



Philip ter Burg + Susanna Tang

Het recht op privacy komt door het grensoverschrijdend zakendoen steeds sneller in het geding. Het is daarom belangrijk de ontwikkeling op het gebied van doorgifte van persoonsgegevens goed in de gaten te houden. Ook is het raadzaam het privacybeleid van je onderneming onder de loep te nemen en waar nodig aan te passen.

Voorkom overtredingen en eventuele boetes

Doorgifte van persoonsgegevens binnen en buiten de EU

Ondernemers hebben dagelijks te maken met de uitwisseling van persoonsgegevens. Ter bescherming van de privacy is het doorgeven van deze gegevens onderworpen aan de regels van de AVG. Voor doorgifte van persoonsgegevens naar landen binnen de EU en de EER gelden andere regels dan voor doorgifte naar landen buiten deze landen. Het is belangrijk hiermee rekening te houden nu een overtreding kan leiden tot flinke boetes.

De Algemene verordening gegevensbescherming (AVG) definieert persoonsgegevens als alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. Voor de hand liggende gegevens zijn bijvoorbeeld een naam of adres van een individu, maar ook locatiegegevens en IP- en e-mailadressen vallen hieronder.

Doorgifte binnen EU/EER

Op de uitwisseling van persoonsgegevens binnen de Europese Unie (EU) en de Europese Economisch Ruimte (EER, de EU plus IJsland, Noorwegen en Liechtenstein) zijn de regels van de AVG van toepassing. De belangrijkste vijf bepalingen zijn:

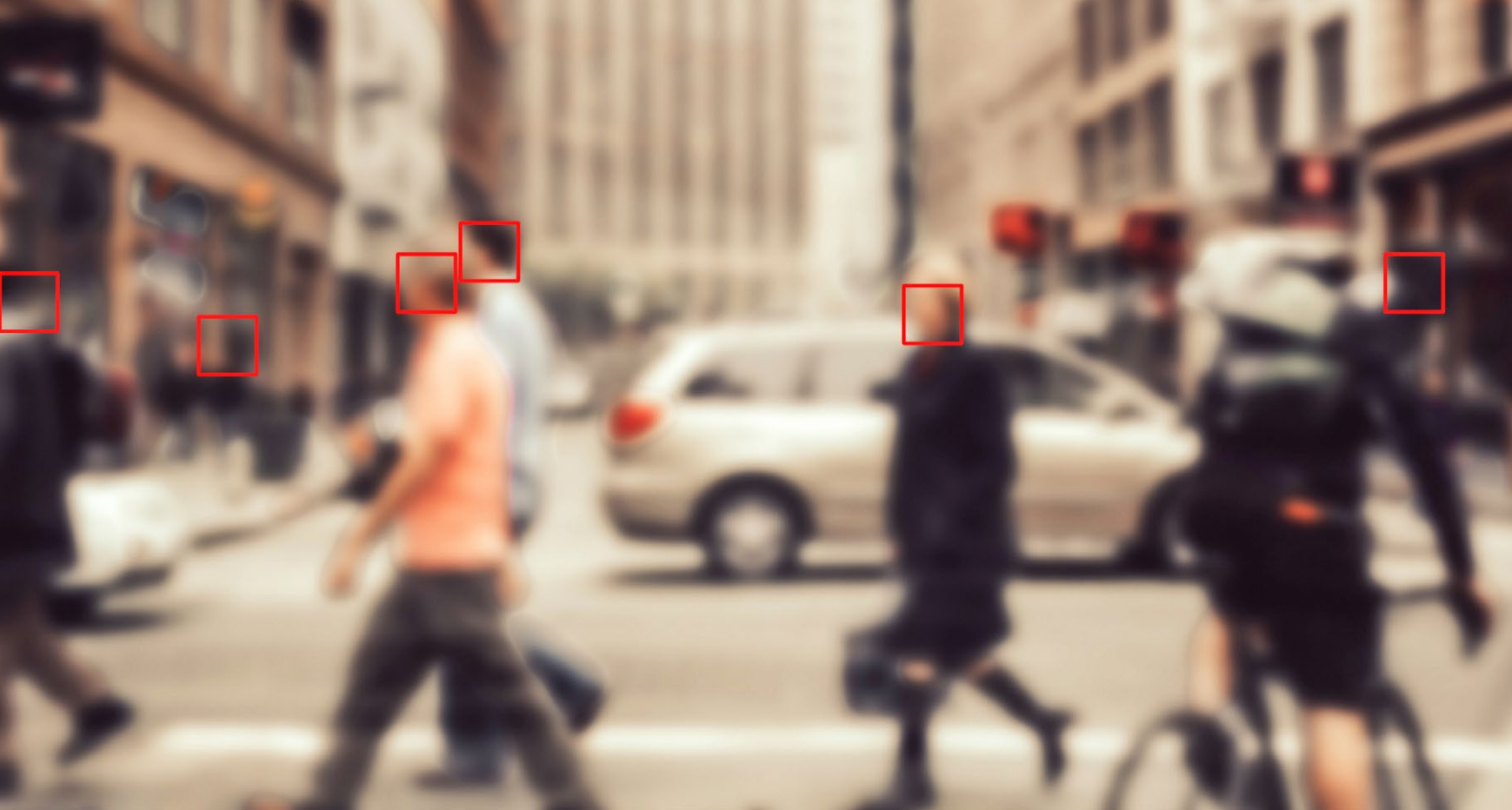
1. De ondernemer mag alleen persoonsgegevens verwerken in overeenstemming met de wet en doet het op een behoorlijke en zorgvuldige manier;

“De AVG schrijft voor welke middelen de privacy voldoende waarborgen bij doorgifte naar derde landen”

2. De ondernemer mag alleen persoonsgegevens verzamelen indien dit wordt gedaan in overeenstemming met de vooraf bekendgemaakte en uitdrukkelijk omschreven doelen en enkel verwerken tot hetgeen strikt noodzakelijk is om deze doelen te bereiken;
3. De ondernemer heeft passende technische of organisatorische maatregelen genomen voor de verwerking van de persoonsgegevens;
4. De betrokkene van de persoonsgegevens is op de hoogte van de identiteit van de ondernemer die deze persoonsgegevens verwerkt en de grondslag van de gegevensverwerking;
5. De betrokkene kan inzage verkrijgen in de gegevens die zijn verzameld door de ondernemer en deze laten corrigeren of verwijderen.

Philip ter Burg is advocaat en partner bij Buren Legal in Den Haag. Susanna Tang is advocaat bij de vestigingen in Amsterdam en Shanghai.





Doorgifte buiten EU/EER

Doorgifte van persoonsgegevens naar landen buiten de EU (derde landen) is toegestaan indien sprake is van een passend beschermingsniveau. Via adequaatheidsbesluiten stelt de EU vast welke derde landen een passend beschermingsniveau van persoonsgegevens hebben. Op dit moment erkent de EU veertien landen; hierbij zijn inbegrepen het Verenigd Koninkrijk, Japan en Israël.

Bij gebreke van een adequaatheidsbesluit mogen persoonsgegevens slechts aan een land buiten de EU/EER worden doorgegeven, indien passende waarborgen zijn genomen ter bescherming van de privacy van betrokkenen en deze over afdwingbare rechten en doeltreffende rechtsmiddelen beschikken. De AVG schrijft voor welke middelen de privacy voldoende waarborgen bij doorgifte naar derde landen. De belangrijkste drie middelen zijn:

1. Bindende afspraken tussen overheden;
2. Bindende bedrijfsvoorschriften overeenkomstig de Binding Corporate Rules (BCR);
3. Standaardbepalingen inzake gegevensbescherming (Standard Contractual Clauses, SCC).

Vergelijkbaar EU-beschermingsniveau

Met de Verenigde Staten (VS) bestond een overeenkomst over de bescherming en ver-

werking van persoonsgegevens van EU-burgers, het EU-VS Privacy Shield. Deze is echter door het Europese Hof van Justitie in de zogenoemde Schrems II-uitspraak van 16 juli 2020 ongeldig verklaard. Amerikaanse overheidsinstanties hadden namelijk toegang tot persoonsgegevens die vanuit de EU afkomstig waren, zonder dat dit was beperkt tot hetgeen strikt noodzakelijk was. Op 25 maart 2022 hebben de EU en de VS een principeakkoord bereikt over nieuwe privacyafspraken. Details over de nieuwe afspraken ontbreken nog. Tot het moment dat het akkoord definitief is, zal voor het doorgeven van gegevens naar de VS daarom gebruik moeten worden gemaakt van SCC of BCR.

Tevens vloeit uit het Schrems II-arrest van het Europese Hof voort dat enkel het sluiten van contracten op basis van de SCC niet voldoende bescherming biedt voor internationale doorgifte van persoonsgegevens. Voorafgaand aan de doorgifte moet de dataexporteur een Data Transfer Impact Assessment (DTIA) uitvoeren. Dit houdt een risicoanalyse in van de uitwisseling van persoonsgegevens en welke aanvullende maatregelen moeten worden getroffen om tot een vergelijkbaar EU-beschermingsniveau te komen. In een DTIA dient in ieder geval rekening te worden gehouden met de volgende drie elementen:

1. De specifieke omstandigheden van de doorgifte;
2. De wetgeving en praktijken van het derde land;
3. Alle relevante contractuele, technische of organisatorische waarborgen die de waarborg uit hoofde van de SCC aanvullen.

China

Voor China bestaat noch een adequaatheidsbesluit, noch een overeenkomst tussen de EU en China betreffende de doorgifte van persoonsgegevens. Voor doorgifte van persoonsgegevens aan China zal dus eveneens gebruik moeten worden gemaakt van SCC. Ook voor doorgifte aan China geldt dat hiervoor vooraf een DTIA vereist is.

Voor ondernemers die in China actief zijn, is het ook relevant rekening te houden met de Personal Information Protection Law (PIPL). Dit is de nieuwe privacywetgeving van China, waarin regels zijn opgenomen voor verwerking van persoonsgegevens van Chinese ingezetenen. De PIPL vertoont op hoofdlijnen grote gelijkenissen met de AVG. Uitzondering hierop is dat niet alleen de onderneming maar ook directe leidinggevendenden risico lopen op boetes en/of strafrechtelijke vervolging bij overtreding van de PIPL. ●●●