Samenwerkingsprotocol DNB en AP - samenloop PSD2 en AVG

De Nederlandsche Bank (**DNB**) en de Autoriteit Persoonsgegevens (**AP**) hebben op donderdag 21 februari een samenwerkingsprotocol ondertekend (**Protocol**). In dit Protocol zijn een aantal uitgangspunten opgenomen voor de wijze waarop de autoriteiten (gezamenlijk) toezicht gaan houden op de bepalingen uit de herziene Payment Service Directive (**PSD2**) zoals deze zijn geïmplementeerd in de Wet op het financieel toezichtrecht en het Besluit prudentiële regels Wft, die betrekking hebben op de bescherming van persoonsgegevens. De samenloop van de financieel toezichtrechtelijke regelgeving en de regelgeving voor de bescherming van persoonsgegevens is al relevant bij het voorbereiden en indienen van een vergunningaanvraag voor het mogen verlenen van betaaldiensten. Bij het aanvragen van een vergunning zal bijvoorbeeld onder meer moeten worden aangetoond dat de bedrijfsvoering zodanig is ingericht dat deze een beheerste en integere uitoefening van het bedrijf waarborgt. Onderdeel van een beheerste bedrijfsvoering is het waarborgen van de bescherming en beveiliging van de persoonsgegevens die de onderneming gaat verwerken. In dit kader zal de onderneming moeten aantonen dat de regels voor de bescherming van persoonsgegevens zoals deze voortvloeien uit de Algemene Verordening Gegevensbescherming (**AVG**) en PSD2 op een juiste wijze in acht zijn genomen.

Hieronder lichten wij een tweetal praktische onderwerpen toe waarmee een onderneming rekening kan houden bij het aanvragen van een vergunning als betaalinstelling.

Data protection impact assessment

Een data protection impact assessment (**DPIA**) is een instrument waarmee ondernemingen de risico's die zijn verbonden aan een (nieuwe) verwerking in kaart kunnen brengen, zodat de onderneming deze risico's kan minimaliseren. De Autoriteit Persoonsgegevens heeft een lijst opgesteld van verwerkingen waarvoor het uitvoeren van een DPIA verplicht is. Op basis van deze lijst is het uitvoeren van een DPIA bijvoorbeeld verplicht in het geval van verwerkingen in het kader van fraudebestrijding, credit scoring en bijhouden/monitoren van iemands financiële situatie. Deze activiteiten kunnen onderdeel zijn van de dienstverlening van een betaaldienstverlener. Het uitvoeren van een DPIA dient dan al plaats te vinden in het kader van de vergunningaanvraag. Als uit de DPIA blijkt dat de verwerking een hoog risico oplevert en de onderneming van mening is dat het niet mogelijk is om het hoge risico te beperken, dient de onderneming eerst de AP, middels het indienen van een verzoek, te raadplegen voordat de beoogde gegevensverwerking mag worden gestart. Indien de onderneming niet op eigen initiatief de AP heeft geraadpleegd, zo blijkt uit het Protocol, dan zal DNB de AP inlichten zodat de AP alsnog een advies kan geven.

Houd bij een vergunningaanvraag dus rekening met het moeten uitvoeren van een DPIA en eventueel het moeten raadplegen van de AP. De AP mag een termijn van 8 weken in acht nemen, welke termijn kan worden verlengd met nog eens 6 weken, om in reactie op het verzoek tot raadpleging een schriftelijk advies te geven.

Bijvangst – silent party data

Betaaldienstverleners zullen de uitdrukkelijke toestemming van de betaaldienstgebruiker moeten krijgen om toegang te krijgen tot diens persoonsgegevens. Wanneer toegang wordt verkregen tot iemands persoonsgegevens, wordt tevens toegang verkregen tot gegevens die zien op andere

personen dan de persoon die zijn/haar toestemming heeft gekregen. Zo zal bijvoorbeeld zichtbaar zijn met welke personen de betaaldienstgebruiker transacties heeft verricht. Deze personen, de zogenaamde 'silent parties' hebben hiertoe niet hun toestemming verleend. Er wordt vanuit gegaan dat deze verwerking mag plaatsvinden op basis van het gerechtvaardigde belang van de betaaldienstverlener om zijn diensten te kunnen verlenen. Zorg ervoor dat ook met deze verwerking, de verwerking van gegevens van silent parties, rekening wordt gehouden bij de vormgeving van de dienstverlening. Zo zal bijvoorbeeld in het privacy statement informatie moeten worden opgenomen waarin wordt toegelicht dat deze verwerking plaatsvindt op basis van een gerechtvaardigd belang van de betaaldienstverlener alsmede een nadere uitleg van het gerechtvaardigde belang.

Benieuwd hoe de samenloop tussen PSD2 en de AVG invloed heeft op jouw onderneming en hoe je hier het beste mee om kan gaan? Neem dan contact op met Sanne Machiels via machiels@fglawyersamsterdam.com of 020-760 31 36