AUTORITEIT
PERSOONSGEGEVENS

Autoriteit Persoonsgegevens
Postbus 93374, 2509 AJ Den Haag
Hoge Nieuwstraat 8, 2514 EL Den Haag
T 070 8888 500 - F 070 8888 501
autoriteitpersoonsgegevens.nl

Minister/Staatssecretaris

Datum
10 november 2022

Ons kenmerk
z2022-00846

Contactpersoon

070 8888 500

Onderwerp
Inzet van Cloud Service Providers

Geachte

De Autoriteit Persoonsgegevens doet onderzoek naar het gebruik van cloud service providers (CSP's) door de landelijke overheden. Dit doen wij samen met Europese collega-toezichthouders in de European Data Protection Board (EDPB) in het kader van een gecoördineerde actie.[1] Het centrale thema in ons onderzoek is de wijze waarop er bij het gebruik van clouddiensten door de landelijke overheidsoverheidsorganisaties rekening wordt gehouden met de Algemene Verordening Gegevensbescherming (AVG). Daarbij is er onder meer aandacht voor de verwerkingsverantwoordelijke-verwerker-relatie, de internationale doorgifte van persoonsgegevens en de rol van gegevensbescherming bij de aanbesteding.

Naar aanleiding van dit onderzoek wil de AP middels deze brief, vooruitlopend op een later te publiceren eindrapport van de EDPB, enkele observaties en aanbevelingen met u delen. Deze worden gevolgd door observaties en aanbevelingen over de rol die een ministerie heeft indien zij diensten van een CSP wil gaan afnemen en de rol die een ministerie vervult indien zij (ook) een Strategisch Leveranciers Management (SLM)-functie vervult.

De AP adviseert u in deze brief ten aanzien van de volgende punten:

1. Uw verantwoordelijkheid als verwerkingsverantwoordelijke bij de inzet van CSP's in relatie tot reeds bestaande SLM-functies binnen de Rijksoverheid.
2. Uniformering van de wijze waarop de/uw SLM-functie wordt vormgegeven en uitgevoerd.

[1] Voor meer informatie: Launch of coordinated enforcement on use of cloud by public sector | European Data Protection Board (europa.eu)

3. De noodzaak tot onderzoek naar de wenselijkheid voor SLM-functies waar deze nu nog niet bestaan.

De AP zal deze punten hieronder verder uitwerken en motiveren.

Scope onderzoek AP

De AP heeft voor het onderzoek drie Strategisch Leveranciers Management (SLM)-functies binnen het Rijk aangeschreven en de reacties geanalyseerd. Daarbij heeft de AP zich gericht op de SLM-functies van het Rijk die een relatie hebben met CSP's. De suggesties van de AP zijn wellicht ook buiten het bestek van het gebruik van clouddiensten bruikbaar. Zeker daar waar breed gebruik wordt gemaakt van leveranciers die persoonsgegevens gaan verwerken of dit reeds doen.

Rol van uw ministerie als gebruiker van (CSP-)diensten

Het is zeer waarschijnlijk dat u gebruik maakt van een dienst van een leverancier waarvoor u niet zelf een SLM-functie heeft ingericht, maar waarbij u gebruikmaakt van een overeenkomst die is gebaseerd op een (mantel)overeenkomst die is gesloten door een van de SLM-functies binnen de Rijksoverheid. Bijvoorbeeld de rijksbrede overeenkomsten die via SLM Rijk zijn afgesloten met Microsoft. Of u nu zelfstandig een contract afsluit met een leverancier of via een rijksbrede mantelovereenkomst, u bent verwerkingsverantwoordelijke voor die verwerkingen van persoonsgegevens die de leverancier/CSP voor u uitvoert. Als verwerkingsverantwoordelijke dient u voor het inschakelen van een leverancier daarom altijd een eigen afweging te maken. De afweging bestaat daaruit dat u, op basis van de risico's die de verwerking met zich meebrengt, bepaalt of de leverancier voldoende passende technische en organisatorische maatregelen heeft getroffen opdat de verwerking aan de vereisten van de AVG voldoet. Hierbij kunt u uiteraard gebruik maken van de maatregelen die reeds zijn overeengekomen in een (mantel)overeenkomst die is afgesloten door een van de SLM-functies. U dient echter wél aantoonbaar te onderzoeken of de maatregelen uit die mantelovereenkomst voldoende zijn voor uw specifieke situatie. Daarbij dient u ook aantoonbaar vast te stellen of de verwerking bij u tot andere risico's leidt dan die waar de SLM-functie (in de DPIA) rekening mee heeft gehouden. Bijvoorbeeld omdat u de dienst voor een ander doel inzet, er gevoelige(re) persoonsgegevens worden verwerkt of doordat het risico op gerichte acties van statelijke actoren bij u prominenter aanwezig is.

Daar waar er sprake is van doorgifte van persoonsgegevens aan landen buiten de EER – wat bij veel CSP-diensten het geval is – geldt bovendien dat dit alleen mag plaatsvinden wanneer persoonsgegevens in dat land op een gelijkwaardige manier worden beschermd. Doorgifte kan ook plaatsvinden doordat persoonsgegevens binnen een groepsonderneming, of via een leverancier, worden doorgezonden naar landen buiten de EER. Van doorgifte is tevens sprake als entiteiten uit landen buiten de EER toegang krijgen tot persoonsgegevens. Wanneer bescherming op een gelijkwaardige manier niet kan worden gegarandeerd, mag de doorgifte niet plaatsvinden en zal er voor een aangepaste of andere CSP-dienst moeten worden gekozen. Ook kan het voor uzelf of uw leverancier nodig zijn om aanvullende maatregelen te treffen om ervoor te zorgen dat de persoonsgegevens in de praktijk daadwerkelijk goed beschermd zijn. Afwegingen die hieraan ten grondslag liggen moeten zorgvuldig worden onderbouwd en gedocumenteerd, en zijn opvraagbaar door de AP als toezichthouder. Het is dan ook raadzaam dergelijke afwegingen

middels een Transfer Impact Assessment (TIA) inzichtelijk te maken en op basis hiervan een besluit te nemen voordat voor een dienst wordt gekozen. Hierbij kan gebruik worden gemaakt van de aanbevelingen van de EDPB.[2]

Hoewel er op dit moment gesprekken plaatsvinden tussen de EU en de VS die mogelijk uitmonden in een adequaatheidsbesluit op basis waarvan doorgifte aan de VS mogelijk lijkt, is op dit moment nog niet duidelijk of deze gesprekken ook gaan leiden tot een rechtmatige basis voor doorgiften aan de VS. Een eventueel adequaatheidsbesluit zal de Europese Commissie nog ter advisering aan de EDPB voorleggen.

De AP adviseert u om te onderzoeken of u voor die situaties waarbij u gebruik maakt van een mantelovereenkomst die is opgesteld door een SLM-functie, aantoonbaar heeft vastgesteld of deze mantelovereenkomst in voldoende mate mitigerende maatregelen voor uw risico's bevat. Daarin dient ook uw Functionaris voor Gegevensbescherming (FG) te worden betrokken. Waar dit laatste nog niet is gedaan dient dit zo alsnog zo snel mogelijk plaats te vinden.

Algemene observaties over de SLM-functies binnen het Rijk

Zoals hierboven reeds is aangegeven, heeft de AP in het kader van het EDPB-onderzoek drie SLM-functies binnen het Rijk aangeschreven. Naar aanleiding van dit onderzoek neemt de AP de volgende zaken waar:

1. De AP moedigt de SLM-functies aan die namens de afnemers onderzoek doen naar de verwerkingen van persoonsgegevens door de CSP door het (laten) uitvoeren van een diepgravende gegevensbeschermingseffectbeoordeling (GEB/DPIA). Dit is een goede methode om de grootste, meest voorkomende risico's die kunnen bestaan bij de afnemers tijdig te identificeren, mitigeren en controles op uit te voeren bij de CSP. De AP begrijpt dat het bundelen van kennis en kunde binnen een SLM-functie inspanning en kosten vergt, maar het brengt grote voordelen met zich mee. Nederland lijkt daar Europees ook in voorop te lopen. Daarbij prijst de AP ook het publiceren van de uitgevoerde DPIA's, die internationaal worden benut.
2. Er is binnen de landelijke overheid in Nederland op plaatsen een SLM-functie die op een professionele en vooruitstrevende wijze invulling geeft aan een deel van de rol die deze landelijke overheidsorganisaties hebben ten aanzien van de bescherming van persoonsgegevens bij de inzet van een CSP. Er is echter ook een SLM-functie waarin deze rol naar de mening van de AP nog onvoldoende professioneel lijkt te zijn.

Mogelijke rol van SLM-functies bij CSP-diensten

Het principe van Privacy by design vraagt dat in een zo vroeg mogelijk stadium rekening wordt gehouden met de privacyaspecten van een gegevensverwerking. Voor overheidsorganisaties die CSP-diensten afnemen is het daarom van belang dat zij voorafgaand aan de ingebruikname van de dienst de risico's in kaart brengen en de benodigde maatregelen treffen. De SLM-functie kan een belangrijke rol spelen om daar in een vroegtijdig stadium aan bij te dragen. De AP heeft naar aanleiding van de vragenlijst en diverse gesprekken vernomen dat er echter geen duidelijk kader bestaat voor de rol en belegging van SLM-functies binnen het Rijk, voor welke CSP's een SLM-functie is bekleed en de vraag in hoeverre SLM-functies steeds

[2] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data | European Data Protection Board (europa.eu)

een rol hebben in het kader van de bescherming van persoonsgegevens. In dat kader wil de AP u als bewindspersonen gezamenlijk wijzen op de volgende aandachtspunten.

1. De criteria waarmee wordt vastgesteld wanneer er voor een bepaalde CSP een SLM-functie moet worden ingericht, en bij welke organisatie deze functie wordt uitgevoerd zijn nog niet helder gedefinieerd. In de huidige opzet lijkt er sprake te zijn van een organisch gegroeide situatie zonder duidelijke richtlijnen. De AP adviseert hiervoor beleid op te stellen en (Rijksbrede) strategische keuzes in te maken, zodat er meer gezamenlijk kan worden opgetrokken. Bijvoorbeeld door uit te gaan van een inventarisatie van de meest gebruikte leveranciers die persoonsgegevens verwerken voor landelijke overheidsorganisaties.

2. De AP adviseert u om te onderzoeken van welke CSP's u diensten afneemt en of u daarbij een SLM-functie vervult of op basis van overeenkomsten van een (SLM-functie bij een) andere landelijke overheidsorganisatie inkoopt. De resultaten van een dergelijke analyse kunnen vervolgens in overleg met de andere landelijke overheidsorganisaties worden besproken, mogelijk via een coördinerende rol vanuit CIO-Rijk, teneinde een goed overzicht te hebben van de in gebruik zijnde leveranciers en mantelovereenkomsten binnen de landelijke overheid. Een dergelijk overzicht kan daarna worden gebruikt om te bepalen waar de SLM-functies binnen de landelijke overheid dienen te worden belegd, ook voor CSP's waarvoor er nu nog geen SLM-functie bestaat. Het is raadzaam deze exercitie ook te doorlopen voor grote leveranciers die geen CSP zijn maar wel een dienst aanbieden waarbij persoonsgegevens worden verwerkt.[3]

3. Voor nieuwe en bestaande SLM-functies is het essentieel dat deze worden voorzien van voldoende mensen en middelen. Zoals reeds aangegeven heeft de AP in haar onderzoek professionele maar ook minder professionele SLM-functies gezien, terwijl de afnemende overheidsorganisaties in de praktijk wel uitgaan van hun expertise. De rol van de SLM-functies strekt zich bij de door ons onderzochte functies ook uit tot het (laten) uitvoeren van controles en audits en het volgen van ontwikkelingen in het privacyveld; ook daarvoor is het belangrijk dat hiervoor voldoende capaciteit en middelen beschikbaar zijn bij de SLM-functie.

4. De invulling van de SLM-functie of een centrale inkoopfunctie, en de rolverdeling tussen deze functie en de uiteindelijke afnemer van de dienst van de CSP, kan ook betekenen dat er sprake is van een additionele rol vanuit de AVG. Bijvoorbeeld indien de wijze van invulling van een SLM-functie inhoudt dat deze SLM-functie ook persoonsgegevens voor een verwerkingsverantwoordelijke landelijke overheid gaat verwerken. Dit kan indien de SLM-functie bijvoorbeeld ook het gebruiksbeheer of licentiebeheer invult. Ook indien een overheidsorganisatie gebruik maakt van de diensten via een door een andere overheidsorganisatie afgesloten contract en zelf geen contract heeft gesloten met de leverancier kan er sprake zijn van een overheidsorganisatie die verwerker is.

[3] De AP merkt op dat bij de inventarisatie van CSP's ook dient te worden onderzocht welke diensten zich "richting de cloud" bewegen. Te denken valt aan meer traditionele diensten zoals de levering van telefoniecentrales die niet vallen onder "videoconferencing" of "beeldbellen". Ook software ten aanzien van fysiek toegangsbeheer verplaatst zich bijvoorbeeld richting een cloudoplossing. Dit brengt nieuwe risico's met zich mee die in voldoende mate moeten worden gemitigeerd.

Er moet dus worden vastgesteld of er sprake is van een situatie waarbij de SLM-functie zelf verwerker is geworden voor de landelijke overheid. Hierbij is het raadzaam dat de SLM-functie binnen de landelijke overheid wordt voorzien van een eenduidige omschrijving van taken, werkzaamheden en verantwoordelijkheden die aansluit op de taken, werkzaamheden en verantwoordelijkheden van de landelijk overheidsorganisaties bij de inkoop van diensten. Aangezien de bescherming van persoonsgegevens het centrale element is in de AVG dient bij de taakomschrijving in ieder geval te worden stilgestaan bij de wijze waarop risico's voor betrokkenen worden geïdentificeerd door de verwerkingsverantwoordelijken en welke rol de SLM-functie heeft binnen het vaststellen van de risico's die zij meenemen in de onderhandelingen van overeenkomsten met CSP's.

5. Ten aanzien van de vraag wat er inhoudelijk in contracten dient te worden opgenomen met CSP's is er voor zover bij de AP bekend nog geen gemeenschappelijke invulling (door de SLM-functies). Dat vraagt om een gezamenlijke visie op de voorwaarden die men hanteert ten aanzien van CSP's. Vanuit het uitgangspunt dat de burger bij alle overheidsdiensten mag vertrouwen op een hoog beschermingsniveau van diens persoonsgegevens is het aan te raden hier invulling aan te gaan geven. In dat kader verwijst de AP ook naar de bijgevoegde reactie ten aanzien van het gepubliceerde cloudbeleid.[4]

De AP adviseert u deze aandachtspunten ook met andere landelijke overheidsorganisaties te bespreken, waaronder de aan uw ministerie gerelateerde ZBO's, agentschappen en overige Rijksonderdelen.

Een afschrift van deze brief zal tevens worden verstrekt aan uw Functionaris voor Gegevensbescherming.

De AP zal deze brief openbaar maken via de website www.autoriteitpersoonsgegevens.nl.

Hoogachtend,
Autoriteit Persoonsgegevens,

Aleid Wolfsen
voorzitter

[4] *Kamerstukken II* 2021/22, 26 643, nr. 904.