

VERWERKERSOVEREENKOMST behorende bij Integraal Parkeerbeheer

Ondergetekenden:

1. **Eindhoven Airport N.V.** gevestigd en kantoorhoudende te Eindhoven aan de Luchthavenweg 13, 5657 EA, ingeschreven in het handelsregister te Eindhoven onder nummer: 17051407, te dezen rechtsgeldig vertegenwoordigd door R.A.J. Hellemons, algemeen directeur (CEO) en M.P.J. van den Bogaard, Chief Operations Officer (COO), hierna te noemen “**EANV**”

en

2. **<Naam bedrijf + rechtsvorm>** gevestigd te **<plaats>** aan de **<adres>**, **<postcode>**, ingeschreven in het handelsregister te **<plaats>** onder nummer: **<KvK-nummer>**¹, te dezen rechtsgeldig vertegenwoordigd door **<naam>** in de functie van **<functie>**, hierna te noemen “**Verwerker**”,

EANV en Verwerker gezamenlijk aan te duiden als “**Partijen**”,

OVERWEGINGEN:

- I. EANV heeft met Verwerker één of meer overeenkomsten gesloten tot het leveren van (diverse) diensten door Verwerker aan EANV of zal een dergelijke overeenkomst sluiten. Deze overeenkomst(en) wordt/worden hierna als de “**Hoofdovereenkomst**” aangeduid en is nader gespecificeerd in de titel van deze verwerkersovereenkomst.
- II. Verwerker zal bij het uitvoeren van de Hoofdovereenkomst gegevens verwerken waarvoor EANV de verantwoordelijke is en blijft. Tot die gegevens behoren persoonsgegevens in de zin van de Algemene Verordening Gegevensbescherming (EU 2016/679), hierna “**AVG**”.
- III. Partijen wensen, gelet op het bepaalde in artikel 28 lid 3 en lid 4, de voorwaarden van de verwerking van deze persoonsgegevens in deze verwerkersovereenkomst vast te leggen.

KOMEN HIERBIJ OVEREEN:

¹ Alleen te gebruiken bij Nederlandse bedrijven anders deze bijzin weghalen

1. Onderwerp van deze Verwerkersovereenkomst

- 1.1 Deze Verwerkersovereenkomst (hierna: “**Verwerkersovereenkomst**”) is alleen van toepassing op de verwerking van persoonsgegevens in het kader van de Hoofdovereenkomst.
- 1.2 Begrippen als “Verwerken”, “Persoonsgegevens”, “Verwerkingsverantwoordelijke”, “Verwerker” en “Betrokkene” hebben de betekenis die daaraan is gegeven in de AVG.
- 1.3 Het kan zijn dat Verwerker gedurende de uitvoering van de Hoofdovereenkomst met EANV persoonsgegevens verwerkt namens EANV (hierna: de “**Persoonsgegevens**”). Een overzicht van de categorieën Persoonsgegevens en doeleinden waarvoor de Persoonsgegevens worden verwerkt zijn uiteengezet in Bijlage 1.

2. Verwerkingsverantwoordelijke en Verwerker

- 2.1 EANV kwalificeert op grond van het toepasselijke recht als de verantwoordelijke partij, de Verwerkingsverantwoordelijke, voor het verwerken van de Persoonsgegevens. Verwerker is door EANV aangesteld en stemt in met het verwerken van Persoonsgegevens namens Verwerkingsverantwoordelijke.
- 2.2 Verwerker garandeert dat zij de Persoonsgegevens uitsluitend zal verwerken op basis van schriftelijke instructie(s) van EANV en op een wijze die – en voor zover dit – noodzakelijk is voor de levering van de diensten uit hoofde van de Hoofdovereenkomst, behalve wanneer dit noodzakelijk is om te voldoen aan een op Verwerker rustende wettelijke verplichting of voor het opvolgen van instructies van EANV. In geen geval verwerkt Verwerker de Persoonsgegevens voor eigen doeleinden.
- 2.3 Indien Verwerker in strijd met de AVG en deze Verwerkersovereenkomst de doeleinden en middelen voor de verwerking van de Persoonsgegevens bepaalt dan wordt Verwerker (voor dat deel van de verwerking) als Verwerkingsverantwoordelijke beschouwd.
- 2.4 In het bijzonder kan EANV instructies geven ten aanzien van de bewaartermijn van ieder van de Persoonsgegevens genoemd in Bijlage 1 en ten aanzien van het corrigeren, anonimiseren, blokkeren, verwijderen of anderszins verwerken van de Persoonsgegevens. Verwerker verleent alle redelijke bijstand, teneinde EANV in staat te stellen te voldoen aan haar wettelijke verplichtingen, in geval een Betrokkene zijn of haar rechten inroept op grond van het toepasselijke recht, waaronder de AVG.
- 2.5 Partijen sluiten de Hoofdovereenkomst om te profiteren van de expertise van Verwerker in de context van de Hoofdovereenkomst en het verwerken van Persoonsgegevens voor de

doeleinden uiteengezet in Bijlage 1. Het is Verwerker toegestaan om naar eigen inzicht de middelen aan te wenden die hij noodzakelijk acht om die doeleinden na te streven.

3. Vertrouwelijkheid

- 3.1 Onverminderd de bestaande contractuele regelingen tussen de Partijen, garandeert Verwerker dat zij alle Persoonsgegevens als strikt vertrouwelijk zal behandelen en dat zij al haar werknemers, vertegenwoordigers en/of door EANV goedgekeurde door Verwerker ingeschakelde Verwerkers (hierna: “**Sub-Verwerkers**”) en eventuele derden van deze Sub-Verwerkers die betrokken zijn bij de verwerking van de Persoonsgegevens, van de vertrouwelijke aard van de Persoonsgegevens op de hoogte zal stellen.
- 3.2 Verwerker zal waarborgen dat dergelijke personen en partijen daartoe een adequate Sub-Verwerkersovereenkomst hebben getekend, zoals nader bepaald in artikel 8. Verwerker zal EANV op diens verzoek van kopieën van deze overeenkomst(en) voorzien.
- 3.3 Partijen zullen alle informatie die Verwerker aan EANV moet verstrekken uit hoofde van artikel 4 van deze Verwerkersovereenkomst als strikt vertrouwelijk behandelen.

4. Beveiliging

- 4.1. Onverminderd de beveiligingsnormen die Partijen (eventueel) in de Hoofdovereenkomst overeen zijn gekomen, zal Verwerker passende technische en organisatorische maatregelen nemen ter beveiliging van de verwerking van de Persoonsgegevens, een en ander nader bepaald in Bijlage 2. Deze maatregelen omvatten in ieder geval, onverminderd het bepaalde in artikel 28 lid 3 en artikel 32 van de AVG:
 - a. maatregelen om te waarborgen dat enkel bevoegd personeel toegang heeft tot de Persoonsgegevens voor de doeleinden die uiteen zijn gezet in Bijlage 1 van deze Verwerkersovereenkomst;
 - b. maatregelen om de Persoonsgegevens te beschermen tegen onopzettelijke of onrechtmatige vernietiging, onopzettelijk verlies of wijziging, onbevoegde of onrechtmatige opslag, Verwerking, toegang tot of openbaarmaking van de Persoonsgegevens;
 - c. maatregelen om (dreigende) inbreuken op de beveiliging te identificeren ten aanzien van de verwerking van Persoonsgegevens in de systemen die worden ingezet voor het verlenen van diensten aan EANV;
 - d. de maatregelen die Partijen in Bijlage 2 zijn overeengekomen.

- 4.2. Verwerker zal de door haar getroffen beveiligingsmaatregelen regelmatig en in ieder geval eenmaal per jaar controleren. Verwerker zal op verzoek van EANV aantonen welke maatregelen zij heeft genomen op basis van artikel 4.1, zal EANV toestaan om dergelijke maatregelen te auditen en testen en zal als gevolg van de bevindingen uit deze audits en testen haar beveiligingsbeleid aanpassen overeenkomstig nadere, schriftelijke instructies van EANV in de context van toepasselijke privacy regelgeving, waaronder mede begrepen maar niet beperkt tot artikel 28 lid 5 van de AVG. Als alternatief kan EANV gebruik maken van een verklaring van een onafhankelijke externe deskundige, die een oordeel geeft over de maatregelen die Verwerker heeft getroffen (Third Party Mededeling).
- 4.3. Verwerker zal alle redelijke medewerking verlenen aan bedoelde audits en testen, waaronder in ieder geval dient te worden begrepen: het verlenen van toegang tot gebouwen en databases en het ter beschikking stellen van alle relevante informatie.
- 4.4. Indien blijkt uit een audit en/of test, dat Verwerker in gebreke is met betrekking tot nakoming van zijn verplichtingen uit hoofde van deze Verwerkersovereenkomst, draagt Verwerker zowel zijn eigen kosten, als ook de kosten van EANV, gemaakt in het kader van de audit en/of de test, een en ander onverlet de overige (wettelijke) rechten van EANV.

5. Verbeteringen van de beveiliging

- 5.1. Partijen erkennen dat beveiligingseisen voortdurend veranderen en dat een effectieve beveiliging frequente evaluaties en regelmatige verbetering van verouderde beveiligingsmaatregelen vereist. Verwerker zal daarom de maatregelen zoals geïmplementeerd op grond van artikel 4 voortdurend evalueren en verscherpen, aanvullen of verbeteren om te blijven voldoen aan de eisen van artikel 4.
- 5.2. EANV heeft het recht om Verwerker te instrueren om aanvullende beveiligingsmaatregelen te nemen. Verwerker zal deze aanvullende beveiligingsmaatregelen binnen redelijke termijn (in beginsel: binnen 4 weken) implementeren. Indien een wijziging van de Hoofdovereenkomst vereist is om een dergelijke instructie op te volgen, zullen Partijen een wijziging van de Hoofdovereenkomst overeenkomen.

6. Gegevensverkeer

- 6.1. Verwerker stelt EANV onverwijld op de hoogte van alle (geplande) permanente of tijdelijke doorgiftes van Persoonsgegevens naar een land buiten de Europese Economische Ruimte²

² Dit zijn de EU landen + Noorwegen, Liechtenstein, IJsland

zonder een passend beschermingsniveau (zoals bedoeld in artikel 44 van de AVG) en zal pas uitvoering geven aan een dergelijke (geplande) doorgifte na schriftelijke toestemming van EANV.

7. Informatieplichten en incidentenmanagement

- 7.1 Verwerker stelt EANV onverwijld – in ieder geval binnen 24 uur nadat de Verwerker daarmee bekend is geraakt – op de hoogte van privacyverzoeken en incidenten met betrekking tot de verwerking van de Persoonsgegevens. Verwerker zal EANV te allen tijde de aan haar door EANV gevraagde medewerking verlenen en zal de schriftelijke instructies van EANV ten aanzien van een dergelijk privacyverzoek en/of incident opvolgen, met als doel om EANV in staat te stellen een deugdelijk onderzoek te verrichten naar (aanleiding van) het privacyverzoek en/of incident, een correcte respons te formuleren en passende vervolgstappen te nemen ten aanzien van het privacyverzoek en/of incident. Tevens is hetgeen bepaald in artikel 10 van deze Verwerkersovereenkomst, inzake aansprakelijkheid en vrijwaring, ook hier van toepassing.
- 7.2 Onder een “privacyverzoek” in artikel 7.1 wordt in ieder geval het volgende verstaan: een klacht of (informatie)verzoek of ieder ander verzoek aangaande zijn rechten zoals opgenomen in de AVG van een Betrokkene of ander natuurlijk persoon met betrekking tot de verwerking van de Persoonsgegevens door Verwerker.
- 7.3 Onder een “incident” in artikel 7.1 wordt in ieder geval het volgende verstaan:
- a. een onderzoek naar of beslaglegging door overheidsfunctionarissen van de Persoonsgegevens, of een vermoeden dat zulks gaat plaatsvinden;
 - b. iedere ongeautoriseerde of onopzettelijke toegang, verwerking, verwijdering, verlies of enige vorm van onrechtmatige verwerking van de Persoonsgegevens;
 - c. een doorbreking van de beveiliging en/of vertrouwelijkheid, zoals uiteengezet in artikel 3 en 4 van deze Verwerkersovereenkomst, die leidt tot onopzettelijke of onrechtmatige vernietiging, verlies, wijziging, onbevoegde openbaarmaking van – of toegang tot – de Persoonsgegevens, of enige aanwijzing dat een dergelijke inbreuk zal plaatsvinden of heeft plaatsgevonden.
- 7.4 Verwerker zal te allen tijde actuele en schriftelijke procedures voorhanden hebben die haar in staat stellen om EANV van een onmiddellijke reactie over een incident te voorzien en om effectief samen te werken met EANV om het incident af te handelen. Verwerker zal EANV voorzien van een exemplaar van dergelijke procedures indien EANV daar schriftelijk om verzoekt.

7.5 Een melding aan de ICT Servicedesk dient ten minste de volgende (beschikbare) informatie te bevatten: **ICT Servicedesk**

Tel: +31 (0) 88 - 0043010

e-mail: privacy@eindhovenairport.nl

De ICT Servicedesk is gedurende werktijden (maandag t/m vrijdag van 08.30 uur tot 17.00 uur) telefonisch bereikbaar. Bij geen gehoor, dient met hoge prioriteit gemaild te worden naar privacy@eindhovenairport.nl.

Een melding aan de ICT Servicedesk dient ten minste de volgende (beschikbare) informatie te bevatten:

- de begin- en eindtijd, de begin- en einddatum en de locatie van de gebeurtenis;
- de aard en de omvang van de gebeurtenis;
- de afdeling of gedeelte van het systeem, waar de gebeurtenis zich voordeed;
- de tijd, benodigd om de schade door het incident vast te stellen;
- de aard en omvang van de getroffen Persoonsgegevens;
- soort en (inschatting van) aantal getroffen Betrokkenen;
- de te verwachten gevolgen, met inbegrip van de gevolgen voor Betrokkenen en een voorstel om schade en andere negatieve gevolgen te voorkomen;
- getroffen en nog te treffen maatregelen om gevolgen van het incident te mitigeren; én
- de naam en contactgegevens van de functionaris gegevensbescherming of ander contactpersoon, waar additionele informatie betreffende het incident kan worden verkregen.

7.6 Het is Verwerker niet toegestaan om, op eigen initiatief betrokkenen die (mogelijk) zijn getroffen door het incident en/of de bevoegde autoriteit, bijvoorbeeld de Autoriteit Persoonsgegevens, in kennis te stellen van het incident.

8. Inschakelen van Sub-Verwerkers

8.1 Verwerker zal haar activiteiten die (deels) bestaan uit het verwerken van de Persoonsgegevens niet uitbesteden aan (een) Sub-Verwerker(s) zonder voorafgaande, schriftelijke toestemming van EANV.

- 8.2 Niettegenstaande de toestemming van EANV, zoals bedoeld in het vorige lid, zal Verwerker volledig aansprakelijk blijven jegens EANV voor de gevolgen van het uitbesteden aan (een) Sub-Verwerker(s) in overeenstemming met artikel 10.
- 8.3 De toestemming van EANV op grond van artikel 8.1 laat onverlet dat voor de inzet van Sub-Verwerkers en hun eventuele derden (inclusief internationale organisaties) in een land buiten de Europese Economische Ruimte zonder passend beschermingsniveau ook toestemming vereist is op grond van artikel 6.
- 8.4 De Verwerker bewerkstelligt dat de Sub-Verwerker(s) en eventuele door de Sub-Verwerker ingeschakelde derde(n) gebonden is/zijn aan de verplichtingen die op de Verwerker rusten uit hoofde van deze Verwerkersovereenkomst en ziet toe op naleving daarvan.

9. Teruggave of vernietiging van de Persoonsgegevens

- 9.1 Bij beëindiging van deze Verwerkersovereenkomst, of op schriftelijk verzoek van EANV, zal Verwerker de Persoonsgegevens onverwijld vernietigen of teruggeven aan EANV, naar keuze van EANV. EANV kan een schriftelijke bevestiging van de vernietiging van Persoonsgegevens opvragen bij Verwerker.
- 9.2 Verwerker zal alle Sub-Verwerkers en overige derden die betrokken zijn bij het verwerken van de Persoonsgegevens op de hoogte stellen van de beëindiging van de Verwerkersovereenkomst en zal waarborgen dat alle betrokken derden de Persoonsgegevens vernietigen of aan EANV overdragen, naar keuze van EANV.

10. Aansprakelijkheid en vrijwaring

- 10.1 Partijen vrijwaren elkaar en stellen elkaar schadeloos voor alle claims, acties en aanspraken van derden voor verliezen, schade, boetes of kosten die aan de zijde van de andere Partij vallen en die rechtstreeks of indirect voortvloeien uit of tot stand komen in verband met een tekortkoming in de nakoming van deze Verwerkersovereenkomst door een Partij. Onder 'schade' wordt begrepen, maar is niet beperkt tot, de kosten die voor EANV gemoeid zijn in verband met het opnieuw samenstellen van bestanden van verloren of (ten onrechte) vernietigde Persoonsgegevens, bijvoorbeeld als gevolg van een incident.
- 10.2 EANV vrijwaart Verwerker niet voor verliezen, schade, boetes of kosten die aan de zijde van Verwerker vallen en die voortvloeien uit of tot stand komen in verband met een verwerking van Persoonsgegevens door Verwerker die niet in overeenstemming is met de rechtmatige instructies van EANV.

11. Duur en beëindiging

11.1 Deze Verwerkersovereenkomst treedt in werking op de ingangsdatum van de Hoofdovereenkomst en eindigt automatisch op het moment dat de Hoofdovereenkomst wordt beëindigd of afloopt. Ingeval van (al dan niet stilzwijgende) verlenging van de Hoofdovereenkomst blijft deze Verwerkersovereenkomst van kracht voor de duur van de verlengingsperiode. Indien deze Verwerkersovereenkomst na een periode van drie (3) jaar nog geldend is, is EANV bevoegd de voorwaarden, waaronder begrepen maar niet beperkt tot, de technische en organisatorische maatregelen ter beveiliging van de verwerking van de Persoonsgegevens opnieuw te beoordelen en aan te passen. Aanpassing van de voornoemde voorwaarden zal geschieden in goed overleg met Verwerker.

11.2 Het beëindigen of aflopen van deze Verwerkersovereenkomst zal Verwerker niet ontslaan van haar vertrouwelijkheidsverplichtingen ingevolge artikel 3 en verplichtingen tot teruggave of vernietiging van de Persoonsgegevens ingevolge artikel 9.

12. Overige bepalingen

12.1 In het geval dat er een tegenstrijdigheid is tussen de bepalingen uit deze Verwerkersovereenkomst en de bepalingen van de Hoofdovereenkomst, dan zullen de bepalingen van deze Verwerkersovereenkomst leidend zijn.

12.2 Deze Verwerkersovereenkomst omvat de algehele overeenstemming tussen Partijen met betrekking tot de verwerking van Persoonsgegevens, zoals gespecificeerd in Bijlage 1 en komt in de plaats van eventueel eerdere mondelinge en/of schriftelijke afspraken tussen Partijen in dit kader.

12.3 In het geval er sprake is van doorgiftes naar landen buiten de Europese Economische Ruimte zonder een passend beschermingsniveau, waarvoor EANV toestemming heeft verleend dan zullen de bepalingen van de Standard Contractual Clauses leidend zijn.

12.4 Wijzigingen van deze Verwerkersovereenkomst zijn uitsluitend geldig indien deze tussen Partijen schriftelijk zijn overeengekomen.

12.5 Op deze Verwerkersovereenkomst is Nederlands recht van toepassing.³ Geschillen over of in verband met deze Verwerkersovereenkomst vallen onder de exclusieve rechtsmacht van de bevoegde rechter in het Arrondissement Oost-Brabant.

³ Als Nederlands recht niet haalbaar is in de onderhandeling dan in ieder geval recht van een ander EU lidstaat.

namens EANV

Naam: R.A.J. Hellemons Naam: M.P.J. van den Bogaard.....

Functie: Algemeen directeur (CEO) Functie: Chief Operations Officer (COO)

Datum: Datum:

Handtekening: Handtekening:

namens Verwerker

Naam:

Functie:

Datum:

Handtekening:

Bijlage 1

Overzicht van de categorieën Persoonsgegevens en de doeleinden waarvoor de Persoonsgegevens worden verwerkt:

Categorie(ën) Persoonsgegevens⁴:

Doeleinde(n)⁵:

Bewaartermijn(en)⁶:

Contactgegevens DPO/privacy officer van Verwerker:

Naam:

E-mail:

Telefoonnummer:

⁴ De proceseigenaar van EANV (zonodig i.o.m. de Verwerker) dient hier een categorie in te vullen (naam, NAW, e-mail, inloggegevens, kenteken, etc.).

Wanneer er sprake is van meerdere categorieën en doeleinden dan die apart eronder benoemen (Categorie: namen, emailadressen, inloggegevens. Doeleinde beheer softwaresysteem waarin deze gegevens voorkomen; Categorie personeelsgegevens, Doeleinde in opdracht uitvoeren van salarisadministratie, etc.)

In de Privacy Risk Assessment staat ook vermeld welke persoonsgegevens het betreft.

⁵ Hier dient de proceseigenaar van EANV de doeleinde in te vullen (b.v. uitoefenen van een beheertaak / leveren van de Dienst / etc.)

⁶ De proceseigenaar dient hier de bewaartermijn van de persoonsgegevens te vermelden. Hoe lang zijn persoonsgegevens nodig voor het vastgestelde doel? In beginsel geldt dat zodra het doel is bereikt, de persoonsgegevens verwijderd moeten worden, tenzij een wettelijke bewaartermijn van toepassing is.

Bijlage 2⁷**1. Beheersen informatiebeveiligingsrisico's**

De Verwerker is verantwoordelijk voor het managen van alle informatiebeveiligingsrisico's die zich kunnen voordoen in het kader van de uitvoering van de opdracht en de verwerking van Persoonsgegevens door de Verwerker, zijn medewerkers en eventuele door hem ingeschakelde derden (waaronder onderaannemers, toeleveranciers, adviseurs). In dit kader zal de Verwerker proactief alle informatiebeveiligingsrisico's identificeren, beperkende c.q. mitigerende maatregelen treffen en evalueren (hierna gezamenlijk: de “**Beveiligingsmaatregelen**”). Verwerker zal, indien EANV hierom verzoekt, aantonen dat adequate Beveiligingsmaatregelen getroffen zijn.

2. Training medewerkers en door Verwerker ingeschakelde derden

Verwerker draagt er zorg voor dat ieder van de bij de uitvoering van de opdracht en de verwerking van Persoonsgegevens betrokken medewerkers en eventuele door hem ingeschakelde derden de juiste training op het gebied van informatiebeveiliging hebben ontvangen in het kader van hun functie en gelet op de verantwoordelijkheden bij het verrichten van de werkzaamheden in het kader van de opdracht en de verwerking van Persoonsgegevens. Om aan deze verplichting te kunnen voldoen, verzorgt Verwerker in ieder geval een security awareness programma, opleidingen en trainingsactiviteiten op basis van geldende good practices.

3. Audits en technische risk assessments

Verwerker dient minimaal éénmaal per jaar voor zijn eigen rekening en risico, een audit op de infrastructuur en de systemen, ten behoeve van de dienstverlening aan EANV uit te voeren, of te laten uitvoeren door een onafhankelijke derde partij. Verwerker voert correctieve acties uit op de bevindingen die geïdentificeerd worden naar aanleiding van dergelijke audits en/of technische risk assessments binnen de vastgestelde tijd. Verwerker stelt EANV op elk door EANV gewenst moment in de gelegenheid om audits uit te voeren, waaronder bijvoorbeeld, maar niet beperkt tot geautomatiseerde scans, PCI-scans, etc. Verwerker zal, indien EANV hierom verzoekt, inzage geven in rapportages van audits en/of assessments die niet ouder dan twee jaar zijn.

⁷ In deze bijlage staan de key security controls voor de beveiliging van (Persoons)gegevens. Let op: de inhoudt van de beveiligingsmaatregelen dient altijd goedgekeurd te worden door ICT. Neem daarom altijd contact op met afdeling ICT.

Niet alle eisen zijn in alle gevallen van toepassing op elke leverancier of dienst/product. In sommige gevallen kunnen bepaalde eisen achterwege gelaten worden. In andere gevallen kan het zo zijn dat er extra beveiligingsmaatregelen overeengekomen worden met een leverancier. Hier beslist ICT over.

4. Encryptie

Verwerker maakt gebruik van cryptografische bewerkingen om de (Persoons)gegevens die hij verwerkt te beveiligen. Er wordt encryptie (versleuteling) toegepast bij verzending van Persoonsgegevens via openbare en/of vanaf internet toegankelijke netwerken, bij de opslag van (Persoons)gegevens op (draagbare) apparatuur en op verwijderbare media, zoals usb-sticks en in andere situaties waar (Persoons)gegevens kwetsbaar zijn voor toegang door onbevoegden (bijvoorbeeld (Persoons)gegevens die via het world wide web kunnen worden benaderd). Voorbeelden van toegestane technologie zijn VPN's, SSH of HTTPS of een vergelijkbare technologie voor netwerkbeveiliging.

- a. Voor opslag van data is de Advanced Encryption Standard (AES) technologie met 256 bits sleutels of langer verplicht. Alle sleutels die hiervoor gebruikt worden moeten adequaat beheerd worden zodat ze niet toegankelijk zijn voor ongeautoriseerde en/of misbruikt worden.
- b. Bij het toepassen van een Internet website maakt Verwerker gebruik van HTTPS om het netwerkverkeer tussen de cliënt en de webserver onleesbaar te maken voor derden. Dit geldt in ieder geval als het gaat om gevoelige gegevens of Persoonsgegevens. Verwerker stelt EANV op elk door EANV gewenst moment in de gelegenheid om audits uit te voeren, waaronder bijvoorbeeld, maar niet beperkt tot Qualys SSL server test met minimaal een A score.
- c. Verwerker draagt er zorg voor dat zijn website gebruik maakt van een SSL/TLS certificaat dat is uitgegeven door een erkende publieke Certificate Authority (CA) zoals Digicert, VeriSign, e.d. Het certificaat zal voldoen aan de courante eisen van de CA/Browser Forum Baseline Requirements for Contents of Publicly Trusted SSL/TLS Certificates. Zogenaamde self-signed certificaten zijn niet toegestaan.

5. Beveiliging wachtwoorden

Verwerker zorgt ervoor dat wachtwoorden van alle accounts, zowel beheer al gebruikers, worden opgeslagen met een one-way-hash mechanisme zoals SHA-2 of SHA-3 met een "salt" toevoeging.

6. Samenstelling wachtwoorden

Verwerker zorgt ervoor dat alle wachtwoorden voor useraccounts sterk zijn (60 bit entropy) en tenminste voldoen aan de volgende eisen:

- i. minimaal 8 karakters en opgebouwd uit ten minste drie van de volgende categorieën: hoofdletters (A - Z), kleine letters (a - z), cijfers (0 - 9), speciaal karakter zo als ! # \$ ^ * - _ = ; : ' " () { } [] | ` @ % & ? / \ +; of
- ii. minimaal 14 karakters en opgebouwd uit ten minste twee van de volgende categorieën: hoofdletters (A - Z), kleine letters (a - z), speciaal karakter zo als ! # \$ ^ * - _ = ; : ' " () { } [] | ` @ % & ? / \ +

Deze wachtwoorden moeten na maximaal 92 dagen vervangen worden. Deze eis moet door de ICT-dienst van de Verwerker afgedwongen worden.

Wachtwoorden voor beheeraccounts die door de Verwerker gebruikt worden moeten heel sterk zijn en ten minste voldoen aan de volgende eisen: minimaal 15 karakters en opgebouwd uit ten minste drie van de volgende categorieën: hoofdletters (A - Z), kleine letters (a - z), cijfers (0 - 9), speciaal karakter zo als ! # \$ ^ * - _ = ; : ' " () { } [] | ` @ % & ? / \ +. Deze wachtwoorden moeten na maximaal 180 dagen vervangen worden.

7. Multi-factor authenticatie

Multi-factor-authenticatie technologie dient gebruikt te worden wanneer beheerders van de Verwerker op afstand toegang moeten hebben tot systemen waarop (Persoons)gegevens verwerkt worden of opgeslagen zijn.

8. Patching

De software die door Verwerker wordt ingezet (OS, Database en applicatiesoftware) is voorzien van alle bekende security patches zoals de Verwerker, leverancier, ontwikkelaar of programmeur van die software heeft uitgebracht en deze worden bij het uitkomen van de patches binnen 14 dagen aangebracht voor een Common Vulnerability Scoring System (CVSS) basis score van 7 of hoger.

9. Accountbeheer

Verwerker heeft formele procedures voor zowel het aanmaken, muteren en verwijderen van accounts. Met name het tijdig verwijderen van accounts uit de applicatie is van belang. Een account dat 90 dagen achtereenvolgend niet is gebruikt, wordt geautomatiseerd of op verzoek van EANV verwijderd binnen 5 werkdagen.

Indien door Verwerker een account wordt verwijderd dan dienen ook alle gerelateerde gegevens onherstelbaar te worden gewist, tenzij de werking van de applicatie daardoor verstoord wordt. In

dat laatste geval dient deze uitzondering afgestemd worden met de ICT Servicedesk (ict@eindhovenairport.nl). Verwerker verwijdert ook de gegevens uit de back-up.

Noot: het is toegestaan de gegevens maximaal 35 dagen te laten bestaan in de back-up.

10. Dataminimalisatie

Verwerker maakt gebruik van dataminimalisatie, waaronder wordt verstaan: het beperken van de verwerking van Persoonsgegevens tot alleen het hoogst noodzakelijke.

11. Retentie

Verwerker draagt er zorg voor dat gegevens tijdig en conform de overeengekomen retentietermijn(en) worden vernietigd.

12. Procedures voor behandeling van informatie-beveiligingsincidenten

De Verwerker heeft schriftelijke procedures voor het tijdig en doeltreffend behandelen van informatie-beveiligingsincidenten en gesignaleerde zwakke plekken in de beveiliging. De Verwerker heeft de verplichting geconstateerde informatiebeveiligings-incidenten en gesignaleerde zwakke plekken in de beveiliging direct te melden bij EANV.

13. Audit IT systeem

Bij de oplevering van het IT systeem dat de Persoonsgegevens bevat kan EANV een audit uit (laten) voeren om te controleren of deze IT middelen security technisch correct en conform bovenstaande eisen zijn ingericht. De Verwerker dient deze audit te faciliteren. Als alternatief kan door EANV gebruik worden gemaakt van een verklaring van een onafhankelijke externe deskundige, die een oordeel geeft over de maatregelen die Verwerker heeft getroffen, een Third Party Mededeling (TPM).

14. Wissen van data en apparatuur

Alle apparatuur van Verwerker die opslagmedia bevat, zoals laptops of smartphones, wordt door Verwerker ontdaan van de nog eventueel aanwezige (Persoons)gegevens, alvorens het apparaat te verwijderen of hergebruiken. De persoons- of andere gegevens moeten onherstelbaar worden gewist of, als de media niet onherstelbaar gewist kan worden (bijvoorbeeld bij SSD), dan moet de media onherstelbaar worden vernietigd.

Bijlage 3

Doorgiften naar landen buiten de Europese Economische Ruimte zonder een passend beschermingsniveau⁸, waarvoor EANV toestemming heeft verleend:

☒ Niet van toepassing⁹

☐ Van toepassing¹⁰

Landen(en):

Partijen komen ten behoeve van een legale doorgifte naar vermelde landen de hierna volgende Standard Contractual Clauses overeen.

⁸ Landen met een passend beschermingsniveau zijn: Andorra, Argentinië, Canada (**Let op: dit geldt alleen voor delen van Canada die vallen onder de Canadian Personal Information Protection and Electronic Documents Act. Onder meer Québec valt hier niet onder**), Faeröer Eilanden, Guernsey, Isle of Man, Israël, Jersey, Uruguay en Zwitserland. De Verenigde Staten alleen voor Passenger Name Record, Informatie van vliegtuigpassagiers doorgegeven aan de United States Bureau of Customs and Border Protection. Actuele info is te vinden op volgende site: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm of bij JBZ.

⁹ ☐ (keuzebox) vervangen door ☒ bij niet van toepassing. Bij Niet van Toepassing de volgende keuzebox open laten en de hierna volgende pagina's (Standard Contractual Clauses) verwijderen uit Bijlage 3.

¹⁰ ☐ (keuzebox) vervangen door ☒ en benoem het land/de landen; Standard Contractual Clauses in Bijlage 3 moeten worden ingevuld en ondertekend door partijen.