

[REDACTED]

Van: [REDACTED] <[REDACTED]@hotmail.com>
Verzonden: dinsdag 15 juli 2025 21:59
Aan: ACNL Info
Onderwerp: Woo-verzoek ACNL

Beste lezer,

Ik verzoek om openbaarmaking voor eenieder van informatie die uw organisatie onder zich heeft op het gebied van haar eigen AVG-compliance in de periode van 2018 tot heden. Hieronder versta ik onder meer AVG- implementatiedocumenten, de in deze periode gemaakte impactanalyses voor de gegevensverwerking (PIA/DPIA), AVG-impactanalyses bij aanbestedingen, algemeen AVG-beleid ten aanzien van gegevens van medewerkers en andere betrokkenen, et cetera.

Ik verzoek u mijn Woo-verzoek binnen de daarvoor geldende termijn te beantwoorden.

Ik verzoek u per e-mail met mij te corresponderen.

Met vriendelijke groet,

[REDACTED]

[REDACTED]

Van: [REDACTED] <[REDACTED]@hotmail.com>
Verzonden: donderdag 14 augustus 2025 12:42
Aan: ACNL Info
Onderwerp: Ingebrekestelling

Beste lezer,

De beslistermijn voor de beantwoording van mijn Woo-verzoek is inmiddels verstreken. Ik stel uw organisatie hierbij in gebreke. Ik ontvang graag een bevestiging van deze ingebrekestelling.

Met vriendelijke groet,

[REDACTED]

Van: [REDACTED]
Verzonden: dinsdag 15 juli 2025 21:59
Aan: info@slotcoordination.nl
Onderwerp: Woo-verzoek ACNL
Beste lezer,

Ik verzoek om openbaarmaking voor eenieder van informatie die uw organisatie onder zich heeft op het gebied van haar eigen AVG-compliance in de periode van 2018 tot heden. Hieronder versta ik onder meer AVG- implementatiedocumenten, de in deze periode gemaakte impactanalyses voor de gegevensverwerking (PIA/DPIA), AVG-impactanalyses bij aanbestedingen, algemeen AVG-beleid ten aanzien van gegevens van medewerkers en andere betrokkenen, et cetera.

Ik verzoek u mijn Woo-verzoek binnen de daarvoor geldende termijn te beantwoorden.

Ik verzoek u per e-mail met mij te corresponderen.

Met vriendelijke groet,

[REDACTED]

Dhr. [REDACTED]
[REDACTED]
[REDACTED]

Deze brief wordt op verzoek alleen per e-mail verzonden naar:

[REDACTED]@hotmail.com



Datum: 11 september 2025
Ons kenmerk: ACNL25-015
Onderwerp: Besluit op Woo-verzoek inzake AVG

Geachte heer [REDACTED],

Uw Woo-verzoek van 15 juli 2025 en ingebrekestelling van 14 augustus 2025 zijn in de spam box terechtgekomen, aangezien u een hotmailadres heeft gebruikt. Airport Coordination Netherlands (ACNL) krijgt normaliter verzoeken van medewerkers in dienst van luchtvaartbedrijven, met name van luchtvaartmaatschappijen, dan wel van de overheid. Bovendien zijn uw e-mails door de zomervakantieperiode later opgemerkt.

ACNL was voorheen de Stichting Airport Coordination Netherlands (SACN) en is sinds 1 april 2020 een publiekrechtelijk zbo. ACNL is de aangewezen coördinator voor slotallocatie en slotmonitoring in Nederland krachtens Verordening (EEG) Nr. 95/93 van de Raad van 18 januari 1993 betreffende gemeenschappelijke regels voor de toewijzing van "slots" op communautaire luchthavens, de Worldwide Airport Slot Guidelines (WASG), artikel 8a.64 lid 1 van de Wet luchtvaart en het Besluit slotallocatie.

In de praktijk houdt dat in dat ACNL de schaarse slotcapaciteit verdeelt over luchtvaartmaatschappijen om op een welbepaalde datum en tijd de gehele voor de uitvoering van een luchtdienst noodzakelijke luchthaveninfrastructuur op een gecoördineerde luchthaven te gebruiken om te landen of op te stijgen. ACNL verwerkt de volgende gegevens ten behoeve van eerdergenoemde taakuitvoering:

- Bedrijfsgegevens;
- persoonsgegevens van geautoriseerde personen in dienst van bedrijven;
- persoonsgegevens van personen in dienst van de overheid;
- persoonsgegevens van een indiener van een verzoek op basis van de Wet open overheid.

Besluit

Op basis van uw verzoek zijn acht documenten aangetroffen. Ik heb besloten om de aangetroffen documenten waar uw Woo-verzoek op ziet en welke niet reeds openbaar gemaakt zijn, openbaar te maken met inachtneming van artikel 5.1, tweede lid, onder e van de Woo. Dit betekent dat persoonsgegevens uit de documenten zijn gelakt.

Overwegingen

ACNL heeft een hersteltermijn overwogen om uw verzoek aan te laten vullen met uw NAW-gegevens en een ondertekening krachtens artikel 4:2 van de Algemene wet bestuursrecht. Daarnaast heeft ACNL overwogen om uw telefoonnummer te verzoeken om te overleggen. Nu er sprake is van een verzoek van de rechtbank met uw NAW-gegevens, heeft ACNL alsnog een besluit genomen op uw Woo-verzoek.

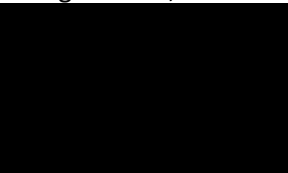
Op grond van artikel 5.1, tweede lid, onder e van de Woo, blijft het verstrekken van informatie achterwege, voor zover het belang van openbaarheid niet opweegt tegen het belang van de eerbiediging van de persoonlijke levenssfeer. In de verzochte documenten staan persoonsgegevens of informatie die raken aan de persoonlijke levenssfeer. Ik ben van mening dat ten aanzien van deze gegevens het belang dat de persoonlijke levenssfeer van de betrokkene wordt geëerbiedigd zwaarder moet wegen dan het belang van openbaarheid. Deze persoonsgegevens zijn dan ook geanonimiseerd in de documenten.

Wijze van openbaarmaking

De stukken die met dit besluit voor eenieder openbaar worden, zullen binnen vijf werkdagen na dagtekening van deze brief op de website van ACNL worden gepubliceerd.

Vertrouwende u hiermee voldoende te hebben geïnformeerd.

Hoogachtend,



Airport Coordination Netherlands

Bezwaar

Eenieder wiens belang rechtstreeks bij dit besluit betrokken is, kan tegen dit besluit binnen 6 weken na de dag van verzending bezwaar indienen bij ACNL middels het adres in de voettekst. Het bezwaarschrift dient te zijn ondertekend en ten minste het volgende te bevatten:

- 1) de naam en het adres van de indiener;*
- 2) de dagtekening;*
- 3) een omschrijving van het besluit waartegen het bezwaar is gericht;*
- 4) de gronden van het bezwaar.*

Airport Coördination Netherlands
T.a.v. de heer [REDACTED]
The Base A
Evert van de Beekstraat 23
1118 CL Schiphol

E-mail: [REDACTED]@slotcoordination.nl

datum

17 april 2018

contactpersoon

[REDACTED]

ons kenmerk

TH 1031883

onderwerp

Aanbod privacy adviseur

Geachte heer [REDACTED]

Tijdens ons gesprek op vrijdag 13 april 2018 heeft u Thorbecke gevraagd een offerte op te stellen voor het opzetten en uitvoeren van een risico-inventarisatie ter beoordeling van de privacyrisico's van gegevensverwerkingsprocessen. Bijgaand treft u het voorstel aan.

Ik hoop dat het een getrouwe weergave is van ons gesprek en dat het aansluit bij de verwachtingen van stichting Airport Coördination Netherlands.

Wij kijken uit naar uw reactie.

Met vriendelijke groet,

[REDACTED]

[REDACTED]

Bijlage: voorstel privacy adviseur

Voorstel privacy adviseur

Context

Stichting Airport Coördination Netherlands (ACNL) is een onafhankelijke non-profit organisatie die verantwoordelijk is voor de toewijzing van tijdslots op de luchthavens Schiphol, Rotterdam en Eindhoven. Op dit moment is er nog weinig aandacht geweest voor privacy en de stichting vraagt zich dan ook af welke stappen ondernomen moeten worden om te voldoen aan wet- en regelgeving.

Op 25 mei 2018 treedt de Algemene Verordening Gegevensbescherming (AVG) in werking. Een voorwaarde om te voldoen aan de nieuwe richtlijnen is dat privacy onder de aandacht wordt gebracht, er transparante keuzes worden gemaakt en maatregelen gedefinieerd en geborgd.

Tijdens het gesprek dat is gevoerd (13 april 2018) tussen de heer [REDACTED] en [REDACTED] (adviseurs Thorbecke) is gebleken dat ACNL op dit moment bezig is met een eerste inventarisatie op het gebied van privacy in aanloop naar de daadwerkelijke invoering van de AVG.

De vraag van ACNL aan Thorbecke is om een eerste inventarisatie uit te voeren en in kaart te brengen welke stappen ondernomen dienen te worden om te voldoen aan wet- en regelgeving. Hierbij moet rekening gehouden worden met het feit dat de organisatie, die op dit moment nog een stichting is, per 1 januari 2020 een publiekrechtelijke organisatie wordt.

Uitdaging

Een inventarisatie van de privacygevoelige gegevens/systemen vormt de basis om een zorgvuldige afweging te kunnen maken tussen de belangen en risico's van alle betrokkenen. Het is de wens van Airport Coördination Netherlands om:

- inzicht te krijgen in de wijze waarop wordt omgegaan met het verwerken van (gevoelige) persoonsgegevens;
- inzicht te krijgen in de stappen die ondernomen moeten worden om te voldoen aan de minimale eisen van de AVG (Algemene verordening gegevensbescherming).

Voorstel

Thorbecke stelt voor im:

- interviews te houden met de (hoofd)proceseigenaren ter beoordeling van de privacyrisico's van gegevensverwerkingsprocessen. Deze gesprekken zullen ook een bijdrage leveren aan een stukje bewustwording op het gebied van privacy.

- een praktische aanpak te hanteren bij het opzetten en uitvoeren van de risico-inventarisatie, door gebruik te maken van overzichtelijke sjablonen.
- een overzichtelijk rapport op te leveren, waarin de huidige stand van zaken is uitgewerkt. En de noodzakelijke maatregelen die u moet nemen om te voldoen aan de minimale eisen van de AVG.

Investing

De werkzaamheden worden uitgevoerd door onze adviseurs [redacted] en [redacted].
[redacted] verzorgt de interviews bij u op locatie.

Wij kunnen u bovengenoemde werkzaamheden aanbieden voor een vast bedrag van:
€ 1.250,- exclusief BTW en inclusief reis- en verblijfkosten.

Ervaring

Thorbecke voert AVG werkzaamheden onder andere uit voor de volgende opdrachtgevers:

- ROVA NV
- Waterschap Zuiderzeeland
- Waterschap DOD
- GBT Hengelo
- Regio Twente
- Groene Norm
- Verschillende gemeenten

Vervolgstappen

Deze offerte ontvangt u per mail. Bij acceptatie van dit voorstel kan een ondertekend exemplaar retour worden gezonden. Na ontvangst van de getekende opdrachtbevestiging, plannen wij een afspraak in en starten wij de werkzaamheden.

Met vriendelijke groet,



Voor akkoord:
Airport Coördination Netherlands



____ (naam)
____ (functie)

VERWERKERSOVEREENKOMST

De ondergetekenden:

1. (Statutaire) Naam opdrachtgever:
Stichting Airport Coordination Netherlands
Adres:
Evert van Beekstraat 23
Postcode:
1118 CL
Vestigingsplaats:
Schiphol
KvK-nummer:
34103386
Naam vertegenwoordigingsbevoegde:
[REDACTED]

hierna te noemen: Opdrachtgever;

en

2. De maatschap **CROP registeraccountants**, tevens handelende onder de naam CROP HR Services, gevestigd en kantoorhoudende te (3823 LL) Amersfoort, aan De Brand 40, ingeschreven in het handelsregister onder nummer 32166733, te dezen vertegenwoordigd door [REDACTED] hierna te noemen: CROP;

hierna gezamenlijk aangeduid als Partijen,

Nemen het volgende in overweging:

- A. Opdrachtgever en CROP dan wel een aan CROP gelieerde entiteit die onderdeel uitmaakt van het samenwerkingsverband waartoe CROP behoort (waaronder in elk geval begrepen CROP belastingadviseurs) zijn een opdracht aangegaan uit hoofde waarvan CROP de volgende werkzaamheden verricht: het uitvoeren van de loon- en salarisadministratie alsmede het verlenen van toegang tot en gebruik van applicaties ten behoeve daarvan en/of aanverwante HR-dienstverlening met betrekking tot de Medewerkers van Opdrachtgever, (hierna: de Opdracht). CROP verwerkt in het kader daarvan de categorieën Persoonsgegevens die vermeld staan in Bijlage 1 bij deze Overeenkomst.
- B. Vanwege het uitvoeren van de Opdracht en met betrekking tot de Persoonsgegevens die CROP zal verwerken zal CROP op grond van de AVG aan te merken zijn als Verwerker en zal Opdrachtgever aan te merken zijn als Verantwoordelijke. In deze Overeenkomst wensen Partijen hun wederzijdse rechten en verplichtingen met betrekking tot het verwerken van de Persoonsgegevens vast te leggen.

Partijen komen het volgende overeen:

Artikel 1 - Definities

In deze Overeenkomst wordt een aantal begrippen gebruikt. De betekenis van die begrippen is hieronder verduidelijkt. De genoemde begrippen worden in deze Overeenkomst met een hoofdletter geschreven. Veelal wordt in de opsomming hieronder gebruik gemaakt van de omschrijving van het begrip uit de wet- en regelgeving op het gebied van privacy.

Betrokkene:	Degene op wie een Persoonsgegeven betrekking heeft;
Verwerker:	Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de Verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen;
Sub-verwerker:	Een andere verwerker die door CROP wordt ingezet om ten behoeve van Opdrachtgever specifieke verwerkingsactiviteiten te verrichten;
Verantwoordelijke:	Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt;
Bijzondere Persoonsgegevens:	Dit zijn gegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid. Alsmede persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen;
Datalek / Inbreuk in verband met persoonsgegevens:	Een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot - of waarbij redelijkerwijs niet uit te sluiten valt dat die kan leiden tot - de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte Persoonsgegevens;
Derden:	Anderen dan Partijen en/of Medewerkers;
Meldplicht Datalekken:	De verplichting tot het melden van Datalekken aan de Autoriteit Persoonsgegevens en (in sommige gevallen) aan Betrokkene(n);
Medewerkers	Personen die werkzaam zijn bij Partijen, al dan niet in dienstbetrekking;
Opdracht:	De opdracht zoals hierboven bedoeld in de overwegingen onder A;

Overeenkomst:	Deze Verwerkersovereenkomst;
Persoonsgegevens:	Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (de Betrokkene) die in het kader van de Opdracht worden verwerkt; als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identifier zoals een naam, een identificatienummer, locatiegegevens, een online identifier of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon;
Persoonsgegevens van gevoelige aard	Persoonsgegevens waarbij verlies of onrechtmatige Verwerking kunnen leiden tot (onder meer) stigmatisering of uitsluiting van Betrokkene, schade aan de gezondheid, financiële schade of tot (identiteits)fraude. Tot deze categorieën van persoonsgegevens moeten in ieder geval worden gerekend: • Bijzondere persoonsgegevens • Gegevens over de financiële of economische situatie van de Betrokkene • (Andere) gegevens die kunnen leiden tot stigmatisering of uitsluiting van de Betrokkene • Gebruikersnamen, wachtwoorden en andere inloggegevens • Gegevens die kunnen worden misbruikt voor (identiteits)fraude;
Verwerken / Verwerking:	Een bewerking of een geheel van bewerkingen 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, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens;
AVG	Algemene Verordening Gegevensbescherming, inclusief de uitvoeringswet van deze verordening. De AVG vervangt de Wet bescherming persoonsgegevens (Wbp) per 25 mei 2018.

Artikel 2 - Toepasselijkheid en duur

- 2.1 Deze Overeenkomst is van toepassing op iedere Verwerking die door CROP wordt gedaan op basis van de Opdracht.
- 2.2 Deze Overeenkomst treedt in werking op de datum van ondertekening van deze Overeenkomst en eindigt op het moment dat CROP geen Persoonsgegevens meer onder zich heeft die zij in het kader van de Opdracht voor Opdrachtgever verwerkt. Het is niet mogelijk om deze Overeenkomst tussentijds op te zeggen.

- 2.3 Artikel 6 en 7 van deze Overeenkomst blijven gelden, ook nadat de Overeenkomst (of de Opdracht) is geëindigd.

Artikel 3 - Verwerking

- 3.1 CROP verwerkt de Persoonsgegevens uitsluitend op de manier die Partijen hebben afgesproken in de Opdracht. Dit verwerken doet CROP niet langer of uitgebreider dan noodzakelijk voor de uitvoering van deze Opdracht. De Verwerking vindt plaats volgens de schriftelijke instructies van Opdrachtgever, tenzij uit wet- en regelgeving anderszins voortvloeit (bijvoorbeeld bij het maken van een afweging of een melding van een "ongebruikelijke transactie" moet worden gedaan in het kader van de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft)). Indien CROP constateert dat een instructie, naar de mening van CROP, een inbreuk maakt op de AVG stelt CROP Opdrachtgever daarvan onmiddellijk in kennis.
- 3.2 De Verwerking vindt plaats onder verantwoordelijkheid van Opdrachtgever. CROP heeft geen zeggenschap over het doel en de middelen van de Verwerking en neemt geen beslissingen over zaken als het gebruik van Persoonsgegevens, de bewaartermijn van de voor Opdrachtgever verwerkte Persoonsgegevens en het verstrekken van Persoonsgegevens aan Derden. Opdrachtgever zal er voor zorgen dat zij het doel en de middelen van de Verwerking van de Persoonsgegevens duidelijk heeft vastgesteld. De zeggenschap over de Persoonsgegevens berust nimmer bij CROP. Indien Medewerkers van CROP een zelfstandige verplichting mochten hebben op basis van wettelijke voorschriften of de voor hen geldende beroeps- en gedragsregels met betrekking tot Verwerking van Persoonsgegevens, dan zal CROP die verplichtingen naleven.
- 3.3 Verantwoordelijke is wettelijk verplicht de vigerende wet- en regelgeving op het gebied van privacy na te leven. In het bijzonder dient Opdrachtgever vast te stellen of er sprake is van een rechtmatige grondslag voor het Verwerken van de Persoonsgegevens. CROP zal voldoen aan de op haar als CROP van toepassing zijnde regelgeving op het gebied van de Verwerking van Persoonsgegevens en de afspraken die Partijen hebben gemaakt in de Opdracht en in deze Overeenkomst.
- 3.4 Opdrachtgever is verantwoordelijk voor de Verwerkingen en bepaalt dat CROP in het kader van de Opdracht Verwerkingen uitvoert ten aanzien van Persoonsgegevens. De Verwerkingen vinden plaats vanwege het verzorgen van de salarisadministratie en alle daarmee verband houdende diensten ten behoeve van Opdrachtgever en de Medewerkers van Opdrachtgever conform de Opdracht, instructies van Opdrachtgever en de van toepassing zijnde wet- en (beroeps)regelgeving.
- 3.5 De Verwerkingen door CROP vinden plaats voor de duur van de Opdracht of voor zo lang dat in verband met wet- of (beroeps)regelgeving noodzakelijk wordt geacht.
- 3.6 CROP zal ervoor zorgen dat alleen haar Medewerkers toegang hebben tot de Persoonsgegevens, behoudens voor zover bepaald in artikel 3.7. CROP zal de toegang tot de Persoonsgegevens beperken tot Medewerkers voor wie de toegang noodzakelijk is voor het uitvoeren van werkzaamheden in het kader van de Opdracht, waarbij de toegang beperkt zal zijn tot Persoonsgegevens die deze Medewerkers nodig hebben voor het uitvoeren van die werkzaamheden. CROP zal er voor zorgen dat de Medewerkers die toegang hebben tot de Persoonsgegevens een juiste en volledige instructie hebben gekregen over de omgang met Persoonsgegevens en dat zij bekend zijn met de verantwoordelijkheden en wettelijke verplichtingen. CROP verplicht haar Medewerkers tot het in acht nemen van vertrouwelijkheid met betrekking tot de Persoonsgegevens.

- 3.7 CROP kan andere verwerkers (Sub-verwerkers) inschakelen voor het uitvoeren van bepaalde werkzaamheden die voortvloeien uit de Opdracht, bijvoorbeeld als deze Sub-verwerkers over specialistische kennis of middelen beschikken waarover CROP niet beschikt. Opdrachtgever geeft hierbij CROP haar toestemming, in algemene zin, om in het kader van de Opdracht gebruik te maken van diensten van Sub-verwerkers binnen de Europese Economische Ruimte alsmede van Sub-verwerkers in landen waarvan de Europese Commissie heeft bepaald dat deze landen een passend beschermingsniveau bieden. Indien CROP gebruik wenst te maken van diensten van Sub-verwerkers gevestigd in een land dat geen passend beschermingsniveau biedt zoals hiervoor bedoeld, dient CROP eerst daartoe voorafgaande schriftelijke toestemming te ontvangen van Opdrachtgever, welke toestemming Opdrachtgever niet op onredelijke gronden zal onthouden. Opdrachtgever zal diens toestemming niet onthouden indien de Sub-verwerker voorkomt op de lijst van actieve gecertificeerde Privacy Shield organisaties die zich dienen te houden aan de Privacy Shield beginselen.
- 3.8 Opdrachtgever geeft hierbij CROP haar toestemming, in algemene zin, om in het kader van de Opdracht gebruik te maken van diensten van Sub-verwerkers zoals gespecificeerd op de website van CROP www.crop.nl/verwerkersovereenkomst. CROP zal alvorens een Sub-verwerker te vervangen dan wel een nieuwe Sub-verwerker in te schakelen, zorgen dat het overzicht op www.crop.nl/verwerkersovereenkomst geüpdatet wordt. Opdrachtgever zorgt voor periodieke raadpleging van www.crop.nl/verwerkersovereenkomst. Indien Opdrachtgever zich op redelijke gronden niet kan verenigen met de voorgenomen wijziging of toevoeging van een bepaalde Sub-verwerker is het Opdrachtgever toegestaan daartegen bezwaar te maken. Het is CROP toegestaan om binnen een termijn van vier (4) weken een alternatief te bieden, om de relevante dienst voort te zetten. Indien CROP geen alternatief biedt, dan is het Opdrachtgever toegestaan om de Opdracht op te zeggen, zonder dat CROP tegenover Opdrachtgever gehouden is tot schadevergoeding wegens de beëindiging. CROP zal aan de door hem ingeschakelde Sub-verwerkers dezelfde verplichtingen opleggen als voor CROP voortvloeien uit deze Overeenkomst.
- 3.9 Indien Opdrachtgever bezwaar maakt als bedoeld in artikel 3.8 en CROP daardoor naar haar oordeel de Opdracht niet langer kan uitvoeren, is CROP gerechtigd de Opdracht (tussentijds) te beëindigen zonder dat CROP tegenover Opdrachtgever gehouden is tot schadevergoeding wegens de beëindiging.
- 3.10 Voor zover mogelijk verleent CROP Opdrachtgever bijstand bij het vervullen van de verplichtingen van Opdrachtgever om verzoeken inzake uitoefening van rechten van Betrokkenen af te handelen. Indien CROP (rechtstreeks) verzoeken ontvangt van Betrokkene(n) inzake uitoefening van hun rechten (bijvoorbeeld inzage, wijziging of verwijdering van Persoonsgegevens), dan zal CROP deze verzoeken verstrekken aan Opdrachtgever. Opdrachtgever zal deze verzoeken zelf afhandelen, waarbij CROP Opdrachtgever behulpzaam kan zijn als CROP in het kader van de Opdracht toegang heeft tot deze Persoonsgegevens. Voor de diensten als bedoeld in dit artikel 3.10 kan CROP kosten in rekening brengen.
- 3.11 CROP zal de Persoonsgegevens alleen Verwerken binnen de Europese Economische Ruimte, tenzij CROP hierover met Opdrachtgever schriftelijk andere afspraken heeft gemaakt of voor zover anders bepaald in deze Overeenkomst.
- 3.12 Indien CROP een verzoek krijgt om Persoonsgegevens ter beschikking te stellen dan zal CROP dit uitsluitend honoreren als het verzoek is gedaan door een daartoe bevoegde instantie. Voorts zal CROP beoordelen of het verzoek naar haar mening bindend is, of dat CROP op grond van gedrags- en beroepsregels gehouden is aan het verzoek voldoen. CROP zal Opdrachtgever

van een dergelijk verzoek in kennis stellen, tenzij dat wet- of regelgeving dat verhindert. CROP zal zich inspannen de kennisgeving aan Opdrachtgever binnen een zodanig korte termijn te doen dat het voor Opdrachtgever mogelijk is om eventuele rechtsmiddelen tegen de verstrekking van de Persoonsgegevens in te stellen. Indien CROP gerechtigd is Opdrachtgever in kennis te stellen dan zullen Partijen overleggen over de wijze waarop en welke gegevens CROP ter beschikking zal stellen.

Artikel 4 - Beveiligingsmaatregelen

- 4.1 CROP treft technische en organisatorische beveiligingsmaatregelen om de Persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. De beveiligingsmaatregelen bieden, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging van de beveiligingsmaatregelen een passend beveiligingsniveau, gelet op de risico's die de verwerking en de aard van de Persoonsgegevens met zich meebrengen.
- 4.2 CROP zal Opdrachtgever informeren als een van de beveiligingsmaatregelen substantieel wijzigt.
- 4.3 CROP biedt passende waarborgen voor de toepassing van de technische en organisatorische beveiligingsmaatregelen met betrekking tot de te verrichten Verwerkingen. Indien Opdrachtgever de wijze waarop CROP de beveiligingsmaatregelen naleeft wil laten inspecteren, dan kan Opdrachtgever hiertoe een verzoek doen. De kosten van een inspectie zijn voor rekening van Opdrachtgever. Opdrachtgever stelt aan CROP een kopie van het inspectierapport ter beschikking.

Artikel 5 - Datalekken

- 5.1 Indien sprake is van een Datalek dan zal CROP Opdrachtgever daarvan op de hoogte stellen. CROP streeft ernaar dit te doen binnen 48 uur nadat CROP dit Datalek heeft ontdekt, of zo snel mogelijk nadat zij daarover door een Sub-verwerker is geïnformeerd. Nadere afspraken over de wijze waarop zijn opgenomen in artikel 11 van deze Overeenkomst. CROP zal Opdrachtgever de informatie verstrekken die Opdrachtgever redelijkerwijs nodig heeft om - indien nodig - een juiste en volledige melding te doen aan de Autoriteit Persoonsgegevens en eventueel de Betrokkene(n) in het kader van de Meldplicht Datalekken c.q. CROP zal de melding van een Sub-verwerker aan Opdrachtgever verstrekken. Voorts zal CROP Opdrachtgever informeren over de door CROP of de Sub-verwerker naar aanleiding van het Datalek genomen maatregelen.
- 5.2 De melding van Datalekken aan de Autoriteit Persoonsgegevens en (eventueel) Betrokkene(n) zal te allen tijde uitsluitend de verantwoordelijkheid van Opdrachtgever zijn. Opdrachtgever zal CROP een afschrift doen toekomen van meldingen als gevolg van een Datalek als bedoeld in artikel 5.1.
- 5.3 Het (bij)houden van een register van Datalekken zal te allen tijde uitsluitend de verantwoordelijkheid van Opdrachtgever zijn.

Artikel 6 - Geheimhouding

- 6.1 Conform het bepaalde in de Opdracht en de algemene voorwaarden van CROP houdt CROP de van Opdrachtgever verkregen Persoonsgegevens geheim en verplicht haar Medewerkers en eventuele Sub-verwerkers ook tot geheimhouding. Geheimhouding kan tevens voortvloeien uit eventuele op de Medewerkers van CROP van toepassing zijnde beroeps- en gedragsregels.

Artikel 7 - Aansprakelijkheid

- 7.1 Opdrachtgever staat er voor in dat de Verwerking van Persoonsgegevens op basis van deze Overeenkomst niet onrechtmatig is en geen inbreuk maakt op de rechten van Betrokkene(n).
- 7.2 CROP is niet aansprakelijk voor enige schade die (direct of indirect) voortvloeit uit het door Opdrachtgever niet naleven van de AVG of andere wet- of regelgeving. Opdrachtgever vrijwaart CROP voor alle aanspraken van Derden en/of Betrokkenen in dat verband. Deze vrijwaring geldt niet uitsluitend voor enige schade die Derden en/of Betrokkenen hebben geleden (daaronder begrepen doch niet beperkt tot immateriële schade), maar tevens voor kosten die CROP in verband daarmee heeft gemaakt, waaronder begrepen doch niet beperkt tot kosten van juridische procedures en boetes die aan CROP worden opgelegd als gevolg van handelen of nalaten van Opdrachtgever.
- 7.3 CROP vrijwaart Opdrachtgever en stelt de Opdrachtgever schadeloos voor alle claims, acties, aanspraken van derden, alsmede boetes van de Autoriteit Persoonsgegevens, die rechtstreeks voortvloeien uit een toerekenbare tekortkoming door CROP en/of diens Sub-verwerkers in de nakoming van zijn verplichtingen onder deze Overeenkomst en/of enige schending door CROP en/of Sub-verwerkers van de van toepassing zijnde wetgeving op het gebied van verwerking van persoonsgegevens.
- 7.4 De in de Opdracht en de algemene voorwaarden van CROP opgenomen beperkingen van de aansprakelijkheid van CROP zijn van overeenkomstige toepassing op het bepaalde in deze Overeenkomst, met dien verstande dat een of meerdere schadevorderingen uit hoofde van deze Overeenkomst en/of de Opdracht nimmer tot overschrijding van de beperkingen kan leiden.
- 7.5 Opdrachtgever behandelt toegangs- en identificatiecodes voor applicaties in verband met de Opdracht vertrouwelijk en met zorg en maakt deze slechts op gepersonaliseerde wijze aan haar geautoriseerde Medewerkers kenbaar. CROP is niet aansprakelijk voor schade of kosten die het gevolg zijn van gebruik of misbruik dat van toegangs- of identificatiecodes wordt gemaakt.

Artikel 8 - Overdraagbaarheid

- 8.1 Het is voor Partijen niet toegestaan om deze Overeenkomst en de rechten en de plichten die daaruit voortvloeien over te dragen aan een Derde, behoudens voor zover Partijen gezamenlijk schriftelijk anders overeenkomen.

Artikel 9 - Beëindiging, teruggave en vernietiging Persoonsgegevens

- 9.1 Ingeval de Opdracht wordt beëindigd, zal CROP de door Opdrachtgever aan CROP verstrekte Persoonsgegevens aan Opdrachtgever terug overdragen of – indien en voor zover Opdrachtgever CROP daar om verzoekt – te vernietigen. CROP zal te allen tijde bevoegd zijn een kopie van de Persoonsgegevens te bewaren als CROP hiertoe op grond van wet- of (beroeps)regelgeving verplicht is.
- 9.2 De kosten van het verzamelen en overdragen van Persoonsgegevens bij het eindigen van de Opdracht zijn voor rekening van Opdrachtgever. Datzelfde geldt voor de kosten van de vernietiging van de Persoonsgegevens. Op verzoek van Opdrachtgever zal CROP vooraf een kosteninschatting geven.

Artikel 10 - Aanvulling en wijziging Overeenkomst

- 10.1 Deze Overeenkomst kan slechts worden aangevuld of gewijzigd door middel van schriftelijke afspraken tussen Partijen. Onder schriftelijk worden ook wijzigingen begrepen die per e-mail zijn overeengekomen.
- 10.2 Een wijziging in de verwerkte Persoonsgegevens of in de betrouwbaarheidseisen, de privacyregelgeving of de eisen van Opdrachtgever kan aanleiding zijn om deze Overeenkomst aan te vullen of te wijzigen. Indien dit leidt tot significante aanpassingen in de Opdracht, of wanneer CROP niet kan voorzien in een passend niveau van bescherming, heeft CROP het recht om de Opdracht (tussentijds) te beëindigen.

Artikel 11 - Overige bepalingen

- 11.1 Op verzoek van Opdrachtgever stelt CROP aan Opdrachtgever alle informatie ter beschikking die nodig is om de nakoming van de in deze Overeenkomst neergelegde verplichtingen aan te tonen. CROP verleent medewerking aan audits, waaronder begrepen inspecties, door Opdrachtgever of een door Opdrachtgever gemachtigde onderzoeker die naar het redelijk oordeel van CROP neutraal en deskundig is. Opdrachtgever draagt zorg dat de onderzoeker is verplicht tot geheimhouding van haar bevindingen tegenover Derden. De kosten van dergelijke verzoeken, audits of inspecties bij CROP en/of Sub-verwerkers zijn voor rekening van Opdrachtgever.
- 11.2 Partijen werken desgevraagd samen met de toezichhoudende autoriteit bij het vervullen van diens taken.
- 11.3 Op deze Overeenkomst is Nederlands recht van toepassing. Alle geschillen die mochten ontstaan naar aanleiding van (de uitvoering van) deze Overeenkomst zullen door Partijen worden voorgelegd aan de daartoe bevoegde rechter van de rechtbank Midden-Nederland.
- 11.4 Indien en voor zover enige bepaling uit deze Overeenkomst afwijkt van de Opdracht, prevaleert het bepaalde in deze Overeenkomst. Algemene voorwaarden van Opdrachtgever zullen uitdrukkelijk niet van toepassing zijn op deze Overeenkomst.
- 11.5 Indien één of meer bepalingen in deze Overeenkomst ongeldig of onverbindend mochten blijken te zijn, dan blijven de overige bepalingen in deze Overeenkomst tussen Partijen onverminderd van kracht. Partijen verbinden zich hierbij reeds nu voor alsdan de betreffende ongeldige of

onverbindende bepaling te (doen) vervangen door een rechtsgeldige bepaling die, gelet op het doel en de strekking van deze Overeenkomst, zoveel mogelijk overeenkomt met de strekking van de betreffende ongeldige of onverbindende bepaling.

- 11.6 Mededelingen in het kader van deze Overeenkomst (inclusief mededelingen in het kader van artikel 5 – Datalekken) zullen door Opdrachtgever en CROP worden gedaan aan onderstaande Medewerkers:

Namens Opdrachtgever:

Naam: [REDACTED]
Werkzaam bij: **Stichting Airport Coordination Netherlands**
e-mail: [REDACTED]@slotcoordination.nl
telefoon: **020-4059730**

Namens CROP:

Naam: [REDACTED]
werkzaam bij: **CROP registeraccountants**
e-mail: [REDACTED]@crop.nl
telefoon: [REDACTED]

Als de gegevens behorend bij de bovengenoemde Medewerkers veranderen, of als zij worden vervangen door andere Medewerkers, dan lichten Partijen elkaar daarover schriftelijk in. Bij gebreke van contactgegevens van de bovenbedoelde Medewerker van Opdrachtgever, zal CROP zich wenden tot de bij CROP bekende contactpersoon van Opdrachtgever.

Aldus overeengekomen,

Opdrachtgever

[REDACTED]

Naam: [REDACTED]

Datum: **5 juni 2018**

CROP registeraccountants

[REDACTED]

[REDACTED]

Klik hier als u een datum wilt invoeren.

Bijlage 1

Persoonsgegevens en Verwerking

Ten behoeve van de Opdracht verwerkt CROP onder meer de volgende categorieën Persoonsgegevens:

- Naam-, adres- woonplaatsgegevens
- Beroepsgegevens
- Burgerservicenummer
- Opleidingsgegevens
- Contactgegevens (o.a. telefoonnummers en e-mailadressen)
- Verlof- en verzuimgegevens
- Familiesamenstelling
- Functioneringsgegevens
- Financiële gegevens / salarisgegevens
- Bankrekeningnummers
- Belonings-, uitkerings- en/of pensioengegegevens
- In-/uitstroombmutaties / dienstverbanden

Bovengenoemde opsomming is niet limitatief. In het kader van de dienstverlening door CROP dan wel de daartoe gebruikte applicatie(s) kunnen aanvullende Persoonsgegevens worden verstrekt en/of kunnen gebruikers (zowel Partijen als Medewerkers van Opdrachtgever) documenten toevoegen. Die documenten kunnen eveneens andere (categorieën) Persoonsgegevens bevatten.



Privacybeleid Stichting Airport Coordination Netherlands (ACNL)

Inleiding

Kerntaak van ACNL is de toewijzing van slots. Op het eerste gezicht heeft ACNL daarom weinig met persoonsgegevens te maken. Toch verricht ook ACNL dagelijks werkzaamheden die op grond van de Algemene verordening gegevensbescherming (Avg) als “verwerking van persoonsgegevens” moeten worden gezien. Zo worden er emailadressen van personen opgeslagen om slots te kunnen toewijzen en te kunnen communiceren over aanvragen van slots en worden er informatieverzoeken van burgers behandeld. Daarnaast zijn er uiteraard diverse persoonsgegevens bekend van het eigen personeel. Het is zaak dat zorgvuldig met deze gegevens wordt omgegaan.

Met het inwerking treden van de Avg gelden er extra eisen aan de wijze waarop met persoonsgegevens moet worden omgegaan en met name de wijze waarop hierover verantwoording wordt afgelegd. In deze notitie Privacybeleid wordt in hoofdlijnen beschreven hoe ACNL invulling geeft aan de wettelijke eisen.

Juridisch kader en verplichtingen

Vanaf 25 mei 2018 geldt de Algemene verordening gegevensbescherming (Avg). Deze Europese verordening heeft gezorgd voor een versterking van de privacyrechten en legt meer verplichtingen neer bij organisaties die persoonsgegevens verwerken. Die verplichtingen komen vooral voort uit de verantwoordingsplicht: een organisatie moet inzichtelijk maken welke gegevens worden verzameld, waarom, hoe lang, wie toegang heeft etc. Ook moet inzichtelijk worden gemaakt wanneer het mis is gegaan met gegevens (datalekken). ACNL voldoet aan deze Avg-verplichtingen door:

- a. Een register verwerkingsactiviteiten op te stellen en bij te houden.
In het register verwerkingsactiviteiten worden alle activiteiten omschreven waarbij persoonsgegevens worden verwerkt. Het register bevat tevens de bewaartermijnen van de gegevens. Het register wordt regelmatig en minimaal twee maal per jaar gecontroleerd en geactualiseerd.
- b. Een registratie van datalekken bij te houden.
Een datalek doet zich voor als persoonsgegevens verloren (kunnen) zijn gegaan bijvoorbeeld door diefstal of verlies, een hack of een brand. ACNL stelt een procedure op voor het intern melden van datalekken, het beoordelen of het lek moet worden gemeld aan de Autoriteit Persoonsgegevens en het beoordelen van de vraag of de betrokkene (degene waarvan persoonsgegevens in het geding zijn) mededeling moet worden gedaan van de inbreuk.
- c. Verwerkersovereenkomsten te sluiten.

Wanneer in het kader van processen van ACNL, persoonsgegevens worden verwerkt door derden, sluit ACNL daarmee verwerkersovereenkomsten. De overeenkomsten voldoen ten minste aan de eisen van de Avg en geven inzicht in verantwoordelijkheden en aansprakelijkheden. Bij het aangaan van een overeenkomst, toetst ACNL of de verwerker voldoende garanties biedt voor de bescherming van de persoonsgegevens.

- d. Samenwerking te zoeken bij het aanwijzen van een Functionaris Gegevensbescherming (FG). De Avg verplicht in de Avg-omschreven organisaties om een functionaris gegevensbescherming aan te wijzen. Deze functionaris heeft onder meer tot taak om toe te zien op de naleving van de Avg binnen de organisatie waar hij werkzaam is. Op dit moment is ACNL nog niet verplicht om een FG aan te stellen maar naar verwachting zal dit wel verplicht zijn op het moment dat ACNL een publiekrechtelijke ZBO wordt (naar verwachting 1 januari 2020). ACNL zal de mogelijkheden onderzoeken om in samenwerking met andere (overheids)organisaties gezamenlijk één FG aan te wijzen.

Uitgangspunten

ACNL hanteert de volgende uitgangspunten die gebaseerd zijn op artikel 5 en 33 van de Avg.

- Voor het uitvoeren van haar taken, heeft ACNL slechts beperkt persoonsgegevens nodig. ACNL vraagt ook niet méér gegevens dan nodig is voor de uitoefening van haar taken. De gegevens worden alleen gebruikt voor het met de verwerking te dienen doel.
- Persoonsgegevens worden niet langer bewaard dan noodzakelijk.
- ACNL borgt middels technische en organisatorische maatregelen dat onbevoegde toegang en onbevoegd gebruik van gegevens wordt voorkomen. De organisatorische maatregelen betreffen mede instructies aan personeelsleden van ACNL voor het voorkomen van beveiligingsincidenten.
- Afhandeling van klachten over privacy-aspecten gebeurt op een laagdrempelige, toegankelijke wijze. Verzoeken om inzage, correctie of wijziging, worden conform de Avg afgehandeld. Via de eigen site zal informatie worden gegeven over de mogelijkheid om een klacht in te dienen en om inzage, correctie en wijziging te verzoeken.
- Beveiligingsincidenten waarbij (mogelijk) persoonsgegevens zijn betrokken, worden geregistreerd en beoordeeld conform Avg op de noodzaak om een melding te doen bij Autoriteit Persoonsgegevens. Tevens worden de te ondernemen acties beoordeeld, ook in de richting van degene waarvan de persoonsgegevens in het geding zijn.

Grondslagen van verwerking

Op grond van de Avg (artikel 6) moet er een grond zijn op basis waarvan de verwerking van persoonsgegevens als rechtmatig wordt aangemerkt. De grondslag om persoonsgegevens te verwerken, zal voor ACNL in de meeste gevallen “het voldoen aan een wettelijke verplichting” dan wel “vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag.” zijn. Waar de verwerking van persoonsgegevens niet kan worden gebaseerd op genoemde gronden, zal expliciet om toestemming worden gevraagd om de persoonsgegevens te verwerken. Dit speelt bijvoorbeeld bij het abonneren op de nieuwsbrief van ACNL. Omdat de abonnees op de nieuwsbrief in het verleden zich expliciet hiervoor hebben aangemeld, wordt voldaan aan de eisen die de Avg stelt ten aanzien van het kunnen aantonen van toestemming.

In de gevallen waarin “toestemming” de grond is voor de verwerking, zal gewezen worden op het recht om de toestemming in te trekken.

Verantwoordelijkheden en financiering

De managing director (md) van ACNL is verantwoordelijk voor de wijze waarop ACNL invulling geeft aan het privacybeleid en zorgt voor voldoende middelen en kaders om privacybescherming passend te waarborgen. Hierbij valt te denken aan:

- Medewerkers hebben voldoende ruimte in hun takenpakket om privacy-gerelateerde taken uit te kunnen voeren (bijv. het behandelen van verzoeken om inzage en wijziging van gegevens);
- De md zorgt voor instructies over het gebruik van laptop, archiveren etc. ;
- De md zorgt voor verwerkersovereenkomsten met bedrijven die voor ACNL persoonsgegevens verwerken en maakt zo nodig aanvullende afspraken (bijvoorbeeld met leverancier ICT-diensten);
- De md onderzoekt de mogelijkheid voor het gezamenlijk met andere overheidsorganisaties aanstellen van een Functionaris Gegevensbescherming en zorgt voor de financiering van het “ACNL-deel” van diens takenpakket. De onafhankelijke positie van de FG zal geborgd worden;
- De md bevordert dat het onderwerp privacybescherming aandacht heeft op de werkvloer, inclusief het doen van meldingen van datalekken.

De aandacht voor privacybescherming en de uitvoering van de regels die de Avg stelt, zal naar verwachting kunnen plaatsvinden binnen de huidige formatie en budgetten, met uitzondering van het aanwijzen van een FG.

Evaluatie

De Avg is vanaf 25 mei 2018 van kracht. Hoewel de privacybescherming en de uitvoering van de Avg-regels natuurlijk constant aandacht behoeven, is het van belang om op enkele momenten nadrukkelijk stil te staan bij de wijze waarop het beleid en de regels door ACNL worden uitgevoerd en tegen welke problemen de medewerkers aanlopen. Te denken valt daarbij aan vragen als:

- Zijn er op de werkvloer voldoende werkbare instructies over hoe moet worden omgegaan met privacy-aspecten?
- Welke technische en/of organisatorische verbeteringen zijn nog mogelijk?
- Hoe verloopt de uitvoering van de verwerkersovereenkomsten door de externe verwerkers?
- Welke privacy-gerelateerde klachten zijn er ontvangen en wat waren de lessen voor ACNL?

De md zal daarom zorgdragen voor het (laten) uitvoeren van evaluaties na 6 en 12 maanden van de startdatum Avg.

Vastgesteld 12 juni 2018



Aanvullende maatregelen bij ACNL ter voorkoming datalekken

d.d. 3 juli 2018

Om het risico op datalekken te verkleinen, gelden bij ACNL de volgende richtlijnen voor het omgaan met persoonsgegevens (zowel papieren dossiers als digitale gegevens):

Organisatorische beveiligingsmaatregelen

- Papieren dossiers met bijzondere categorieën persoonsgegevens worden bewaard in afgesloten kast.
- Laptops worden niet onbeheerd achtergelaten (deur afsluiten indien er niemand aanwezig is).
- Laptops worden vergrendeld als de medewerker de werkplek verlaat.
- Laptops worden niet achtergelaten in auto.
- Indien privé-pc of laptop wordt gebruikt, worden documenten bij voorkeur niet hierop opgeslagen. Wanneer dit toch gewenst is, worden documenten waarin persoonsgegevens zijn opgenomen, niet langer dan noodzakelijk op privé-pc/-laptop bewaard.
- Oude documenten met persoonsgegevens worden op juiste manier vernietigd (d.w.z. worden aangeboden in de papierbak waarvan de inhoud periodiek wordt vernietigd).
- USB-sticks worden zo minimaal mogelijk gebruikt. Wanneer USB-stick toch wordt gebruikt, worden documenten met persoonsgegevens z.s.m. weer gewist.
- Geen cloudopslag buiten EU, geen opslag van persoonsgegevens op servers als Google Drive, Dropbox.

Technische beveiligingsmaatregelen

- Bij gebruik privé-pc/laptop zorgt de medewerker voor een adequate virusscan.
- Bij gebruik email op telefoon dient ontgrendeling van de telefoon plaats te vinden met code o.i.d.
- Gebruik sterke wachtwoorden voor je (privé) pc/laptop.

Om te bespreken met [REDACTED]:

- bescherming tegen hackers en malware
- moderne IPS/firewall
- goed beveiligde draadloos netwerk
- up-to-date security software op de endpoints

Verwerkersovereenkomst

Stichting Airport Coordination Netherlands, gevestigd te Schiphol aan de Evert van Beekstraat 23 rechtsgeldig vertegenwoordigd door de heer [REDACTED], hierna te noemen: Verwerkingsverantwoordelijke;

en

100% Oegstgeest B.V., gevestigd te Leiden aan de Flemingstraat 91, rechtsgeldig vertegenwoordigd door de mevrouw [REDACTED] en mevrouw [REDACTED], hierna te noemen: 'Verwerker',

hierna gezamenlijk aan te duiden als: "Partijen";

overwegende dat:

1. Verwerkingsverantwoordelijke de Verwerker opdracht heeft gegeven tot het leveren van een product of dienst, waarvan de Verwerking van Persoonsgegevens van Betrokkenen deel uit maakt;
2. Partijen het volgende overeenkomen voor bestaande en toekomstige Overeenkomsten waarvan Verwerking van Persoonsgegevens onderdeel is;

verklaren en komen als volgt overeen:

Artikel 1. Definities

1. In deze Verwerkersovereenkomst hebben onderstaande begrippen de volgende betekenis:
 - a. Verwerkingsverantwoordelijke: natuurlijk persoon of rechtspersoon, een overheidsinstantie of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt;
 - b. Verwerker: natuurlijk persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt;
 - c. Betrokkene: natuurlijk persoon op wie de verwerkte persoonsgegevens betrekking hebben;
 - d. Verwerkersovereenkomst: deze verwerkersovereenkomst, welke deel uitmaakt van de Overeenkomst;
 - e. Overeenkomst(en): elke tussen Verwerkingsverantwoordelijke en Verwerker gesloten overeenkomst, bestaand en toekomstig, op grond waarvan Verwerker werkzaamheden verricht met door Verwerkingsverantwoordelijke via een door Verwerker aangeboden product of dienst verzamelde Persoonsgegevens;
 - f. Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (de Betrokkene). Als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, locatiegegevens, digitale identificators etc. of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon;
 - g. Verwerking: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens;
 - h. Datalek: 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 toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens;
 - i. Autoriteit Persoonsgegevens: toezichthoudende autoriteit. Een onafhankelijke overheidsinstantie verantwoordelijk voor het toezicht op de naleving van de wet in verband met de verwerking van persoonsgegevens;
 - j. AVG: Algemene Verordening Gegevensbescherming.

Artikel 2. Duur, looptijd en beëindiging

1. Deze Verwerkersovereenkomst komt tot stand op de datum van ondertekening en is vanaf dat moment van toepassing op alle Overeenkomsten tussen Partijen.
2. In geval van beëindiging van de Overeenkomst, zullen Partijen in overleg treden omtrent de overdracht van de Persoonsgegevens aan Verwerkingsverantwoordelijke. De Verwerker is verplicht de door Verwerkingsverantwoordelijke vereiste medewerking te verlenen.
3. De Verwerkersovereenkomst eindigt op het moment dat Verwerker geen persoonsgegevens meer onder zich heeft die zij in het kader van de tussen partijen gesloten Overeenkomst verwerkt.

Artikel 3. Verplichtingen Verwerkingsverantwoordelijke

1. Verwerkingsverantwoordelijke staat er jegens Verwerker voor in dat de Verwerking en de inhoud, het gebruik en/of de Persoonsgegevens niet onrechtmatig zijn en geen inbreuk maken op enig recht van een derde.
2. Een beschrijving van de verwerkingsactiviteiten, de verwerkingsdoelen, de subverwerkers die verwerker met instemming verwerkingsverantwoordelijke kan inschakelen, de verwerkte persoonsgegevens, de locaties van de verwerkingen en de bewaartermijnen zijn opgenomen in bijlage 1.

Artikel 4. Verplichtingen Verwerker

1. Verwerker verwerkt de Persoonsgegevens slechts in opdracht van de Verwerkingsverantwoordelijke en zal alle redelijke instructies van Verwerkingsverantwoordelijke dienaangaande opvolgen.
2. Verwerkingsverantwoordelijke geeft verwerker toestemming om in het kader van de uitvoering van de Overeenkomst en deze Verwerkersovereenkomst gebruik te maken van de diensten van sub-verwerkers gevestigd binnen de Europese Unie.
3. Verwerker treft technische en organisatorische beveiligingsmaatregelen om de Persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. De beveiligingsmaatregelen bieden, rekening houdend met de stand van de techniek en de kosten van tenuitvoerlegging van de beveiligingsmaatregelen een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van de Persoonsgegevens met zich meebrengen.
4. Indien er bij Verwerker – of bij een door hem ingeschakelde derde partij (sub verwerker) – sprake is van een beveiligingsincident en/of datalek als bedoeld in de AVG, zal Verwerker dit altijd onverwijld aan Verwerkingsverantwoordelijke melden. Daarbij geeft hij tevens aan:
 - a. Wat de oorzaak is van het beveiligingsincident/datalek;
 - b. Wat de mogelijke gevolgen zijn van het beveiligingsincident/datalek;
 - c. Op welke manier door Verwerker maatregelen zullen worden genomen om deze gevolgen te beperken.
5. In het geval dat een Betrokkene een verzoek tot inzage, of tot verbetering, aanvulling, wijziging of afscherming richt aan Verwerker, zal Verwerker het verzoek doorzetten naar Verwerkingsverantwoordelijke, en zal Verwerkingsverantwoordelijke het verzoek verder afhandelen. Verwerker geeft hierbij op verzoek en op kosten van Verwerkingsverantwoordelijke haar medewerking. Verwerker mag de Betrokkene van deze afspraak op de hoogte stellen.
6. Partijen stellen de ander onverwijld op de hoogte van relevante wijzigingen in de Verwerkingsprocessen.
7. Verwerker zal de persoonsgegevens niet verwerken in of zonder toestemming van verwerkingsverantwoordelijke doorgeven aan subverwerkers gevestigd in landen buiten de Europese Unie. Voor de subverwerkers genoemd in bijlage 1 wordt de toestemming geacht te zijn gegeven.

Artikel 5. Audits

1. Verwerkingsverantwoordelijke heeft het recht om maximaal één keer per jaar een audit uit te voeren ter controle van de afspraken onder deze Verwerkersovereenkomst.

2. Verwerker zal de voor de audits benodigde ondersteunende gegevens zoals systeemlogs bewaren.
3. De personen die de audit uitvoeren zullen zich conformeren aan de beveiligingsprocedures zoals die bij Verwerker van kracht zijn.
4. Verwerker zal aan de audit meewerken en alle voor de audit redelijkerwijs relevante informatie zo tijdig mogelijk ter beschikking stellen.
5. Alle kosten van een audit worden door Verwerkingsverantwoordelijke gedragen. Verwerker kan alle door haar gemaakte kosten doorbelasten aan Verwerkingsverantwoordelijke.
6. Verwerkingsverantwoordelijke zal niet eerder aanvangen met een audit dan één maand na voorafgaande schriftelijke aankondiging. Indien datum en tijdstip van de audit Verwerker niet gelegen komt, zullen Partijen een nieuwe datum vaststellen in goed overleg.

Artikel 6. Aansprakelijkheid

1. Partijen zijn ieder verantwoordelijk en aansprakelijk voor hun eigen handelen.
2. Verwerker vrijwaart Verwerkingsverantwoordelijke en stelt de Verwerkingsverantwoordelijke schadeloos voor alle claims, acties, aanspraken van derden, alsmede boetes van de Autoriteit Persoonsgegevens, die rechtstreeks voortvloeien uit een toerekenbare tekortkoming door verwerker en/of diens subverwerkers in de nakoming van zijn verplichtingen onder deze Verwerkersovereenkomst en/of enige schending door Verwerker en/of subverwerkers van de van toepassing zijnde wetgeving op het gebied van verwerking van persoonsgegevens.
3. Verwerkingsverantwoordelijke vrijwaart verwerker en stelt de verwerker schadeloos voor alle claims, acties, aanspraken van derden, alsmede boetes van de Autoriteit Persoonsgegevens, die rechtstreeks voortvloeien uit een toerekenbare tekortkoming door verwerkingsverantwoordelijke in de nakoming van zijn verplichtingen onder deze Verwerkersovereenkomst en/of enige schending door Verwerkingsverantwoordelijke van de van toepassing zijnde wetgeving op het gebied van verwerking van persoonsgegevens.

Artikel 7. Eigendomsrechten

1. Alle industriële of intellectuele eigendomsrechten met betrekking tot de onder deze Verwerkersovereenkomst te verwerken of verwerkte Persoonsgegevens berusten te allen tijde bij de Verwerkingsverantwoordelijke.

Artikel 8. Toepasselijk recht en geschillenoplossing

1. Op deze Verwerkersovereenkomst is uitsluitend Nederlands recht van toepassing.
2. Alvorens een beroep te doen op de rechter zijn Partijen verplicht zich optimaal in te spannen om het geschil in onderling overleg te beslechten.
3. Tenzij de wet daarvan dwingend afwijkt, wordt uitsluitend de bevoegde rechter binnen het arrondissement van de vestigingsplaats van Verwerker aangewezen om van geschillen kennis te nemen.

Artikel 9. Geheimhouding

1. Personen in dienst van, dan wel werkzaam ten behoeve van de verwerker, zijn verplicht tot geheimhouding met betrekking tot de persoonsgegevens waarvan zij kennis kunnen nemen, behoudens voor zover een bij, of krachtens de wet gegeven voorschrift tot verstrekking verplicht. De medewerkers van de verwerker tekenen hiertoe een geheimhoudingsverklaring.
2. Indien de verwerker op grond van een wettelijke verplichting gegevens dient te verstrekken, zal de verwerker de grondslag van het verzoek en de identiteit van de verzoeker verifiëren en zal de verwerker de verwerkingsverantwoordelijke onmiddellijk voorafgaand aan de verstrekking, ter zake informeren, tenzij wettelijke bepalingen dit verbieden.



Aldus besproken, in tweevoud opgemaakt, ondertekend en op iedere pagina geparafeerd te Schiphol op 19 november 2018.

Verwerkingverantwoordelijke

Stichting Airport Coordination Netherlands

Schiphol, 19 november 2018

A large black rectangular box redacting the signature of the responsible person.

De heer

A black rectangular box redacting the name of the responsible person.

Verwerker

100% Oegstgeest B.V.

Leiden, 10 mei 2018

A black rectangular box redacting the signature of the processor.

A black rectangular box redacting the name of the processor.

A black rectangular box redacting the title of the processor.

A black rectangular box redacting the title of the processor.



BIJLAGE 1# De gegevens die verwerkt worden

- a. Beschrijving verwerkingsactiviteiten door Verwerker:
 - 1. Analyse van website statistieken
 - 2. Updaten van de WordPress installatie voor de website
 - 3. Contactformulier website
- b. Verwerkingsdoelen:
 - 1. Betere functionaliteit van de website
 - 2. Veiligheid en back up
 - 3. Informatie aanvraag back up bestand (de gegevens komen tevens in de mailbox aan van de verwerkingsverantwoordelijke)
- c. Sub verwerkers:
 - 1. Google
 - 2. Webstack
- d. Verwerkte Persoonsgegevens:
 - 1. IP Adres
 - 2. WP Gebruikersnaam
 - 3. NAW gegevens
- e. Locatie verwerkingen:
 - 1. Bij 100% Leiden (te Leiden)
 - 2. Bij Webstack (te Alphen aan de Rijn)
 - 3. Bij Google
- f. Bewaartermijn:
 - 1. 2 jaar
 - 2. 1 jaar
 - 3. 1 jaar

Verwerkersovereenkomst Mirage ICT Services B.V.

Ondergetekenden:

Stichting Airport Coordination, gevestigd te Schiphol, hierna te noemen "eigenaar", hierbij vertegenwoordigd door: de heer [REDACTED]

En

Mirage ICT Services B.V., gevestigd te Amsterdam Zuid-Oost, hierna te noemen als "leverancier", Mirage ICT Services wordt hierbij vertegenwoordigd door de heer [REDACTED]

Hierna gezamenlijk te noemen als "partijen".

Overwegende dat:

- A. Partijen afspraken rondom uitwisseling van (persoons) gegevens in deze verwerkersovereenkomst willen vastleggen.

Verklaren te zijn overeengekomen als volgt:

Artikel 1. Definities

- 1.1 **Persoonsgegevens**; elk gegeven betreffende of het herleidbaar tot een geïdentificeerd of identificeerbaar natuurlijk persoon;
- 1.2 **Gegevens**; alle andere gegevens (data) niet zijnde persoonsgegevens;
- 1.3 **Betrokkene**; degene op wie de persoonsgegevens betrekking hebben.;
- 1.4 **ICT-Oplossing**; de door leverancier geboden dienst;
- 1.5 **Verwerkersovereenkomst**; deze overeenkomst tussen eigenaar en leverancier;
- 1.6 **Overeenkomst**; overeenkomst tussen leverancier en eigenaar betrekking hebbend op de door leverancier aan eigenaar geleverde dienst(en);
- 1.7 **Verwerken**; elk soort handeling (of deel daarvan) met betrekking tot persoonsgegevens);
- 1.8 **AVG**; Algemene Verordening Gegevensbescherming.

Artikel 2. Verantwoordelijkheid verwerkersovereenkomst

- 2.1 Eigenaar is verantwoordelijk ten aanzien van de aan leverancier verstrekte en te verstrekken (persoons)gegevens. Leverancier handelt als verwerker in opdracht van de eigenaar en verwerkt de (persoons)gegevens slechts in opdracht van de eigenaar of wettelijke regelgeving.
- 2.2 Leverancier zal de ontvangen (persoons)gegevens uitsluitend verwerken ten behoeve van de levering van de geboden ICT-oplossingen aan de eigenaar.

2.3 Alle (intellectuele) eigendommen, auteursrecht en databankenrecht inbegrepen, op de geleverde (persoons)gegevens blijven te allen tijde berusten bij de eigenaar (dan wel de betrokkene).

2.4 Partijen komen de AVG na. Voor zover de afspraken tussen partijen niet voorzien in wettelijke vereiste regelingen, komen partijen overeen te handelen in overeenstemming met de toepasselijke wet- en regelgeving op het gebied van bescherming van persoonsgegevens (volgens het Nederlandse Wetboek).

Artikel 3. Looptijd verwerkersovereenkomst

3.1 Deze verwerkersovereenkomst eindigt op het moment dat Leverancier geen persoonsgegevens meer onder zich heeft die zij in het kader van de tussen partijen gesloten overeenkomst verwerkt.

3.2 Na tussentijds beëindiging van deze verwerkersovereenkomst, blijven bepalingen in deze overeenkomst van toepassing tot einde overeenkomst.

3.3 Na beëindiging van de overeenkomst, en/of na beëindiging van de dienstverlening aan eigenaar, is leverancier gehouden om binnen 30 dagen na beëindiging de door leverancier verstrekte (persoons)gegevens terug te geven (dan wel om eigenaar in de gelegenheid te stellen deze gegeven digitaal te verkrijgen). Eventuele resterende (kopieën van) (persoons)gegevens en/of back-ups dienen daarop door de leverancier te worden vernietigd.

3.4 Leverancier zal een kopie van (persoons)gegevens bewaren als leverancier hiertoe verplicht is op grond van wet- of (beroeps)regelgeving.

3.5 De kosten van het verzamelen en overdragen van persoonsgegevens bij het eindigen van de onderliggende opdracht zijn voor de rekening van de eigenaar. Datzelfde geldt voor de kosten van de vernietiging van de persoonsgegevens. Als eigenaar daarom vraagt dan zal leverancier daar een kosteninschatting voor geven.

3.6 Artikel 5 van deze overeenkomst blijft gelden, ook nadat de overeenkomst is beëindigd.

Artikel 4. Beveiliging

4.1 Leverancier zal zorgdragen voor passende technische en organisatorische maatregelen om (persoons)gegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. De te nemen maatregelen sluiten aan bij de stand van de techniek en kosten van de tenuitvoerlegging.

4.2 De veiligheidsmaatregelen bieden een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen.

4.3 De veiligheidsmaatregelen zijn adequaat en voldoen aan de relevante standaarden en kwaliteitseisen conform de overeenkomst tussen beide partijen.

4.4 Leverancier is verantwoordelijk voor het regelen van adequaat beveiligde toegang tot de (persoons)gegevens door de eigenaar.

4.5 Eigenaar heeft het recht om in overleg met leverancier de door leverancier genomen technische en organisatorische (beveiligingen)maatregelen – op kosten van de eigenaar te (laten) toetsen door een daartoe gecertificeerd en onafhankelijk auditor. Beide partijen zullen de uitkomsten van deze audit ter beschikking krijgen.

4.6 Uitkomsten van de audit dienen door beide partijen te worden gebruikt om de veiligheid te vergroten van risicofactoren.

4.7 Leverancier stelt eigenaar omgaand op de hoogte over ieder veiligheidsincident.

4.8 Er zijn veiligheidsmaatregelen door de leverancier getroffen. Echter kan leverancier niet garanderen dat deze maatregelen onder alle omstandigheden doeltreffend zijn.

Artikel 5. Geheimhouding en vertrouwelijkheid

5.1 Op leverancier rust een wettelijke geheimhoudingsverplichting. Leverancier is gehouden de ontvangen gegevens als vertrouwelijk te behandelen.

5.2 Leverancier verplicht zijn (oud) werknemers en/of sub verwerker tot geheimhouding met betrekking tot alle (persoons)gegevens.

5.3 De verstrekte (persoons)gegevens worden door leverancier niet zonder voorafgaande toestemming van eigenaar aan derden ter beschikking gesteld, tenzij leverancier daartoe krachtens enige wetsbepaling, voorschrift of andere regelgeving verplicht is, of indien de bekendmaking en/of verstrekking in het kader van dienstverlening noodzakelijk is.

5.4 Voor zover leverancier (persoons)gegevens aan andere dan eigenaar levert, zal leverancier met deze derde gelijksoortige bepalingen als deze overeenkomst overeenkomen.

5.5 Leverancier zal zijn volledige medewerking verlenen in geval dat een betrokkene zijn rechten uitoefent op grond van wetgeving.

5.6 Leverancier zal Eigenaar terstond op de hoogte stellen van iedere kennisneming, verstrekking of andere vorm van verwerken van persoonsgegevens indien een betrokkene zijn rechten uitoefent.

5.7 Leverancier zorgt ervoor dat het personeel van leverancier alleen toegang heeft tot (persoons)gegevens als dit bedoeld is ten behoeve van zijn of haar werkzaamheden.

5.8 Leverancier kan derden (sub-verwerkers) inschakelen voor het uitvoeren van bepaalde werkzaamheden, bijvoorbeeld als deze derden over specialistische kennis of middelen beschikt. Verwerking mag niet zonder toestemming van eigenaar plaatsvinden door een sub-verwerker buiten de Europese Economische Ruimte.

Leverancier zal met de sub-verwerker gelijksoortige bepalingen als deze overeenkomst overeenkomen.

5.9 Leverancier is niet aansprakelijk voor (persoons)gegevens die door eigenaar worden opgeslagen op de hardware die is geleverd en/of ter beschikking is gesteld door de leverancier.

Artikel 6. Aansprakelijkheid

6.1 Leverancier is verantwoordelijk voor schade of nadeel, voortvloeiende uit het niet-nakomen van deze verwerkersovereenkomst, voorschriften bij of krachtens wet- en regelgeving aangaande de technische bescherming van (persoons)gegevens, voor zover de schade of het nadeel is ontstaan door de werkzaamheid van de leverancier voor de eigenaar. De leverancier vrijwaart de eigenaar voor de kosten van juridische procedures en boetes door de fouten van de leverancier. Dit artikel is niet van toepassing wanneer er sprake is van overmacht.

6.2 Leverancier is gehouden tot het (onmiddellijk) beperken van schade en/of voorkomen van verder nadeel van betrokkene en/of eigenaar.

6.3 Leverancier is niet aansprakelijk voor de schade die het gevolg is van het door eigenaar niet naleven van de wetgeving persoonsgegevens, of andere wet- of regelgeving. Eigenaar vrijwaart leverancier voor aanspraken van derden op grond van zulke schade. De vrijwaring geldt niet alleen voor de schade die derden hebben geleden (materieel maar ook immaterieel), maar ook voor de kosten die leverancier en eigenaar hebben moeten maken in de juridische procedure, zoals bijvoorbeeld griffierechten en kosten voor een advocaat en eventuele boetes die de eigenaar worden opgelegd. De aansprakelijkheid van eigenaar is niet van toepassing wanneer er sprake is van overmacht.

Artikel 7. Verwerking

7.1 De verwerking vindt plaats onder de verantwoordelijkheid van de eigenaar. Leverancier heeft geen zeggenschap over het doel en de middelen van de verwerking en neemt geen beslissingen over zaken als het gebruik van (Persoons)gegevens, de bewaartermijn van de te verwerken (persoons)gegevens en het verstrekken van (persoons)gegevens aan derden.

7.2 De leverancier is verantwoordelijk voor het duidelijk vastleggen hoe (persoons)gegevens worden verwerkt.

7.3 Als leverancier wordt verzocht (persoons)gegevens ter beschikking te stellen dan doet leverancier dat alleen als het verzoek is gedaan door een daartoe bevoegde instantie. Als er geen strafrechtelijke of andere juridische belemmeringen zijn, dan stelt leverancier de eigenaar op de hoogte van het verzoek. Leverancier probeert dat op korte termijn te doen, zodat het voor de eigenaar mogelijk is om eventuele rechtsmiddelen tegen de verstrekking van (persoons)gegevens in te stellen.

7.4 Persoonsgegevens die worden verwerkt door Leverancier kan worden opgevraagd door de eigenaar.

7.5 Technische en organisatorische maatregelen t.b.v. (persoons)gegevens worden inzichtelijk gemaakt door Leverancier. Met deze maatregelen wordt er getracht verlies en/of onrechtmatige verwerking van (persoons)gegevens tegen te gaan.

7.6 Leverancier stelt Eigenaar onverwijld op de hoogte van alle (geplande) permanente of tijdelijke doorgiften van Persoonsgegevens naar een land buiten de Europese Economische Ruimte (E.E.R.) en zal pas uitvoering geven aan een dergelijke (geplande) doorgifte na schriftelijke toestemming van Verantwoordelijke, aan welke toestemming Verantwoordelijke voorwaarden kan stellen.

Artikel 8. Datalekken en andere beveiligingsincidenten

8.1 Indien er een data lek bekend is bij leverancier stelt de leverancier de eigenaar daar volgens het data lek protocol van op de hoogte. Leverancier voorziet in de informatie die redelijkerwijs nodig is om een juiste melding te maken in het kader van de meldplicht datalekken. Data lekken worden binnen 24 uur na het ontdekken bekend gemaakt bij de eigenaar.

8.2 De melding van datalekken aan de Autoriteit Persoonsgegevens en (eventueel) betrokkene(n) is altijd de verantwoordelijkheid van de eigenaar.

Artikel 9. Algemeen

9.1 Bepalingen in de algemene voorwaarden, overeenkomsten of (mondelinge) afspraken tussen partijen, met betrekking tot de bescherming van de verstrekte (persoons)gegevens, die afwijken van hetgeen in deze verwerkersovereenkomst is geregeld, zijn niet van toepassing.

9.2 Het is voor beide partijen, behalve als partijen gezamenlijk schriftelijke anders afspreken, niet toegestaan om deze overeenkomst en de rechten en plichten die samenhangen met deze overeenkomst over te dragen aan een ander.

9.3 Aanvullingen en wijzigingen op deze overeenkomst zijn alleen geldig als ze op schrift zijn gesteld. Onder schriftelijk worden ook wijzigingen begrepen die per e-mail zijn gecommuniceerd, gevolgd door een akkoord per e-mail van de andere partij.

9.4 Op deze overeenkomst is Nederlands recht van toepassing, de Nederlandse rechter is bevoegd kennis te nemen van alle geschillen die voortvloeien uit of samenhangen met deze overeenkomst.

9.5 Deze overeenkomst is hoger in rang dan andere door beide partijen gesloten overeenkomsten. Als eigenaar algemene voorwaarden gebruikt dan zijn deze niet van toepassing op deze overeenkomst. De bepalingen uit deze overeenkomst gaan boven de bepalingen in algemene voorwaarden van leverancier, tenzij er expliciet naar een bepaling in de algemene voorwaarden wordt verwezen.

9.6 Als één of meerdere bepalingen in deze overeenkomst niet geldig blijken te zijn, dan heeft dit geen gevolgen voor de geldigheid van de andere bepalingen in deze overeenkomst. Leverancier treedt dan met eigenaar in overleg om gezamenlijk een nieuwe bepaling op te stellen. Deze bepaling zal zoveel als mogelijk in de geest zijn van de ongeldige bepaling, maar dan uiteraard zo vormgegeven dat de bepaling wel geldig is.

9.7 De in deze overeenkomst genoemde voorbeelden dienen ter verduidelijking van de in de overeenkomst opgenomen regeling en zijn geen limitatieve opsomming.

Aldus overeengekomen, in tweevoud en ondertekend

Eigenaar: SACN

Leverancier: Mirage

Naam:

Naam:

Functie:

Functie:

Datum:

20-11-2018

Datum: 24-5-2018

Instructie melding datalekken ACNL

Deze instructie beschrijft de procedure die binnen ACNL moet worden gevolgd bij een datalek. De instructie is gebaseerd op de regels van de Algemene verordening gegevensbescherming (Avg).

Achtergrond

De Avg regelt ten aanzien van datalekken het volgende:

- De Avg spreekt van “inbreuk in verband met persoonsgegevens” en definieert dit als: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens.
Datalekken kunnen dus door diverse oorzaken ontstaan, bijvoorbeeld door moedwillig handelen (cybercriminaliteit), technisch falen, menselijke fouten (verlies, verkeerd verzenden van informatie) of calamiteiten (brand).
- Degene die verantwoordelijk is voor de gegevens (de verwerkingsverantwoordelijke), moet melding doen van een datalek bij de Autoriteit Persoonsgegevens (AP). Dit betekent dat ACNL ook de melding moet doen als er bij het bedrijf dat de salarisadministratie voor ACNL doet, een datalek is in gegevens van ACNL.
- De melding aan AP moet binnen 72 uur nadat kennis is genomen van het datalek, gedaan worden.
- De melding aan AP kan achterwege blijven indien niet waarschijnlijk is dat de inbreuk tot een risico heeft geleid voor de rechten en vrijheden van een natuurlijk persoon.
- ACNL moet de datalekken documenteren (register datalekken).
- Wanneer de inbreuk waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van een natuurlijk persoon, moet deze persoon (de betrokkene) over de inbreuk geïnformeerd worden.
- In enkele gevallen kan worden afgezien van mededeling aan de betrokkene, bijvoorbeeld als er maatregelen zijn getroffen waardoor er geen risico's meer zijn voor de betrokkene.

Werkwijze ACNL

- Iedere medewerker is gehouden om een datalek waarvan hij/zij kennis neemt, per omgaande te melden aan de managing director (md).
- De md onderzoekt de melding /draagt er zorg voor dat de melding wordt onderzocht op in ieder geval op de volgende aspecten :
 - Aard van het datalek (wat voor gegevens zijn verloren gegaan en van wie);
 - Periode dat er een datalek was;
 - Wat is de oorzaak;
 - Is er sprake van niet-nakomen van of een tekortkoming in de procedures;
 - Wat kan er gedaan worden om de gevolgen van het datalek te beperken.
- De md is verantwoordelijk voor de beoordeling of de AP moet worden geïnformeerd over het datalek en voor het zo nodig doen van de melding (binnen 72 uur).

- Indien er melding aan de AP moet worden gedaan, gebeurt dit via het meldloket datalekken: <https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0>
- De md is verantwoordelijk voor de beoordeling of de betrokkene moet worden geïnformeerd over het datalek en voor het zo nodig informeren van de betrokkene (“onverwijld”).
- De md draagt zorg voor het (laten) opnemen van het lek in het register datalekken.
- De md draagt zorg voor het (laten) ondernemen van herstelacties, aanpassing van procedures etc.

Register verwerkingen persoonsgegevens ACNL

Verwerkingsverantwoordelijke:

Airport Coordination Netherlands
The Base, Toren A
Evert van Beekstraat 1-23
1118 CL Schiphol

Functionaris gegevensverwerking

	naam verwerking	doel verwerking	betrokkenen	gegevens	Ontvangers	bewaartermijn	verwerkersovereenkomst
Personeel en beheer							
	Werving en selectie	Werving en selectie van kandidaten voor een vacature	Kandidaten die reageren op vacature	N.a.w. E-mail correspondentie CV-gegevens Motivatiefbrief	Managing Director Office Manager Extern wervingsbureau Medewerkers betrokken bij werving kandidaat	4 weken na afwijzing	
	Bezwaar en beroep personeel	Behandeling bezwaar- en beroepschriften personeelsleden	Personen in dienst ACNL	N.a.w. E-mailadres	Managing Director Huisadvocaat	5 jaar na afhandeling	
	Dossier kopie ID-bewijzen	Uitvoering wet ID-plicht	Personen in dienst ACNL	Kopie ID-bewijs	Managing director Office Manager	5 jaar na uitdiensttreding	
	Verlofregistratie	Registratie verlofuren	Personen in dienst ACNL	Naam Verlofuren	Managing Director Office Manager Medewerkers (ieder voor eigen registratie)	2 jaar	
	Website ACNL	Publiceren informatie over ACNL	Personen in dienst ACNL	Naam Foto Functie	Een ieder die website ACNL raadpleegt 100%Leiden	Na uitdiensttreding worden gegevens verwijderd	100% Leiden
	Personeelsdossiers	Berekenen en vaststellen salaris, vergoedingen, belastingen, premies t.b.v. personeelslid, personeelsmanagement, begeleiding ziekteverzuim, evaluatie functioneren, ontwikkeling personeel, jubilea, bijzonder verlof	Personen in dienst ACNL	N.a.w., telefoon-nummer, kopie ID, geb. datum, geb. plaats, BSN, opleidingen, cursussen, diploma's, verslagen, arbeidsovereenkomst, beoordelingsgesprekken, ziekteverzuim, nevenfuncties, VOG,	Managing Director Office Manager Ieder personeelslid voor zijn eigen gegevens; voor zover voor het doel geautoriseerd: belastingdienst UWV Arbodienst HR-accountant	7 jaar	

				klachten, waarschuwingen			
	Salarisadministratie	Berekenen salaris en vergoedingen	Personeel in dienst ACNL	n.a.w. BSN betalingsgegevens	Salarisverwerker, UWV, belastingdienst, ABP	7 jaar na jaarafsluiting van salarisadministratie	Crop Registeraccountants
	Bestand contactpersonen calamiteiten personeelsleden	Informeren/alarmeren contactpersonen bij calamiteiten rond personeelsleden	Personen in dienst ACNL, aangemelde contactpersonen	Naam, telefoonnummer	Alle medewerkers ACNL	Na uitdiensttreding	
Financiële administratie							
	Inkoop: offerteaanvraag en opdrachtverlening	Aanvragen van offertes voor producten en diensten	Aanbieders van offerte	Bedrijfsgegevens, contactgegevens	Managing Director Office Manager Medewerker(s) ACNL betrokken bij offerte- traject	Opdrachten: 7 jaar na beëindiging overeenkomst	
	Relatiebeheer crediteuren- debiteuren	Voeren financiële administratie	Debiteuren/crediteuren	N.a.w. E-mail Bankrekeningnummer,	Managing Director Office Manager Accountant	7 jaar na uitbetaling	
	Declaraties	Uitbetalen diverse declaraties personeelsleden (kosten gemaakt tijdens dienstreizen, aankopen t.b.v. ACNL etc.)	Personeelsleden ACNL	N.a.w. E-mail bankrekeningnummer gegevens aankopen/uitgaven, reisgegevens	Managing Director, Office Manager, Medewerkers ACNL (ieder voor eigen declaraties)	7 jaar	
Juridische zaken							
	Bezwaar, beroep en klachtbehandeling	Voeren wettelijke procedures t.a.v. bezwaar, beroep, klachten	Reclamanten en appellanten	Naam E-mail In enkele gevallen n.a.w./IBAN derdenrekening	Medewerkers ACNL Rechtbank, Advocatenbureau (zowel van appellanten als huisadvocaat), ingeschakelde deskundigen	5 jaar	
	WOO	Communicatie met WOO- indiener/verzoeker	Indieners WOO, personen die voorkomen in WOO opgevraagd document.	N.a.w. E-mailadressen	Behandelaar WOO, Medewerkers ACNL, indiener WOO Advocatenbureau	5 jaar	
Primair proces							
	Registratie/identificatie personen airlines	Toegang tot aanvragen slots	Personen werkzaam bij airlines die slots willen aanvragen	Naam E-mailadres	Slotcoördinatoren	5 jaar	
	Slot-proces behandeling,	Behandelen aanvragen slots	Aanvragers slots	Naam E-mailadres	Slotcoördinatoren, RTM, EIN.	5 jaar	

	aanvragen, wijzigingen etc.						
	Slot-proces monitoring	Monitoring	Airlines betreffende NOOPS en NORECS	Naam E-mailadres	Slotcoördinatoren	5 jaar	
	Slot-proces- wachtlĳst	Registratie belangstelling voor slots	Geïnteresseerde airlines	Naam E-mailadres	Slotcoördinatoren	5 jaar	
	Communicatiebestan den	Contactpersonen ACNL	Stakeholders, externe contacten	Naam E-mailadres Adres Telefoonnummers	Managing Director Medewerkers ACNL	Verwijdering na wijziging van het contact	
	Nieuwsberichten ACNL	Informatievoorziening	Mensen die zich hebben aangemeld voor de nieuwsbrief	E-mailadressen	██████████ ██████████ 100%Leiden	Op verzoek (unsubscribe)	100% Leiden