Stappenplan: Data Export
Wat moet je concreet al doen?

☐ **Stap 1:** maak een inventaris van alle gegevens die je exporteert naar derde landen.

Als je al een dataregister hebt, is dit een eenvoudige stap voor jou en kan je ineens naar de volgende stap gaan. Klinkt het woord 'dataregister' Chinees voor jou, dan leggen we dit graag even uit. De GDPR legt aan elke verwerkingsverantwoordelijke de verplichting op om alle verwerkingsactiviteiten vast te leggen die onder haar verantwoordelijkheid plaatsvinden. Concreet breng je in zo'n dataregister een aantal zaken in kaart voor alle gegevens die je verzamelt: de doeleinden, de middelen, de rechtsgrond, de risico's voor de privacy van de betrokkenen, de toegang tot die gegevens, de doorgifte aan derden, … Zo krijg je een overzicht van alle datastromen binnen de onderneming. Dit vereenvoudigt de eventuele controles en audits aanzienlijk. Je kan hiervoor gebruikmaken van een aantal kwalitatieve vragenlijsten of evaluatietools, maar uiteraard kan Sirius legal je hierbij gespecialiseerde ondersteuning bieden.

☐ **Stap 2:** contacteer je dienstverleners/contractpartijen in het derde land.

Je doet er goed aan om al je contractpartijen, dienstverleners en dergelijke te informeren over het Schrems-II arrest en de gevolgen hiervan. Sirius Legal heeft hiervoor een standaard brief template gemaakt met een Data Export Vendor Assessment. Je kan deze template gratis downloaden onderaan dit blogbericht. Met 'derde land' willen we niet elk ander land dan je eigen land zeggen, maar wel elk land dat buiten de Europese Economische Ruimte ligt, dat is de EU uitgebreid met Noorwegen, Ijsland en Liechtenstein.

☐ **Stap 3:** ga na of er een beslissing over een passend beschermingsniveau in het derde land is.

Voor sommige derde landen heeft de Europese Commissie beslist dat dit land een passend beschermingsniveau biedt ('een adequaatheidsbesluit'), dus kan je de gegevensexport naar die landen op basis van die beslissing doen. De volledige lijst van die landen kan je op de website van de Europese Commissie vinden. Momenteel zijn er onderhandelingen bezig met Zuid-Korea. We volgen dit uiteraard op en houden je via onze blog en sociale media continu op de hoogte over eventuele wijzigingen.

☐ **Stap 4:** beoordeel de juridische situatie van het derde land.

Wanneer er sprake is van gegevensexport naar een derde land waar geen beslissing over een passend beschermingsniveau is, dan komen we bij de volgende stap. De gegevensbeschermingsautoriteit van Baden-Württemberg raadt in dat geval aan om de juridische situatie van dat derde land grondig te onderzoeken. Het is in dit kader vooral interessant om na te gaan of nationale veiligheidsinstanties toegang kunnen krijgen tot de geëxporteerde gegevens. Je kan hiervoor ten rade gaan bij je nationale gegevensbeschermingsautoriteit (in België is dat de GBA, in Nederland de AP, in Frankrijk de CNIL en in Engeland de ICO), de Europese Commissie, de EDPB, het nationaal ministerie van buitenlandse zaken, … We begrijpen maar al te goed dat dit een ingewikkeld en tijdsintensief karwei is. Sirius Legal beschikt over een omvangrijk netwerk van buitenlandse advocaten gespecialiseerd in deze materies. Zo kunnen we voor bijna elk derde land onze eigen 'gepastheidsbeoordeling' maken.

☐ **Stap 5:** beoordeel of standaard contractuele clausules volstaan.

Nu je op de hoogte bent van de juridische situatie in het derde land is het tijd om te beoordelen of de standaard contractuele clausules (SCCs) volstaan. Deze zijn in het leven geroepen door de Europese Commissie voor gegevensexport naar derde landen. Het zijn overeenkomsten die je kan sluiten met de verwerkingsverantwoordelijke of verwerker in dat derde land. Als er geen problemen werden gevonden in de bovenstaande stap, dan kan je deze SCCs zonder meer gebruiken. Hou wel in het achterhoofd dat de Europese Commissie deze SCCs aan het herzien zijn. Als de SCCs niet volstaan, ga dan naar de volgende stap.

☐ **Stap 6:** creëer aanvullende garanties en gebruik aangepaste SCC's.

De gegevensbeschermingsautoriteit van Baden-Württemberg stelt een aantal aanvullende garanties voor. Ten eerste de encryptie (versleuteling) van de gegevens aan jouw kant. Zorg er in dat geval voor dat jij als exporteur de enige bent met de 'sleutel' om de gegevens te ontcijferen en dat de encryptie niet zomaar kan worden ontsleuteld. We nodigen je uit om het artikel "Is encryptie verplicht onder GDPR?" te lezen als je meer wil weten over encryptie. Ten tweede de anonimisering of pseudonimisering van de gegevens aan jouw kant. Zo zorg je ervoor dat de ontvanger van de gegevens niet zomaar kan weten over wie het nu werkelijk gaat. Denk eraan dat dit proces vaak al begint voor je de gegevens nog maar ingeeft of ergens uploadt. Vervolgens stelt de gegevensbeschermingsautoriteit van Baden-Württemberg een aantal concrete aanpassingen en aanvullingen voor op de SCCs:

- ☐ Een verplichting voor de gegevensexporteur om de betrokkene te informeren dat zijn of haar gegevens naar een derde land gaan dat geen passend beschermingsniveau biedt;
- ☐ Een verplichting voor de gegevensimporteur om zowel de exporteur als de betrokkene op de hoogte te brengen van elk verzoek tot inzage van de gegevens. Als dit niet mogelijk is, de verplichting om de nationale gegevensbeschermingsautoriteit van de exporteur hiervan op de hoogte te brengen;
- ☐ Een verplichting voor de gegevensimporteur om juridische stappen te nemen tegen elk verzoek om inzage en deze uit te putten;
- ☐ De toekenning van meer rechten aan de betrokkene in een geschil met de gegevensimporteur en de toevoeging van een compensatieclausule.

☐ **Stap 7:** en als dat allemaal niet helpt…

Het is mogelijk dat alle bovenstaande maatregelen ofwel niet mogelijk zijn ofwel nog steeds onvoldoende waarborgen bieden. In dat geval vermeldt de gegevensbeschermingsautoriteit van Baden-Württemberg dat er nog een alternatieve optie bestaat, maar dat deze alternatieven heel strikt geïnterpreteerd worden en dus weinig aanvaard als reden om gegevens te exporteren naar een derde land. Hieronder valt bijvoorbeeld de mogelijkheid om de toestemming van de betrokkene te vragen voor de gegevensexport. Deze toestemming moet wel voldoen aan alle vereisten van de GDPR. Met andere woorden: de toestemming moet vrij zijn, specifiek, geïnformeerd en ondubbelzinnig. Als al het bovenstaande niet heeft mogen baten is het allicht veiliger om de samenwerking met de partner te stoppen.