CONSIDERATI

DPIA migratie AWS Cloud

SIDN

Considerati

15 oktober 2024

Prof. mr. dr. Bart W. Schermer

Mr. Emilie Roosen

Mr. Marc Bonofacio

Versiebeheer

Versie	Datum	Eigenaar	Wijzigingen
0.1	4 juli 2024	BWS	-
0.9	2 september 2024	BWS	Wijzigingen nav. nieuw LZ document en commentaar SIDN doorgevoerd.
0.95	10 oktober 2024	BWS	Verwerken feedback SIDN.
1.0	15 oktober	BWS	Finale wijzigingen

Management Samenvatting

SIDN is voornemens de applicaties Fury (beoogd domeinnaamregistratieplatform), Merkbewaking (merkbewaking), DMAP (DNS analyse) en .nl Control (domeinnaambescherming) te migreren naar de AWS Cloud. De voornaamste reden om te kiezen voor een hyperscaler als AWS, is dat SIDN gebruik kan maken van hun robuuste infrastructuur, technische kennis en tools. Het in eigen beheer ontwikkelen en onderhouden van een infrastructuur die qua veiligheid en robuustheid vergelijkbaar is met AWS is nagenoeg onmogelijk en daarnaast zeer kostbaar. Door te kiezen voor AWS kan SIDN de veiligheid en continuïteit van haar dienstverlening beter garanderen.

Omdat de keuze voor AWS betekent dat de gegevens worden ondergebracht in de cloud omgeving van een Amerikaanse aanbieder, acht SIDN het van belang om een Data Protection Impact Assessment (DPIA) uit te voeren om de risico's voor de rechten en vrijheden van betrokkenen in kaart te brengen.

De SIDN-omgeving wordt gehost in de EU regio van AWS (Frankfurt en Ierland). Alle klantgegevens blijven hiermee binnen de Europese Unie. Om de applicaties te beheren en te benaderen wordt een Landing Zone ingericht. Een Landing Zone is een multi-account AWS-omgeving van waaruit diverse 'workloads' kunnen worden opgestart en beheerd. Deze workloads zijn in het geval van SIDN de applicaties. Voor het realiseren van de omgeving worden verschillende AWS-diensten afgenomen zoals EC2 (compute), S3 (storage) en Aurora (database engine).

De onderstaande privacyrisico's zijn geïdentificeerd bij het gebruik van AWS. Bij de identificatie van deze risico's gaan wij in beginsel uit van een situatie *zonder* (aanvullende) risicobeperkende maatregelen.

#	Risico	Beschrijving	Kans	Impact	Totaal
1	Verlies van de vertrouwelijkheid van content gegevens door toegang AWS.	AWS heeft toegang tot de klantgegevens in de SIDN-omgeving.	Hoog	Gemiddeld	Hoog
2	Verlies van de vertrouwelijkheid van content gegevens door toegang van (onder andere) de Amerikaanse overheid.	De Amerikaanse overheid kan AWS dwingen om klantgegevens te overhandigen. Ook kunnen andere overheden zich met vorderingen tot AWS richten.	Gemiddeld	Hoog	Hoog
3	Verlies van de vertrouwelijkheid van content gegevens door toegang door (sub)verwerkers.	Ongeautoriseerde derden krijgen toegang tot de klantgegevens in de SIDN-omgeving.	Gemiddeld	Gemiddeld	Gemiddeld
4	Verlies van de vertrouwelijkheid van content gegevens door ongeautoriseerde toegang.	Inbreuken op de beveiliging kunnen leiden tot ongeoorloofde toegang tot SIDN-klantgegevens.	Laag	Hoog	Gemiddeld

5	Doorgifte van gegevens van medewerkers naar de VS.	Gegevens van medewerkers kunnen tijdens het gebruik van de AWS-diensten worden doorgegeven aan AWS in de VS.	Hoog	Laag	Gemiddeld
6	Analyse van het gedrag van medewerkers op basis van loggegevens.	Het gedrag van medewerkers kan met behulp van loggegevens worden geanalyseerd.	Hoog	Laag	Gemiddeld
7	Analyse van het gedrag van gebruikers op basis van loggegevens.	Het gedrag van gebruikers kan met behulp van loggegevens worden geanalyseerd.	Hoog	Gemiddeld	Gemiddeld
8	Gegevens worden actief door SIDN gedeeld met AWS.	SIDN kan actief content gegevens delen met AWS, bijvoorbeeld in het kader van een support verzoek.	Hoog	Gemiddeld	Hoog
9	Gegevens zijn (tijdelijk) onbeschikbaar.	Gegevens kunnen door AWS (on)bewust onbeschikbaar worden gemaakt, of de dienstverlening kan door andere redenen (langdurig) onbeschikbaar zijn.	Zeer Laag	Gemiddeld	Gemiddeld

In haar dienstverlening gaat AWS uit van een shared responsibility model. Dit betekent dat de beveiliging van de AWS-infrastructuur de verantwoordelijkheid is van AWS. De inrichting van de omgeving en daarbinnen genomen beveiligingsmaatregelen zijn de verantwoordelijkheid van de klant (in dit geval SIDN).

Naast de 'standaard' technische en organisatorische maatregelen die AWS neemt voor haar infrastructuur neemt SIDN de volgende (aanvullende) technische en organisatorische maatregelen om de privacyrisico's te minimaliseren.

#	Maatregel	Beschrijving	Mitigeert risico's
1	Encryptie (at rest)	Content wordt versleuteld opgeslagen zodat derden geen toegang kunnen krijgen tot de daadwerkelijke gegevens.	1, 2, 3, 4
2	Encryptie (in transit)	Netwerkverkeer wordt versleuteld zodat het niet afgeluisterd kan worden.	1, 2, 3, 4

3	Beveiligde server infrastructuur	Gegevens worden in een streng beveiligde omgeving gebracht, waardoor zij tijdens het bewerken ontoegankelijk zijn voor derden, inclusief AWS.	1, 2, 3, 4
4	Access & Identity management	Er is alleen toegang voor geautoriseerde medewerkers. Er wordt gebruik gemaakt van een federated identity systeem, waardoor er geen gebruikers accounts (met persoonsgegevens) in AWS aangemaakt hoeven te worden.	4, 5, 6
5	Beperking netwerkverkeer, logging en monitoring	Alleen geautoriseerd netwerkverkeer is toegestaan. Netwerkverkeer en gebruikershandelingen worden gemonitord en gelogd.	4, 5, 6
6	Contractuele afspraken	AWS wordt door een verwerkersovereenkomst gebonden.	6, 7, 8
7	Regels voor het gebruik voor medewerkers SIDN	SIDN medewerkers worden getraind in de zorgvuldige omgang met gegevens.	8
8	Exit strategie	SIDN heeft een exit strategie om bij het uitvallen van AWS snel de dienstverlening buiten AWS voort te zetten.	9

De belangrijkste privacyrisico's hebben betrekking op de mogelijkheid voor AWS om kennis te nemen van persoonsgegevens. AWS zou deze gegevens voor eigen doeleinden kunnen gebruiken, maar ook -al dan niet onder dwang- kunnen doorgeven aan de Amerikaanse overheid. Het risico heeft voornamelijk betrekking op de klantgegevens (content gegevens), maar ook het gebruik van de SIDN-omgeving door klanten en medewerkers van SIDN is potentieel inzichtelijk voor AWS.

SIDN heeft dit risico echter tot een acceptabel niveau teruggebracht door zorg te dragen voor de versleuteling van de gegevens (at rest en in transit). Daarnaast zorgt de beveiligde server infrastructuur van AWS ervoor dat de gegevens tijdens de verwerking niet toegankelijk zijn voor AWS en daarmee ook niet voor derden zoals de Amerikaanse overheid.

Voor de gegevens van medewerkers geldt dat de kans dat medewerkers geïdentificeerd worden laag is, omdat geen van de medewerkers een account heeft in AWS. In plaats daarvan wordt gebruik gemaakt van tijdelijke security credentials. Deze bevatten geen persoonsgegevens en daardoor is het voor AWS zeer waarschijnlijk onmogelijk, of vormt het op zijn minst een onevenredige inspanning, om het gebruik van de AWS-omgeving te relateren aan een individuele natuurlijke persoon. Daarbij moet ook worden aangetekend dat de handelingen in de AWS-omgeving van individuele medewerkers waarschijnlijk niet van dien aard zijn dat zij überhaupt relevant zijn voor AWS.

Tenslotte is sinds 2023 het EU-US Data Privacy Framework van toepassing. Dit is het nieuwe adequaatheidsbesluit van de Europese Commissie voor de Verenigde Staten. Omdat AWS een deelnemer is aan het EU-US DPF moet zij zich committeren aan met de AVG vergelijkbare regels voor de verwerking van persoonsgegevens. Dit in samenhang met de verwerkersovereenkomst maakt het dat de verwerking in de cloud ook omgeven is met juridische waarborgen ter bescherming van de privacy.

Naar het oordeel van Considerati worden met de standaard beveiligingsmaatregelen van AWS, de voorgenomen inrichting van de SIDN-omgeving, de aanvullende risicobeperkende maatregelen en de deelname van AWS aan het EU-US Data Privacy Framework, de privacyrisico's tot een acceptabel niveau teruggebracht.

Inhoudsopgave

1 Inleiding

SIDN wil een aantal applicaties, waaronder haar beoogde domeinnaam registratieplatform Fury, overbrengen naar Amazon Web Services (AWS). SIDN heeft Considerati verzocht een Data Protection Impact Assessment (DPIA) uit te voeren op de migratie van deze applicaties van de huidige IT-omgeving naar AWS.

1.1 Scope

De DPIA heeft betrekking op de bovengenoemde migratie van een aantal SIDN-applicaties naar de AWS Cloud. Meer specifiek gaat het om:

- Fury (beoogd domeinnaam registratieplatform)
- Merkbewaking (merkbewaking)
- DMAP (DNS analyse)
- .nl Control (domeinnaam bescherming)

Naast de migratie van deze applicaties wordt er ook een 'Landing Zone' gebouwd in AWS op basis van AWS best practices. Deze Landing Zone vormt de 'toegangspoort' tot de applicaties. Zo krijgen gebruikers privileges toegewezen via de Landing Zone en wordt het netwerkverkeer gemanaged via de Landing Zone. De Landing Zone vormt een onderdeel van de scope van deze DPIA en zal verder worden toegelicht in hoofdstuk 2.
In deze DPIA analyseert Considerati de privacyrisico's die gepaard gaan met de migratie naar de AWS cloud. De DPIA omvat geen technische analyse van de fysieke en globale AWS-infrastructuur. Daadwerkelijke toegang tot/inzicht in de infrastructuur van AWS is niet mogelijk en daarmee buiten scope van deze DPIA. Om toch inzicht te krijgen in (onafhankelijke) informatie over de wereldwijde AWS-infrastructuur wordt zoveel mogelijk gebruik gemaakt van analyses van derde partijen (audit rapporten, third party memoranda et cetera) en antwoorden op vragen door SIDN en Considerati gesteld aan AWS.

Nota bene: Considerati is zich bewust van het feit dat er momenteel een (politieke) discussie gaande is over de wenselijkheid om Fury in de AWS cloud onder te brengen. Deze DPIA heeft enkel betrekking op de mogelijke risico's voor de bescherming van persoonsgegevens.

1.2 Methodologie

De basis van dit onderzoek is gelegen in de bestudering van door SIDN aangeleverde documentatie, openbaar beschikbare documentatie betreffende de AWS-infrastructuur (AWS documentatie en whitepapers, bestaande DPIA's, contracten, verwerkersovereenkomsten, externe audit rapporten et cetera). Om een goed inzicht te krijgen in de technische en functionele beschrijving van de voorgenomen SIDN-omgeving zijn werksessies georganiseerd met kennishouders binnen SIDN. Tenslotte zijn enkele gerichte vragen gesteld aan AWS.

1.3 Leeswijzer

Deze DPIA rapportage is als volgt opgebouwd.

In hoofdstuk 2 wordt een overzicht gegeven van de wijze waarop SIDN haar omgeving wil inrichten in de AWS cloud.

Hoofdstuk 3 geeft een overzicht van de verschillende applicaties die naar de AWS cloud gemigreerd worden.

In hoofdstuk 4 beschrijven wij de persoonsgegevens die worden verwerkt in de AWS cloud en in hoofdstuk 5 de doelen voor de verwerking van deze gegevens.

Hoofdstuk 6 geeft een overzicht van de relevante actoren en hun respectievelijke rollen op basis van de AVG.

Hoofdstuk 7 geeft een overzicht van de rechtsgrondslagen voor de verwerking van persoonsgegevens door SIDN en in hoofdstuk 8 stellen wij vast of er sprake is van gegevensdoorgifte.

Hoofdstuk 9 en 10 vormen de kern van deze DPIA. In deze hoofdstukken worden respectievelijk de privacyrisico's en risicobeperkende maatregelen besproken. Op basis van deze informatie vormen wij ons een definitief oordeel over de privacy impact van de migratie naar de AWS cloud in hoofdstuk 11.

Hoofdstuk 12 sluit af met een korte samenvatting en conclusie.

2 Overzicht SIDN AWS omgeving

2.1 Inleiding

In dit hoofdstuk beschrijven wij hoe binnen AWS de SIDN-omgeving wordt opgebouwd. Hierbij beschrijven wij ook enkele van de belangrijkste diensten die SIDN afneemt van AWS om deze omgeving te realiseren. SIDN volgt bij de inrichting van haar AWS-omgeving de uitgangspunten van het 'AWS Well Architected Framework'.[1] Dit raamwerk biedt uitgangspunten, ontwerpprincipes, best practices en tools om een veilige, betrouwbare en efficiënte AWS-omgeving in te richten.

2.2 Overzicht SIDN AWS omgeving

Het doel van de migratie naar AWS is om vier applicaties onder te brengen in de AWS cloud, te weten:

- Fury (beoogd domeinnaam registratieplatform)
- Merkbewaking (merkbewaking)
- DMAP (analyse gebruik .nl domeinnamen)
- .nl Control (domeinnaam bescherming)

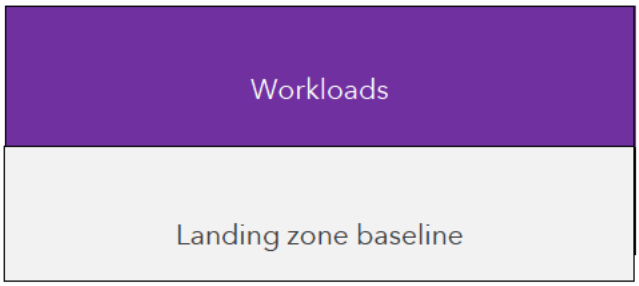
Om deze applicaties te beheren en te benaderen wordt een Landing Zone ingericht. Zowel gebruikers van de applicaties (klanten van SIDN) als medewerkers van SIDN die verantwoordelijk zijn voor de ontwikkeling, het beheer en het gebruik van de applicaties, kunnen de applicaties alleen rechtstreeks benaderen wanneer zij daartoe geautoriseerd zijn via de Landing Zone.

2.2.1 Landing Zone

Alvorens we de opbouw van de SIDN-omgeving kunnen bespreken is het zinvol om het concept van een AWS-landingszone te bespreken. Een AWS-landingszone is een veilige en schaalbare multi-account AWS-omgeving van waaruit workloads kunnen worden opgestart.

Het ontwerp van een AWS-landingszone bestaat uit de configuratie van twee conceptuele lagen: de basislaag en de workloads of applicaties. De basislaag bevat een minimale set diensten en configuraties om een landingszone te bedienen, en deze functionaliteit kan verder worden uitgebreid of aangepast. Workloads of applicaties zoals hierboven benoemd draaien bovenop deze basislagen.

[1] https://aws.amazon.com/architecture/well-architected/?wa-lens-whitepapers.sort-by=item.additionalFields.sortDate&wa-lens-whitepapers.sort-order=desc&wa-guidance-whitepapers.sort-by=item.additionalFields.sortDate&wa-guidance-whitepapers.sort-order=desc



Figuur 1: Opbouw landing zones

[redacted]

SIDN heeft in haar landing zone (verder: SIDN landing zone of Landing Zone) een scheiding gemaakt tussen Landing Zone- en Workload accounts. [redacted]

De SIDN landing zone is het centrale element van de voorgenomen SIDN omgeving en functioneert als het knooppunt van SIDN binnen de AWS cloud. [redacted] Medewerkers van SIDN krijgen via de Landing Zone hun toegangsrechten toegewezen voor de verschillende applicaties. Verder bepaalt de Landing Zone niet alleen de specifieke veiligheidsmaatregelen (audit logging,

[2] Voor meer informatie over de inrichting van het access en identity management (IAM) zie hoofdstuk 10 (risico beperkende maatregelen).

encryptie, threat detection et cetera), maar ook het management en het gebruik van de Landing Zone.

2.2.2 Applicaties

[redacted] Om de applicaties te benaderen en voor netwerkverkeer tussen de applicaties moet gebruik worden gemaakt van de SIDN Landing Zone.

2.3 AWS-infrastructuur en diensten

In deze paragraaf beschrijven wij op hoofdlijnen hoe AWS haar dienstverlening opbouwt en de diensten die worden afgenomen van AWS om de SIDN-omgeving te realiseren. Het gaat daarbij primair om compute diensten, opslag van gegevens en netwerkconnectiviteit.

2.3.1 Regio's en Availability Zones

De AWS Cloud infrastructuur is opgebouwd uit Regio's en Availability Zones (AZ's). Een Regio is een fysieke locatie in de wereld waar meerdere Availability Zones worden ingezet. Availability Zones bestaan uit een of meer discrete datacenters, elk met redundante stroomvoorziening, netwerken en connectiviteit, gehuisvest in een of meer afzonderlijke faciliteiten.[3] Availability Zones zijn met elkaar verbonden via snelle, private glasvezelnetwerken, waardoor AWS-klanten eenvoudig applicaties kunnen ontwerpen die automatisch en zonder onderbreking fail-over uitvoeren tussen Availability Zones.

De door SIDN gekozen regio's voor de Landing Zone zijn *EU-central-1* (Frankfurt) en *EU-west-1* (Ireland). Frankfurt is de 'home' regio. Ireland is de disaster recovery (DR) regio.

Vanuit een gegevensbeschermingsperspectief betekent dit dat de gegevens die opgeslagen en verwerkt worden niét buiten de Europese Unie komen.

[redacted]

[redacted]

[redacted]

2.3.4 Connectiviteit

AWS-landingszones bieden een standaard netwerkconfiguratie met Virtual Private Clouds (VPC's), subnets, route-tabellen en netwerkconnectiviteit tussen accounts. Dit zorgt voor veilig en efficiënt dataverkeer en netwerkbeheer, met de mogelijkheid om VPN's en Direct Connect te implementeren voor verbindingen met on-premise netwerken of andere cloud providers.

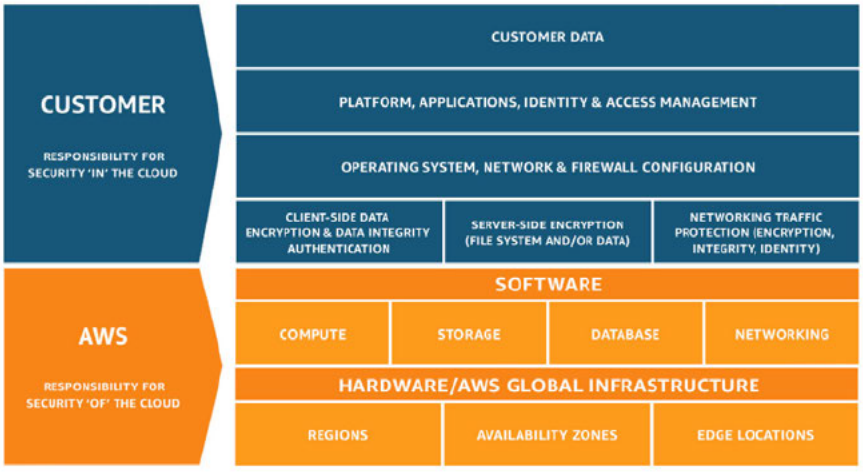
[redacted]

[redacted]

[redacted]

2.4 Beveiliging

AWS hanteert een 'shared responsibility model' waarbij de beveiliging van de AWS-omgeving de verantwoordelijkheid is van AWS en de beveiliging van de omgeving die de klant zelf opbouwt en inricht de verantwoordelijkheid is van de klant.[11]



Met betrekking tot het deel van de inrichting waar AWS voor verantwoordelijk is, betekent dit dat SIDN géén invloed heeft op de door AWS genomen maatregelen.

[11] https://aws.amazon.com/compliance/shared-responsibility-model/

Om aan te tonen dat de door haar genomen maatregelen toereikend zijn heeft AWS tal van audits door onafhankelijke auditoren en cybersecurity bedrijven laten doen. AWS ondersteunt en is compliant met 143 (beveiligings)standaarden waaronder PCI-DSS, HIPAA/HITECH, FedRAMP, FIPS 140-2 en NIST 800-171.[12]

2.4.1 Inrichting beveiliging SIDN

SIDN heeft gekozen voor een security model waarbij de applicaties van elkaar zijn geïsoleerd.

[redacted]

De vanuit een privacy perspectief relevante beveiligingsmaatregelen worden besproken in hoofdstuk 10 (risico beperkende maatregelen).

[12] Zie: https://aws.amazon.com/compliance/ . AWS geeft geen direct inzicht in haar infrastructuur. Als zodanig zijn de conclusies met betrekking tot de inrichting van de infrastructuur primair gebaseerd op deze onafhankelijke auditrapporten.

[redacted]

3 Applicaties

Hieronder beschrijven wij kort de applicaties Fury, Merkbewaking, DMAP en .nl Control.

3.1 Fury domeinnaam registratieplatform

Fury, ontwikkeld door de Canadese ccTLD registry CIRA en mede-eigendom van SIDN, is een geavanceerd domeinnaam registratieplatform. Een domeinnaam registratieplatform is een systeem waarmee voor een of meerdere domeinnaamextensies de administratie beheerd wordt van alle domeinnamen binnen die extensie. Via het systeem kunnen nieuwe domeinnamen geregistreerd worden waarbij de bijbehorende registratiegegevens, zoals de gegevens van de houder van de domeinnaam, in het systeem worden vastgelegd. Via het systeem kunnen de domeinnaam en de bijbehorende registratiegegevens vervolgens ook beheerd worden en kunnen wijzigingen worden doorgevoerd. Onderdeel van de registratiegegevens zijn de nameservergegevens. Dit zijn de bereikbaarheidsgegevens van servers op het internet. Veelal in de vorm van een adres als ns1.sidn.nl maar ook wel als een IP-adres. Het systeem vormt daarmee de basis voor de zonefile die SIDN ieder half uur genereert. De zonefile bestaat uit de lijst met alle domeinnamen in het systeem met de daaraan gekoppeld de voor die domeinnaam opgegeven nameservergegevens.

Fury is tevens de basis voor de zoekfunctie (Whois) waarmee van een domeinnaam (een deel van) de registratiegegevens opgevraagd kan worden. Daarbij wordt gebruik gemaakt van het RDAP-protocol.

SIDN en CIRA zijn samen eigenaar van Fury. Ze werken samen aan de doorontwikkeling van Fury en zijn met het oog hierop een strategisch partnerschap voor de langere termijn aangegaan.

Het is van belang om te benadrukken dat Fury slechts de registratie van domeinnamen verzorgt (bijvoorbeeld wie is de houder van een domeinnaam) en niét het daadwerkelijke DNS is. Wel is Fury van kritiek belang voor het goed functioneren van het DNS omdat mutaties van domeinnamen (registratie nieuwe domeinnamen, veranderingen in houderschap, nieuwe technische contacten et cetera) niet mogelijk zijn zonder Fury.

3.2 Merkbewaking

Merkbewaking is een merkbewakingsplatform dat organisaties in staat stelt om hun merken te beschermen. Het is een online monitoringsservice die waarschuwt bij de registratie van een domeinnaam die lijkt op een bestaand merk. Merkbewaking verkleint de kans dat een merk wordt misbruikt voor phishing, mailfraude, identiteitsfraude of CEO-fraude.

3.3 DMAP

De DNS Ecosystem Mapper (DMAP) is een meetinstrument dat door SIDN is ontwikkeld om het DNS-ecosysteem te meten. DMAP genereert meer dan 100 informatiepunten betreffende de kwaliteit, veiligheid, validiteit en het gebruik van een domeinnaam. Dit doet DMAP op de volgende wijze:

- het automatisch crawlen van verschillende toepassingsprotocollen voor domeinnamen (DNS, HTTP, TLS/SSL, SMTP, zowel over IPv4 als IPv6) en;

- het opslaan van de resultaten in een relationele database. Op deze manier kunnen onderzoekers snel hypothesetests uitvoeren met behulp van structured query language (SQL).[14]

DMAP maakt gebruik van verschillende classificatoren, waaronder diegene die de taal van een webpagina herkennen en bepalen welk content management systeem (CMS) wordt gebruikt. Als resultaat genereert DMAP een reeks aan verschillende kenmerken voor een specifieke domeinnaam. SIDN maakt gebruik van DMAP om periodieke scans van de volledige .nl-zone uit te voeren ter ondersteuning van projecten die gericht zijn op het verbeteren van zowel de veiligheid als de stabiliteit van het DNS.

3.4 .nl Control

Het doel van .nl Control is om een domeinnaamhouder extra controle te geven over het wijzigen van de registratiegegevens van een domeinnaam. Als een domeinnaamhouder gebruik maakt van .nl Control wordt een specifiek aangewezen vertegenwoordiger van de domeinnaamhouder in alle gevallen door SIDN gebeld voordat er een wijziging van de registratiegegevens wordt doorgevoerd en wordt er bij deze persoon geverifieerd of de domeinnaamhouder ook daadwerkelijk de wijziging door wil laten voeren. Indien telefonisch geverifieerd, moet de gebruiker vervolgens nog een schriftelijk akkoord geven. Op deze manier kan worden voorkomen dat iemand ongewild een domeinnaam omleidt naar een ander adres. Dit verbetert de veiligheid van domeinnamen en voorkomt onder andere hacking en phishing. De bescherming geldt voor de volgende veranderingen: veranderen van domeinnaamgegevens, domeinnaam verhuizen, domeinnaam opheffen, en het wijzigen van de glue records van de in-zone nameserver en/of DNSSEC-sleutelmateriaal.

[14] Wullink, M, en anderen. *'Dmap: Automating Domain Name Ecosystem Measurements and Applications'*

4 Gegevensverwerkingen

4.1 Categorisering gegevens verwerkt door AWS

AWS verwerkt verschillende type persoonsgegevens. In haar privacy statement maakt AWS het volgende onderscheid:

- *Information You Give Us: We collect any information you provide in relation to AWS Offerings.*
- *Automatic Information: We automatically collect certain types of information when you interact with AWS Offerings.*
- *Information from Other Sources: We might collect information about you from other sources, including service providers, partners, and publicly available sources.*[15]

In haar Data Privacy FAQ specificeert AWS de gegevens verder.[16] Op basis daarvan kunnen we het volgende voor deze DPIA relevante onderscheid maken:

1. Content of customer data;
2. Contact en account data (authorised user account data);
3. Support data;
4. Meta data.

4.1.1 Content of customer data

Content of customer data zijn persoonlijke en niet-persoonlijke gegevens die door klanten worden geüpload naar een opslag en/of database in de AWS cloud. Dergelijke inhoud kan elk type gegeven zijn, zoals tekst, audio, video, gegevens, afbeeldingen, of software (inclusief machineafbeeldingen) die een klant of eindgebruiker naar AWS overdraagt voor verwerking, opslag of hosting door AWS-services in verband met het account van een desbetreffende klant.

4.1.2 Contact- en account data (authorised user account data)

Contact- en accountdata bevat informatie die verstrekt wordt tijdens het aanmaken of beheren van een klantaccount. Hoewel accountinformatie persoonsgegevens kan omvatten (bijvoorbeeld een email adres met daarin voornaam en achternaam), is er in de opzet van de SIDN-omgeving voor gekozen om voor alle accounts functionele namen te hanteren (in het formaat <rol>@sidn.nl). Alleen voor het account waarmee de AWS-omgeving is aangemaakt en voor de billing informatie geldt dit niet. Maar voor deze twee uitzonderingen gaat het in

[15] https://aws.amazon.com/privacy/
[16] https://aws.amazon.com/compliance/data-privacy-faq/

beginsel om gegevens over SIDN (bijvoorbeeld het factuuradres), niet over natuurlijke personen.

4.1.3 Support data

Support data wordt gegenereerd wanneer een klant technische ondersteuning aanvraagt zoals bij een support verzoek. Een support verzoek kan bijlagen bevatten waarin persoonsgegevens staan, zoals een schermafbeelding van de inhoud van een database.

AWS verzamelt ook metagegevens over de support verzoeken die door zijn klanten zijn ingediend. Deze gegevens zijn altijd gekoppeld aan een identificeerbare AWS-klant (beheerdersaccount).

4.1.4 Meta data

Meta data is data die informatie verschaft over andere data. Met andere woorden, meta data is data over data. Voor AWS omvat meta data logbestanden waarin onder andere operationele logs en beveiligingslogs kunnen staan. Daarnaast wordt er ook configuratie-informatie (informatie over de instellingen en configuratie van de diensten die door de klant worden gebruikt) verzameld. Ook worden er prestatiegegevens (informatie over de prestatie van de gebruikte diensten) verzameld. Als laatste verzamelt AWS meta data over bezoeken aan zijn openbare en beperkt toegankelijke websites.[17]

4.2 Onderscheid verwerking van persoonsgegevens in deze DPIA

Voor de context van deze DPIA is het volgende onderscheid tussen gegevens met name relevant:

1) Gegevens die de applicaties van SIDN gebruiken (content gegevens);
2) Gegevens die worden vastgelegd van gebruikers door AWS (klanten van SIDN die interacteren met de applicaties)
3) Gegevens die worden vastgelegd van medewerkers van SIDN door AWS.

Ad 1) Content gegevens of klantgegevens

De eerste categorie gegevens komt overeen met de hierboven omschreven 'content of customer data'. Het betreft de gegevens die in de applicaties opgeslagen zijn en die worden verwerkt bij het gebruik van de applicaties. Het gaat dan met name om de klantgegevens in de databases. Deze gegevens zijn met name van belang voor deze DPIA omdat deze gegevens potentieel het meest gevoelig zijn.

Ad 2) Gebruiksgegevens (klanten)

[17] Deze laatste categorie is buiten scope voor deze DPIA.

De tweede categorie betreft het door AWS vastleggen van gegevens van klanten die contact maken met de applicaties van SIDN (denk aan de registrars voor Fury en de klanten van Merkbewaking en .nl Control). Het gaat dan primair om het loggen van bevragingen van klanten op netwerkniveau (gebruikt protocol, poort et cetera).[18]

Ad 3) Gebruiksgegevens (medewerkers)

De derde categorie betreft gegevens die van / via medewerkers van SIDN worden verkregen door AWS. Het gaat dan allereerst om het emailadres en het bedrijfs-/factuuradres van medewerkers (contact en account data), ten tweede om gegevens die worden vastgelegd over het gebruik van de AWS diensten door medewerkers (meta data).[19] Ten derde gaat het om het vastleggen van gegevens uit interacties tussen AWS en SIDN medewerkers (support data). Denk bijvoorbeeld aan supportgesprekken en support tickets, emails en chatberichten.

4.3 Overzicht verwerkte persoonsgegevens

In deze paragraaf geven wij aan welke persoonsgegevens binnen de verschillende hierboven genoemde categorieën vallen en verwerkt (kunnen) worden.

4.3.1 Content gegevens (klantgegevens)

Met betrekking tot de categorie content data gaat het om de gegevens die worden verwerkt binnen de applicaties van SIDN. Onderstaand geven wij een overzicht van de persoonsgegevens die binnen de verschillende applicaties worden verwerkt.

Nota bene: in dit overzicht gaat het enkel om de gegevens van klanten. Medewerkers van SIDN kunnen ook accounts hebben in deze systemen. Deze gegevens zijn niet meegenomen in dit overzicht. Vanuit een privacyperspectief gelden dezelfde overwegingen als voor klantgegevens.

4.3.1.1 Fury

Naam gegeven	Beschrijving	Type persoonsgegeven	Toelichting
NAW-gegevens registrant (domeinnaamhouder)	Voornaam, achternaam registrant. Adres registrant (straat, postcode, plaats, land) en organisatie registrant waar van toepassing.	Gewoon	Naam van de natuurlijke persoon of organisatie die houder is van de domeinnaam.
Contactgegevens registrant	Email en telefoonnummer van de registrant,	Gewoon	

[18] Domeinnaamhouders interacteren met Brandguard en .nl Control. Registrars kunnen interacteren met Fury. De gegevens die verwerkt worden betreffen dan in beginsel gegevens over de registrar (het bedrijf) en niet gegevens over natuurlijke personen.
[19] In de voorgenomen opzet van SIDN waarbij gewerkt wordt met rollen en een federated identity systeem (zie risicobeperkende maatregelen) is in de praktijk de kans dat AWS daadwerkelijk gebruiksgegevens kan koppelen aan medewerkers zeer klein.

NAW-gegevens admin contact registrant	Voornaam, achternaam admin contact registrant. Adres admin contact (straat, postcode, plaats) en organisatie admin contact waar van toepassing.	Gewoon	Naam van de contactpersoon / organisatie waarmee contact opgenomen kan worden voor administratieve zaken aangaande het domein.
Contactgegevens admin contact registrant	Email en telefoonnummer van de admin.	Gewoon	
NAW-gegevens tech contact registrant	Voornaam, achternaam tech contact registrant. Adres tech contact (straat, postcode, plaats) en organisatie tech contact waar van toepassing.	Gewoon	Naam van de contactpersoon / organisatie waarmee contact opgenomen kan worden voor technische zaken aangaande het domein.
Contactgegevens tech contact registrant	Email en telefoonnummer van het tech contact	Gewoon	
KvK-nummer	Registratienummer van de registrant indien opgegeven.	Gewoon	Gegeven ter identificatie van de houder. Persoonsgegeven indien het gaat om bijvoorbeeld eenmanszaken.
Domeinnaam	Een domeinnaam is een unieke naam op het internet. Een domeinnaam heeft als adres het IP-adres. Aangezien het IP-adres lastig te onthouden is, wordt een domeinnaam gebruikt. Het domeinnaamsysteem (DNS) vertaalt het IP-adres naar een domeinnaam.	Gewoon	Domeinnamen kunnen als persoonsgegeven worden aangemerkt wanneer zij wat zeggen over de houder en deze houder een natuurlijke persoon is. In een beperkt aantal gevallen kan ook de domeinnaam zelf persoonsgegevens bevatten.
NS-records	De nameservergegevens (namenservers of IP-adressen) die aan een domeinnaam gekoppeld worden waardoor de domeinnaam op het internet naar die gegevens verwijst.	Gewoon	NS-records kunnen als persoonsgegevens worden aangemerkt wanneer zij wat zeggen over de houder en deze houder een natuurlijke persoon is.
NAW en contactgegevens registrar	Contactgegevens van de registrar die door de registrant is gebruikt voor het aanvragen van de domeinnaam.	Gewoon	De registrar is de organisatie die namens de registrant domeinnaam aanvraagt en na registratie beheert.

Toelichting:

De gegevens die in Fury worden verwerkt hebben betrekking op de houder van een domeinnaam (de registrant). Deze houders kunnen zowel rechtspersonen als natuurlijke personen zijn. Naast de houders van domeinnamen kunnen ook de aangewezen contacten

(admin en tech) natuurlijke personen zijn. Vanuit een privacy perspectief is het met name relevant dat via deze gegevens een natuurlijke persoon geassocieerd kan worden met een domeinnaam (in de praktijk vaak een website). Dit is doorgaans niet bijzonder privacygevoelig, maar afhankelijk van de context (denk bijvoorbeeld aan politieke of levensbeschouwelijke websites) kunnen deze gegevens wel gevoelig zijn. In Fury worden van domeinnamen, waaronder domeinnamen die geregistreerd zijn door natuurlijke personen, ook andere zaken vastgelegd, zoals welke wijzigingen hebben plaatsgevonden. Deze gegevens blijven buiten beschouwing in dit overzicht omdat deze gegevens geen relevante privacy impact hebben.

4.3.1.2 Merkbewaking

Naam gegeven	Beschrijving	Type persoonsgegeven	Toelichting
NAW en contactgegevens merkhouder	Naam, adres, woonplaats. Email en telefoonnummer.	Gewoon	
Geregistreerde merken	Geregistreerde merken	Gewoon	De merken die door de merkhouder aangemeld zijn bij SIDN voor Merkbewaking in die gevallen dat het merk eigendom is van een natuurlijke persoon.
IP-adres	Het nummer waarmee een computer, aangesloten op het internet of netwerk, zichtbaar is voor alle andere computers op het internet.	Gewoon	IP-adres van de merkhouder die contact maakt met de Merkbewaking applicatie.

Toelichting

Merkhouders kunnen zich aanmelden voor Merkbewaking. Hiertoe worden hun NAW en contactgegevens vastgelegd alsmede de merken die in aanmerking komen voor merkbewaking.

Wanneer er sprake is van een potentiële merkinbreuk dan kunnen de gegevens uit Fury worden gebruikt voor het identificeren van de inbreukmakende partij.

Tenslotte is voor Merkbewaking vanuit een privacy perspectief nog relevant dat de klant (de gebruiker van Merkbewaking) interacteert met de applicatie. Deze interacties kunnen in beginsel worden vastgelegd door AWS.

4.3.1.3 DMAP

Naam gegeven	Beschrijving	Type persoonsgegeven	Toelichting
KvK-nummer	Registratienummer	Gewoon	Per domeinnaam kan de landingspagina worden gecrawled (de content van de pagina zoals vastgelegd in de HTML code). Op deze pagina kunnen afhankelijk van het type gegeven persoonsgegevens staan. KvK-nummer wordt gebruikt om te bepalen of een website voor zakelijk gebruik is. Is een persoonsgegeven indien het gaat om bijvoorbeeld eenmanszaken.
IP-adressen	Het nummer waarmee een computer, aangesloten op het internet of netwerk, zichtbaar is voor alle andere computers op het internet.	Gewoon	De IP-adressen zijn van servers waarop bepaalde diensten draaien, zoals een website of mailserver. Ook mogelijk dat een klein aantal IP-adressen aan DSL/kabel (thuis)gebruikers toebehoren.
Telefoonnummer		Gewoon	Per domeinnaam kan de landingspagina worden gecrawled (de content van de pagina zoals vastgelegd in de HTML code). Op deze pagina kunnen afhankelijk van het type gegeven persoonsgegevens staan. Een telefoonnummer kan worden gebruikt om te bepalen of een website voor zakelijk gebruik is.
Bankrekeningnummer		Gewoon	Per domeinnaam kan de landingspagina worden gecrawled (de content van de pagina zoals vastgelegd in de HTML code). Op deze pagina kunnen afhankelijk van het type gegeven persoonsgegevens staan. De aanwezigheid van een bankrekeningnummer kan een indicatie zijn dat het om een zakelijke website gaat.
Screenshot door DMAP-crawler	Bevat mogelijk persoonsgegevens	Gewoon / bijzonder / strafrechtelijk	De crawler kan een screenshot maken van de landingspagina, afhankelijk van de inhoud kunnen hierop verschillende soorten gegevens staan, waaronder mogelijk bijzondere persoonsgegevens.

Toelichting:

Met behulp van DMAP worden technische kenmerken van domeinen en de daarbij behorende websites gescand. Het gaat dan bijvoorbeeld om de lengte van de domeinnaam, het type CMS dat wordt gebruikt voor een website, de geldigheid van het TLS certificaat et cetera.

Ook kan de HTML-content van een site worden gecrawld voor specifieke karakteristieken zoals de aanwezigheid van een bankrekeningnummer of een KvK nummer. In de opsomming hierboven zijn de karakteristieken aangegeven die het meest specifiek als persoonsgegeven aangemerkt kunnen worden.

De DMAP-crawler heeft ook de mogelijkheid om een screenshot van een landingspagina te maken. In de screenshot kunnen mogelijk persoonsgegevens zijn opgenomen. Deze functionaliteit is standaard uitgeschakeld, maar kan voor specifieke onderzoeken en toepassingen worden ingeschakeld. Wanneer deze functionaliteit is ingeschakeld kunnen dus persoonsgegevens worden verwerkt indien die op de betreffende landingspagina staan. Het is niet op voorhand duidelijk welke persoonsgegevens dit zijn.

In de bovenstaande tabel zijn de meeste relevante gegevens genoemd die potentieel een persoonsgegeven zijn. Voor een uitgebreider overzicht verwijzen naar de website van SIDN.[20]

4.3.1.4 .nl Control

Naam gegeven	Beschrijving	Type persoonsgegeven	Toelichting
NAW-gegevens gebruiker .nl Control	. Naam, adres, woonplaats. Email en telefoonnummer.	Gewoon	
Naam en contactgegevens contactpersoon gebruiker .nl Control	Voornaam, achternaam, telefoonnummer en emailadres van de contactpersoon van de klant	Gewoon	
Handtekening	Gegeven ter identificatie	Gewoon	Om te verifiëren dat de persoon inderdaad geautoriseerd is om wijzigingen door te voeren.

Toelichting:

Met betrekking tot .nl Control is het met name relevant dat de naam, handtekening en contactgegevens van de autoriserende klant worden vastgelegd. Met behulp van deze gegevens kan een natuurlijke persoon worden geassocieerd met het betreffende domein. Dit kan in bepaalde gevallen privacygevoelig zijn (zie toelichting bij Fury).

[20] https://dmap.sidnlabs.nl/datamodel

4.3.1.5 Landing Zone

De Landing Zone verwerkt niet zoals bovenstaande applicaties persoonsgegevens van klanten. De Landing Zone is wel geassocieerd met diverse accounts zoals die voor security of betaling. Deze accounts kunnen contactgegevens van natuurlijke personen bevatten. De persoonsgegevens van ingelogde medewerkers zijn voor SIDN pseudoniem. AWS kan deze gegevens niet relateren aan de achterliggende medewerkers. Als zodanig nemen wij deze gegevens niet mee als persoonsgegevens in dit hoofdstuk omdat zij voor AWS *de facto* anoniem zijn. Voor meer informatie zie het kopje Identity en Access management in hoofdstuk 10 (risico beperkende maatregelen).

Naam gegeven	Beschrijving	Type persoonsgegeven	Toelichting
Contactgegevens	Gebruikersnaam. Mogelijk contactgegevens van de contactpersoon bij SIDN voor bijvoorbeeld betaling.	Gewoon	De aangemaakte AWS-accounts kunnen persoonsgegevens bevatten.

4.3.2 Gebruiksgegevens (klanten)

De tweede categorie betreft het door AWS vastleggen van gegevens van klanten die contact maken met de applicaties van SIDN (denk aan de registrars voor Fury en de klanten van Merkbewaking en .nl Control).

Naam gegeven	Beschrijving	Type persoonsgegeven	Toelichting
IP-adres	Het nummer waarmee een computer, aangesloten op het internet of netwerk, zichtbaar is voor alle andere computers op het internet.	Gewoon	Wordt vastgelegd wanneer een gebruiker een applicatie bevraagt.
Meta data	Gegevens betreffende het netwerkverkeer (verkeersgegevens).	Gewoon	Meta data (verkeersgegevens) omvat gegevens betreffende de gemaakte netwerkconnectie (gebruikt protocol, poort, duur van de connectie et cetera). Deze gegevens bevatten geen informatie over de inhoud van het verkeer.

Toelichting:

Het gaat hier primair om het loggen van gebruikersverzoeken op netwerkniveau. Het is mogelijk dat hierbij het IP-adres wordt vastgelegd op het moment dat een klant een applicatie bevraagt. Verder kunnen meta data (verkeersgegevens) worden verzameld over de gemaakte netwerkconnectie. Het kan dan gaan om het gebruikte protocol, de bevraagde poort, de duur van de connectie et cetera. Deze gegevens bevatten geen info over de inhoud van het verkeer. [redacted] AWS kan in beginsel ditzelfde doen voor haar eigen doeleinden (zie hoofdstuk 9 risico's).

4.3.3 Gebruiksgegevens (gebruikers zijnde medewerkers van SIDN die toegang hebben tot AWS-resources)

AWS verzamelt gegevens van gebruikers van haar diensten, onder andere ten behoeve van ondersteuning van gebruikers, diagnostiek en beveiliging. Op basis van het privacy statement van AWS verwerkt AWS tenminste de volgende gegevens wanneer de AWS-diensten worden gebruikt door medewerkers van SIDN.[21]

Naam gegeven	Beschrijving	Type persoonsgegeven	Toelichting
NAW gegevens	Gegevens zoals naam, adres, en woonplaats.	Gewoon	
Contactgegevens	Gegevens zoals het emailadres.	Gewoon	
Locatiegegevens	Gegevens over de locatie.	Gewoon	
Inloggegevens	Gebruikersnaam	Gewoon	
Correspondentie met AWS	Inhoud telefoongesprekken, support tickets, chats et cetera.	Gewoon	
Netwerkverkeer	IP-adres, meta data.	Gewoon	
Interacties met de AWS-omgeving	API-calls	Gewoon	

Toelichting:

AWS kan verschillende gegevens van gebruikers vastleggen. Zoals hierboven uiteengezet en nader toegelicht in hoofdstuk 11 (risicobeperkende maatregelen) zorgen de maatregelen van SIDN ervoor dat in de praktijk er maar een kleine kans is dat AWS-interacties met de AWS omgeving kan koppelen aan een natuurlijke persoon. Voor de overige gegevens (met

[21] Https://aws.amazon.com/privacy/

uitzondering van het netwerkverkeer) geldt dat SIDN-medewerkers deze actief moeten verstrekken aan AWS, bijvoorbeeld in de context van een support verzoek.

5 Doeleinden voor de verwerkingen

Hieronder worden de doeleinden voor de verwerkingen van SIDN per applicatie uiteengezet. Omdat er in beginsel geen persoonsgegevens van klanten of medewerkers op de Landing Zone worden verwerkt, wordt de Landing Zone in dit overzicht niet meegenomen.

5.1 Fury

Doel	Uitleg
Domeinnaamregistratie	Het faciliteren van de registratie van domeinnamen voor klanten via het platform.
Beheer van domeinnamen	Het beheren van bestaande domeinregistraties, inclusief het bijwerken van contactinformatie, het overdragen van domeinen, en het verwerken van verlengingen.
Verlening van klantondersteuning	Het bieden van ondersteuning aan klanten en registrars bij vragen of problemen met betrekking tot domeinregistraties.

5.2 Merkbewaking

Doel	Uitleg
Merkbescherming en fraude- en phisingpreventie.	Het detecteren en voorkomen van inbreuken op merken zoals het registeren van domeinnaamregistraties die lijken op een geregistreerd merk.
Risicobeoordeling en -mitigatie.	Het analyseren van risico's die verbonden zijn aan bepaalde domeinregistraties om organisaties te helpen bij het nemen van voorzorgsmaatregelen.

5.3 DMAP

Doel	Uitleg
Het meten van verschillende aspecten van het DNS ecosysteem om zo de veiligheid en werking van het Nederlandse DNS te verbeteren.	De DNS Ecosystem Mapper (DMAP) is een meetinstrument dat is ontworpen om het DNS-ecosysteem te meten.

5.4 .nl Control

Doel	Uitleg
Beveiligingsmonitoring	Het bewaken van domeinen op mogelijke veiligheidsrisico's, zoals DNSSEC-status, certificaatproblemen, of andere beveiligingskwesties.
Domeinbeheer	Het beheren van de technische en administratieve aspecten van .nl-domeinen, zoals het monitoren van statusveranderingen.
Ondersteuning van registrars	Het bieden van tools en informatie aan registrars om klanten beter te bedienen en domeinen effectief te beheren.

6 Actoren

6.1 Betrokken partijen

Hieronder wordt uiteengezet wie de verwerkingsverantwoordelijken en verwerkers zijn binnen de hierboven genoemde applicaties van SIDN. De betrokken partijen zijn SIDN, AWS en eventuele subverwerkers.

6.2 Verwerkingsverantwoordelijken en verwerkers

Een verwerkingsverantwoordelijke is een natuurlijke of rechtspersoon, een overheidsinstantie, dienst of ander orgaan die, alleen of samen met anderen, het doel en de middelen voor de verwerking van persoonsgegevens vaststelt (artikel 4 lid 7 AVG). Een verwerker is een natuurlijke of rechtspersoon, een overheidsinstantie, dienst of ander lichaam die gegevens verwerkt namens de verwerkingsverantwoordelijke (artikel 4 lid 8 AVG).

De verwerkingsverantwoordelijke is dus de entiteit die bepaalt hoe en met welk doel persoonsgegevens worden verwerkt. In dit geval is SIDN de verwerkingsverantwoordelijke voor de applicaties omdat SIDN beslist welke gegevens worden verwerkt, voor welk doel, en op welke manier. SIDN is verantwoordelijk voor de naleving van de Algemene verordening gegevensbescherming (AVG) en moet zorgen dat de verwerking rechtmatig en transparant gebeurt.

De verwerker is de entiteit die persoonsgegevens verwerkt namens de verwerkingsverantwoordelijke. In dit geval treedt AWS op als verwerker voor de applicaties omdat het de infrastructuur en diensten levert waarop SIDN zijn gegevens opslaat en verwerkt. AWS heeft geen eigen zeggenschap over de doeleinden van en de manier waarop gegevens worden verwerkt.[22]

Daarnaast maakt AWS voor haar werkzaamheden gebruik van derde partijen die in dit geval vallen onder de noemer subverwerker. AWS schakelt subverwerkers in in overeenstemming met het AWS Data Processing Addendum om namens de klant (in dit geval SIDN) verwerkingsactiviteiten uit te voeren.[23] In theorie kunnen deze subverwerkers, voor de uitvoering van hun werkzaamheden, toegang krijgen tot klantgegevens van SIDN.

Volgens de website AWS maakt AWS gebruik van drie soorten subverwerkers:

1. AWS-entiteiten die de infrastructuur leveren waarop de AWS-diensten draaien;
2. AWS-entiteiten die specifieke AWS-diensten ondersteunen waarvoor het nodig kan zijn dat deze entiteiten klantgegevens verwerken; en
3. derden waarmee AWS een contract heeft afgesloten om verwerkingsactiviteiten te verrichten voor specifieke AWS-diensten.[24]

[22] Let op: AWS is wel verwerkingsverantwoordelijke voor de doeleinden van AWS. Denk bijvoorbeeld aan de helpdesk van AWS.
[23] AWS, 'AWS Sub-processors,' https://aws.amazon.com/compliance/sub-processors/
[24] Ibid.

Een volledig overzicht van de verschillende subverwerkers is te vinden op de website van AWS.[25] SIDN wordt geïnformeerd over wijzigingen in de subverwerkers en kan schriftelijk bezwaar maken tegen nieuwe subverwerkers. Zoals dit gebruikelijk is voor grote cloud aanbieders, kan het niet accepteren van nieuwe subverwerkers consequenties hebben voor het aanbieden van de dienstverlening.

AWS heeft als cloud provider zelf ook haar eigen verwerkingsdoelen zoals beveiliging en diagnostiek. Voor deze doelen is AWS de verwerkingsverantwoordelijke.

[25] Ibid.

7 Legitimiteit van de verwerkingen

In dit hoofdstuk wordt de rechtmatigheid van de gegevensverwerkingen beoordeeld. Dit hoofdstuk bevat een bespreking van de rechtsgrondslagen en een korte beoordeling van de noodzaak en evenredigheid van de verwerkingen. Omdat het hier niet gaat om nieuwe verwerkingen en de rechtmatigheid van deze gegevensverwerkingen reeds door SIDN in een eerder stadium is beoordeeld, is de rechtmatigheid marginaal getoetst.

7.1 Rechtsgrondslagen

Persoonsgegevens dienen te worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is. Als uitwerking van dit beginsel is geregeld dat een gegevensverwerking enkel rechtmatig is indien deze gebaseerd kan worden op een rechtsgrond uit artikel 6 AVG. Daarnaast stelt de AVG ten aanzien van de verwerking van bijzondere categorieën persoonsgegevens, strafrechtelijke persoonsgegevens en het nationaal identificatienummer aanvullende eisen.

Voor de verwerking van persoonsgegevens heeft SIDN de volgende rechtsgrondslagen:

Applicatie	**Rechtsgrondslag(en)**
Fury	• Noodzakelijk voor de uitvoering van de overeenkomst *(artikel 6 lid 1 sub b AVG)* • Gerechtvaardigd belang *(artikel 6 lid 1 sub f AVG)*.
DMAP	• Gerechtvaardigd belang *(Artikel 6 lid 1 sub f AVG)*.
Merkbewaking	• Noodzakelijk voor de uitvoering van de overeenkomst *(artikel 6 lid 1 sub b AVG)*. • Gerechtvaardigd belang *(artikel 6 lid 1 sub f AVG)*.
NL-control	• Noodzakelijk voor de uitvoering van de overeenkomst *(artikel 6 lid 1 sub b AVG)*.

7.1.1 Fury

Fury is een domeinnaam registratieplatform dat verantwoordelijk is voor het registreren en beheren van domeinnamen. Fury maakt gebruik van RDAP: een protocol dat het gestructureerd opzoeken van informatie over domeinnaamhouders mogelijk maakt.26 Voor wat betreft het gebruik van RDAP is de grondslag 'gerechtvaardigd belang' van toepassing. Daarnaast heeft SIDN een overeenkomst met iedere domeinnaamhouder. Voor wat betreft de gegevens van de houder vormt de noodzakelijkheid voor de uitvoering van de overeenkomst de grondslag.

[26] Het Registratie Data Access Protocol (RDAP) is de opvolger van het WHOIS protocol, dat gebruikt wordt om relevant registratie data op te zoeken zoals domeinnamen, IP-adressen en AS-nummers.

7.1.2 Merkbewaking

Merkbewaking is een online monitoringsservice die waarschuwt bij de registratie van een domeinnaam die lijkt op een bestaand merk. Klanten kunnen deze dienst afnemen van SIDN. De grondslag voor de verwerking van klantgegevens is de noodzakelijkheid voor de uitvoering van de overeenkomst. Voor wat betreft de andere persoonsgegevens zoals gevonden domeinnamen en de daaraan gekoppelde gegevens is de grondslag het gerechtvaardigd belang. SIDN streeft naar een betrouwbaar en veilig .nl-domein. Domeinnamen die lijken op handelsnamen of merken van organisaties worden onder andere gebruikt voor phishing en oplichting. Dit maatschappelijke risico wordt verkleind door Merkbewaking. Daarnaast hebben de klanten van SIDN een gerechtvaardigd belang om hun intellectuele eigendommen en reputatie te beschermen. Tegenover deze zwaarwegende belangen staat een geringe privacyinbreuk (het verwerken van een domeinnaam).

Voor de klanten die logodetectie via Merkbewaking afnemen, wordt gebruik gemaakt van screenshots vanuit DMAP. Hiervoor is de grondslag eveneens het gerechtvaardigd belang. Er bestaat een zeer kleine een kans dat bij het nemen van de screenshots bijzondere persoonsgegevens worden gedocumenteerd. In dit geval moet hierop een uitzonderingsgrond van toepassing zijn, volgens artikel 9 van de AVG.

7.1.3 DMAP

SIDN maakt gebruik van DMAP om periodieke scans van DNS zones (domeinen) uit te voeren ter ondersteuning van projecten die gericht zijn op het verbeteren van zowel de veiligheid als de stabiliteit van het DNS.[27] Daarnaast maakt DMAP gebruik van screenshots. De resultaten van DMAP worden vervolgens gebruikt om de kwaliteit, stabiliteit en veiligheid van .nl en het internet te onderzoeken en waar mogelijk te verbeteren. Hiervoor hanteert SIDN de grondslag gerechtvaardigd belang (6f AVG). De verwerkte gegevens zullen doorgaans geen persoonsgegevens zijn, maar er bestaat een kleine kans dat persoonsgegevens worden verwerkt, meer specifiek wanneer HTML-content wordt gecrawled.

Zoals hierboven bij Merkbewaking benoemd, bestaat er ook een kleine kans dat bij het nemen van screenshots bijzondere persoonsgegevens worden gedocumenteerd. In dit geval moet ook hierop een uitzonderingsgrond van toepassing zijn, volgens artikel 9 van de AVG. De screenshot functionaliteit staat overigens standaard uit.

7.1.4 .nl Control

.nl Control geeft aanvullende controle over het wijzigen van een domeinnaam aan de gebruiker. Op deze manier wordt voorkomen dat iemand ongewild een domeinnaam omleidt naar een ander (nep) adres. Om de applicatie te kunnen laten werken heeft SIDN enkele persoonsgegevens nodig van de gebruiker. Hiervoor hanteert SIDN de grondslag noodzakelijkheid voor de uitvoering van de overeenkomst.

[27] Wullink, M, en anderen. *'Dmap: Automating Domain Name Ecosystem Measurements and Applications'*, 2-3.

8 Doorgiften van persoonsgegevens

8.1 Content data

Alle contentgegevens worden opgeslagen in de AWS regio's EU-Central-1 (Frankfurt) en EU-West-1 (Ireland). Deze gegevens worden door AWS niet buiten deze regio's gebracht, tenzij SIDN daar specifiek om verzoekt (artikel 12.1 Amazon Data Processing Addendum).

Wel geeft AWS gehoor aan legitieme vorderingen van bevoegde autoriteiten (zoals de Amerikaanse overheid). In het *Supplementary Addendum to AWS Data Processing Addendum* geeft AWS aan dat zij haar klanten informeert over eventuele verzoeken (tenzij haar dit verboden wordt). Ook verweert zij zich tegen (te) vergaande verzoeken (artikel 1.2). Desalniettemin is het niet (volledig) uit te sluiten dat AWS klantgegevens overdraagt aan de bevoegde autoriteiten (meer specifiek de Amerikaanse overheid). Zie hierover verder hoofdstuk 9 (Risico's).

8.2 Gegevens gebruikers

AWS verwerkt zelf persoonsgegevens in de hoedanigheid van verwerkingsverantwoordelijke via monitoring en logging. Het gaat dan met name om de logging van netwerkverkeer. Het is niet uit te sluiten dat deze gegevens buiten de EU worden verwerkt.

Ook is het niet uit te sluiten dat gegevens van klanten die in het kader van een support verzoek worden gedeeld met AWS, buiten de Europese Unie worden verwerkt.

8.3 Gegevens medewerkers

AWS verwerkt zelf persoonsgegevens in de hoedanigheid van verwerkingsverantwoordelijke via monitoring en logging. Het gaat dan om de logging van netwerkverkeer en het loggen van API-calls. Het is niet uit te sluiten dat deze gegevens buiten de EU worden verwerkt.

Met betrekking tot de gegevens van medewerkers die bijvoorbeeld een support ticket indienen is ook niet uit te sluiten dat deze gegevens in de Verenigde Staten worden verwerkt.

9 Risico's

Onderstaand wordt een overzicht gegeven van de risico's. De inschatting van de kans en de impact zijn *zonder* risico beperkende maatregelen.

#	Risico	Beschrijving	Kans	Impact	Totaal
1	Verlies van de vertrouwelijkheid van content gegevens door toegang AWS.	AWS heeft toegang tot de klantgegevens in de SIDN-omgeving.	Hoog	Gemiddeld	Hoog
2	Verlies van de vertrouwelijkheid van content gegevens door toegang van (onder andere) de Amerikaanse overheid.	De Amerikaanse overheid kan AWS dwingen om klantgegevens te overhandigen. Ook kunnen andere overheden zich met vorderingen tot AWS richten.	Gemiddeld	Hoog	Hoog
3	Verlies van de vertrouwelijkheid van content gegevens door toegang door (sub)verwerkers.	Ongeautoriseerde derden krijgen toegang tot de klantgegevens in de SIDN-omgeving.	Gemiddeld	Gemiddeld	Gemiddeld
4	Verlies van de vertrouwelijkheid van content gegevens door ongeautoriseerde toegang.	Inbreuken op de beveiliging kunnen leiden tot ongeoorloofde toegang tot SIDN klantgegevens.	Laag	Hoog	Gemiddeld
5	Doorgifte van gegevens van medewerkers naar de VS.	Gegevens van medewerkers kunnen tijdens het gebruik van de AWS-diensten worden doorgegeven aan AWS.	Hoog	Laag	Gemiddeld
6	Analyse van het gedrag van medewerkers op basis van loggegevens.	Het gedrag van medewerkers kan met behulp van loggegevens worden geanalyseerd.	Hoog	Laag	Gemiddeld
7	Analyse van het gedrag van gebruikers op basis van loggegevens.	Het gedrag van gebruikers kan met behulp van loggegevens worden geanalyseerd.	Hoog	Gemiddeld	Gemiddeld
8	Gegevens worden actief door SIDN gedeeld met AWS.	SIDN kan actief content gegevens delen met AWS, bijvoorbeeld in het kader van een support verzoek.	Hoog	Gemiddeld	Hoog
9	Gegevens zijn (tijdelijk) onbeschikbaar.	Gegevens kunnen door AWS (on)bewust onbeschikbaar worden gemaakt, of de dienstverlening kan door andere redenen (langdurig) onbeschikbaar zijn.	Zeer Laag	Gemiddeld	Gemiddeld

9.1.1 1. Toegang tot content gegevens door AWS

Omdat de gegevens van SIDN-applicaties worden opgeslagen in de AWS cloud, bestaat het risico dat medewerkers van AWS (al dan niet geautoriseerd) toegang krijgen tot de gegevens van SIDN.

AWS heeft technische en organisatorische maatregelen genomen om ervoor te zorgen dat er geen (ongeautoriseerde) toegang is tot gegevens van haar klanten.[28] Echter, het enkele feit dat de hardware en software wordt beheerd door AWS maakt het dat het niet uit te sluiten valt dat AWS zichzelf toegang verschaft tot deze gegevens. AWS stelt zelf ook dat zij bijvoorbeeld content kan verwijderen wanneer dit in strijd is met de gebruiksovereenkomst.[29]

9.1.2 2. Toegang tot content gegevens door de (Amerikaanse) overheid

Indien AWS bij de content gegevens kan (zie risico 1) dan is het ook mogelijk dat zij deze gegevens doorgeeft aan derden, waaronder bevoegde autoriteiten.

AWS geeft in haar *Data Processing Addendum* (artikel 12.1) aan dat zij gehoor geeft aan legitieme vorderingen van bevoegde autoriteiten. Overheden, meer specifiek de Amerikaanse overheid, kunnen dus gegevens vorderen bij AWS. AWS honoreerde in de tweede helft van 2023 (de meest recent gepubliceerde cijfers) 1651 vorderingen. Daar waar het gaat om het vorderen van gegevens maakt AWS een onderscheid tussen non-content data en content data.[30]

Non-content data omvat met name de registratiegegevens van klanten van AWS (in dit geval SIDN). Het gaat dan bijvoorbeeld om namen en contactgegevens van SIDN-medewerkers. Content data omvat de daadwerkelijke gegevens die zijn opgeslagen in de AWS cloud.

1639 van de gehonoreerde vorderingen (99,3%) hadden betrekking op non-content data en 12 vorderingen (0,7%) hadden betrekking op content data. De Amerikaanse overheid heeft in de eerste helft geen enkele keer toegang gekregen tot content data van AWS-klanten die niet in de Verenigde Staten gehost waren aldus AWS.

Het transparantie rapport van AWS laat zien dat de kans dat AWS content data uitlevert zeer klein, maar niet nul is. Er bestaat dus een risico dat AWS, wanneer het daartoe rechtmatig wordt gedwongen, content gegevens uitlevert aan autoriteiten (specifiek binnen de regio's waarin de content gehost is naar het zich laat aanzien).

De kans dat de Amerikaanse overheid op grond van de CLOUD Act rechtstreeks gegevens via AWS vordert, is naar verwachting klein, omdat deze gegevens ook via de Nederlandse overheid via een rechtshulpverzoek bij SIDN zelf kunnen worden opgevraagd.[31] Niet alleen maakt dit de

[28] Zie: EY (2024), Amazon Systems and Organization Controls 2 (SOC 2) Report

[29] Zie: Artikel 1.4 AWS Customer Agreement (via: https://aws.amazon.com/agreement/) en Ernst & Young (2024), Amazon Systems and Organization Controls 3 (SOC 3) Report, p. 50

[30] Zie: Amazon Information Request Report H12024 via: https://d1.awsstatic.com/Security/pdfs/Amazon_AWS_Information_Request_Report_H1_2024.pdf

[31] AWS stelt ook dat in de eerste helft van 2024 geen data op grond van de CLOUD Act zijn overgeleverd.

kans groter dat er daadwerkelijk (onversleutelde) content wordt verkregen groter, het is ook politiek minder gevoelig omdat er dan geen jurisdictie conflicten ontstaan.

Er bestaat wel een theoretische mogelijkheid dat de Amerikaanse overheid geïnteresseerd is in de registratiegegevens van alle .nl domeinnamen (in plaats van informatie betreffende een specifieke domeinnaam). In dergelijke gevallen zal een vordering niet gehonoreerd worden door de Nederlandse autoriteiten en zou de Amerikaanse overheid zich in theorie rechtstreeks tot AWS moeten wenden. AWS geeft aan dat zij bezwaar maken tegen te brede vorderingen.

9.1.3 3. Toegang tot content gegevens door (sub)verwerkers

Voor haar werkzaamheden maakt AWS gebruik van derde partijen (subverwerkers). Deze partijen kunnen -afhankelijk van de geleverde diensten- in theorie toegang krijgen tot klantgegevens van SIDN in het kader van de uitvoering van hun werkzaamheden. Een volledig overzicht van (sub)verwerkers is te vinden op de website van AWS.[32]

AWS bindt haar verwerkers door middel van een verwerkersovereenkomst. Daarnaast neemt AWS veiligheidsmaatregelen om ongeautoriseerde toegang te voorkomen en te detecteren.[33]

9.1.4 4. Verlies van de vertrouwelijkheid door ongeautoriseerde toegang

AWS hanteert een shared responsiblity model voor beveiliging. De beveiliging van de AWS-infrastructuur en diensten is de verantwoordelijkheid van AWS. De inrichting van de cloud omgeving is de verantwoordelijkheid van de klant (SIDN).

AWS neemt uitgebreide technische en organisatorische maatregelen om de gegevens van haar klanten te beveiligen en is compliant met diverse beveiligingstandaarden.[34] AWS is onder andere ISO 27001 gecertificeerd en PCI-compliant.[35] Als zodanig beoordelen wij het risico dat de vertrouwelijkheid, integriteit en beschikbaarheid van gegevens binnen de AWS cloud in het geding komen als laag.

De verantwoordelijkheid voor de beveiliging van persoonsgegevens binnen de applicaties is de verantwoordelijkheid van SIDN zelf. SIDN is ook ISO 27001 gecertificeerd. De belangrijkste beveiligingsmaatregelen die SIDN heeft getroffen in het ontwerp voor de AWS-omgeving worden beschreven onder risicobeperkende maatregelen.

9.1.5 5. Doorgifte van medewerkergegevens naar de VS

AWS is een Amerikaanse aanbieder. Ondanks het feit dat de content gehost wordt in de regio Europa, valt niet uit te sluiten dat persoonsgegevens door het gebruik van AWS naar de VS worden overgebracht. Het gaat dan in eerste instantie om de gegevens (meer specifiek meta data betreffende netwerkverkeer en API-interacties) van medewerkers van SIDN. Medewerkers van SIDN die vanuit een technisch, operationeel of commercieel perspectief betrokken zijn bij de verschillende applicaties, interacteren met de AWS-infrastructuur en met AWS als organisatie. In het kader van deze interacties kunnen gegevens worden verwerkt in de VS voor

[32] https://aws.amazon.com/compliance/sub-processors/

[33] Zie: EY (2024), Amazon Systems and Organization Controls 2 (SOC 2) Report

[34] Zie: https://aws.amazon.com/compliance/programs/

[35] Zie: https://d1.awsstatic.com/certifications/iso_27001_global_certification.pdf en https://aws.amazon.com/compliance/pci-dss-level-1-faqs/

technische, administratieve of commerciële doeleinden. Dit blijkt uit onder andere de privacy statement van AWS, maar ook uit de DPIA op AWS van SLMRijk.[36] Het feit dat persoonsgegevens buiten de Europese Unie worden gebracht kan een privacyrisico opleveren.

De discussie over de doorgifte van persoonsgegevens naar de VS speelt al lange tijd. Voornaamste discussiepunt is de vraag of de VS een land is met een adequaat niveau van gegevensbescherming. Ten tijde van het schrijven van deze DPIA geldt een nieuw adequaatheidsbesluit voor de VS: het EU-US Data Privacy Framework (DPF). AWS is deelnemer aan het DPF en we mogen er daarmee vanuit gaan dat AWS, ook in de VS, een adequaat niveau van gegevensbescherming biedt. Als zodanig schatten wij dit privacyrisico laag in.

9.1.6 6. Analyse van medewerkergedrag op basis van log gegevens

AWS logt diverse gegevens ten behoeve van gebruikers en zichzelf. [redacted]

AWS houdt voor zichzelf ook logfiles bij, met name voor diagnostische- en veiligheidsdoeleinden.[37] AWS geeft geen inzage in de logs die zij bijhoudt voor haar eigen doeleinden. Dit is ook geconstateerd in de DPIA van SLMRijk.[38]

AWS heeft Considerati geen inzicht gegeven in de wijze van logging of de inhoud van de logbestanden. In de DPIA van SLMRijk is AWS op hetzelfde onderwerp bevraagd. De auteurs van de DPIA (Nas en Terra) hebben ook geen inzicht gekregen in de logbestanden. Daarnaast is door hen een inzageverzoek gedaan wat beperkt resultaat heeft opgeleverd.[39] Nas en Terra stellen dat de gegevens die AWS logt en gebruikt voor veiligheidsdoeleinden niet excessief lijken te zijn, maar tekenen daar ook bij aan dat zij niet met zekerheid kunnen bevestigen dat er geen excessieve verwerking van gegevens plaatsvindt. AWS geeft in haar privacy statement aan dat zij deze gegevens niet voor andere doeleinden gebruikt en in lijn handelt met de waarborgen van het EU-US Data Privacy Framework. Op basis van het AWS SOC Type 2 rapport kunnen we concluderen dat AWS de gelogde gegevens enkel voor billing, incident management en security incident management doeleinden gebruikt. De auditors hebben in deze geen onregelmatigheden geconstateerd.

9.1.7 7. Analyse van gebruikers gedrag op basis van log gegevens.

Ten behoeve van onder andere de veiligheid leggen zowel SIDN als AWS-logbestanden aan betreffende het ingaande en uitgaande netwerkverkeer. In theorie kan AWS het gedrag van gebruikers volgen wanneer zij interacteren met de onderdelen van de AWS-infrastructuur.

[36] Nas, S., Terra, F. (2023), DPIA Amazon Web Services, SLMRijk

[37] EY (2024), Amazon Systems and Organization Controls 2 (SOC 2) Report, p. 39. Zie ook: https://aws.amazon.com/privacy/. AWS heeft tegenover Considerati ook bevestigd dat zij gegevens verzamelt voor veiligheids- en diagnostische doeleinden.

[38] Nas, S., Terra, F. (2023), DPIA Amazon Web Services, SLMRijk, pagina 44-46

[39] Nas, S., Terra, F. (2023), DPIA Amazon Web Services, SLMRijk, pagina 44-46

Hiermee kan een (beperkt) beeld worden verkregen van het gedrag van SIDN-gebruikers binnen de AWS cloud.

9.1.8 8. Gegevens worden door SIDN gedeeld met AWS

Medewerkers van SIDN die technische problemen ondervinden met de AWS Cloud omgeving kunnen een support verzoek (ticket) indienen bij AWS. In het kader hiervan kunnen medewerkers informatie delen met AWS (bijvoorbeeld in de vorm van screenshots). Hiermee worden mogelijk persoonsgegevens buiten de EU gebracht omdat de dienstdoende support afdelingen van AWS niet persé in de EU gevestigd zijn.

9.2 9. Gegevens zijn (tijdelijk) onbeschikbaar

Eén van de belangrijkste zorgen van critici is dat door het verplaatsen van het domeinnaam registratieplatform Fury naar AWS het Nederlandse domeinnaamsysteem deels afhankelijk wordt van AWS. Wanneer AWS haar dienstverlening staakt, al dan niet daartoe gedwongen door de Amerikaanse overheid, dan is het registratieplatform (tijdelijk) onbeschikbaar. Ook kunnen kwaadwillende derden door middel van bijvoorbeeld dDos aanvallen proberen de dienstverlening ontoegankelijk te maken. Vanuit een privacyperspectief betekent dit dat de persoonsgegevens (tijdelijk) onbeschikbaar zijn.

10 Risicobeperkende maatregelen

Om de hierboven gesignaleerde risico's te adresseren zijn risicobeperkende maatregelen noodzakelijk. Bij deze maatregelen is het van belang om te vermelden dat sinds 10 juli 2023 het EU-US Data Privacy Framework van kracht is. Amazon (waaronder begrepen AWS) is aangesloten bij het EU-US Data Privacy Framework.[40] Het EU-US Data Privacy Framework, de opvolger van het Privacy Shield raamwerk, is het nieuwe adequaatheidsbesluit voor de Verenigde Staten. Dit betekent dat alle partijen die aangesloten zijn bij het DPF zich moeten houden aan met de EU vergelijkbare privacyregels. Hierdoor worden risico's zoals ongeautoriseerde kennisname door AWS en subverwerkers gemitigeerd. Het adequaatheidsbesluit betekent ook dat gegevens naar aangesloten organisaties in de Verenigde Staten mogen worden geëxporteerd zonder aanvullende waarborgen, waardoor de risico's 5, 6 en 8 in beginsel niet meer relevant zijn vanuit een juridisch perspectief.[41] Het betekent ook dat het niet langer noodzakelijk is om een DTIA (Data Transfer Impact Assessment) te doen.

Hoewel Het EU-US DPF aanvullende privacywaarborgen biedt, acht SIDN het van belang om desalniettemin tenminste de volgende aanvullende risicobeperkende maatregelen te treffen:

#	Maatregel	Beschrijving	Mitigeert risico's
1	Encryptie (at rest)	Content wordt versleuteld opgeslagen zodat derden geen toegang kunnen krijgen tot de daadwerkelijke gegevens.	1, 2, 3, 4
2	Encryptie (in transit)	Netwerkverkeer wordt versleuteld zodat het niet afgeluisterd kan worden	1, 2, 3, 4
3	Beveiligde server infrastructuur	Gegevens worden op een beveiligde server infrastructuur verwerkt, waardoor de gegevens tijdens verwerking ontoegankelijk zijn voor AWS en derden.	1, 2, 3, 4
4	Access & Identity management	Er is alleen toegang voor geautoriseerde medewerkers. Er wordt gebruik gemaakt van een federated identity systeem, waardoor er geen gebruikers accounts (met persoonsgegevens) in AWS aangemaakt hoeven te worden.	4, 5, 6
5	Beperking netwerkverkeer, logging en monitoring	Alleen geautoriseerd netwerkverkeer is toegestaan. Netwerkverkeer en	4, 5, 6

[40] Zie: https://www.dataprivacyframework.gov/list (zoekterm Amazon)
[41] https://ec.europa.eu/commission/presscorner/detail/en/IP_23_3721

		gebruikershandelingen worden gemonitord en gelogd.	
6	Contractuele afspraken	AWS wordt door een verwerkersovereenkomst gebonden.	6, 7, 8
7	Regels voor het gebruik voor medewerkers SIDN	SIDN medewerkers worden getraind in zorgvuldige omgang met gegevens.	8
8	Exit strategie	SIDN heeft een exit strategie om bij het uitvallen van AWS snel de dienstverlening buiten AWS voort te zetten.	9

10.1 1. Encryptie (at rest)

De content gegevens in de AWS omgeving worden versleuteld opgeslagen. Hierdoor is de inhoud van de gegevens niet toegankelijk voor onbevoegde derden zolang de gegevens niet bewerkt worden (encryption at rest).

[redacted]

SIDN maakt gebruik van SIDN-owned keys. AWS kan deze niet gebruiken voor het decrypteren van de gegevens zonder instemming van SIDN. Encryptie zorgt ervoor dat het risico dat AWS en andere (ongeautoriseerde) derden bij de gegevens van SIDN-klanten kunnen sterk verkleind wordt. Hiermee worden de risico's 1,2, 3 en 4 gemitigeerd.

10.2 2. Encryptie (in transit)

Om het risico te verkleinen dat ongeautoriseerden binnen en buiten de AWS-omgeving het netwerkverkeer kunnen afluisteren wordt gebruik gemaakt van versleutelde verbindingen. Het verkeer wordt binnen AWS op verschillende netwerklagen (fysiek, netwerk en applicatie) versleuteld. De verantwoordelijkheid voor het inregelen van de versleuteling op de applicatielaag is de verantwoordelijkheid van SIDN.

Het versleutelen van netwerkverkeer zorgt er ook voor dat AWS een beperkt beeld kan krijgen van het gedrag van gebruikers omdat alleen gegevens zoals IP-adres, gebruikte protocol en bevraagde poorten dan zichtbaar is. De inhoud van het IP-verkeer is voor AWS niet zichtbaar.

[redacted]

10.3 3. Beveiligde server infrastructuur

AWS maakt gebruik van een beveiligde server infrastructuur onder de naam AWS Nitro. Nitro is een standaardonderdeel van de AWS EC2 infrastructuur.

Het AWS Nitro-systeem is zo ontworpen dat operators geen toegang hebben tot gegevens van AWS-klanten. Er is geen mechanisme waarmee een systeem of persoon kan inloggen op EC2 Nitro hosts, toegang kan krijgen tot het geheugen van EC2 instanties, of toegang kan krijgen tot klantgegevens die zijn opgeslagen op lokale versleutelde instance opslag of externe versleutelde EBS volumes. Als een AWS-operator, inclusief degenen met de hoogste privileges, onderhoudswerkzaamheden moet uitvoeren aan een EC2-server, kunnen ze alleen gebruikmaken van een beperkte reeks geauthenticeerde, geautoriseerde, gelogde en gecontroleerde beheer-API's. Geen van deze API's biedt de mogelijkheid om in te loggen op een EC2-server en toegang te krijgen tot klantgegevens. Omdat dit ontworpen en geteste technische beperkingen zijn die in het Nitro-systeem zelf zijn ingebouwd, kan geen enkele AWS-operator deze controles en beveiligingen omzeilen.[43] De veiligheid van het AWS Nitro systeem is onafhankelijk geverifieerd door de NCC Group.[44]

10.4 4. Access & Identity management

Identity & Access Management is een belangrijk onderdeel van de Landing Zone, waarbij ervoor wordt gezorgd dat alleen geautoriseerde en geverifieerde gebruikers toegang hebben tot bronnen, en alleen op een manier die de bedoeling is. [redacted]

Vanuit een beveiligingsperspectief maakt SIDN gebruik van een federated identity systeem. Dit heeft ook voordelen vanuit een privacy perspectief. SIDN-medewerkers hebben geen eigen gebruikers account in AWS. In plaats daarvan hebben de medewerkers een account in het

[43] The Security Design of AWS Nitro, p. 19

[44] Via: https://research.nccgroup.com/2023/05/03/public-report-aws-nitro-system-api-security-claims/

eigen corporate IdP systeem van SIDN [redacted], dat buiten de AWS cloud draait. Medewerkers identificeren, authenticeren en autoriseren zich in dit externe systeem. Vervolgens wordt een tijdelijke 'security credential' aangemaakt die gebruikt kan worden om één van de rollen aan te nemen binnen de AWS cloud. De security credentials bevatten geen persoonsgegevens en zijn tijdelijk. Hierdoor is het voor AWS of een kwaadwillende derde bijzonder moeilijk om te achterhalen welke persoon een bepaalde rol aanneemt binnen de SIDN-omgeving.[45]

[redacted] Gebruikers moeten de eerste keer dat ze inloggen een virtueel MFA-apparaat registreren en moeten dit apparaat bij alle volgende aanmeldingen gebruiken. Het Het corporate IdP systeem gebruikt specifieke password policies om user accounts te managen. Hiermee wordt het risico dat ongeautoriseerde gebruikers zich toegang kunnen verschaffen tot de SIDN-omgeving verder verkleind.

10.5 5. Beperking netwerkverkeer, monitoring en logging

Om de vertrouwelijkheid, integriteit en beschikbaarheid van de dienstverlening en de daarbij verwerkte persoonsgegevens te waarborgen beperkt en monitort SIDN zowel het netwerkverkeer als interacties met de AWS-infrastructuur (API calls). Hiertoe maakt SIDN gebruik van verschillende AWS-diensten. Hieronder bespreken wij de voor deze DPIA meest relevante aspecten.

10.5.1 Beperking netwerkverkeer

[redacted]

10.5.2 Monitoring en logging netwerkverkeer

[redacted]

[redacted]

[redacted]

10.5.3 Monitoring SIDN omgeving

SIDN monitort op verschillende manieren de veiligheid van haar omgeving.

Met behulp van AWS CloudTrail kan het gedrag van gebruikers (API-activiteit) worden [redacted]

10.6 6. Contractuele afspraken

SIDN zal een verwerkersovereenkomst sluiten met AWS. Het betreft de standaard Data Processing Addendum van AWS, dat onderdeel uitmaakt van de hoofdovereenkomst.[50] De inhoud van deze verwerkersovereenkomst is in overeenstemming met de vereisten van artikel 28 lid 3 AVG.

10.7 7. Regels voor het gebruik

De waarborgen van het EU-US Data Privacy Framework bieden bescherming voor de gegevens die met support medewerkers en/of accountmanagers van AWS worden gedeeld. In aanvulling daarop zal SIDN het personeel specifiek instrueren om terughoudend om te gaan met het delen van screenshots, tabellen uit databases, teamviewers et cetera.

10.8 8. Exit strategie

In het uitzonderlijke geval dat AWS bewust of onbewust gegevens ontoegankelijk maakt, moet er snel terug gevallen kunnen worden op een alternatieve infrastructuur. In een dergelijke exit strategie is voorzien door SIDN. De exit strategie wordt gebaseerd op het Rijks Cloud Beleid en volgt het implementatiekader risicoafweging cloudgebruik van de rijksoverheid.[51] Hoewel de exit strategie primair bedoeld is om de continuïteit van de dienstverlening te waarborgen, beperkt het ook de privacyrisico's van het niet beschikbaar zijn van gegevens.

[49] https://aws.amazon.com/cloudwatch/features/

[50] Zie: https://d1.awsstatic.com/legal/aws-dpa/aws-dpa.pdf

[51] Zie: https://www.digitaleoverheid.nl/nieuws/regels-voor-verantwoord-cloudgebruik-rijksoverheid/

11 Beoordeling restrisico

In dit hoofdstuk analyseren wij het restrisico van de migratie naar AWS. Dat wil zeggen, op basis van de risicobeperkende maatregelen die in hoofdstuk 10 zijn beschreven wordt gekeken in hoeverre de risico's die in hoofdstuk 9 zijn geïdentificeerd tot een acceptabel niveau zijn teruggebracht.

Op basis van de risicobeperkende maatregelen die zijn voorgesteld, schat Considerati het restrisico als volgt in:

#	Risico	Beschrijving	Kans	Impact	Totaal
1	Verlies van de vertrouwelijkheid van gegevens door toegang AWS	AWS heeft toegang tot de klantgegevens in de SIDN-omgeving.	Zeer Laag	Gemiddeld	Laag
2	Verlies van de vertrouwelijkheid van content gegevens door toegang door (onder andere) de Amerikaanse overheid.	De Amerikaanse overheid kan AWS dwingen om klantgegevens te overhandigen. Ook kunnen andere overheden zich met vorderingen tot AWS richten.	Zeer Laag	Hoog	Laag
3	Verlies van de vertrouwelijkheid van content gegevens door toegang door (sub)verwerkers.	Ongeautoriseerde derden krijgen toegang tot de klantgegevens in de SIDN-omgeving.	Zeer Laag	Gemiddeld	Laag
4	Verlies van de vertrouwelijkheid van content gegevens door ongeautoriseerde toegang.	Inbreuken op de beveiliging kunnen leiden tot ongeoorloofde toegang tot SIDN-klantgegevens.	Zeer Laag	Hoog	Laag
5	Doorgifte van medewerkergegevens naar de VS.	Gegevens van medewerkers kunnen tijdens het gebruik van de AWS-diensten worden doorgegeven aan AWS.	Zeer laag	Laag	Laag
6	Analyse van het gedrag van medewerkers op basis van loggegevens.	Het gedrag van medewerkers kan met behulp van loggegevens worden geanalyseerd.	Zeer laag	Laag	Laag
7	Analyse van het gedrag van gebruikers op basis van loggegevens.	Het gedrag van gebruikers kan met behulp van log gegevens worden geanalyseerd.			
8	Gegevens worden actief door SIDN gedeeld met AWS.	SIDN kan actief content gegevens delen met AWS, bijvoorbeeld in het kader van een support verzoek.	Laag	Gemiddeld	Laag

9	Gegevens zijn (tijdelijk) onbeschikbaar.	Gegevens kunnen door AWS (on)bewust beschikbaar worden gemaakt, of de dienstverlening kan door andere redenen langdurig onbeschikbaar zijn.	Zeer Laag	Zeer laag	Zeer laag

Door de toepassing van encryptie in rust en in transit voor de gegevens en het gebruiken van beveiligde server infrastructuur, is de kans dat ongeautoriseerde derden toegang krijgen tot content gegevens zeer sterk verkleind. Dit in samenhang met de andere beveiligingsmaatregelen zorgt ervoor dat de kans op ongeautoriseerde toegang (de risico's 1 tot en met 4) tot een acceptabel niveau (laag) worden teruggebracht.

Het feit dat AWS zich heeft gecommitteerd aan het EU-US Data Privacy Framework en een verwerkersovereenkomst, alsmede de keuze voor een federated identity systeem, zorgen ervoor dat het risico dat gegevens van medewerkers worden vastgelegd en het risico dat het gedrag van medewerkers wordt gevolgd (risico's 5 en 6) tot een acceptabel niveau (laag) zijn teruggebracht.[52]

Het feit dat AWS zich heeft gecommitteerd aan het EU-US Data Privacy Framework en een verwerkersovereenkomst, alsmede het gebruik van versleutelde verbindingen, zorgt ervoor dat het risico dat gebruikers kunnen worden gevolgd (risico 7) tot een acceptabel niveau (laag) is teruggebracht. Omdat AWS geen inzicht geeft in haar logging is het daadwerkelijke privacyrisico niet met volledige zekerheid vast te stellen. Maar gegeven het feit dat auditoren bij AWS geen onregelmatigheden hebben geconstateerd bij het gebruik van logfiles door AWS en de DPIA van SLMRijk het privacyrisico van logging door AWS acceptabel acht (laag risico), gaan wij er vanuit dat het risico laag is.[53] Deze inschatting wordt verder mede ingegeven door het feit dat de privacy impact van logging door AWS niet heel groot is, omdat de handelingen van SIDN medewerkers en gebruikers in de AWS Cloud niet bijzonder privacygevoelig zijn en weinig tot niets prijsgeven over het persoonlijke leven van de betrokkenen.

De kans dat contentgegevens worden gedeeld in de context van bijvoorbeeld een supportverzoek kan worden teruggebracht tot een acceptabel niveau door medewerkers duidelijke instructies te geven wat zij wel en niet mogen delen met AWS. Verder biedt de verwerkersovereenkomst en het EU-US DPF een aanvullende waarborg om dit risico te mitigeren. Hiermee is ook dit laatste risico tot een acceptabel niveau (laag) teruggebracht.

[52] Hoewel in het verleden de trans-Atlantische gegevensuitwisseling meerdere malen succesvol ter discussie is gesteld door Max Schrems, vormt het EU-US DPF in samenhang met de verwerkersovereenkomst vooralsnog een aanvullende waarborg voor een veilige gegevensverwerking.

[53] Zie: EY (2023), ISAE 3000 (Revised) Type 2 Report on Management's Description of the Amazon Web Services, Inc.'s System on German Federal Office for Information Security BSI Cloud Computing Compliance Controls Catalogue (C5) for the Period October 1, 2022, to September 30, 2023

Tenslotte is de kans dat AWS dienstverlening onbeschikbaar is op zichzelf al zeer klein. Een van de belangrijkste voordelen van de AWS cloud is dat zij een zéér hoge beschikbaarheid heeft. Considerati acht de kans dat AWS gedwongen wordt door de Amerikaanse overheid om haar dienstverlening aan SIDN te staken als theoretisch. Los van het feit dat AWS een dergelijk verzoek waarschijnlijk tot de hoogste rechter aanvecht met het oog op de gevolgen voor haar reputatie, is de kans dat een bondgenoot het Nederlandse domeinnaam registratiesysteem moedwillig uitschakelt ook zeer klein. De exit strategie van SIDN zorgt ervoor dat de eventuele impact van het manifesteren van dit risico ook beperkt is, omdat SIDN snel op een alternatieve infrastructuur kan overschakelen. Tenslotte is door het nemen van aanvullende anti-dDos maatregelen de kans dat de SIDN-omgeving onbeschikbaar wordt gemaakt door kwaadwillende derden ook verkleind.

12 Conclusies en aanbevelingen

SIDN is voornemens de applicaties Fury, Merkbewaking, DMAP en .nl Control in de AWS cloud te hosten. De belangrijkste reden voor deze migratie is het verder verbeteren van de veiligheid en continuïteit van de dienstverlening van SIDN. Daartegenover staan de mogelijke privacyrisico's van het verplaatsen van de gegevens naar de AWS cloud.

Momenteel worden de applicaties en de daarbij behorende gegevens ook al gehost bij een derde partij. Het voornaamste verschil ten opzichte van de huidige situatie is dat de gegevens in de toekomst worden ondergebracht in een (Europese) cloud omgeving die het eigendom is van en beheerd wordt door een Amerikaanse partij (AWS), in plaats van de huidige situatie waarbij SIDN serverruimte huurt bij twee Nederlandse datacentra. De voornaamste redenen om gebruik te maken van een hyperscaler als AWS, is dat SIDN gebruik kan maken van hun robuuste infrastructuur, technische kennis en tools. Het in eigen beheer ontwikkelen en onderhouden van eenzelfde niveau van kennis is nagenoeg onmogelijk en daarnaast zeer kostbaar. Door te kiezen voor AWS kan SIDN de veiligheid en continuïteit van haar dienstverlening beter garanderen.

De gegevens die SIDN verwerkt, in het bijzonder de gegevens van het domeinnaam registratieplatform Fury, zijn niet zeer gevoelig van aard. Sterker nog, een deel van deze gegevens is openbaar beschikbaar via de WHOIS / RDAP. Desalniettemin acht SIDN het van het grootste belang dat de gegevens deugdelijk worden beschermd.

De belangrijkste privacyrisico's hebben betrekking op de toegankelijkheid van de persoonsgegevens door AWS. AWS zou deze gegevens voor eigen doeleinden kunnen gebruiken, maar ook -al dan niet onder dwang- kunnen doorgeven aan de Amerikaanse overheid. Het risico heeft voornamelijk betrekking op de gegevens in de verschillende applicaties (content gegevens), maar ook gegevens betreffende de interactie van gebruikers (klanten van SIDN) en medewerkers met de SIDN-omgeving zouden in theorie toegankelijk kunnen zijn voor AWS. SIDN heeft dit risico echter tot een acceptabel niveau teruggebracht door zorg te dragen voor de versleuteling van de gegevens en het gebruiken van een beveiligde server infrastructuur. Hierdoor zijn de gegevens in rust, tijdens transport en tijdens de verwerking niet toegankelijk voor AWS-medewerkers en daarmee ook niet voor derden zoals de Amerikaanse overheid.

Voor SIDN-medewerkers geldt dat de kans dat zij geïdentificeerd worden laag is, omdat geen van de medewerkers een account heeft in AWS. In plaats daarvan wordt gebruik gemaakt van tijdelijke security credentials. Deze bevatten geen persoonsgegevens en daardoor is het voor AWS waarschijnlijk onmogelijk, of vormt het op zijn minst een onevenredige inspanning, om het gebruik van de SIDN-omgeving te relateren aan een individuele medewerker. Daarbij moet ook worden aangetekend dat de handelingen in de SIDN-omgeving van individuele medewerkers waarschijnlijk niet van dien aard zijn dat zij überhaupt relevant zijn voor AWS.

Tenslotte is sinds 2023 het EU-US Data Privacy Framework van toepassing. Dit is het nieuwe adequaatheidsbesluit van de Europese Commissie voor de Verenigde Staten. Omdat AWS een deelnemer is aan het EU-US DPF moet zij zich committeren aan met de AVG vergelijkbare regels voor de verwerking van persoonsgegevens. Dit in samenhang met de verwerkersovereenkomst

maakt het dat de verwerking in de cloud ook omgeven is met juridische waarborgen ter bescherming van de privacy.

Naar het oordeel van Considerati worden met de voorgenomen inrichting van de SIDN-omgeving, de aanvullende risicobeperkende maatregelen en de deelname van AWS aan het EU-US Data Privacy Framework, de privacyrisico's tot een acceptabel niveau teruggebracht.

CONSIDERATI

Technologie en data bieden kansen voor elke organisatie. De toepassing hiervan is voorpaginanieuws geworden. Maar deze vernieuwing wringt. Organisaties lopen tegen juridische vraagstukken en maatschappelijke belangen aan. En als organisatie wilt u hierin de regie behouden.

Considerati is het juridisch en public affairs adviesbureau voor de digitale wereld, met kantoren in Amsterdam en Den Haag. Wij helpen organisaties maatschappelijk verantwoord te innoveren met digitale technologie en data. Dit doen we met drie gespecialiseerde teams:

Legal: voor een datastrategie die compliant is met privacyregelgeving

Responsible Tech: voor een ethisch kompas bij innoveren met data en algoritme

Public Affairs: voor maatschappelijk en politiek draagvlak voor innovaties

En dit doen we al meer dan 15 jaar voor zowel grote bedrijven en overheden als groeiende organisaties.

Contact

Neem contact met ons op via **info@considerati** of bel naar 020 73 70 069. Voor meer informatie kunt u ook kijken op onze website via **www.considerati.nl**.