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

Aangetekend
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Staatssecretaris Koninkrijksrelaties en Digitalisering
Mevrouw drs. A.C. van Huffelen
Postbus 20011
2500 EA Den Haag

Datum
11 november 2022

Ons kenmerk
z2022-05319

Contactpersoon

070 8888 500

Uw kenmerk
2022-0000478290

Onderwerp
Rijksbreed cloudbeleid 2022

Geachte mevrouw Van Huffelen,

Aanleiding
Op 29 augustus 2022 heeft u de Tweede Kamer per brief geïnformeerd over het "Rijksbreed cloudbeleid 2022". Dit Rijksbrede cloudbeleid is opgesteld in samenwerking met alle Nederlandse ministeries. Het opstellen van dit door alle ministeries gedragen Rijksbrede cloudbeleid is een belangrijke stap in de uniformering en professionalisering van de wijze waarop binnen de Rijksoverheid met clouddiensten en clouddienstverleners wordt omgegaan.

Bescherming persoonsgegevens bij inzet clouddiensten
De Autoriteit Persoonsgegevens (AP) neemt waar dat ook nu al sprake is van gebruik van publieke clouddiensten door overheidsdiensten, maar dat een uniforme aanpak ontbeert. De AP heeft daarom met belangstelling kennisgenomen van het cloudbeleid en wil u, in uw coördinerende verantwoordelijkheid voor dit beleid, graag via deze weg wijzen op een aantal wezenlijke privacyrisico's die volgen uit de Algemene Verordening Gegevensbescherming (AVG) bij de inzet van cloud. Juist vanwege de aard van de gegevens die door overheidsdiensten worden verwerkt en de (in potentie) grote hoeveelheid van gegevens die in de cloud worden opgeslagen, is het van groot belang dat het fundamentele recht op de bescherming van persoonsgegevens goed wordt gewaarborgd bij alle overheidsdiensten. Nederlandse burgers, maar ook voor overheidsdiensten werkzame personen, moeten er immers op kunnen vertrouwen dat de overheid zorgvuldig met hun persoonsgegevens omgaat. De AP is van mening dat de privacyrisico's die het gebruik van (public) cloud-oplossingen door overheden met zich meebrengen nadrukkelijker moeten worden onderkend en gemitigeerd. In dat kader geeft de AP u en de ministeries die u vertegenwoordigt, enkele aandachtspunten en adviezen ten aanzien van het Rijksbrede cloudbeleid en de implementatie daarvan.

Datum
11 november 2022

Ons kenmerk
z2022-05319

De AP heeft deze op 3 november met u besproken en waardeert uw toezegging dat u deze adviezen ter harte neemt.

Hoofdlijnen adviezen AP

De adviezen van de AP zien in hoofdlijnen op de volgende punten:

1. Vollediger adresseren van de privacyrisico's en dit leidend maken bij de vraag of een clouddienst rechtmatig kan worden ingezet.
   De nu in het cloudbeleid doorgevoerde scheiding tussen public en private clouddiensten is niet bepalend voor de vraag of en zo ja welke mogelijke privacyrisico's er bestaan. In plaats daarvan dient onafhankelijk van de vorm van de clouddienst (publiek, privaat of hybride) te worden bepaald of de gegevensverwerking voldoet aan de eisen van de AVG. Vanuit de AVG en de voortrekkersrol die de Rijksoverheid speelt is het noodzakelijk de risico's juist en volledig te adresseren in een dergelijk cloudbeleid. Dit klemt temeer nu het in essentie hier gaat om het waarborgen van een grondrecht en schendingen daarvan ernstig afbreuk kunnen doen aan het vertrouwen dat burgers mogen hebben in de Rijksoverheid. Een dergelijke aanpak is ook meer in lijn met wat u aangaf in uw "Hoofdlijnen beleid voor digitalisering" waar staat: "*We hebben de plicht om grondrechten en publieke waarden (veiligheid, democratie, zelfbeschikking, non-discriminatie, participatie, privacy en inclusiviteit) te beschermen en de taak om een gelijk economisch speelveld te creëren: met eerlijke concurrentie, consumentenbescherming en brede maatschappelijke samenwerking.*"[1]

2. Nadrukkelijk adresseren van de specifieke risico's die spelen bij de doorgifte van persoonsgegevens naar landen buiten de EER, waaronder ook de mogelijke toegang tot persoonsgegevens van buiten de EER.
   Ten aanzien van de doorgifte van persoonsgegevens naar landen buiten de EER bestaan al langere tijd zorgen, gelet op het verminderde beschermingsniveau. Dit vraagt om nadere uitwerking en strategische keuzes, zodat voldoende kan worden bepaald of de grondrechten van EU-burgers niet ook van buiten de EER worden geschonden en tegelijkertijd de continuïteit van de essentiële dienstverlening van het Rijk niet in gevaar komt.

3. Verzekeren van de uitvoering van dit cloudbeleid om te voorkomen dat de privacyrisico's niet, of onvoldoende, worden geïdentificeerd door overheidsinstellingen.
   Van de overheid mag worden verwacht dat deze een hoog beschermingsniveau hanteert voor de bescherming van persoonsgegevens. Een goed cloudbeleid kan daaraan bijdragen, maar slechts indien de naleving en opvolging van dat cloudbeleid binnen de gehele overheid is verzekerd. Daarvoor is het noodzakelijk dat de mate van vrijblijvendheid voor ministeries om de regels in het Rijksbeleid cloudbeleid na te leven zo beperkt mogelijk is en dat er wordt zorggedragen voor een controleerbare implementatie en naleving van dit cloudbeleid. Het versterken van de rol van strategisch leveranciersmanagement-functies (SLM-functie) binnen het Rijk zou hieraan kunnen bijdragen.

[1] Kamerstukken 2021-2022, 26643 nr. 842, Hoofdlijnen beleid voor digitalisering.

De AP zal deze punten hieronder verder uitwerken en motiveren.

Inhoudelijke opmerkingen ten aanzien van het Rijksbrede cloudbeleid:

- In het Rijksbrede cloudbeleid wordt een onderscheid gemaakt tussen de publieke, private en hybride cloud. Daarbij is in de bijlage opgenomen: "*Als één overheidsorganisatie toegang heeft tot computermiddelen, dan spreken we van een private cloud. Een private cloud kan in beheer zijn van de Rijksoverheid zelf of exclusief door een marktpartij worden aangeboden. Een mengvorm van de private en publieke cloud heet een hybride cloud. Een hybride cloud is opgebouwd uit meerdere delen, waarvan sommige in een publieke en sommige in een private cloud zijn ondergebracht. Om goed overzicht te houden op de informatie in dat samenspel van diensten wordt een informatiearchitectuur gebruikt.*"
  Op grond van de AVG is het essentieel om vast te stellen welke partijen persoonsgegevens verwerken en welke partijen toegang hebben tot de persoonsgegevens, waaronder ook telemetriegegevens, die worden verwerkt bij de inzet van de clouddienst. Het nu doorgevoerde onderscheid is vanuit de optiek van bescherming van persoonsgegevens niet direct relevant. De gelaagdheid van clouddiensten brengt namelijk met zich mee dat SaaS-diensten in de private cloud niet geheel 'privé' zijn als deze functioneren op niet public IaaS-dienst.

- Specifieke aandacht dient er te zijn voor de doorgifte van persoonsgegevens buiten de EER, ook bij de private cloud. Indien bijvoorbeeld de dienstverlener of een onderaannemer de cloud beheert of toegang heeft vanuit een land buiten de EER. Indien dit plaatsvindt dient te worden onderzocht of er voor de doorgifte bijvoorbeeld kan worden gesteund op een adequaatheidsbesluit.[2] Dit vergt een nauwkeurige analyse van de opbouw van een clouddienst en de onderaannemers (subverwerkers) die daarbij zijn betrokken. Dit geldt uiteraard ook ten aanzien van een public cloud en hybrid cloud. De AP adviseert in het Rijksbrede cloudbeleid, wanneer er sprake is van de verwerking van persoonsgegevens, de vraag of deze persoonsgegevens binnen of buiten de EER worden verwerkt leidend te laten zijn. En daarbij telkens ook aandacht te besteden aan de vraag of er telemetriegegevens worden verwerkt en of er voor het betreffende land sprake is van een adequaatheidsbesluit op basis waarvan de doorgifte kan plaatsvinden.

- De AP merkt op dat er ten aanzien van de doorgifte van persoonsgegevens naar landen buiten de EER al langere tijd zorgen bestaan, die hebben geresulteerd in diverse rechterlijke uitspraken die van invloed zijn op veel clouddienstverleners. Deze zorgen zien in ieder geval op rechtmatigheid van de doorgifte van persoonsgegevens aan de VS, die in de praktijk bij veel clouddiensten plaatsvindt.[3] Doorgifte kan ook plaatsvinden doordat persoonsgegevens binnen een groepsonderneming, of via een leverancier, worden doorgezonden naar entiteiten buiten de EER en mogelijk onrechtmatig is. De AP is van mening dat het Rijksbrede cloudbeleid hier onvoldoende rekening mee houdt. De AP adviseert dan ook nadrukkelijk om, voorafgaand aan het

[2] Art. 45 AVG
[3] HvJEU C-311/18 Schrems II.

inzetten van een clouddienst, een Transfer Impact Assessment (TIA) uit te (laten) voeren.[4] Hierdoor kunnen risico's tijdig worden geïdentificeerd zodat er, indien mogelijk, aanvullende maatregelen kunnen worden getroffen om ervoor te zorgen dat het fundamentele recht op bescherming van persoonsgegevens wordt gewaarborgd bij de inzet van een clouddienst en tevens de continuïteit van essentiële dienstverlening kan worden gewaarborgd. Daarbij wil de AP opmerken dat ook bij een zorgvuldig uitgevoerde analyse al dan niet conform een handreiking vanuit CIO Rijk, met ontwikkelingen rond internationale doorgifte rekening dient te worden gehouden. Dat betekent onder meer dat wetswijzigingen in derde landen waarnaar gegevens worden doorgegeven gemonitord moeten worden, zodat er een heroverweging kan plaatsvinden wanneer dergelijke wijzigingen op gespannen voet staan met het beschermingsniveau van persoonsgegevens dat wettelijk verankerd is in de AVG. Dit kan erin resulteren dat een bepaalde soort doorgifte niet (langer) rechtmatig is. Gezien de aard en de (mogelijk) grote hoeveelheid van persoonsgegevens is het immers juist bij overheidsdiensten van wezenlijk belang dat er goed zicht is op internationale datastromen bij een keuze voor een clouddienst, zodat gegevens van Nederlandse burgers goed worden beschermd.

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.

- In de bijlage bij het Rijksbrede cloudbeleid is opgenomen: "*De private Rijkscloud is uiteindelijk niet gerealiseerd, omdat geen gemeenschappelijke behoeftestelling heeft plaatsgevonden.*" De AP acht deze stelling onvoldoende onderbouwd en overweegt het volgende. Hoewel er wellicht geen volledig alternatief bestaat voor clouddiensten die commerciële partijen - al dan niet van buiten de EER - aanbieden, kan dit wellicht op onderdelen wel zo zijn.[5] Bijvoorbeeld indien er wel alternatieven zijn voor IaaS- of PaaS-diensten. Bij gebrek aan onderzoek hiernaar worden ontwikkelingen door hoogtechnologische Nederlandse ondernemingen en ondernemingen in de rest van de EER onvoldoende geïdentificeerd. Datzelfde geldt voor ontwikkelingen zoals GAIA-X. Juist vanuit een centraal Rijksbreed cloudbeleid kunnen deze ontwikkelingen worden gestimuleerd en, op termijn, als alternatief gaan dienen voor grote commerciële partijen, al dan niet van buiten de EER. Door dit onvoldoende te onderzoeken of onvoldoende bij te dragen aan de ontwikkeling hiervan ontstaat juist een situatie waarbij een te grote afhankelijkheid bestaat van grote commerciële partijen van buiten de EER. Indien er daarbij vragen rijzen, aangaande de rechtmatigheid van doorgifte van persoonsgegevens aan die aanbieders van buiten de EER, heeft de overheid zichzelf in een lastige positie gemanoeuvreerd. De AP merkt daarbij op dat bij gelijke functionaliteiten en mitigerende maatregelen betreffende de risico's inzake verwerking van persoonsgegevens, alleen

[4] Zie in dit verband ook de aanbevelingen van de European Data Protection Board (EDPB) over het treffen van noodzakelijke aanvullende maatregelen bij internationale doorgiften: 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)
[5] Zie in dat verband bijvoorbeeld de Marktstudie Clouddiensten van de ACM ACM/INT/440323.

al op basis van het aspect van de internationale doorgifte, een clouddienstverlener die volledig binnen de EER verwerkt de voorkeur zou moeten genieten vanuit het oogpunt van bescherming van persoonsgegevens. Dit uitgangspunt kwam echter wel naar voren in uw "Hoofdlijnen beleid voor digitalisering" waar staat: "*Op het gebied van cruciale digitale diensten dragen we bij aan de ontwikkeling van Europese alternatieven op het gebied van clouddiensten, zoals GAIA-X.".*[6] De AP mist een dergelijk uitgangspunt in het Rijksbrede cloudbeleid en adviseert u dit te adresseren.

- De AP adviseert u te overwegen nader uit te werken op welke wijze clouddienstverleners die binnen Nederland of de EER persoonsgegevens verwerken, kunnen bijdragen aan dienstverlening waarbij de risico's voor betrokkenen langdurig worden gemitigeerd. Bijvoorbeeld door het in samenspraak met het ministerie van EZK opvolging geven aan een reeds eerder gestart pilotonderzoek van het CBS.[7] Een dergelijk onderzoek kan bijdragen aan een schets van de mogelijkheden die clouddienstverleners die volledig in Nederland of de EER verwerken, bieden. Het actueel houden van een dergelijk overzicht zou naar de mening van de AP een actie moeten zijn die onderdeel is van het Rijksbrede cloudbeleid.

Opmerkingen ten aanzien van de implementatie en naleving van het Rijksbrede cloudbeleid:

- Het Rijksbrede cloudbeleid bepaalt dat CIO Rijk een implementatierichtlijn risicoafweging cloudgebruik opstelt, waarmee de departementale CIO-office bij gebruik van een clouddienst desgevraagd aan CIO Rijk een gegevensbeschermingseffectbeoordeling met daarin een samenhangende risicoanalyse kan overhandigen. Uit het Rijksbrede cloudbeleid kan ten onrechte de indruk ontstaan dat de implementatierichtlijn een handreiking is en dus in principe (nog) geen formele status heeft. In het door u met de AP gevoerde gesprek heeft u echter aangegeven dat het in de Ministerraad zal worden vastgesteld en dus dwingend is voor alle departementen en dienstonderdelen. De AP merkt op dat er vanuit de AVG geen vrijblijvendheid bestaat ten aanzien van het uitvoeren van een DPIA bij grootschalige verwerkingen van bijzondere categorieën van persoonsgegevens of persoonsgegevens van strafrechtelijke veroordelingen en strafbare feiten. De AVG stelt immers dat een DPIA dan "*met name vereist*" is.[8] Daarnaast is het gezien de aard, de omvang, de context en de doeleinden van verwerkingen waarvoor de clouddiensten zullen worden ingezet vrijwel uitgesloten dat er geen sprake is van verwerkingen die leiden tot een hoog risico. Ook in die gevallen is een DPIA verplicht.[9] De AP acht het daarom noodzakelijk stevigere en dwingende regievoering te nemen op de verplichtingen uit de AVG. Bijvoorbeeld door het cloudbeleid en het daaruit volgende implementatiekader te codificeren in een Rijksbrede regeling gebaseerd op artikel 2 van het Coördinatiebesluit organisatie, bedrijfsvoering en informatiesystemen rijksdienst. Middels een dergelijke regeling kan een noodzakelijke coördinerende en monitorende rol van het ministerie van BZK worden verankerd.

[6] Kamerstukken 2021-2022, 26643 nr. 842, Hoofdlijnen beleid voor digitalisering.
[7] https://www.cbs.nl/nl-nl/maatwerk/2021/20/pilotonderzoek-nederlandse-cloudaanbieders-2019
[8] Artikel 35 lid 3 AVG.
[9] Artikel 35 lid 1 AVG.

- Het plan lijkt het belang en de omvang van de gegevensverwerkingen door zelfstandige bestuursorganen te onderschatten door te stellen: "*Onderdelen van de overheid die niet tot de Rijksdienst behoren wordt geadviseerd om dit Rijksbeleid te volgen. Aan de departementen wordt gevraagd dit voor de onder hun minister vallende ZBO's en eventueel andere organisaties te stimuleren.*"
  De AP constateert dat er door dit "*stimuleren*" te veel vrijblijvendheid bestaat bij een aantal overheidsinstanties die grootschalig (bijzondere) persoonsgegeven verwerken van zeer veel (kwetsbare) burgers, zoals het UWV, CBS, SVB en CAK. Gezien het feit dat dit Rijksbrede cloudbeleid en de daarin genoemde risicoafweging de juiste invulling van het grondrecht op privacy dienen te waarborgen, acht de AP het noodzakelijk te overwegen dit steviger te borgen in de implementatieafspraken met ZBO's.[10] Op grond van Kaderwet ZBO's artikel 41, eerste lid zijn dwingender afspraken t.a.v. dit cloudbeleid ook mogelijk. Hier is immers expliciet aangegeven dat ZBO's verplicht zijn om "op de voet van de ter zake voor de Rijksdienst geldende voorschriften" zorg te dragen voor de nodige technische en organisatorische voorzieningen ter beveiliging van hun gegevens tegen verlies of aantasting en tegen onbevoegde kennisneming, wijziging en verstrekking van die gegevens.

- Het Rijksbrede cloudbeleid formuleert voor een aantal situaties een "*comply or explain*"-aanpak. Er is daarbij echter geen duidelijke procedure opgenomen betreffende de vraag hoe er invulling aan dit principe wordt gegeven. Zo is bijvoorbeeld onduidelijk welke maatregelen CIO Rijk kan treffen bij een onvoldoende onderbouwde vaststelling van het "comply"-deel dan wel een onvoldoende motivatie bij het "explain"-deel. De AP adviseert om de hiertoe te volgen procedure, met verduidelijking van de rollen en bevoegdheden van de betrokken partijen, op te nemen in de implementatierichtlijn voor dit cloudbeleid. De AP merkt daarbij op dat er alleen binnen de kaders van de AVG sprake kan zijn van een "explain", aangezien de overheid zich te allen tijde dient te houden aan de AVG. Daar waar een passage in het Rijksbrede cloudbeleid raakt aan een verplichting uit de AVG adviseert de AP u deze toe te voegen.

- Voor overheidsorganisaties die clouddiensten/CSP-diensten afnemen is het van belang dat zij *voorafgaand* aan de ingebruikname van een clouddienst de risico's in kaart brengen en de benodigde maatregelen treffen om de rechten van betrokkenen te kunnen beschermen. De strategisch leveranciersmanagement-functie binnen het Rijk (SLM-functie) kan een belangrijke rol spelen om daar in een vroegtijdig stadium aan bij te dragen. De AP heeft in het kader van de gecoördineerde actie naar de inzet van clouddiensten door overheidsinstellingen onderzoek gedaan bij een aantal SLM-functies binnen het Rijk bij de verwerving van clouddiensten. Een aantal eerste observaties naar aanleiding van dit onderzoek zijn per brief aan u en andere bewindslieden medegedeeld.[11] Uit het onderzoek is gebleken dat er op plaatsen een SLM-functie is ingericht 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 clouddienst. Er is echter ook een SLM-functie waarin deze rol naar de mening van de AP nog onvoldoende professioneel lijkt te zijn. De AP heeft daarbij

[10] Artikel 41 van de Kaderwet zelfstandige bestuursorganen zou daartoe wellicht mogelijkheden kunnen bieden.
[11] Zie brief z2022-00846 d.d. 18 oktober 2022

vernomen dat er geen duidelijk kader bestaat voor de rol en belegging van SLM-functies binnen het Rijk alsmede voor welke CSP's een SLM-functie is bekleed. De AP adviseert om beleid te formuleren waarin de rol en positie van de SLM-functies wordt verduidelijkt en steviger wordt verankerd bij de verwerving van clouddiensten. Het is daarbij essentieel dat de SLM-functies voorzien zijn van voldoende mensen en middelen. Daarnaast adviseert de AP een duidelijke inkoopstrategie te formuleren waar alle CSP's aan dienen te voldoen en waar de SLM-functies op kunnen toetsen. De AP geeft daarbij in overweging deze strategie vast te leggen in het cloudbeleid dan wel in andere documenten, zodat deze leidend zijn voor alle departementen.

Ten overvloede merkt de AP op dat:

- de bijlage bij het Rijksbrede cloudbeleid een opsomming van landen bevat die de overstap lijken te maken van een private naar een hybride of public cloud. De AP merkt op dat een onderbouwing voor dit standpunt ontbreekt en dat met deze keuze nog niet is gezegd dat er gebruik kan worden gemaakt voor een clouddienstverlener die buiten de EER persoonsgegevens verwerkt. Daarnaast worden er in de opsomming landen genoemd van buiten de EER die niet aan de AVG gebonden zijn en waarvoor ook geen adequaatheidsbesluit in de zin van art 45 van de AVG is genomen. Vanuit het oogpunt van de bescherming van persoonsgegevens is dat onderscheid van wezenlijk belang omdat daar een ander beschermingsniveau voor persoonsgegevens kan gelden. De AP adviseert u ten aanzien van landen die overstappen naar een hybride of public cloud duidelijk te maken of deze landen een gelijkwaardig beschermingsniveau ten aanzien van persoonsgegevens bieden zodat een eventueel verschil met de Nederlandse situatie duidelijk is. Voor zover deze landen voorwaarden stellen aan het soort gegevens die men in de hybride of public cloud kan verwerken adviseert de AP u dat ook te vermelden.
- het Rijksbrede cloudbeleid een aantal voordelen benoemt bij het inzetten van clouddiensten. De AP neemt waar dat in de destijds benoemde voordelen en nadelen er geen opmerking is gemaakt ten aanzien van de bescherming van persoonsgegevens.[12] De AP adviseert u gezien de bovenstaande adviezen de bescherming van persoonsgegevens ook op te nemen in de beoordeling van de voor- en nadelen van clouddienstverlening en deze periodiek te beoordelen. Een dergelijke beoordeling kan dan worden gebruikt bij het herzien van het Rijksbrede cloudbeleid.

De AP adviseert u deze brief, de daarin opgenomen adviezen van de AP en uw reactie daarop te verstrekken aan de Tweede Kamer ten behoeve van de behandeling van het "Rijksbreed cloudbeleid 2022".

De AP adviseert u tevens minimaal jaarlijks, of indien daar anderszins aanleiding toe is, de overwegingen die hebben geleid tot uitspraken in het "Rijksbreed cloudbeleid 2022" te herzien.

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.

[12] Kamerstukken 2010-2011, 26643 nr. 172, Bijlage evaluatie ICT-beleid Rijksoverheid.

Datum
11 november 2022

Ons kenmerk
z2022-05319

Hoogachtend,
Autoriteit Persoonsgegevens,

Aleid Wolfsen
voorzitter