AUTORITEIT
PERSOONSGEGEVENS

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

Uitsluitend aangeboden via de Bestandenpostbus aan:
[redacted]@hotmail.com

T.a.v. [redacted]

Datum
20 februari 2025

Ons kenmerk
[redacted]

Contactpersoon
[redacted]
070 8888 500

Onderwerp
Woo-besluit

Geachte [redacted]

Op 5 december 2024 heeft u de Autoriteit Persoonsgegevens (hierna: AP) per e-mail verzocht om openbaarmaking van informatie. U beroept zich hierbij op de Wet open overheid (hierna: Woo).

Op 16 december 2024 heeft de AP de ontvangst van uw Woo-verzoek per brief aan u bevestigd.

Op 30 december 2024 verdaagde de AP de termijn om te beslissen met twee weken per brief aan u.

Besluit
De AP besluit uw verzoek om openbaarmaking van informatie in te willigen. De AP gaat over tot gedeeltelijke openbaarmaking, met inachtneming van het bepaalde in artikel 5.1, eerste lid, onder c en tweede lid, onder e, van de Woo.

De AP licht hierna het besluit aan u toe.

Verzoek
U vraagt de AP in uw verzoek om:

- *"Plan van aanpak, draaiboek, werkinstructie, algemene informatie of praktijkhandleiding ten aanzien van het beleid dat de Autoriteit Persoonsgegevens voert voor datamigratie, o.a. (maar niet uitsluitend) in de context van het overstappen naar cloud oplossingen en andere (cloud)leveranciers.*
- *De informatie die verwachtingen/vereisten van de AP bevat gericht op verwerkingsverantwoordelijken/verwerkers bij de ingebruikname van nieuwe systemen, cloudoplossingen, data migratie en overstap van on-premise ontwikkelingen naar cloud oplossingen, inclusief enige vorm van (informele en formele) handhaving door de AP op deze onderwerpen.*

- *alle (informele en formele) handhaving door de AP met betrekking tot artikel 48 AVG."*

Wettelijk kader
De AP behandelt uw verzoek als een verzoek om openbaarmaking van informatie. De AP neemt hierbij het wettelijk kader van de Woo in acht. De AP willigt een Woo-verzoek in (artikel 4.1, zevende lid, van de Woo), voor zover:

- de AP over de informatie beschikt;
- de informatie niet al openbaar is, en
- de uitzonderingsgronden van hoofdstuk 5 van de Woo hieraan niet in de weg staan.

Zoekslag
De AP verricht vanwege uw verzoek een zoekslag naar de gevraagde informatie. De AP zoekt hierbij binnen de beschikbare applicaties. De AP heeft hierbij er alles aan gedaan om tot een zo volledig mogelijke zoekslag te komen. De AP treft vervolgens één document aan. Ten aanzien van punt twee en drie van uw verzoek heeft de AP geen documenten aangetroffen.

Overigens is de Woo niet van toepassing op reeds openbare documenten. Documenten die al openbaar zijn gemaakt, kunnen niet nogmaals openbaar worden gemaakt. De AP verwijst naar de vindplaatsen van de twee reeds openbare documenten:

- https://autoriteitpersoonsgegevens.nl/uploads/imported/brief_over_rijksbreed_cloudbeleid_2022.pdf
- https://www.autoriteitpersoonsgegevens.nl/documenten/brief-minister-van-onderwijs-cultuur-en-wetenschap

Motivering voor het gedeeltelijk openbaar maken van informatie
De AP weegt voor het openbaar maken van informatie het algemeen belang af tegen de uitzonderingsgronden die in hoofdstuk 5 van de Woo zijn vastgelegd.

Vertrouwelijk gedeelde bedrijfs- en fabricagegegevens
De AP maakt geen informatie openbaar als dit bedrijfs- en fabricagegegevens betreffen, die vertrouwelijk aan de overheid zijn verstrekt. Dat de gegevens vertrouwelijk zijn verstrekt, kan blijken uit een expliciete verklaring, of wanneer de verstrekker mocht aannemen dat het om vertrouwelijke gegevens gaat. Het gaat om alle informatie over de technische bedrijfsvoering, het productieproces, de afzet van producten of de kring van afnemers of leveranciers. Ook gegevens die uitsluitend de financiele bedrijfsvoering betreffen kunnen hieronder vallen.

In het aangetroffen document staan dergelijke bedrijfs- of fabricagegegevens. Het gaat om informatie waaruit de kring van afnemers of leveranciers kan worden afgeleid. Openbaarmaking van (delen van) het document kan de leverancier, die de informatie heeft verstrekt, schaden. De informatie wordt daarom gedeeltelijk openbaar gemaakt. De AP maakt gegevens die herleidbaar zijn tot leveranciers dus niet openbaar. De AP verwijst voor deze absolute uitzonderingsgrond naar artikel 5.1, eerste lid, onder c, van de Woo.

Datum
20 februari 2025

Ons kenmerk
[redacted]

Eerbiediging van de persoonlijke levenssfeer

De AP onderschrijft de eerbiediging van de persoonlijke levenssfeer. Er staan persoonsgegevens in het document, dat door de AP gedeeltelijk openbaar wordt gemaakt. Dit zijn gegevens die herleidbaar zijn tot een persoon, eventueel in combinatie met andere gegevens. De AP geeft als voorbeelden: persoonsnamen, telefoonnummers, e-mailadressen, handtekeningen, initialen en zaaknummers (o.m. aangemaakt door de AP).

De AP vindt dat het openbaar maken van persoonsgegevens een inbreuk maakt op de persoonlijke levenssfeer van betrokkenen (inclusief ambtenaren). In het verzochte document staan persoonsgegevens die herleidbaar zijn tot een persoon. De AP weegt het belang van de eerbiediging van de persoonlijke levenssfeer daarom zwaarder dan het algemeen belang van het openbaar maken ervan.

De informatie wordt gedeeltelijk openbaar gemaakt. De AP maakt gegevens die herleidbaar zijn tot een persoon dus niet openbaar. De AP verwijst voor deze relatieve uitzonderingsgrond naar artikel 5.1, tweede lid, onder e, van de Woo.

Publicatie

De AP publiceert dit besluit en het document geanonimiseerd op haar website. Daardoor wordt de verzochte informatie toegankelijk voor iedereen.

Vragen?

Heeft u vragen? Wilt u een toelichting op het besluit? Neem dan contact op met de contactpersoon bovenaan de brief. De contactpersoon neemt dan samen met u het besluit door.

Hoogachtend,
Autoriteit Persoonsgegevens,
Namens deze,

[redacted]

Adviseur Staftaken / Bedrijfsvoering

Datum
20 februari 2025

Ons kenmerk
[redacted]

Rechtsmiddelenclausule
Bezwaar maken
Bent u het niet eens met de inhoud van dit besluit? Dan kunt u binnen zes weken na de verzenddatum van dit besluit digitaal of schriftelijk bezwaar indienen. Op autoriteitpersoonsgegevens.nl/bezwaar-maken leest u hoe u dit doet.

Op autoriteitpersoonsgegevens.nl/bezwaar-maken vindt u het digitale formulier waarmee u uw bezwaar indient.

Als u schriftelijk bezwaar wilt maken, dan moet u uw brief binnen zes weken na de verzenddatum van dit besluit sturen naar het bovenaan deze brief genoemde postadres. Vermeld op de envelop 'Awb-bezwaar' en zet 'bezwaarschrift' in de titel van uw brief.

Neem in uw bezwaar ten minste op:
- uw naam en adres;
- de datum van uw bezwaar;
- de reden(en) waarom u het niet eens bent met dit besluit;
- uw handtekening;
- het bovenaan deze brief genoemde kenmerk of een kopie van dit besluit.

AUTORITEIT
PERSOONSGEGEVENS

Memo

Datum
14 mei 2020

Van
[redacted]

Aan
Stuurgroep project Nieuw Zaaksysteem

Onderwerp
Clouddiensten en informatiebeveiliging

Adviesvraag
Naar aanleiding van twee lopende projecten is mij gevraagd om, als [redacted], te adviseren over het gebruik van cloudoplossingen. Om tot een advies te komen heb ik meerdere bronnen onderzocht, waarvan "BIO Thema: Cloud diensten" d.d. 20-11-2019 opgesteld door BZK-Werkgroep BIO (bestaande uit o.a. Min. Fin, Min. BZK, Min. EZenK, Dictu, Politie, Belastingdienst, JustID) specifiek genoemd moet worden, omdat hier de kaders worden beschreven die gelden voor AP als overheidsorganisatie. Dit document is toegevoegd als bijlage.

Scope
Het advies is van toepassing op twee lopende projecten, het project Nieuw zaaksysteem (vervanging Wiske) en project Meldloket Datalekken. In beide projecten kan gekozen worden voor een cloudoplossing waar een leverancier de gegevens verwerkt en/of bewaard op gedeelde apparatuur en infrastructuur, of een on-premise oplossing waar AP alle data in huis houdt op eigen apparatuur.

Het converteren van gesloten dossiers in Wiske naar een digitaal archief, dat on-premise of in de cloud gehost kan worden, is buiten scope van dit advies. De kaders in dit advies kunnen gebruikt worden als input voor dit (deel)project om een afweging te maken, maar er dient ook rekening gehouden te worden met de archiefwet.

Cloudoplossingen
De volgende definities zijn bepaald door NIST (National Institute of Standards and Technology, Amerikaans wetenschappelijk instituu) en worden wereldwijd gehanteerd in informatiebeveiligingsstandaarden:

- Private cloud (met dedicated infrastructuur): Ingericht voor één klant en uitsluitend te gebruiken door één klant, ingericht conform de standaarden van de provider.
- Community cloud (met geheel of gedeeltelijk gedeelde infrastructuur, ook bekend als Private/Shared cloud): De IT-voorzieningen zijn toegankelijk voor één klant en delen om kosten te besparen de infrastructuur met andere klanten (bijvoorbeeld de opslag en het netwerk).
- Public cloud: de IT-voorzieningen zijn toegankelijk via het internet. De voorzieningen worden gedeeld met andere klanten.
- Hybrid cloud: een combinatie van (elementen uit) bovenstaande cloud varianten.

Datum
7 mei 2020

Private cloud en Community cloud zijn geschikt voor AP, het opslaan en verwerken van departementaal vertrouwelijke gegevens (rubriceringsniveau dat AP hanteert) en persoonsgegevens is toegestaan.

Het kiezen voor een cloudoplossing heeft een aantal specifieke voordelen t.o.v. "zelf doen":
- De organisatie kan de focus houden op kerntaken.
- Het kan leiden tot efficiëntere bedrijfsvoering en het verlagen van total cost of ownership.
- De organisatie kan in een kort tijdbestek beschikken of nieuwe IT-functionaliteit.
- Zekerheid over gekwalificeerd personeel.
- Het verlagen van IT complexiteit in specifieke situaties.
- Het verbeteren van beschikbaarheid.

[redacted]
De beoogde leverancier van het nieuwe zaaksysteem is [redacted] [redacted] biedt overheidsorganisaties een cloudoplossing aan met de naam [redacted], dat zich bevind in een datacenter in [redacted] Mondeling heeft [redacted] gezegd dat het gaat om een cloudoplossing die alleen gebruikt kan worden door overheidsorganisaties, hiermee is geïnsinueerd dat [redacted] een Community cloudoplossing is.

In de stukken die [redacted] heeft toegestuurd staat niet beschreven hoe de [redacted] cloudoplossing is ontworpen. In [redacted]pdf" is de [redacted] cloudoplossing beschreven, dit document is verstrekt door [redacted] Er is niet beschreven dat [redacted] afwijkt van de [redacted] Cloud, daarom moet er van uit worden gegaan dat de white paper ook van toepassing is op [redacted]
Opvallend is de volgende passage (pagina 5):
"**Elements of the public and community cloud definition apply to the [redacted] Cloud** however it is not provided for open use by the general public, but solely to [redacted] business customers. Due to this distinction, although the [redacted] Cloud offers a shared cloud infrastructure (with virtual and logical segregation between customers), **throughout this paper we have referred to [redacted] cloud offering as a private/hybrid cloud rather than a "public cloud"**."

[redacted] heeft op 14 mei 2020 per mail bevestigd dat de cloudoplossing die AP is aangeboden een Community cloudoplossing is. Dataopslag is volledig afgeschermd en daarmee private, processorkracht en netwerk infrastructuur en ontsluiting worden uitsluitend gedeeld met 'tenants' [redacted] klanten).

Advies 1:
Conform de normen die benoemd zijn in de BIO is het toegestaan om gebruik te maken van de [redacted] cloudoplossing die [redacted] heeft aangeboden. Vanuit informatiebeveiligingsoptiek zijn er geen bezwaren tegen de inrichting.

In het programma van eisen staat dat toegang tot de AP [redacted] omgeving uitsluitend mogelijk mag zijn vanaf het AP netwerk, en niet vanaf het internet. [redacted] heeft gezegd dat zij aan deze eis kunnen voldoen. De omgeving wordt echter wel gedeeld met andere klanten en dit is van invloed op de risico's die AP loopt bij het gebruik van de cloudoplossing.

Datum
7 mei 2020

In het geval van zero day leaks die gedeelde elementen treffen van de [redacted] cloudoplossing moeten passende maatregelen getroffen worden. Deze maatregelen gaan verder dan bij een on-premise oplossing. Bij een on-premise oplossing zijn opslag, processorkracht en infrastructuur alleen bestemd voor AP, in deze setting is uitsluitend opslag bestemd voor AP geïsoleerd en wordt processorkracht en infrastructuur gedeeld met andere klanten. Daarom is de kans op misbruik van een beveiligingslek significant groter dan on-premise, en de circle of control en circle of influence van AP is kleiner omdat AP niet maatregelen op kan leggen aan andere tenants.

De kans op misbruik verkleinen tijdens een zero day leak kan door preventief maatregelen te nemen, waarvan de meest voor de hand liggende maatregel het niet gebruiken van het [redacted] systeem is. Data van AP wordt versleuteld opgeslagen en zo lang deze data "in rust" is blijft de data versleuteld. Bij het raadplegen of bewerken van AP data wordt gedeelde processorkracht gebruikt om de data te ontsleutelen en gedeelde infrastructuur gebruikt om de data te tonen via het [redacted] systeem. Zo lang er niets met de data gebeurt tijdens een zero day leak is de data in principe afgeschermd.

Dit heeft natuurlijk gevolgen voor de processen van AP. Daarom luidt het advies om voor livegang op grote lijnen een strategie te bepalen hoe AP zal reageren op zero day leaks en soortgelijke incidenten. Het is wijs om soortgelijke processen te groeperen en hier passende maatregelen aan te verbinden. Zo is de impact op een afdeling met langlopende dossiers kleiner dan bijvoorbeeld IMP die meerdere dossiers per dag verwerken. De nieuwe backend van het meldloket datalekken wordt ingericht in de [redacted] omgeving, bij maatregelen dient rekening gehouden te worden met organisaties die meldplichtig zijn.

Dit risico verkleinen kan door te kiezen voor een volledig private cloudoplossing, met exclusieve infrastructuur en hardware voor AP. De kosten zullen aanzienlijk hoger zijn in verhouding tot een cloudoplossing waarbij generieke elementen gedeeld worden tussen klanten en de kosten gezamenlijk worden gedragen. De kans dat een zero day leak zich voor doet is gering, en het is de vraag of de mogelijk hoge extra kosten gerechtvaardigd kunnen worden.

Advies 2:
Vraag een kostenindicatie aan [redacted] voor een volledig private cloudoplossing die niet wordt gedeeld met andere klanten. Bepaal of de extra kosten te rechtvaardigen zijn om de impact van zero day leaks te beperken.

Advies 3:
Bepaal de strategie hoe omgegaan wordt met kwetsbaarheden, zoals zero day leaks, die de gedeelde elementen van de [redacted] cloudoplossingen kunnen treffen. Denk hierbij aan langlopende en hoog volume processen binnen AP, en processen die raakvlak hebben met externe organisaties en hun wettelijke verplichtingen, zoals de meldplicht datalekken. Maatregelen, workarounds en communicatieplannen worden gebaseerd op deze strategie. Het inventariseren groeperen van processen kan meegenomen worden in de IB/DPIA werkzaamheden van het project.

Datum
7 mei 2020

[redacted]
Voor het meldloket datalekken moet een webformulier gehost worden. [redacted] is hiervoor de geselecteerde leverancier. Het is inmiddels duidelijk dat de omgeving gehost zal worden door [redacted], de provider van J&V. Daarom valt de frontend buiten scope van dit advies. De [redacted] cloudoplossing dient als backend van het systeem, daarom dient dit proces wel benoemd te worden in de maatregelen voor zero day leaks.

Advies 4:
Het webformulier datalekken draait niet in een cloudoplossing maar binnen de beschermde J&V infrastructuur gehost door provider [redacted] De [redacted] omgeving is echter wel de backend van dit systeem. Kwetsbaarheden in [redacted] zijn direct van invloed op het meldloket datalekken, daarom dient dit proces beschouwd te worden bij het bepalen van een passende strategie in het omgaan met zero day leaks. De impact van maatregelen is mogelijk groter dan bij interne AP processen, dit kan direct andere organisaties treffen (meldplicht datalekken). Besteed extra aandacht aan een aanvaardbare workaround.

Beleid, uitvoering en control

De diensten die AP af neemt van de provider dienen te voldoen aan de gestelde eisen en condities, ze dienen meetbaar en voorspelbaar te zijn, compliant aan wet- en regelgeving, en moeten beveiligd en beheerst zijn.
Specifieke cloud security controls zijn geformuleerd in “BIO Thema: Cloud diensten” die als handvat dienen om dit te bereiken. Een aantal van deze punten zullen gedekt zijn in de overeenkomst onder ARBIT/ARVODI voorwaarden, waaronder de offertes zijn uitgevraagd. Het is wijs om de invulling van de dienst te toetsen aan de controls die beschreven zijn in dit document.

Advies 5:
Toets en conformeer de overeenkomst, service level agreement (SLA) en nadere overeenkomst (NOK) van de cloudoplossing aan de controls in “BIO Thema: Cloud diensten” pagina 15 en 16. De [redacted] zorgt voor een overzicht van mijlpalen waarbij hij geraadpleegd dient te worden om te helpen de juiste controls te treffen.

Aandachtspunten

Omdat AP niet “in de keuken kan kijken” bij de leverancier is het belangrijk om extra aandacht te besteden goede overeenkomsten en de leverancier scherp te houden door controle en monitoring binnen de regieorganisatie.
Eenzijdige tariefverhoging of verplaatsing van data naar een andere locatie (bijvoorbeeld naar het buitenland) door de leverancier zijn situaties die voorkomen kunnen worden met een goede overeenkomst.

Een exit strategie bepalen is noodzakelijk bij gebruik van een cloudoplossing, want elk contract loopt af. AP moet er op toezien dat clouddiensten zo zijn ingericht dat deze inter-operabel zijn, en de dataset

overdraagbaar is. Zo wordt "vendor lock-in" voorkomen. AP wil niet lange tijd afhankelijk zijn van één leverancier.

Advies 6:
Controleer dat de overeenkomst en aanvullende afspraken worden nageleefd. Wie doet wat?

Advies 7:
Bepaal een exit strategie vóór de clouddienst in gebruik wordt genomen.

Adviezen

Advies 1:
Conform de normen die benoemd zijn in de BIO is het toegestaan om gebruik te maken van de [redacted] cloudoplossing die [redacted] heeft aangeboden. Vanuit informatiebeveiligingsoptiek zijn er geen bezwaren tegen de inrichting.

Advies 2:
Vraag een kostenindicatie aan [redacted] voor een volledig private cloudoplossing die niet wordt gedeeld met andere klanten. Bepaal of de extra kosten te rechtvaardigen zijn om de impact van zero day leaks te beperken.

Advies 3:
Bepaal de strategie hoe omgegaan wordt met kwetsbaarheden, zoals zero day leaks, die de gedeelde elementen van de [redacted] cloudoplossingen kunnen treffen. Denk hierbij aan langlopende en hoog volume processen binnen AP, en processen die raakvlak hebben met externe organisaties en hun wettelijke verplichtingen, zoals de meldplicht datalekken. Maatregelen, workarounds en communicatieplannen worden gebaseerd op deze strategie. Het inventariseren groeperen van processen kan meegenomen worden in de IB/DPIA werkzaamheden van het project.

Advies 4:
Het webformulier datalekken draait niet in een cloudoplossing maar binnen de beschermde J&V infrastructuur gehost door provider [redacted] De [redacted] omgeving is echter wel de backend van dit systeem. Kwetsbaarheden in [redacted] zijn direct van invloed op het meldloket datalekken, daarom dient dit proces beschouwd te worden bij het bepalen van een passende strategie in het omgaan met zero day leaks. De impact van maatregelen is mogelijk groter dan bij interne AP processen, dit kan direct andere organisaties treffen (meldplicht datalekken). Besteed extra aandacht aan een aanvaardbare workaround.

Advies 5:
Toets en conformeer de overeenkomst, service level agreement (SLA) en nadere overeenkomst (NOK) van de cloudoplossing aan de controls in "BIO Thema: Cloud diensten" pagina 15 en 16. De [redacted] zorgt voor een overzicht van mijlpalen waarbij hij geraadpleegd dient te worden om te helpen de juiste controls te treffen.

Advies 6:
Controleer dat de overeenkomst en aanvullende afspraken worden nageleefd. Wie doet wat?

Advies 7:
Bepaal een exit strategie vóórdat de clouddienst in gebruik wordt genomen.

Toelichting grondslagen

In dit document kunt u secties vinden die onleesbaar zijn gemaakt. Deze informatie is achterwege gelaten op basis van de Wet open overheid (Woo). De letter die hierbij is vermeld correspondeert met de bijbehorende grondslag in onderstaand overzicht.

C Art. 5.1 lid 1 sub c

Deze informatie betreft bedrijfs- en fabricagegegevens die vertrouwelijk aan de overheid zijn meegedeeld

J Art. 5.1 lid 2 sub e

Het belang van de openbaarmaking van deze informatie weegt niet op tegen het belang van de eerbiediging van de persoonlijke levenssfeer van betrokkenen