als iedereen aan de regels van Safe Harbor voldeed?**

In de rechtszaak die speelde werd door het Europese hof van justitie geïdentificeerd dat de Amerikaanse overheid binnen de Amerikaanse wetgeving persoonlijke data mag verzamelen van servers die in de VS staan zonder dat zij hiervoor een opt-in nodig heeft van de eigenaar van de data. Dit betekent dat de Amerikaanse overheid in principe altijd in persoonlijke data mag snuffelen zonder dat de persoon in kwestie hiervan op de hoogte hoeft te worden gebracht. Hiermee worden privacy rechten van Europese burgers geschonden, de basis principes van het Safe Harbor Framework ontweken en is het framework niet toepasbaar, wat uiteindelijk dan ook leidde tot de uitspraak dat het framework "invalid" is.

## **Illegale praktijken**

Hoe zit het nu na deze uitspraak? Strikt genomen zijn alle Amerikaanse organisaties die momenteel persoonlijke data intercontinentaal verwerken en buiten Europa opslaan illegaal bezig, toch? Ook al hebben de bedrijven zich aan de afspraken gehouden, volgens de letter van de uitspraak is momenteel iedere datatransfer van persoonlijke data naar servers die zich buiten de EU bevinden, illegaal. Organisaties zullen hier dus een antwoord op moeten vinden. In de tussentijd heeft Vera Jourova, de EU commissaris voor Data Protectie aangegeven dat men door kan gaan zolang andere veiligheden gegarandeerd kunnen worden. Wat dat precies is, kan per EU land zelfs verschillen en zal een behoorlijke uitzoekklus worden voor een Facebook, Google, etcetera. Met name zal naar de voorwaarden gekeken gaan worden, de eigen "code of conduct" en de bedrijfspolicies. En dan moet de eindgebruiker deze natuurlijk nog accepteren..

## **Hoe verder?**

Dit is de hamvraag die momenteel de Amerikaanse en Europese beleidsmakers enorm bezig houdt. Het is niet erg aannemelijk dat de Amerikaanse overheid haar wetten gaat aanpassen om EU burgers betere privacy bescherming te kunnen bieden. Aan de andere kant (van de oceaan) probeert de EU uiteraard nu wel om betere beschermingsregels te kunnen opstellen die de data en privacy van EU burgers juist beter kan beschermen. Dit lijkt een bijzonder lastige klus te worden voor de beleidsmakers en betrokken juristen.

Als dit positiever bekeken kan worden, biedt het een enorme mogelijkheid om de soms nog behoorlijk verschillende privacy regels binnen de EU landen beter op elkaar af te stemmen. Zeker is dat als de uitspraak overeind blijft, dat data dat door EU burgers opgeslagen wordt, de Europese unie niet mag verlaten. Een geweldige kans voor Europese datacenters en providers. En uiteindelijk voor de Europese Cloud industrie.

## **Security Statement BPdelivery**

Voor de goede orde: BPdelivery maakt uitsluitend gebruik van Europese datacenters waarbij de data uitsluitend op Europese bodem opgeslagen wordt en onder Europese wetgeving valt. Lees hiervoor onze data security statement op de website ([www.bpdelivery.com](http://www.bpdelivery.com)).

## **Over BPdelivery**

**BP**delivery richt zich op de optimalisatie van de interne bedrijfsprocessen tussen de service- of facilitaire organisatie, hun interne gebruikers en externe leveranciers. Het unieke concept van BPdelivery is dat de relatie tussen alle partijen niet wordt beïnvloed door de service. Omdat de service via het internet werkt (the Cloud), is deze altijd beschikbaar. U kunt onze dienst gebruiken voor elk product dat u intern levert. Wij leveren volledig User management, Product Management, Contract Management, Portfolio Management en Factuur Management.