Tekst **Martijn Kortier**
Martijn Korter is advocaat intellectuele eigendom, ict-recht en privacy bij Elferink & Kortier Advocaten

Centrale opslag paspoortgegevens

Het kabinet heeft het plan opgevat om alle gegevens die nodig zijn voor de aanvraag van een paspoort of ID-kaart centraal op te slaan. Op dit moment slaan alle gemeenten de gegevens nog zelf decentraal op. Het plan kwam het kabinet op felle kritiek van de Autoriteit Persoonsgegevens (AP) te staan. Het laat zich raden dat die kritiek vooral over privacybescherming gaat.

Om welke gegevens gaat het eigenlijk? In principe alle gegevens die ook op het paspoort en de ID-kaart staan. Denk dus aan vingerafdrukken, pasfoto's, handtekeningen en burgerservicenummers. Het betreft heel gevoelige persoonsgegevens, waaronder biometrische gegevens. De AP stelt dat het opslaan van die gegevens een goudmijn is voor kwaadwillende hackers. Alle gevoelige gegevens van alle Nederlanders staan immers bij elkaar. Is men eenmaal binnen in dat systeem, dan staan alle data die men nodig heeft voor bijvoorbeeld identiteitsfraude netjes bij elkaar.

De AP wijst met name op het risico van hacken, maar ziet ook andere risico's. Een centrale database geeft de rijksoverheid mogelijk te veel macht. De gegevens worden wellicht nu nog voor het doel van paspoortuitgifte opgeslagen en gebruikt, maar in de toekomst wellicht ook voor andere doeleinden (denk aan opsporing van overtredingen en misdrijven). Waarborgen om dat te voorkomen ontbreken vooralsnog.

Het risico bestaat dat de bescherming van persoonsgegevens onder druk komt te staan als er te veel gegevens centraal in een database opgeslagen worden. Hoe meer gegevens bij elkaar staan, hoe groter de kans is dat bij een datalek in die database, herleidbare en/of gevoelige gegevens op straat komen te liggen. Hoe meer gegevens bij elkaar, hoe groter de impact daarvan op de betrokkene. Niet voor niets vereist de AVG dat de verwerkingsverantwoordelijke, de partij die verantwoordelijk is voor de verwerking van persoonsgegevens, binnen zijn organisatie, passende technische en organisatorische maatregelen moet treffen om ze tegen onder andere verlies en ongeoorloofde toegang te beschermen. Een van die maatregelen zou het scheiden van gegevens in verschillende databases en/of pseudonimisering kunnen zijn. Mocht dan worden ingebroken op een database dan zouden de gegevens uit de andere databases mogelijk niet gelekt worden, waardoor de schade en de impact van dat datalek potentieel veel lager of zelfs non-existent zijn.

De advocaten en juristen van Elferink & Kortier Advocaten schrijven op deze plek regelmatig een column, waarin zij een praktisch probleem op het gebied van de AVG in relatie tot informatiebeheer behandelen. Heeft u een praktijkvraag die u behandeld wilt zien? Stuur deze naar Od@publiekdenken.nl.