Persoonsgegevens doorgeven naar de VS na het Schrems-II arrest?

Mr. Bart Van den Brande
Partner
bart@siriuslegal.be

Het is de Oostenrijker Max Schrems alweer gelukt om zijn slag thuis te halen in één van de vele privacyrechtzaken die hij al jaren met regelmaat voert. De gevolgen zijn aanzienlijk deze keer. Nadat eerder al het "Safe Harbor" systeem onderuit werd gehaald, is nu ook het "Privacy Shield" - op volkomen logische gronden overigens- gesneuveld.

Het "Privacy Shield" tussen de EU en de VS zorgde ervoor dat persoonsgegevens veilig en conform GDPR uitgevoerd konden worden door Europese bedrijven naar de Verenigde Staten. Heel wat Amerikaanse clouddiensten, apps en software tools baseerden zich op het Privacy Shield om juridisch compliant hun diensten te kunnen aanbieden aan Europese klanten.

Maar dat Privacy Shield blijkt nu dus zelf helemaal niet conform de Europese privacyregels te zijn en het EHJ haalt het hele systeem onderuit.

Wat betekent dit voor jouw bedrijf? We overlopen een en ander hieronder.

Doorgifte van persoonsgegevens buiten de EU?

Persoonsgegevens doorgeven aan personen of bedrijven buiten de Europese Unie mag niet zomaar onder GDPR. De Europese wetgever gaat er van uit dat landen buiten de EU (of beter de EER, dat is de EU uitgebreid met Noorwegen, Ijsland en Liechtenstein) niet per definitie hetzelfde niveau van privacybescherming kunnen bieden als het niveau dat door GDPR in Europa bestaat. Daarom mogen persoonsgegevens alleen doorgegeven worden buiten de EER onder zeer specifieke voorwaarden.

LexGO sprl - www.lexgo.be - (c) 2021 - All rights reserved

In de eerste plaats bestaat er een (zeer korte) lijst met “veilige” landen, die geacht worden een gelijkaardig niveau van bescherming te bieden op basis van hun eigen wetgeving. Op deze lijst staan, naast een aantal landen uit het Britse Gemenebest, bijvoorbeeld Japan, Canada, Argentinië en Israël.

Wie gegevens wil doorgeven naar een ontvanger in een land dat niet op deze lijst staat, kan dat grosso modo doen op basis van twee systemen. Als het gaat om doorgifte binnen een groep van bedrijven, dan kan men intern zogenaamde “Binding Corporate Rules” opstellen. Dat is een soort van intern reglement dat goedgekeurd moet worden door de overheid en dat binnen de groep de veiligheid van doorgifte moet garanderen. Als men data wil doorgeven aan een bedrijf dat niet tot dezelfde groep behoort, zoals bijvoorbeeld een cloud provider, een externe software developer, een offshore call center, etc… daarentegen zal men moeten zorgen dat er een overeenkomst getekend wordt met de ontvanger waarin een hele reeks waarborgen expliciet voorzien is. De Europese Commissie heeft met dit doel standaard contractclausules in het leven geroepen die één op één gekopieerd kunnen worden in zo’n overeenkomst.

Wie persoonsgegevens doorgeeft en daarbij niet kan terugvallen op één van deze juridische constructies, riskeert bijzonder hoge boetes.

Privacy Shield?

Heel wat technologiebedrijven zitten in de Verenigde Staten en er is dan ook heel wat data-export of export van persoonsgegevens van de EU naar de VS. Omdat de privacywetgeving in de VS echter absoluut niet hetzelfde “adequate” niveau haalt als de strenge vereisten die GDPR in de EU vooropstelt, is de VS nooit op de korte lijst met “veilige landen” geplaatst door de EU.

Om ervoor te zorgen dat Amerikaanse bedrijven toch handel konden blijven voeren met partners in de EU heeft men al geruime tijd geleden een ander en specifiek systeem opgezet voor gegevensuitwisseling tussen Europa en de Verenigde Staten. Dat systeem heette achtereenvolgens het Safe Harbor systeem en later het Privacy Shield en voorkwam dat Amerikaanse bedrijven een overeenkomst met standaard contractclausules moesten afsluiten met hun klanten in de EU telkens er gegevens aan hen doorgegeven moesten worden, bijvoorbeeld omdat die op hun servers bewaard of verwerkt moesten worden. Safe Harbor en Privacy Shield zorgen ervoor dat Amerikaanse bedrijven geacht worden een adequaat niveau van veiligheid voor persoonsgegevens te kunnen garanderen als zij aan een aantal strikte voorwaarden voldoen en daartoe in de VS gecertifieerd worden. Het is dus niet de Amerikaanse wetgeving, maar wel het veiligheidsniveau aangeboden door Amerikaanse bedrijven dat “adequaat” is.

De eerste versie van dit systeem, Safe Harbor, werd in 2015 al succesvol aangevallen door Max Schrems, die van oordeel was dat geen enkel Amerikaans bedrijf een “adequaat” niveau van veiligheid voor persoonsgegevens kan garanderen omdat de Amerikaanse wetgeving aan

LexGO sprl - www.lexgo.be - (c) 2021 - All rights reserved

Amerikaanse inlichtingendiensten vergaande rechten verleent om persoonsgegevens te monitoren en te analyseren. Deze klacht leidde er uiteindelijk toe dat het Safe Harbor systeem ongeldig werd verklaard en werd vervangen door een gelijkaardig systeem dat onder de naam Privacy Shield ging.

Over de geldigheid van dat Privacy Shield, zegt het Europees Hof nu zeer terecht dat ook deze regeling niet kan zorgen voor een beschermingsniveau dat gelijkwaardig is aan het beschermingsniveau dat bestaat binnen de EU. Opnieuw is de reden daarvoor de vergaande inmenging van Amerikaanse inlichtingendiensten, die systematisch en op grote schaal data monitoren uit bijvoorbeeld e-mails en cloudopslagdiensten op basis van bijvoorbeeld de Foreign Intelligence Surveillance Act of Executive Order 12333 of nog de Presidential Policy Directive. Het Hof verklaart het Privacy Shield dan ook -terecht- ongeldig.

Wat betekent dit voor mijn bedrijf?

Deze beslissing heeft verstrekkende gevolgen. Héél wat online dienstverleners uit de VS baseren zich immers op het Privacy Shield om rechtsgeldig persoonsgegevens van hun Europese klanten te kunnen verwerken. Heel dat systeem valt nu met één pennentrek in duigen en duizenden Amerikaanse bedrijven voldoen niet meer aan de minimale voorwaarden om persoonsgegevens van Europese burgers te bewaren of verwerken. Het gaat dan bijvoorbeeld om cloudopslagdiensten, hostingdiensten, allerlei online tools voor online marketing, CRM, boekhoudpakketten, ERP, maar bijvoorbeeld ook lokale software developers, consultants, call centers, etc…

Strikt genomen mogen Europese bedrijven van de ene dag op de andere niet meer samenwerken met deze Amerikaanse partners. Als zij dat toch doen stellen ze zich bloot aan immense boetes en als er zich enige vorm van datalek zou voordoen bij zo’n niet conforme partner in de VS, dreigen de betrokken Europese bedrijven bovendien op te draaien voor alle aan zo’n datalek verbonden schade, bovenop de reeds vernoemde boetes.

Een bijkomend probleem: Brexit

LexGO sprl - www.lexgo.be - (c) 2021 - All rights reserved

Niet enkel gegevensexport naar de VS onder het Privacy Shield is overigens een probleem. Tegen eind 2020 tekent zich een even groot juridisch probleem af voor Europese bedrijven die gegevens uitvoeren naar het Verenigd Koninkrijk. Als er tegen eind 2020 geen Brexit deal is, wordt het VK vanaf dat ogenblik immers een “derde” land, dat voorlopig geen adequaatheidsbesluit van de Europese Commissie heeft en waarnaar dus niet langer automatisch persoonsgegevens geëxporteerd mogen worden.

Britse bedrijven bevinden zich met andere woorden tegen eind dit jaar in dezelfde situatie als Amerikaanse bedrijven: zij zullen met hun Europese klanten dataexportovereenkomsten moeten afsluiten op basis van de standaard contractclausules van de Europese Commissie, bij gebreke waaraan Europese bedrijven niet meer met hen zullen mogen samenwerken.

De oplossing

Het Hof oordeelde gelukkig wel dat het systeem van standaard contractclausules wél rechtsgeldig kan blijven bestaan. De oplossing ligt dan ook voor de hand: Europese bedrijven moeten ervoor zorgen dat alle samenwerkingen met Amerikaanse partners die gebaseerd waren op het Privacy Shield zo snel mogelijk vervangen worden door een overeenkomst op basis van de standaard contractclausules van de Europese Commissie…

De Commissie heeft overigens gewerkt aan de modernisering van die standaard clausules, die teruggaan tot 2010 en niet meer GDPR conform zijn. Men heeft even gewacht tot de Schrems-II zaak was opgelost, maar we mogen nu de bijgewerkte clausules eerstdaags verwachten. Wie zich in het verleden baseerde op de oude clausules, zal deze dus binnenkort wellicht ook moeten updaten…

Wat moet je dan precies doen?

1. Kijk goed uit naar nieuwe richtlijnen van jouw lokale Gegevensbeschermingsautoriteit, de EDPB en de Europese Commissie.
2. Doe intussen een interne audit op je lopende overeenkomsten en let op voor:
    - Gegevensoverdracht naar Amerikaanse partners die tot nu toe onder het Privacy Shield vielen
    - Gegevensoverdracht naar Britse partners die tot nu toe binnen de EU vielen
    - Gegevensoverdracht naar elk ander land op basis van de “oude” standaard contractclausules
    - Gegevensoverdracht die afhankelijk is van bindende bedrijfsregels en die

LexGO sprl - www.lexgo.be - (c) 2021 - All rights reserved

gegevensoverdracht naar de VS met zich meebrengt. Het EHJ vermeldt geen Binding Corporate Rules, maar ze zijn een vorm van “passende bescherming” overeenkomstig artikel 46, dus de algemene opmerkingen over de noodzaak om de wet van het importerende land te beoordelen zouden hier ook van toepassing kunnen zijn. Begeleiding op dit punt van toezichthoudende autoriteiten zou bijzonder welkom zijn.

3. Beoordeel voor elke partner of het bestaande kader nog voldoende is
4. Zorg waar nodig voor een nieuwe dataexportovereenkomst op basis van de nieuw af te kondigen standaard contractsclausules
5. Hou in het achterhoofd dat doorgifte van gegevens buiten de EU in se enkel kan als die noodzakelijk is en kies bij voorkeur voor Europese partners
6. Hou rekening met de noodzaak die het Europees Hof van Justitie ook oplegt om het “passend” karakter van de lokale wetgeving te beoordelen, zelfs als er standaard contractclausules (of Binding Corporate Rules binnen een groep van bedrijven) gebruikt worden.
7. Controleer dus, eventueel op basis van een Vendor Assessment List, de volgende punten:
    - Naar welk land persoonlijke gegevens worden overgedragen
    - Of overheidsinstanties in dat land recht zouden kunnen hebben op toegang tot de gegevens
    - Worden de gegevens tijdens het transport versleuteld of getokeniseerd (zie hieronder)
    - Of er, zoals GDPR vereist, naast de standaard contractclausules of Binding Corporate Rules voldoende waarborgen genomen zijn door de ontvanger om het gebrek aan gegevensbescherming in zijn of haar land te compenseren. De gegevensexporteur heeft de plicht te zorgen voor “passende waarborgen”, vooral wat betreft de toegang van overheidsinstanties tot gegevens. Als de (Europese) gegevensimporteur verplicht kan zijn om gegevens ter inzage aan zijn of haar overheid voor te leggen, kan hij niet voldoen aan de vereiste van een “gepast beschermingsniveau en moet hij dat vooraf melden aan de gegevensexporteur. Dit is met name voor de VS een immens probleem omwille van de al eerder aangehaalde wetgeving rond inlichtingendiensten… In dat geval moet de gegevensexporteur elke doorgifte onmiddellijk stopzetten.
8. Stop desnoods de samenwerking met partners die niet kunnen of willen voldoen aan de vereiste voorwaarden. De potentiële gevolgen voor jouw bedrijf zijn veel te groot om risico’s te nemen…

Is elke gegevensoverdracht naar de VS dan illegaal?

LexGO sprl - www.lexgo.be - (c) 2021 - All rights reserved

Dit arrest legt een tijdbom onder zowat élke gegevensoverdracht naar de VS, overigens. Vrijwel alle Europese data wordt immers via onderwaterkabels op de bodem van de oceaan naar de VS overgebracht. Het EHJ merkt op dat de Amerikaanse NSA systematisch toegang heeft tot deze kabels en gegevens kan verzamelen en bewaren voordat deze in de VS aankomen.

Het EHJ zegt terecht dat dit de facto betekent dat persoonsgegevens nooit “veilig” zijn in de VS en nooit verwerkt kunnen worden “*met de minimale waarborgen … met als gevolg dat de bewakingsprogramma’s die op deze bepalingen zijn gebaseerd, niet kunnen worden beschouwd als beperkt tot wat strikt noodzakelijk is*“. Het EHJ merkt verder op dat: “*In die omstandigheden de beperkingen op de bescherming van persoonsgegevens die voortvloeien uit de nationale wetgeving van de Verenigde Staten betreffende de toegang tot en het gebruik door de Amerikaanse overheid van dergelijke gegevens die van de Europese Unie naar de Verenigde Staten worden overgedragen Staten, die de Commissie in het Privacy Shield besluit heeft beoordeeld, zijn niet zodanig omschreven dat zij voldoen aan eisen die in wezen gelijkwaardig zijn aan die welke krachtens het EU-recht vereist zijn … “*.

Dit betekent met andere woorden dat de Amerikaanse wet op zich onverenigbaar is met de minimale gegevensbeschermingsvereisten van de EU. Aangezien alle gegevens die via een onderzeese kabel naar de VS worden verzonden, gevoelig lijken te zijn voor toegang door de NSA, is het moeilijk te zien hoe een gegevensexporteur zou kunnen concluderen dat zijn gegevens voldoende worden beschermd door de ontvanger in de VS. Het is nog even afwachten om te zien hoe de verschillende Gegevensbeschermingsautoriteiten en de EDPB hierop reageren…

LexGO sprl - www.lexgo.be - (c) 2021 - All rights reserved