Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2022–2023

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 965

BRIEF VAN DE STAATSSECRETARIS VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 24 januari 2023

De Autoriteit Persoonsgegevens (AP) heeft op 11 november 2022 een brief inzake het Rijksbreed Cloudbeleid 2022 uitgebracht[1]. Via deze brief ontvangt u de beleidsreactie van het kabinet, namens de Staatssecretaris van BZK, op de brief van de AP.

Aanleiding

In de ministerraad van 19 augustus 2022 is het Rijksbreed cloudbeleid 2022 goedgekeurd. Met het Rijksbreed cloudbeleid 2022 is het voor departementen onder strenge voorwaarden toegestaan om gebruik te maken van publieke clouddiensten.

Naar aanleiding van het Rijksbreed cloudbeleid 2022 heeft de AP een brief gestuurd met daarin drie adviezen om privacyrisico's nadrukkelijker te onderkennen en mitigeren. In deze brief worden de adviezen van de AP geadresseerd.

Adviezen van de AP

De AP neemt waar dat overheidsdiensten nu ook al gebruik maken van publieke clouddiensten, maar dat er van een uniforme aanpak geen sprake is. Volgens de AP is het Rijksbreed cloudbeleid 2022 een belangrijke stap in de uniformering en professionalisering van de wijze waarop binnen de rijksoverheid met clouddiensten en clouddienstverleners wordt omgegaan.

Wel constateert de AP dat er een aantal wezenlijke privacyrisico's zijn bij de inzet van clouddiensten. In dat kader geeft de AP enkele aandachtspunten en adviezen ten aanzien van het Rijksbreed cloudbeleid 2022 en de implementatie daarvan:

[1] Zie bijlage.

kst-26643-965
ISSN 0921 - 7371
's-Gravenhage 2023

1. Vollediger adresseren van de privacyrisico's en dit leidend maken bij de vraag of een clouddienst rechtmatig kan worden ingezet.;
2. Nadrukkelijk adresseren van de specifieke risico's die spelen bij de doorgifte van persoonsgegevens naar landen buiten de Europese Economische Ruimte (EER).; en
3. Verzekeren van de uitvoering van dit cloudbeleid om te voorkomen dat de privacyrisico's niet, of onvoldoende worden geïdentificeerd door overheidsinstellingen.

In de rest van de brief werkt de AP deze adviezen gemotiveerd verder uit.

Beleidsreactie op de adviezen

Advies AP:

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.»

Reactie:

Het Rijksbreed cloudbeleid 2022 stelt aanvullende voorwaarden vast voor het gebruik van de public cloud. Overige wet- en regelgeving, maar in het bijzonder de AVG, blijven onverkort van toepassing. Het beleid gaat nooit boven wettelijke verplichtingen zoals de AVG. Voor rechtmatige inzet van een clouddienst zijn privacyaspecten een randvoorwaarde.

Het klopt dat het vanuit het gegevensbeschermingsrecht niet direct relevant is voor welk type clouddienst gekozen wordt, i.e. of dat publiek, privaat of hybride is. Voor elk type geldt immers dat aan dezelfde standaarden moet zijn voldaan wanneer persoonsgegevens worden verwerkt. Voor overige disciplines, waaronder informatiearchitectuur en leveranciersmanagement, of innovatiemogelijkheden, is dit onderscheid van wezenlijk belang. Het is belangrijk om op te merken dat het Rijksbreed cloudbeleid 2022 niet alleen privacy betreft, maar breder gaat.

Advies AP:

2. Nadrukkelijk adresseren van de specifieke risico's die spelen bij de doorgifte van persoonsgegevens naar landen 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.

Reactie:

Zoals gezegd dient de verwerking van persoonsgegevens ook bij het gebruik van Clouddiensten rechtmatig plaats te vinden. Wanneer sprake is van doorgifte van persoonsgegevens naar landen buiten de EER, dan moet voldaan zijn aan de voorwaarden van hoofdstuk V van de AVG. Daarbij is het van belang dat de richtsnoeren die op 18 juni 2021 zijn vastgesteld door het Europees Comité voor Gegevensbescherming (EDPB) worden gevolgd. Deze richtsnoeren bieden handvatten bij de beoordeling welke aanvullende maatregelen kunnen worden getroffen bij de verwerking van persoonsgegevens door derden.

In het voor de Rijksdienst verplichte implementatiekader, dat op 20 december door de Interdepartementale Commissie Bedrijfsvoering Rijk (ICBR) is vastgesteld, is opgenomen dat departementen die gebruik willen maken van de public cloud specifieke risico's ten aanzien van de doorgifte van persoonsgegevens naar landen buiten de EER mee moeten nemen, waarbij telemetrie specifiek is genoemd in artikel 7. Ook het Data Transfer Impact Assessment (DTIA) is in het implementatiekader opgenomen. Zo is er al een Data Transfer Impact Assessment uitgevoerd op Microsoft Teams. Op dit moment loopt een DTIA naar Google Workspace. Uiteraard worden ook sub-verwerkers in deze DTIA's meegenomen.

De vraag of er verwerking buiten de EER is, is daarmee onderdeel van de analyse voor elke inzet van een clouddienst. Hierbij moet voldaan worden aan de eisen vanuit de AVG en gelden genoemde adviezen van het EDPB en de AP als uitgangspunt.

We delen de visie dat het eenvoudiger is om, conform artikel 5.2 van de AVG, aantoonbaar te voldoen aan de AVG als de clouddienstverlening volledig vanuit de EER plaatsvindt. In de evaluatie van het Rijksbreed cloudbeleid 2022 en bijbehorend implementatiekader zal beoordeeld worden of dit ook in het beleid een plek moet krijgen.

Advies AP:

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 Rijksbreed 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.

Reactie:

Ik deel de opvatting dat de overheid het goede voorbeeld moet geven waar het gaat om de naleving van wettelijke regels, zo ook inzake het gegevensbeschermingsrecht. Het Rijksbreed cloudbeleid 2022 stelt dan ook aanvullende voorwaarden vast voor het gebruik van de public cloud

om te waarborgen dat daarvan sprake is en de standaarden van de AVG niet uit het oog worden verloren.

Op basis van het Rijksbreed cloudbeleid 2022 stelt CIO Rijk twee stukken op, namelijk een implementatiekader en een handreiking. Het implementatiekader heeft formele status en een verplichtend karakter en is op 20 december 2022 vastgesteld in de ICBR. De handreiking biedt de Rijksdienst een verzameling «best practices» als voorbeelden en verdere ondersteuning voor verantwoord gebruik van de public cloud.

Het Rijksbreed cloudbeleid 2022 is van toepassing op de Rijksdienst. Onderdelen van de overheid die niet tot de Rijksdienst behoren worden geadviseerd om dit Rijksbeleid te volgen. De omvang en het belang van gegevensverwerkingen door ZBO's kunnen tevens zeer groot zijn. Vanuit een Rijksbreed beleid kunnen wij voor zelfstandige bestuursorganen echter niet verplicht beleid opstellen. Hiervoor is wel ruimte in het, vanuit het Rijksbreed cloudbeleid 2022 verplicht gestelde, departementale cloudbeleid en -strategie.

ZBO's worden wel geacht om in lijn met het overheidsbeleid invulling te geven aan informatiebeveiliging. Ongeacht het Rijksbreed cloudbeleid 2022 moeten ook ZBO's zich houden aan alle wet- en regelgeving waaronder de AVG. Tijdens de evaluatie van het beleid zullen we ook onderzoeken of de ZBO's het Rijksbreed cloudbeleid 2022 toepassen.

Naast bovenstaande adviezen raadt de AP tevens aan om onderzoek uit te voeren om 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. Momenteel worden er al gesprekken gevoerd met clouddienstverleners binnen Nederland en de EER. Deze gesprekken gaan onder andere over de langdurige bescherming van persoonsgegevens van betrokkenen.

De AP heeft op 10 november 2022 een andere brief gestuurd inzake de inzet van Cloud Service Providers.[2] Zij gaat in deze brief in op de rol van de Strategisch Leveranciers Management (SLM)-functie. Ten aanzien van de rol van de SLM-functie binnen het Rijk stuur ik u een aparte beleidsreactie.

Tot slot

In het komende jaar zal vanaf het derde kwartaal het Rijksbreed cloudbeleid 2022 en het bijbehorend implementatiekader geëvalueerd worden. Tevens zal ik over de voortgang van de implementatie rapporteren om daarmee uw Kamer de gelegenheid te geven om nadere vragen te stellen.

De Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,
A.C. van Huffelen

[2] Autoriteit Persoonsgegevens 2022, Inzet van Cloud Service Providers, opgehaald van: brief_over_inzet_cloud_service_providers.pdf (autoriteitpersoonsgegevens.nl).