AUTORITEIT
PERSOONSGEGEVENS

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

[redacted]
Toezending uitsluitend per email: [redacted]

Datum	Ons kenmerk	Uw verzoek van
24 mei 2024	[redacted]	10 juli 2023

Contactpersoon
[redacted]
070 8888 500

Onderwerp
Woo-besluit

Geachte [redacted]

Op 10 juli 2023 heeft u per email de Autoriteit Persoonsgegevens (hierna: AP), met een beroep op de Wet open overheid (hierna: Woo), verzocht om openbaarmaking van informatie. De AP heeft uw verzoek doorgezonden naar het ministerie van Jusititie en Veiligheid (hierna: ministerie van JenV), waarna het ministerie van JenV op 19 januari 2024 een besluit op uw Woo-verzoek heeft genomen. Naar aanleiding van dat besluit van het ministerie van JenV, neemt de AP hierbij een nieuw besluit op uw Woo-verzoek.

Uw verzoek ziet op de openbaarmaking van informatie die betrekking heeft op het gebruik van de Amazon clouddienst door de AP. Meer specifiek vraagt u om relevante documenten voor het gebruik van de Amazon clouddienst door de AP, zoals een gegevensbeschermingseffectbeoordeling en een verwerkersovereenkomst.

Op 11 juli 2023 is de ontvangst van uw Woo-verzoek per email aan u bevestigd. Ondanks onze inspanningen is het ons helaas niet gelukt om binnen de wettelijke termijn te beslissen op uw verzoek, waarvoor onze excuses.

Besluit
De AP besluit uw verzoek om openbaarmaking van informatie in te willigen en over te gaan tot gedeeltelijke openbaarmaking van de door ons aangetroffen documenten.

Hieronder licht de AP dit besluit aan u toe.

Wettelijk kader
De AP behandelt uw verzoek als een verzoek om openbaarmaking van informatie op grond van de Wet

open overheid. Een Woo-verzoek wordt ingewilligd (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.

Hieronder legt de AP uit wat dit betekent voor uw Woo-verzoek.

Zoekslag; inventarisatie documenten
Naar aanleiding van uw verzoek heeft de AP naar de gevraagde informatie gezocht binnen de beschikbare systemen. De directie Bedrijfsvoering heeft geïnventariseerd welke documenten de AP heeft die binnen de reikwijdte van uw Woo-verzoek vallen. De directie Bedrijfsvoering gaat binnen de AP namelijk over het opstellen van gegevensbeschermingseffectbeoordelingen en verwerkersovereenkomsten, vanwege contracten of afspraken die met anderen worden aangegaan. Tijdens de zoekslag zijn twee documenten gevonden die binnen de reikwijdte van uw Woo-verzoek vallen.

Naast die twee documenten is één ander document aangetroffen. Dit document valt buiten de toepassing van de Woo, in verband met de toepassing van artikel 8.8 van de Woo. Op grond van dit artikel wijkt de Woo voor bijzondere openbaarmakingsregelingen. Wanneer één van deze bijzondere openbaarmakingsregelingen van toepassing is, gaat deze regeling voor op de algemene openbaarmakingsregeling van de Woo. De bijzondere openbaarmakingsregelingen zijn opgenomen in de bijlage van artikel 8.8 van de Woo, en alleen van toepassing voorzover vallend onder de artikelen genoemd in die regelingen. In de genoemde bijlage zijn de artikelen 2.53, derde lid, en 2.57, eerste en tweede lid van de Aanbestedingswet 2012 opgenomen. De informatie in het document valt onder deze artikelen, en de daarin bepaalde reikwijdte steeds aangehaald met 'voor zover'. Het betreffende document kan daarom niet op grond van de Woo openbaar worden gemaakt.

Zienswijzen; derde-belanghebbende
Een belanghebbende is gevraagd zijn mening te geven over de voorgenomen openbaarmaking van de door u gevraagde informatie. De terugkoppeling van de betrokken belanghebbende heeft de AP meegenomen in de belangenafweging.

Overwegingen
Ingevolge artikel 4.1, zevende lid, van de Woo wordt een verzoek om informatie ingediend met inachtneming van het bepaalde in hoofdstuk 5 van de Woo. Het recht op openbaarmaking op grond van de Woo dient uitsluitend het publieke belang van een goede en democratische bestuursvoering en komt iedere burger in gelijke mate toe. Daarom kan ten aanzien van de openbaarheid geen onderscheid worden gemaakt naar gelang de persoon of de bedoeling of belangen van de verzoeker. Bij de belangenafweging worden daarom het algemene belang van openbaarmaking en de te beschermen belangen door de weigeringsgronden betrokken. Het specifieke belang van de verzoeker wordt hierbij niet betrokken. Verder wordt de informatie die aan u openbaar wordt gemaakt ook aan eenieder openbaar gemaakt. In dit licht vinden de onderstaande belangenafwegingen dan ook plaats.

<u>De eerbiediging van de persoonlijke levenssfeer (artikel 5.1, tweede lid, onder e, van de Woo)</u>
In het document dat gedeeltelijk openbaar wordt gemaakt, staan persoonsgegevens. Dit

zijn gegevens die, al dan niet in samenhang met andere gegevens, herleidbaar zijn tot een persoon, zoals persoonsnamen, telefoonnummers, e-mailadressen, handtekeningen, initialen en zaaknummers (aangemaakt door de AP). Voor zaaknummers geldt daarbij dat openbaarmaking het risico zou vergroten dat (persoons)gegevens uit dossiers van de AP terecht kunnen komen bij onbevoegden.

Openbaarmaking van de genoemde (persoons)gegevens zou een inbreuk op de persoonlijke levenssfeer van de betrokkenen maken. Onder de betrokkenen behoren ook ambtenaren. Wij wegen het belang van eerbiediging van de persoonlijke levenssfeer zwaarder dan het belang van openbaarmaking. Deze informatie wordt dan ook niet openbaar gemaakt.

<u>De beveiliging van personen en bedrijven en het voorkomen van sabotage (artikel 5.1, tweede lid, onder h, van de Woo)</u>
Er wordt geen informatie openbaar gemaakt wanneer dit de beveiliging van personen en bedrijven en/of het voorkomen van sabotage belemmert. Dit belang weegt zwaarder dan het belang van openbaarheid. De gegevensbeschermingseffectbeoordelingen zien op beveiligingsmaatregelen. Hiervan zal de openbaarmaking voor het geheel worden geweigerd. Uit de gegevensbeschermingseffectbeoordelingen kan direct of indirect worden afgeleid welke passende technische of organisatorische maatregelen zijn getroffen om sabotage te voorkomen, de systemen veilig te houden, te voldoen aan wet- en regelgeving en welke rollen er toegang hebben tot welke informatie. Wanneer deze gegevens worden geopenbaard, kan dit voor kwaadwillenden sabotage in de hand werken waardoor de veiligheid van de aan de beoordeling onderworpen organisaties in het geding kan komen. De AP vindt het belang om geen zicht te bieden op de beveiligingsmaatregelen zwaarder wegen dan het belang van openbaarheid. Deze informatie wordt niet openbaar gemaakt. De achtergrond hiervan is dat anders de informatiebeveiliging van de AP zelf in het geding kan komen.

<u>Het goed functioneren van de Staat, andere publiekrechtelijke lichamen ofbestuursorganen (artikel 5.1, tweede lid, onder i, van de Woo)</u>
Het belang van het goed functioneren van de AP als bestuursorgaan weegt naar het oordeel van de AP zwaarder dan het algemene belang van openbaarheid. Onder verwijzing naar de eerder genoemde overwegingen, kan het goed functioneren van de AP in het geding komen. Dit is het geval als informatie over de genomen beveiligingsmaatregelen van de beoordeelde organisaties openbaar wordt, als gevolg waarvan onbevoegden zich toegang kunnen verschaffen tot de informatie die deze organisaties onder zich hebben. Nadien kan dit met zich meebrengen dat organisaties minder snel geneigd zijn (volledig) mee te werken aan vergelijkbare beoordelingen. Door deze terughoudendheid kan het goed functioneren van de AP in het geding komen. Het belang van het goed functioneren van de AP dient dan ook zwaarder te wegen dan het belang van de openbaarheid. De achtergrond hiervan is dat anders de informatiebeveiliging van de AP zelf in het geding kan komen.

Publicatie
Dit besluit, de inventarislijst en het te openbaren document, zal de AP geanonimiseerd publiceren op haar website.

Datum
24 mei 2024

Ons kenmerk
[redacted]

Afschrift aan belanghebbende
Een kopie van dit besluit verzenden we naar de derde-belanghebbende.

Bezwaar
Indien u het niet eens bent met dit besluit, kunt u bezwaar maken. Meer informatie over de bezwaarprocedure vindt u in de bijlage die bij dit besluit is gevoegd.

Hoogachtend,
Autoriteit Persoonsgegevens,

[redacted]

Datum
24 mei 2024

Ons kenmerk
[redacted]

Bijlage 1 – Rechtsmiddelenclausule

Rechtsmiddelenclausule
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.

Datum
24 mei 2024

Ons kenmerk
[redacted]

Bijlage 2 – Inventarislijst

Nr.	Document	Beoordeling	Uitzonderingsgrond WOO
1	20201012 Verwerkersovereenkomst AP - getekend	Deels openbaar	5.1.2.e
2	DPIA	Niet openbaar	5.1.2.h, 5.1.2.i

Inhoud

Verwerkersovereenkomst

Contractnummer: 40100001888.

De ondergetekenden:

1. De **Autoriteit Persoonsgegevens** ("AP"), waarvan de zetel is gevestigd te Den Haag, aan de Bezuidenhoutseweg 30 (2594 AV), vertegenwoordigd door [redacted], in de functie van [redacted],
hierna te noemen: Opdrachtgever,

en

2. **Solvinity B.V.**, gevestigd te Amsterdam aan Hogehilweg 3 (1101 CA), te dezen vertegenwoordigd door de heer [redacted]
hierna te noemen: Opdrachtnemer,

hierna gezamenlijk te noemen: Partijen;

OVERWEGENDE DAT:

- Opdrachtnemer Persoonsgegevens Verwerkt ten behoeve van Opdrachtgever in het kader van de Dienstverleningsovereenkomst, Opdrachtgever krachtens artikel 4, onderdeel 7 en onderdeel 8, van de Verordening kwalificeert als verwerkingsverantwoordelijke voor de Verwerking van Persoonsgegevens en Opdrachtnemer als verwerker;
- Partijen in deze Verwerkersovereenkomst, zoals bedoeld in artikel 28, derde lid, van de Verordening, hun afspraken over de Verwerking van Persoonsgegevens door Opdrachtnemer wensen vast te leggen.

KOMEN OVEREEN:

Artikel 1. Begrippen

In deze Verwerkersovereenkomst wordt een aantal begrippen met een beginhoofdletter gebruikt. Aan deze begrippen komt de betekenis toe die hieraan wordt gegeven in artikel 1 van de Algemene Rijksvoorwaarden bij IT overeenkomsten 2010 (ARBIT-2010). In aanvulling daarop wordt onder de volgende begrippen in deze Verwerkersovereenkomst verstaan:

1.1 Betrokkene: degene op wie een Persoonsgegeven betrekking heeft.

1.2 Inbreuk in verband met Persoonsgegevens: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins Verwerkte gegevens.

1.3 Dienstverleningsovereenkomst: de tussen Opdrachtgever en Opdrachtnemer afgesloten Raamovereenkomst inzake Beveiligingsinfrastructuur, (complexe) webhostingdiensten en daarmee samenhangende aanvullende diensten (JuBIT2) met kenmerk 276485, de verlenging van JuBit2 van 10 november 2016 met kenmerk MJK20102016, de daarop van toepassing zijnde ARBIT-2010 en de Nadere Overeenkomst van 25 april 2019 met kenmerk 41500000121.

1.4 Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon, die Opdrachtnemer in het kader van de Dienstverleningsovereenkomst ten behoeve van Opdrachtgever Verwerkt.

1.5 Verordening: Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van de Richtlijn 95/46/EG (algemene verordening gegevensbescherming).

1.6 Verwerkersovereenkomst: deze overeenkomst inclusief overwegingen en bijbehorende bijlagen.

1.7 Verwerking: een bewerking of een geheel van bewerkingen in het kader van de Dienstverleningsovereenkomst met betrekking tot Persoonsgegevens, of een geheel van Persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen.

Artikel 2. Voorwerp van deze Verwerkersovereenkomst

2.1 Deze Verwerkersovereenkomst regelt de Verwerking van Persoonsgegevens door Opdrachtnemer in het kader van de Dienstverleningsovereenkomst.

2.2 Het onderwerp, de aard en het doel van de Verwerking, het soort Persoonsgegevens en de categorieën van Persoonsgegevens, Betrokkenen en ontvangers zijn in Bijlage 1 omschreven.

2.3 Opdrachtnemer garandeert te voldoen aan de vereisten van de toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens, waaronder begrepen, maar niet uitsluitend, de Verordening en de Uitvoeringswet Algemene Verordening Gegevensbescherming.

Artikel 3. Inwerkingtreding en duur

3.1 Deze Verwerkersovereenkomst treedt in werking op het moment waarop deze door Partijen is ondertekend.

3.2 Deze Verwerkersovereenkomst is van kracht gedurende de looptijd van de Dienstverleningsovereenkomst. Indien de Dienstverleningsovereenkomst eindigt, eindigt deze Verwerkersovereenkomst van rechtswege. Bepalingen die naar hun aard bedoeld zijn om voort te duren na het einde van de Verwerkersovereenkomst (waaronder geheimhoudingsbepalingen) behouden hun werking.

3.3 Geen van Partijen kan deze Verwerkersovereenkomst tussentijds opzeggen.

Artikel 4. Omvang verwerkingsbevoegdheid Opdrachtnemer

4.1 Opdrachtnemer Verwerkt de Persoonsgegevens uitsluitend in opdracht en op basis van schriftelijke instructies van Opdrachtgever, tenzij een op Opdrachtnemer van toepassing zijnde Unierechtelijke of lidstaatrechtelijke bepaling hem tot Verwerking verplicht; in dat geval stelt Opdrachtnemer Opdrachtgever, voorafgaand aan de Verwerking, in kennis van dat wettelijk voorschrift en de op grond daarvan te verrichten Verwerking, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt. In dat

geval informeert Opdrachtnemer Opdrachtgever zo spoedig mogelijk nadat het verbod om te informeren niet meer geldt. Opdrachtnemer zal alvorens aan het verzoek of bevel te voldoen i) de identiteit van de partij die het verzoek of het bevel doet verifiëren en ii) juridisch laten toetsen in hoeverre Opdrachtnemer wettelijk verplicht is om aan het verzoek of bevel te voldoen. Opdrachtnemer zal niet meer of andere Persoonsgegevens verstrekken dan strikt noodzakelijk is om aan het verzoek of bevel te voldoen.

4.2 Indien een instructie als bedoeld in het eerste lid naar het oordeel van Opdrachtnemer in strijd is met een wettelijk voorschrift inzage gegevensbescherming, stelt hij Opdrachtgever daarvan onmiddellijk in kennis.

4.3 Opdrachtnemer heeft geen zeggenschap over het doel van en de middelen voor de Verwerking van Persoonsgegevens. Opdrachtgever heeft die zeggenschap. Voor zover niet anders is bepaald in deze Verwerkersovereenkomst, neemt Opdrachtnemer geen beslissingen over o.a. het gebruik van de Persoonsgegevens, de verstrekking aan derden en de duur van de opslag van Persoonsgegevens. De zeggenschap over de Persoonsgegevens verstrekt onder deze Verwerkersovereenkomst komt nimmer bij Opdrachtnemer te berusten.

4.4 Opdrachtnemer Verwerkt Persoonsgegevens niet buiten de Europese Unie, tenzij hij daarvoor uitdrukkelijk schriftelijk toestemming heeft verkregen van Opdrachtgever en behoudens afwijkende Unierechtelijke of lidstatelijke (wettelijke) verplichtingen. Opdrachtnemer is verplicht om op eerste verzoek van Opdrachtgever aan Opdrachtgever opgave te doen van de locaties waar Opdrachtnemer de Persoonsgegevens Verwerkt en/of mogelijk zal Verwerken.

Artikel 5. Beveiliging van de Verwerking

5.1 Onverminderd artikel 19 van de ARBIT-2010 neemt Opdrachtnemer, rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen. Bij de beoordeling van het passende beveiligingsniveau wordt met name rekening gehouden met de verwerkingsrisico's, vooral als gevolg van de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins Verwerkte Persoonsgegevens, hetzij per ongeluk hetzij onrechtmatig. Opdrachtnemer garandeert de toepassing van zodanige passende technische en organisatorische maatregelen, dat de Verwerking aan de vereisten van de Verordening voldoet en de bescherming van de rechten van de Betrokkene is gewaarborgd. Onder de in dit artikellid bedoelde beveiligingsmaatregelen worden in ieder geval begrepen de technische en organisatorische beveiligingsmaatregelen zoals beschreven in Bijlage 2. maatregelen als beschreven in bijlage 2.

5.2 Partijen erkennen dat het waarborgen van een passend beveiligingsniveau voortdurend kan dwingen tot het treffen van aanvullende beveiligingsmaatregelen. Opdrachtnemer waarborgt een op het risico afgestemd beveiligingsniveau.

5.3 Opdrachtnemer dient Opdrachtgever schriftelijk te informeren voordat een van de technische of organisatorische beveiligingsmaatregelen als bedoeld in artikel 5.1 wijzigt.

5.4 Opdrachtgever kan aanpassing van de beveiligingsmaatregelen weigeren of voorwaarden aan een wijziging verbinden.

5.5 Indien en voor zover Opdrachtgever daarom uitdrukkelijk schriftelijk verzoekt, zal Opdrachtnemer aanvullende maatregelen treffen met het oog op de beveiliging van de Persoonsgegevens.

5.6 Onverminderd het bepaalde in artikel 9 informeert Opdrachtnemer Opdrachtgever zonder onredelijke vertraging zodra hij kennis heeft genomen van onrechtmatige Verwerkingen van Persoonsgegevens of inbreuken op beveiligingsmaatregelen zoals genoemd in het tweede en derde lid.

Artikel 6. Geheimhouding door Personeel van Opdrachtnemer

6.1 De Persoonsgegevens hebben een vertrouwelijk karakter als bedoeld in artikel 17.1 van de ARBIT-2010.

6.2 Opdrachtnemer toont op verzoek van Opdrachtgever aan dat Personeel van Opdrachtnemer en de door Opdrachtnemer tot het Verwerken van de Persoonsgegevens gemachtigde personen zich ertoe heeft verbonden vertrouwelijkheid en geheimhouding in acht te nemen als bedoeld in artikel 17.2 van de ARBIT-2010.
Opdrachtnemer verplicht bedoeld personeel en bedoelde gemachtigde personen hiertoe een geheimhoudingsverklaring te laten tekenen, waarin van hen geëist wordt dat ze met betrekking tot de Persoonsgegevens geheimhouding en vertrouwelijkheid betrachten.

6.3 Uitsluitend voor zover dat noodzakelijk is voor de nakoming van de Dienstverleningsovereenkomst door Opdrachtnemer, verschaft Opdrachtnemer het Personeel van Opdrachtnemer en de door Opdrachtnemer tot het Verwerken van de Persoonsgegevens gemachtigde personen toegang tot de Persoonsgegevens. Het Personeel van Opdrachtnemer en de door Opdrachtnemer tot het Verwerken van de Persoonsgegevens gemachtigde personen mogen slechts die handelingen met betrekking tot de Persoonsgegevens verrichten, die noodzakelijk zijn voor nakoming van de Dienstverleningsovereenkomst door Opdrachtnemer.

Artikel 7. Subverwerker

7.1 Wanneer Opdrachtnemer, met inachtneming van het bepaalde in artikel 23 van de ARBIT-2010, een subverwerker inschakelt om ten behoeve van Opdrachtgever verwerkingsactiviteiten te verrichten, worden aan deze andere subverwerker bij een overeenkomst dezelfde verplichtingen inzake gegevensbescherming opgelegd als die welke in deze Verwerkersovereenkomst zijn opgenomen.

7.2 Op de voet van artikel 7.1 ingeschakelde subverwerkers mogen op hun beurt zelf geen derden (subsubverwerkers) inschakelen dan na voorafgaande schriftelijke toestemming van Opdrachtgever. Opdrachtgever kan aan de schriftelijke toestemming voorwaarden verbinden, onder meer op het gebied van geheimhouding, ter naleving respectievelijk controle van de verplichtingen uit de Verwerkersovereenkomst. Artikel 7.1 is van overeenkomstige toepassing.

7.3 Opdrachtnemer blijft bij de uitbesteding aan een of meer derden (waaronder begrepen sub(sub)verwerkers) te allen tijde aanspreekpunt en verantwoordelijk voor de naleving van de bepalingen uit de Verwerkersovereenkomst en de AVG. Niet naleving van enige bepaling uit de Verwerkersovereenkomst of uit het bij of krachtens de wet gestelde, door inschakeling van sub(sub)verwerkers, komt voor rekening en risico van Opdrachtnemer.

7.4 Opdrachtnemer is verplicht om op eerste verzoek van Opdrachtgever een lijst van de derden te overleggen waaraan Opdrachtnemer met inachtneming van de artikelen 7.1 t/m

7.3 van de Verwerkersovereenkomst, (een deel van) de werkzaamheden voor Opdrachtgever heeft uitbesteed.

Artikel 8. Verlening bijstand door Opdrachtnemer aan Opdrachtgever

8.1 Opdrachtnemer verleent Opdrachtgever rekening houdend met de aard van de Verwerking door middel van passende technische en organisatorische maatregelen bijstand bij het vervullen van diens plicht om verzoeken om uitoefening van de in hoofdstuk III van de Verordening vastgelegde rechten van de Betrokkene tijdig te beantwoorden.

8.2 Rekening houdend met de aard van de Verwerking en de hem ter beschikking staande informatie, verleent Opdrachtnemer Opdrachtgever bijstand bij het tijdig doen nakomen van de verplichtingen uit hoofde van de artikelen 32 tot en met 36 van de Verordening.

Artikel 9. Inbreuk in verband met Persoonsgegevens

9.1 Opdrachtnemer informeert Opdrachtgever zonder onredelijke vertraging, zodra hij kennis heeft genomen van een Inbreuk in verband met Persoonsgegevens, overeenkomstig de afspraken zoals vastgelegd in Bijlage 3.

9.2 Opdrachtnemer informeert Opdrachtgever zolang de Inbreuk in verband met Persoonsgegevens voortduurt ook na een melding op grond van het eerste lid over de ontwikkelingen betreffende de Inbreuk in verband met Persoonsgegevens, en in ieder geval iedere 24 uur.

9.3 Opdrachtnemer doet zelf geen melding van een Inbreuk in verband met Persoonsgegevens bij de Autoriteit Persoonsgegevens en de Betrokkenen, tenzij Opdrachtgever daar uitdrukkelijk en schriftelijk om heeft verzocht of mee heeft ingestemd. In dat geval dragen Opdrachtgever en Opdrachtnemer elk de door henzelf in verband met de melding aan de bevoegde toezichthoudende autoriteit en Betrokkene te maken kosten.

9.4 Indien sprake is van een Inbreuk in verband met Persoonsgegevens, neemt Opdrachtnemer al dan niet in opdracht van Opdrachtgever, zo spoedig mogelijk alle maatregelen om deze Inbreuk te herstellen, gevolgen van deze Inbreuk te beperken en verdere Inbreuken in verband met Persoonsgegevens te voorkomen.

9.5 Opdrachtnemer doet aan derden, waaronder begrepen media, geen mededelingen ten aanzien van een Inbreuk in verband met Persoonsgegevens, behoudens voor zover Opdrachtgever daarvoor voorafgaande schriftelijke toestemming heeft gegeven en Opdrachtgever ook voorafgaand schriftelijk heeft ingestemd met de inhoud van de mededeling.

Artikel 10. Terugbezorgen of wissen Persoonsgegevens

10.1 Na afloop van de Dienstverleningsovereenkomst of op eerste verzoek van Opdrachtgever draagt Opdrachtnemer, naar gelang de keuze van Opdrachtgever, onverwijld zorg voor het terugbezorgen aan Opdrachtgever of het wissen van alle of een deel van de Persoonsgegevens. Opdrachtnemer verwijdert tevens onverwijld eventueel aanwezige kopieën van Persoonsgegevens.

10.2 Opdrachtnemer wist de Persoonsgegevens binnen één maand na afloop van de Dienstverleningsovereenkomst, bij gebreke waarvan Opdrachtnemer een boete verschuldigd is van € 250,- per dag, met een maximum van € 5.000,-.

10.3 Opdrachtnemer verstrekt Opdrachtgever bewijs van wissing van de Persoonsgegevens en de eventuele kopieën daarvan. Dit bewijs bestaat in ieder geval uit een verklaring van een onafhankelijke partij dat de Persoonsgegevens en de eventuele kopieën daarvan zijn gewist.

10.4 Indien naar het redelijk oordeel van Opdrachtnemer een zelfstandige wettelijke verplichting het geheel of gedeeltelijk vernietigen door Opdrachtnemer verbiedt of beperkt, zal hij Opdrachtgever zo spoedig mogelijk schriftelijk in kennis stellen van de wettelijke verplichting en daarbij alle relevante informatie verstrekken die Opdrachtgever redelijkerwijs nodig heeft om te bepalen of vernietiging kan plaatsvinden en, zo ja, onder welke voorwaarden. Indien naar het redelijk oordeel van Opdrachtgever de wettelijke verplichting (gedeeltelijke) vernietiging van Persoonsgegevens door Opdrachtnemer toelaat, zal Opdrachtnemer daartoe op verzoek van Opdrachtgever onverwijld overgaan. Is Opdrachtgever van oordeel dat vernietiging niet mag plaatsvinden, dan zal hij Opdrachtnemer daarvan schriftelijk op de hoogte stellen. Opdrachtnemer garandeert in dat geval de vertrouwelijkheid van Persoonsgegevens jegens Opdrachtgever en zal Persoonsgegevens niet Verwerken behalve ter voldoening aan haar bovenbedoelde wettelijke verplichting of na schriftelijke opdracht van Opdrachtgever.

10.5 De kosten die Opdrachtnemer ter uitvoering van artikel 10 maakt, komen voor zijn rekening.

Artikel 11. Informatieverplichting en audit

11.1 Opdrachtnemer stelt op verzoek van Opdrachtgever alle door de Opdrachtgever verzochte informatie ter beschikking die Opdrachtgever nodig acht om aan te tonen dat de verplichtingen uit deze Verwerkersovereenkomst zijn en worden nagekomen. Ingeval van niet of onvoldoende nakoming van de Verwerkersovereenkomst dient Opdrachtnemer de aanbevelingen van Opdrachtgever op te volgen.

11.2 Opdrachtnemer verstrekt jaarlijks aan Opdrachtgever een rapportage waarin verslag wordt gedaan van de Verwerking van de Persoonsgegevens en waarin beveiligingsrisico's worden gesignaleerd. Van de rapportage maken in ieder geval, maar niet uitsluitend, de volgende onderdelen deel uit:
a. een overzicht van de derden waaronder de Persoonsgegevens zich bevinden;
b. een overzicht van de beveiligingsrisico's die zich in de afgelopen zes maanden voorafgaand aan de rapportage binnen de organisatie van Opdrachtnemer hebben voorgedaan, waaronder, maar niet uitsluitend, datalekken en beveiligingsincidenten die buiten het toepassingsbereik van de Verwerkersovereenkomst vallen;
c. een overzicht van de voorgenomen wijzigingen van de beveiligingsmaatregelen.
Ter voldoening aan het bepaalde in dit artikel onder b. en c. kan Opdrachtnemer volstaan met overlegging van de ten aanzien van Opdrachtnemen uitgevoerde ISO 27001 rapportage.

11.3 Onverminderd het bepaalde in artikel 11.1 staat Opdrachtnemer toe dat Opdrachtgever of een door Opdrachtgever in te schakelen onafhankelijke derde een audit uitvoert naar de vraag of Opdrachtnemer in overeenstemming handelt met de Verwerkersovereenkomst (waaronder de in bijlage 2 beschreven maatregelen), de Verordening, de Uitvoeringswet Algemene Verordening Gegevensbescherming en/of andere toepasselijke wet- en regelgeving waarin eisen aan het Verwerken van Persoonsgegevens worden gesteld. Opdrachtnemer verleent in dit verband binnen een redelijke termijn alle door Opdrachtgever verlangde medewerking, waaronder begrepen, maar niet uitsluitend:

- het verschaffen van alle door Opdrachtgever gevraagde informatie en inlichtingen;
- het verlenen van toegang aan Opdrachtgever en/of een door Opdrachtgever ingeschakelde derde tot de locaties van Opdrachtnemer;

- het verlenen van toegang aan Opdrachtgever en/of een door Opdrachtgever ingeschakelde derde tot de systemen van Opdrachtnemer; en
- het beschikbaar stellen van het personeel van Opdrachtnemer voor het geven van een toelichting aan Opdrachtgever en/of een door Opdrachtgever ingeschakelde derde.

11.4 Binnen een redelijke termijn na uitvoering van de audit als bedoeld in 11.3 zal door of namens Opdrachtgever verslag worden gedaan van de audit. Opdrachtnemer is gehouden de in het verslag gedane aanbevelingen binnen de in het verslag vermelde termijn uit te voeren. Uitvoering van de in het verslag gedane aanbevelingen binnen de gestelde termijn, doet niet af aan het recht van Opdrachtnemer om haar schade op Opdrachtnemer te verhalen.

11.5 De kosten voor de inschakeling van de onafhankelijke derde als bedoeld in artikel 11.3 komen voor rekening van Opdrachtgever, tenzij uit de audit blijkt dat Opdrachtnemer in strijd handelt met de Verwerkersovereenkomst, de Verordening, de Uitvoeringswet Algemene Verordening Gegevensbescherming en/of andere toepasselijke wet- en regelgeving waarin eisen worden gesteld aan het Verwerken van Persoonsgegevens. In dat geval komen de kosten van het inschakelen van de onafhankelijke derde voor rekening van Opdrachtnemer. Deze mogelijk voorvloeiende kosten zijn voor Opdrachtnemer gemaximeerd tot een bedrag van €5000. De kosten die het uitvoeren van de audit meebrengt voor de eigen organisaties van Opdrachtgever en Opdrachtnemer zijn voor eigen rekening.

Artikel 12. Aansprakelijkheid

12.1. Onverminderd de aanspraken op grond van wettelijke regels, is Opdrachtnemer aansprakelijk voor alle schade of nadeel voortvloeiende uit of verband houdend met het handelen in strijd met de Verwerkersovereenkomst, de AVG en/of andere regelgeving waarin eisen aan het Verwerken van Persoonsgegevens worden gesteld.

12.2. Opdrachtnemer vrijwaart Opdrachtgever tegen aanspraken van derden, waaronder Betrokkenen, in verband met het handelen van Opdrachtnemer in strijd met de Verwerkersovereenkomst, de Verordening en/of andere regelgeving waarin eisen aan het Verwerken van Persoonsgegevens worden gesteld. Opdrachtnemer zal alle daarmee verband houdende en daaruit voortvloeiende kosten (waaronder mede begrepen kosten van juridische bijstand) en schade van Opdrachtgever vergoeden.

12.3 De aansprakelijkheid van Opdrachtnemer uit hoofde van deze Verwerkersovereenkomst, is te allen tijde - dus inclusief o.a. eventuele vrijwaringen en boetes - beperkt conform de aansprakelijkheidsregeling van artikel 26 van de ARBIT-2010"

Artikel 13. Overdracht rechten en plichten

De rechten en verplichtingen uit de Verwerkersovereenkomst kunnen door Opdrachtnemer niet aan derden worden overgedragen zonder de voorafgaande schriftelijke toestemming van Opdrachtgever.

Artikel 14. Deelbaarheid

Indien één of meer bepalingen van de Verwerkersovereenkomst niet rechtsgeldig blijkt te zijn, zal de Verwerkersovereenkomst voor het overige van kracht blijven. Partijen zullen over enige bepalingen welke niet rechtsgeldig is overleg plegen en deze vervangen door een bepaling die wel rechtsgeldig is en zoveel mogelijk aansluit bij de strekking van de te vervangen bepaling.

Artikel 15. Wijziging

15.1 De Verwerkersovereenkomst kan slechts gewijzigd worden door een door Partijen bevoegdelijk ondertekende overeenkomst.

Artikel 16. Toepasselijk recht en geschillen

16.1. Op de Verwerkersovereenkomst en op alle geschillen die daaruit voortvloeien of daarmee samenhangen is Nederlands recht van toepassing.

16.2. Alle geschillen voortvloeiende uit of samenhangende met de Verwerkersovereenkomst zullen uitsluitend worden voorgelegd aan de bevoegde rechter van de Rechtbank Den Haag.

Artikel 17. Contactgegevens

17.1 Onverminderd het bepaalde in Bijlage 3 dient Opdrachtnemer, indien Opdrachtnemer over en/of ter uitvoering van de Verwerkersovereenkomst contact met Opdrachtgever wil en/of moet opnemen, zich daarvoor te wenden tot:

De heer [redacted]
Mobielnummer [redacted]
E-mailadres: e[redacted]@autoriteitpersoonsgegevens.nl

17.2 Indien Opdrachtgever over en/of ter uitvoering van de Verwerkersovereenkomst contact met Opdrachtgever wil en/of moet opnemen, dient Opdrachtgever zich daarvoor te wenden tot:

De heer [redacted]
E-mailadres [redacted]@Solvinity.com

Aldus op de laatste van de twee hierna genoemde data overeengekomen en in tweevoud ondertekend,

Den Haag, 1 oktober 2020
Autoriteit Persoonsgegevens
Namens deze,

[redacted]

Amsterdam [redacted] 12 oktober 2020
Solvinity B[redacted]

[redacted]

Bijlage 1. De Verwerking van Persoonsgegevens

Het onderwerp, de aard en doel van de Verwerking	De Autoriteit Persoonsgegevens heeft diverse webformulieren op haar website www.autoriteitpersoonsgegevens.nl. Solvinity is de organisatie die de opslag en de website database faciliteert; waar de webformulieren in zijn opgenomen. Solvinity draagt het dagelijkse beheer van deze website database. Mensen die een klacht/tip/bezwaar willen melden bij de AP (en met de komst van het Hybride webformulier: een klacht willen aanvullen/intrekken), kunnen dit doen middels een op de website beschikbaar gesteld webformulier. Hierbij kan de melder relevante informatie en persoonsgegevens invullen en eventuele bijlagen uploaden. De AP ontvangt het volledig ingevulde webformulier als kopie in een AP mailbox voor het uitvoeren van haar toezichtstaken. De melder ontvangt een automatische bevestigingsmail (waarin, qua persoonsgegevens, enkel het e-mailadres van de melder wordt opgenomen).
Beschrijving categorieën Persoonsgegevens	Persoonsgegevens: naam, geslacht, BSN, adres, e-mailadres, telefoonnummer, toegangs- of identificatiegegevens, financiële gegevens, (kopieën van) paspoorten of andere legitimatiebewijzen, locatiegegevens, strafrechtelijke gegevens en veiligheidsmaatregelen. Bijzondere Persoonsgegevens: Godsdienst of levensovertuiging, ras of etnische afkomst, politieke opvattingen, lidmaatschap van een vakbond, gezondheid/medisch, biometrische gegevens met het oog op unieke identificatie (zoals vingerafdruk), genetische gegevens, seksueel gedrag of seksuele gerichtheid
Beschrijving categorieën Betrokkenen	De melder, verwerkingsverantwoordelijken (voor zover dit persoonsgegevens betreffen) en andere in de klacht/tip/bezwaar genoemde personen.
Beschrijving categorieën ontvangers van Persoonsgegevens	n.v.t.

Bijlage 2. Passende technische en organisatorische maatregelen

Geheimhoudingsovereenkomst
Medewerkers die te maken hebben met persoonsinformatie van Opdrachtgever dienen een geheimhoudingsverklaring te ondertekenen. Hierbij wordt tevens vastgelegd dat na beëindiging van de functie, de betreffende persoon gehouden blijft aan die geheimhouding.

Labeling en verwerking van informatie
Opdrachtnemer heeft maatregelen genomen zo dat niet geautoriseerde(n) geen kennis kunnen nemen van Persoonsgegevens.

Rollen en verantwoordelijkheden
Het Personeel van Opdrachtnemer en derden moeten kennis hebben van de verantwoordelijkheden ten aanzien van de bewerking van Persoonsgegevens voor Opdrachtgever.

Screening
Voor personen is een recente Verklaring Omtrent het Gedrag (VOG) vereist met punten die door Opdrachtgever zijn aangedragen, tenzij dit centraal in het contract geregeld is.

Blokkering van toegangsrechten
Toegangsrechten van medewerkers van Opdrachtnemer worden direct geblokkeerd als geen toegang voor de bewerking van Persoonsgegevens noodzakelijk is.

Fysieke toegangsbeveiliging
Toegang tot beveiligde zones of gebouwen waar Persoonsgegevens van Opdrachtgever zich bevinden is alleen mogelijk na autorisatie van Opdrachtnemer daartoe.

Beveiliging van kantoren, ruimten en faciliteiten
Papieren documenten en mobiele gegevensdragers die Persoonsgegevens of andere vertrouwelijke gegevens van Opdrachtgever bevatten worden beveiligd opgeslagen.

Capaciteitsbeheer
De ICT-voorzieningen voldoen aan het voor de dienst overeengekomen niveau van beschikbaarheid. Er worden voorzieningen geïmplementeerd om de beschikbaarheid van componenten te bewaken (bijvoorbeeld de controle op aanwezigheid van een component en metingen die het gebruik van een component vaststellen). Op basis van voorspellingen van het gebruik wordt actie genomen om tijdig de benodigde uitbreiding van capaciteit te bewerkstelligen. Op basis van een risicoanalyse wordt bepaald wat de beschikbaarheidseis van een ICT-voorziening is en wat de impact bij uitval is. Afhankelijk daarvan worden maatregelen bepaald zoals automatisch werkende mechanismen om uitval van (fysieke) ICT-voorzieningen.

Maatregelen voor netwerken
1) Gegevensuitwisseling tussen vertrouwde en niet vertrouwde zones dient inhoudelijk geautomatiseerd gecontroleerd te worden op aanwezigheid van malware.
2) Bij transport van vertrouwelijke informatie over niet vertrouwde netwerken tussen Opdrachtnemer en Opdrachtgever, zoals over het internet, dient altijd geschikte en door de Opdrachtgever aangewezen encryptie te worden toegepast.

Beveiliging van netwerkdiensten
Beveiligingskenmerken, niveaus van dienstverlening en beheer eisen voor alle netwerkdiensten behoren te worden geïdentificeerd en opgenomen in elke overeenkomst voor netwerkdiensten, zowel voor diensten die intern worden geleverd als voor uitbestede diensten door een verwerker.

Uitwisselingsovereenkomsten
Verantwoordelijkheid en aansprakelijkheid in het geval van informatiebeveiligingsincidenten zijn beschreven, evenals procedures over melding van incidenten van Opdrachtnemer naar de Opdrachtgever.

Fysieke media die worden getransporteerd
Opdrachtnemer neemt maatregelen om vertrouwelijke informatie te beschermen, zoals:
- Versleuteling.
- Bescherming door fysieke maatregelen, zoals afgesloten containers.
- Gebruik van verpakkingsmateriaal waaraan te zien is of getracht is het te openen
- Persoonlijke aflevering.
- Opsplitsing van zendingen in meerdere delen en eventueel verzending via verschillende routes.

Aanmaken auditlogbestanden
1) Door Opdrachtnemer worden rapportages van logbestanden gemaakt die periodiek worden beoordeeld. Deze periode dient te worden gerelateerd aan de mogelijkheid van misbruik en de schade die kan optreden.
2) Een logregel bevat minimaal:
- Een tot een natuurlijk persoon herleidbare gebruikersnaam of ID.
- De gebeurtenis.
- Waar mogelijk de identiteit van het werkstation of de locatie.
- Het object waarvoor de handeling werd uitgevoerd.
- Het resultaat van de handeling.
- De datum en het tijdstip van de gebeurtenis.

3) In een logregel wordt in geen geval gevoelige gegevens opgenomen. Dit betreft onder meer gegevens waarmee de beveiliging doorbroken kan worden (zoals wachtwoorden, inbelnummers, et cetera).

Controle van systeemgebruik
De volgende gebeurtenissen worden in ieder geval opgenomen in de logging:
- Gebruik van technische beheerfuncties, zoals het wijzigingen van configuratie of instelling: uitvoeren van een systeemcommando, starten en stoppen, uitvoering van een back-up of restore.
- Gebruik van functioneel beheerfuncties, zoals het wijzigingen van configuratie en instellingen, release van nieuwe functionaliteit, ingrepen in gegevenssets (waaronder databases).
- Handelingen van beveiligingsbeheer, zoals het opvoeren en afvoeren gebruikers, toekennen en intrekken van rechten, wachtwoord reset, uitgifte en intrekken van cryptosleutels.
- Beveiligingsincidenten (zoals de aanwezigheid van malware, testen op vulnerabilities, foutieve inlogpogingen, overschrijding van autorisatiebevoegdheden, geweigerde pogingen om toegang te krijgen, het gebruik van niet operationele systeemservices, het starten en stoppen van security services)
- Verstoringen in het productieproces (zoals het vollopen van queues, systeemfouten, afbreken tijdens executie van programmatuur, het niet beschikbaar zijn van aangeroepen programmaonderdelen
of systemen).
- Handelingen van gebruikers, zoals goede en foute inlogpogingen, systeemtoegang, gebruik van online transacties en toegang tot bestanden door systeembeheerders.

Bescherming van informatie in logbestanden
Logbestanden worden zodanig beschermd dat deze niet aangepast of gemanipuleerd kunnen worden.

Bescherming van informatie in logbestanden
De beschikbaarheid van loginformatie is gewaarborgd binnen de termijn waarin loganalyse noodzakelijk wordt geacht, met een minimum van drie maanden, conform de wensen van de

Opdrachtgever. Bij een (vermoed) informatiebeveiligingsincident is de bewaartermijn één jaar, dan wel zoveel langer als nodig is om het incident af te wikkelen.

Synchronisatie van systeemklokken
Er worden maatregelen genomen om ervoor te zorgen dat de logbestanden die verzameld worden aan elkaar te relateren zijn, op basis van het tijdstip waarin ze zijn opgetreden.

Authenticatie van gebruikers bil externe verbindingen.
Als externe toegang nodig is tot Persoonsgegevens van Opdrachtgever door Personeel van Opdrachtgever, of Personeel van Opdrachtnemer, dienen geschikte authenticatie methodes te worden gebruikt.

Scheiding van netwerken
Zonering wordt ingericht met voorzieningen waarvan de functionaliteit is beperkt tot het strikt noodzakelijke (hardening van voorzieningen).

Beveiligde inlogprocedures
Toegang tot Persoonsgegevens van Opdrachtgever wordt verleend op basis van 2-factorauthenticatie.

Beveiligde inlogprocedures
Het wachtwoord wordt niet getoond op het scherm tijdens het ingeven. Er wordt geen informatie getoond die herleidbaar is tot de authenticatiegegevens.

Beveiligde inlogprocedures
Voorafgaand aan het aanmelden wordt aan de gebruiker een melding getoond dat alleen geautoriseerd gebruik is toegestaan voor expliciet door de organisatie vastgestelde doeleinden.

Beveiligde inlogprocedures
Bij een succesvol loginproces wordt de datum en tijd van de voorgaande login of loginpoging getoond. Deze informatie kan de gebruiker enige informatie verschaffen over de authenticiteit en/of misbruik van het systeem.

Beveiligde inlogprocedures
Nadat voor een gebruikersnaam 3 keer een foutief wachtwoord gegeven is, wordt het account minimaal 10 minuten geblokkeerd. Indien er geen lock-out periode ingesteld kan worden, dan wordt het account geblokkeerd totdat de gebruiker verzoekt deze lock-out op te heffen of het wachtwoord te resetten.

Gebruikersidentificatie en authenticatie
Bij uitgifte van authenticatiemiddelen wordt minimaal de identiteit vastgesteld, evenals het feit dat de gebruiker recht heeft op het authenticatiemiddel.

Systemen voor wachtwoord beheer
Er wordt automatisch gecontroleerd op goed gebruik van wachtwoorden (onder andere voldoende sterke wachtwoorden, regelmatige wijziging, directe wijziging van initieel wachtwoord).

Time-out van sessies
De periode van inactiviteit van een werkstation is vastgesteld op maximaal 15 minuten. Daarna wordt de PC vergrendeld.

Beperking van verbindingstijd
De toegang voor onderhoud op afstand door een leverancier wordt alleen opengesteld op basis van een wijzigingsverzoek of storingsmelding, met 2-factor authenticatie en tunneling.

Beperking van toegang tot informatie
1) In de soort toegangsregels wordt ten minste onderscheid gemaakt tussen lees- en schrijfbevoegd heden.
2) Managementsoftware heeft de mogelijkheid gebruikerssessies af te sluiten.
3) Bij extern gebruik vanuit een niet vertrouwde omgeving vindt sterke authenticatie (two-factor) van gebruikers plaats.

Analyse en specificatie van beveiligingseisen
In projecten ten behoeve van systemen voor Opdrachtgever wordt een beveiligingsrisicoanalyse en maatregelbepaling opgenomen als onderdeel van het ontwerp. Ook bij wijzigingen worden de veiligheidsconsequenties meegenomen.

Validatie van invoergegevens
Er moeten controles worden uitgevoerd op de invoer van gegevens. Daarbij wordt minimaal gecontroleerd op grenswaarden, ongeldige tekens, onvolledige gegevens, gegevens die niet aan het juiste format voldoen, toevoegen van parameters (SQL-Injectie) en inconsistentie van gegevens.

Beheersing van interne gegevensverwerking
Er bestaan voldoende mogelijkheden om reeds ingevoerde gegevens te kunnen corrigeren door er gegevens aan te kunnen toevoegen.

Integriteit van berichten
Er behoren eisen en geschikte beheersmaatregelen te worden vastgesteld en geïmplementeerd, voor het bewerkstelligen van authenticiteit en het beschermen van integriteit van berichten in toepassingen.

Validatie van uitvoergegevens
De uitvoerfuncties van programma's maken het mogelijk om de volledigheid en juistheid van de gegevens te kunnen vaststellen (bijvoorbeeld door check-sums).

Beleid voor het gebruik van cryptografische beheersmaatregelen
De gebruikte cryptografische algoritmen voor versleuteling zijn als open standaard gedocumenteerd en zijn door onafhankelijke betrouwbare deskundigen getoetst.

Sleutelbeheer
In het sleutelbeheer is minimaal aandacht besteed aan het proces, de actoren en hun verantwoordelijkheden.

Beheersing van operationele software
Alleen geautoriseerd Personeel van Opdrachtnemer kan functies en software installeren of activeren.

Procedures voor wijzigingsbeheer
Er is aantoonbaar wijzigingsmanagement ingericht volgens gangbare best practices, zoals voor applicaties ASL.

Technische beoordeling van toepassingen na wijzigingen in het besturingssysteem
Van aanpassingen (zoals updates) aan softwarematige componenten van de technische infrastructuur wordt vastgesteld dat deze de juiste werking van de technische componenten niet in gevaar brengen en de beveiliging zoals afgesproken met Opdrachtgever te niet doen.

Uitlekken van informatie
Op het grensvlak van een vertrouwde en een niet vertrouwde omgeving vindt content-scanning plaats. Er dient een proces te zijn om aan Opdrachtgever te melden dat (persoons)

informatie is uitgelekt.

Beheersing van technische kwetsbaarheden
Er is een proces ingericht voor het beheer van technische kwetsbaarheden. Dit omvat minimaal het melden van incidenten aan Opdrachtgever, het uitvoeren van periodieke penetratietests, het uitvoeren van risicoanalyses van kwetsbaarheden en patching van systemen en hardware.

Rapportage van informatiebeveiligingsgebeurtenissen
Er is een procedure voor het rapporteren van beveiligingsgebeurtenissen aan Opdrachtgever vastgesteld, in combinatie met een reactie- en escalatieprocedure voor incidenten, waarin de handelingen worden vastgelegd die moeten worden genomen na het ontvangen van een rapport van een beveiligingsincident.
Alle beveiligingsincidenten worden vastgelegd in een systeem en geëscaleerd aan de Opdrachtgever.
Vermissing of diefstal van apparatuur of media die gegevens van Opdrachtgever kunnen bevatten wordt altijd ook aangemerkt als informatiebeveiligingsincident.

Verzamelen van bewijsmateriaal
Voor een vervolgprocedure naar aanleiding van een beveiligingsincident behoort bewijsmateriaal te worden verzameld, bewaard en gepresenteerd in overeenstemming met de voorschriften voor bewijs die voor het relevante rechtsgebied zijn vastgelegd.

Bescherming van bedrijfsdocumenten
De registraties van Opdrachtgever behoren te worden beschermd tegen verlies, vernietiging en vervalsing, in overeenstemming met wettelijke en regelgevende eisen, contractuele verplichtingen en bedrijfsmatige eisen.

Bescherming van gegevens en geheimhouding van Persoonsgegevens
De bescherming van gegevens en privacy behoort te worden bewerkstelligd in overeenstemming met relevante wetgeving, voorschriften en indien van toepassing contractuele bepalingen.

Voorschriften voor het gebruik van cryptografische beheersmaatregelen
Er is vastgesteld aan welke overeenkomsten, wetten en voorschriften de toepassing van cryptografische technieken moet voldoen.

Naleving van beveiligingsbeleid en normen
Opdrachtnemer is verantwoordelijk voor uitvoering en beveiligingsprocedures en toetsing daarop (onder andere de jaarlijkse in control verklaring). Conform deze Verwerkersovereenkomst en andere contractuele eisen zorgt Opdrachtnemer voor het toezicht op de uitvoering van het beveiligingsbeleid ten behoeve van de gegevens van Opdrachtgever. Daarbij behoren ook periodieke beveiligingsaudits. Deze kunnen worden uitgevoerd door, of vanwege de Opdrachtgever.

Controle op technische naleving
Informatiesystemen van Opdrachtnemer ten behoeve van Opdrachtgever worden regelmatig gecontroleerd op naleving van beveiligingsnormen. Dit kan door bijvoorbeeld kwetsbaarheidsanalyses en penetratietesten.

Bijlage 3: Afspraken betreffende Inbreuken in verband met Persoonsgegevens

Opdrachtnemer zal per omgaande een telefonische kennisgeving verrichten aan de contactpersoon van Opdrachtgever de heer [redacted] (mobielnummer [redacted]). Bij afwezigheid van [redacted] kan de kennisgeving worden verricht aan [redacted] (mobielnummer: [redacted]). Een telefonische kennisgeving van een Inbreuk in verband met Persoonsgegevens bevat in elk geval de volgende informatie:

a) een mededeling dat sprake is van een Inbreuk in verband met Persoonsgegevens als bedoeld in artikel 33 van de Verordening;

b) de contactgegevens van de melder (naam, functie, telefoonnummer en e-mailadres) en eventuele vervanger van de melder;

c) een korte algemene omschrijving van de Inbreuk in verband met Persoonsgegevens en een eerste inschatting van de waarschijnlijke gevolgen van de Inbreuk in verband met Persoonsgegevens. Hierbij dient in elk geval de volgende informatie te worden verstrekt: het tijdstip, de omvang, de duur, de oorzaak, de aard van de Inbreuk in verband met Persoonsgegevens, overige relevante omstandigheden, het soort en de hoeveelheid Persoonsgegevens dat is gelekt en het (vermoedelijke) aantal Betrokkenen waarover Persoonsgegevens is gelekt;

d) een inschatting van de maatregelen die nodig zijn om de Inbreuk in verband met Persoonsgegevens zo spoedig mogelijk (blijvend) te beëindigen en de eventuele nadelige gevolgen van de Inbreuk in verband met Persoonsgegevens zo snel mogelijk op te heffen/te beperken;

e) Indien Opdrachtnemer reeds maatregelen heeft getroffen ter beëindiging van de Inbreuk in verband met Persoonsgegevens, informeert Opdrachtnemer Opdrachtgever hierover.