

**Overeenkomst tussen gezamenlijke verwerkingsverantwoordelijken VOOR DE VERWERKING VAN
PERSOONSgegevens IN HET KADER VAN HET VASTGOEDINFORMATIEPLATFORM**

TUSSEN:

- (1) Het agentschap Justitie en Handhaving, zijnde een intern verzelfstandigd agentschap zonder rechtspersoonlijkheid, vertegenwoordigd door leidend ambtenaar Bob Van den Broeck, administrateur-generaal, ingeschreven in het KBO met nummer 0316.380.841, waarvan de administratieve zetel zich bevindt te Simon Bolivarlaan 17, 1000 Brussel, hierna afgekort "AJH"

Contactgegevens: dpo.ajh@vlaanderen.be

EN

- (2) De naamloze vennootschap het Vlaams Datanutsbedrijf met merknaam Athumi, zijnde een privaatrechtelijk vormgegeven extern verzelfstandigd agentschap, vertegenwoordigd door CEO Björn De Vidts, ingeschreven in het KBO met nummer 0795.547.478, waarvan de administratieve zetel zich bevindt te Havenlaan 88 bus C, 1000 Brussel (hierna: het Vlaams Datanutsbedrijf)

Contactgegevens: privacy@athumi.eu;

Hierna elk afzonderlijk 'Partij' en gezamenlijk de 'Partijen' genoemd.

OVERWEGENDE DAT,

- A. Het Agentschap Justitie en Handhaving is een intern verzelfstandigd agentschap zonder rechtspersoonlijkheid en staat in voor de opdrachten, vermeld in artikel 4 van het besluit van de Vlaamse Regering van 3 september 2021 tot oprichting van het intern verzelfstandigd 'Agentschap Justitie en Handhaving', waaronder 8°: het algemeen Handhavingsbeleid op bestuurlijk en strafrechtelijk niveau ontwikkelen en coördineren, en de uitvoering van het kaderdecreet bestuurlijke handhaving implementeren.
- B. Het Vlaams Datanutsbedrijf met merknaam Athumi is een privaatrechtelijk vormgegeven extern verzelfstandigd agentschap van de Vlaamse overheid met onder meer de taak om platformen te ontwikkelen en beheren en diensten te verlenen die zorg dragen voor de veilige en gewaarborgde afhandeling van de transacties tussen de betrokken burgers, overheidsinstanties of aanvragers, dit overeenkomstig artikel 5, §1, 5° van het decreet van 2 december 2022 houdende machtiging tot oprichting van het privaatrechtelijk vormgegeven extern verzelfstandigd agentschap Vlaams Datanutsbedrijf in de vorm van een naamloze vennootschap.
- C. In dat kader biedt het Vlaams Datanutsbedrijf het Vastgoedinformatieplatform (hierna: VIP) aan waarbij ze de vastgoedinformatiestromen tussen overheid, bedrijven en burgers veilig en efficiënt organiseren.

- D. AJH treedt samen met het Vlaams Datanutsbedrijf op als Gezamenlijke Verwerkingsverantwoordelijke in de zin van artikel 26 van de Algemene Verordening Gegevensbescherming (hierna: AVG), voor het ter beschikkingstellen van producten, in overeenstemming met art. 7, 2°, b) van het Decreet van 22 december 2023 over het Vastgoedinformatieplatform (hierna: VIP-decreet). De nodige afspraken, onder meer met betrekking tot hun respectieve verantwoordelijkheid voor de nakoming van de verplichtingen uit hoofde van de AVG, met name met betrekking tot de uitoefening van de rechten van de Betrokkene en de transparantieplichting, worden geformaliseerd in de voorliggende overeenkomst tussen gezamenlijke verwerkingsverantwoordelijken (hierna: de Overeenkomst).
- E. De Partijen dienen, in overeenstemming met artikelen 26 en art. 28 van de AVG, hun afspraken met betrekking tot de uitvoering en organisatie van deze Verwerking van Persoonsgegevens te formaliseren in deze Overeenkomst voor de Verwerking van Persoonsgegevens.
- F. Gelet op de latere inwerkingtreding van het Besluit tot toevoeging van het product maatregelenregister voor overdracht en de geplande opstart op 1 april 2026 van het maatregelenregister voor de handhaving van de Vlaamse Codex Ruimtelijke Ordening zoals bepaald in artikel 6 van het besluit van 26 september 2025 van de Vlaamse Regering tot wijziging van het besluit van de Vlaamse Regering van 17 november 2023 over de digitalisering van de handhaving van diverse Vlaamse regelgeving, wat betreft de implementatie van het Kaderdecreet Vlaamse Handhaving van 14 juli 2023, zal het Vlaams Datanutsbedrijf optreden als Verwerker van het Agentschap Justitie en Handhaving tot de volledige inwerkingtreding van het Besluit. De modaliteiten van deze verwerkersopdracht worden omschreven in Bijlage 3. Vanaf de voorgenoemde inwerkingtreding zullen beide partijen optreden als Gezamenlijke Verwerkingsverantwoordelijken.

WERD OVEREENGEKOMEN WAT VOLGT:

1 DEFINITIES

Begrippen die in deze Overeenkomst met hoofdletter worden gebruikt, moeten worden geïnterpreteerd zoals in dit artikel of elders in de Overeenkomst gedefinieerd.

AVG	Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming);
Betrokkene	De geïdentificeerde of identificeerbare natuurlijke persoon op wie een Persoonsgegeven betrekking heeft zoals bepaald in artikel 4, (1) AVG;
Besluit tot toevoeging van het product maatregelenregister voor overdracht	Besluit van de Vlaamse Regering tot toevoeging van het product maatregelenregister voor overdracht op het Vastgoedinformatieplatform, in het kader van de

	informatieplichten, vermeld in artikel 83, §4 en §5, van het Kaderdecreet Vlaamse Handhaving van 14 juli 2023, en tot wijziging van het besluit van de Vlaamse Regering van 20 september 2024 houdende uitvoering van het decreet van 22 december 2023 over het Vastgoedinformatieplatform, wat betreft de retributies en de controle, schorsing en opheffing van de toegang tot het VIP en tot wijziging van diverse besluiten
EER	Europese Economische Ruimte;
Medewerker	Elke werknemer, agent, aannemer, werknemer in loondienst of elke andere persoon die onder rechtstreeks gezag van de Verwerker werkt;
Subverwerker	Elke derde die Persoonsgegevens Verwerkt in opdracht of onder toezicht van Verwerker, maar die niet onder het directe gezag van Verwerker valt;
Toepasselijke Gegevensbeschermingswetgeving	De AVG, de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, en alle wet- en regelgeving en sectorale aanbevelingen die regels bevatten voor de bescherming van de Betrokkenen met betrekking tot de Verwerking, met inbegrip van maar niet beperkt tot de veiligheidseisen voor en het vrije verkeer van Persoonsgegevens;
VIP-decreet	Decreet van 22 december 2023 over het Vastgoedinformatieplatform;
Vastgoedinformatieplatform of VIP	Een elektronisch informatiesysteem om vastgoedinformatie te ontsluiten, samen te voegen en ter beschikking te stellen, zoals bepaald in artikel 2, 20° VIP Decreet;
Inbreuk in verband met persoonsgegevens of Datalek	Een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt of kan leiden tot de vernietiging, het verlies of de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens;
Persoonsgegevens	Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon, zoals bepaald in artikel 4, 1) AVG, die verwerkt wordt;

Gezamenlijke Verwerkingsverantwoordelijken	De Partijen die, <i>in casu</i> , tot de vaststelling van de doeleinden van en de middelen voor de Verwerking van Persoonsgegevens bijdragen en zich, bijgevolg, zodanig beschouwen in de zin van artikel 26 van de AVG;
Unierechtelijke of lidstaatrechtelijke bepaling	Een bepaling opgelegd door de Unierechtelijke of (EU) lidstaatrechtelijke wetgeving;
Verwerken / Verwerking	Elke bewerking of 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, zoals ook gedefinieerd in artikel 4, 2) AVG;
Verwerkingsverantwoordelijke	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; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen;
Verwerker	Een natuurlijke persoon, een rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat namens de (Gezamenlijke) Verwerkingsverantwoordelijke Persoonsgegevens verwerkt;
Overeenkomst	Deze overeenkomst, die de afspraken tussen Partijen regelt in de in van artikelen 26 en 28 AVG, , waarin afspraken worden gemaakt ten aanzien van de Verwerking;

De begrippen van deze Overeenkomst moeten worden gelezen in het licht van het VIP-decreet.

De bepalingen in deze Overeenkomst moeten worden geïnterpreteerd in het licht van de Toepasselijke Gegevensbeschermingswetgeving. Indien deze wetgeving geen duidelijke en ondubbelzinnige interpretatie biedt, moet aan de begrippen de betekenis gegeven worden die de intentie van de Partijen zo dicht mogelijk benadert.

2 ALGEMENE BEPALINGEN

2.1 VOORWERP

De bepalingen inzake Gezamenlijke Verwerkingsverantwoordelijken in deze Overeenkomst gelden uitsluitend in het kader van het ter beschikking stellen van gegevens uit het maatregelenregister in de vorm van een product, zoals bedoeld in artikel 2, 17° VIP-decreet, via het Vastgoedinformatieplatform.

Partijen verbinden zich ertoe om de standaarden inzake informatieveiligheid en de wet- en regelgeving inzake de bescherming van natuurlijke personen bij de Verwerking van Persoonsgegevens na te leven, in het bijzonder de AVG.

Elke andere Verwerking anders dan noodzakelijk in het kader van de Overeenkomst is strikt verboden, met inbegrip van de doorgifte van Persoonsgegevens aan derden, een derde land of aan een internationale organisatie, behoudens uitdrukkelijke toestemming van alle Partijen.

2.2 GEPLANDE GEGEVENSSTROMEN

2.2.1 AANBIEDEN MAATREGELENREGISTER

Het Vlaams Datanutsbedrijf voegt, a.d.h.v. het VIP, gegevensstromen samen in een product¹ en stelt deze ter beschikking aan de ontvangende entiteiten die hier toegang toe mogen krijgen.

AJH neemt de rol op van aanleverende entiteit. Het Vlaams Datanutsbedrijf neemt hierbij de rol op van platformbeheerder, wat inhoudt dat de gegevensstromen via VIP gestroomlijnd worden volgens de VIP informatiestandaard.

Deze Overeenkomst richt zich enkel tot het product “maatregelenregister voor overdracht”. Het product bevat als informatie de gegevens zoals vermeld in artikel 82, eerste lid Kaderdecreet Vlaamse Handhaving (hierna: Kaderdecreet) .

De gegevens uit het maatregelenregister zullen conform artikel 83 Kaderdecreet ter beschikking gesteld worden aan instrumenterende ambtenaren en vastgoedmakelaars. De instrumenterende ambtenaren krijgen toegang tot de volledige inhoud van het product zoals vastgelegd in artikel 83, §4 Kaderdecreet. De vastgoedmakelaars krijgen, in lijn met artikel 83, §5 Kaderdecreet, slechts beperkt toegang tot de informatie in het product, met name:

- de beschrijving in tijd, ruimte en materialiteit van de te voorkomen of te herstellen publieke schade of misdrijven, inbreuken en normschendingen;
- de datum en type van de bestuursdocumenten aanwezig in het maatregelenregister, zonder de inhoud van het betreffende document.

Zoals bepaald in artikel 7, eerste lid VIP-decreet zal het Vlaams Datanutsbedrijf voorzien in een detailbeschrijving van welke velden in deze informatierubrieken gedeeld worden. Deze productcatalogus kan geraadpleegd worden op de publieke gebruikersomgeving van het VIP.

¹ Een product is een welbepaalde combinatie van vastgoedinformatie over één perceel, of een onderdeel ervan, die vooraf door het Vlaams Datanutsbedrijf is vastgelegd en die op aanvraag wordt ontsloten door de aanleverende entiteiten.

2.2.2 INNEN VAN RETRIBUTIES

Bij het aanvragen van het product dient de aanvrager een retributie te betalen, deze bestaat uit een platform retributie (artikel 19 VIP-decreet) en een bronretributie (artikel 83, §6, tweede lid Kaderdecreet, en artikel 5 Besluit tot toevoeging van het product maatregelenregister voor overdracht). Het Vlaams Datanutsbedrijf staat in voor het innen van beide retributies tijdens het verwerken van aanvraag van de aanvrager. Vervolgens maakt het Vlaams Datanutsbedrijf de bronretributie over aan AJH.

2.3 NALEVING WETGEVING

Partijen verbinden zich ertoe om de Toepasselijke Gegevensbeschermingswetgeving na te leven.

Indien een Partij van oordeel is dat een of meerdere Verwerkingen waarvoor Partijen gezamenlijk verantwoordelijk zijn, niet of niet meer in overeenstemming zijn met Toepasselijke Gegevensbeschermingswetgeving, licht ze de andere Partijen daarover in. Elke Partij zal hieromtrent advies vragen aan hun functionaris voor gegevensbescherming (DPO) en vervolgens gezamenlijk beslissen of deze Verwerkingen al dan niet tijdelijk of permanent dienen te worden stopgezet.

2.4 TRANSPARANTIE

Partijen informeren de Betrokkenen over de Verwerking en het gebruik van hun Persoonsgegevens overeenkomstig de artikelen 12, 13 en 14 AVG.

Partijen zijn elk verantwoordelijk voor het opstellen, bijwerken en eventueel corrigeren van hun privacyverklaring waarin informatie verschaft wordt aan de betrokkene met betrekking tot de Verwerking van Persoonsgegevens.

De Betrokkene zal in duidelijke en begrijpbare taal over zijn rechten worden geïnformeerd alsook over de manier waarop hij die op laagdrempelige wijze kan uitoefenen. De informatie zal gemakkelijk toegankelijk zijn via de privacyverklaring die op het Vastgoedinformatieplatform geplaatst wordt.

2.5 BEWAARTERMIJNEN

De meegedeelde gegevens zullen door de Partijen op het VIP gedurende een periode van maximaal één jaar bewaard worden. De gegevens worden niet langer bewaard dan noodzakelijk.

Het product "maatregelenregister voor overdracht" dient tot één jaar na aflevering nog consulteerbaar te zijn voor aanvragers op het VIP.

2.6 UITOEFENING RECHTEN VAN BETROKKENEN

Partijen communiceren op een duidelijke en eenvoudige wijze met de Betrokkenen overeenkomstig artikel 12 AVG.

Partijen spreken af dat de contacten met de Betrokkenen verlopen zoals hiernavolgend uiteengezet. Het Vlaams Datanutsbedrijf neemt de coördinatie van de uitoefening van de rechten van betrokkenen voor zijn rekening. Indien blijkt dat het verzoek betrekking heeft op Persoonsgegevens die de onder de bevoegdheid van AJH vallen, maakt het Vlaams Datanutsbedrijf het verzoek zo snel mogelijk over aan AJH.

Indien een Betrokkene rechtstreeks contact opneemt met AJH om zijn individuele rechten uit te oefenen, zal AJH het verzoek overmaken aan het Vlaams Datanutsbedrijf. Het Vlaams Datanutsbedrijf zal in voorkomend geval de samenwerking tussen Partijen coördineren om op het verzoek te antwoorden. In geval er acties ondernomen moeten worden door een (Sub)Verwerker, zal het Vlaams Datanutsbedrijf daarvoor afstemmen met de betrokken (Sub)Verwerker.

2.7 CONTACTEN MET DERDEN

Partijen spreken af dat de contacten met derden in het kader van de Verwerking van Persoonsgegevens in eerste instantie verlopen via het Vlaams Datanutsbedrijf, die de coördinatie van de activiteiten voor haar rekening neemt. Indien blijkt dat het concreet gaat over de Verwerking van Persoonsgegevens die behoren tot de bevoegdheid van een andere Partij, maakt het Vlaams Datanutsbedrijf de vraag of het verzoek binnen redelijke termijn over aan de andere Partij.

2.8 RELATIES MET EN AANDUIDING VAN VERWERKERS

Partijen komen overeen dat de relaties met de Verwerker(s) die instaan voor de concrete uitvoering van de Verwerkingen in het kader van het VIP, in eerste instantie toekomen aan het Vlaams Datanutsbedrijf.

Het Vlaams Datanutsbedrijf gaat namens alle Partijen na of de Verwerker de passende technische en organisatorische maatregelen neemt om de Verwerking te beveiligen.

Het Vlaams Datanutsbedrijf waakt er over dat de Verwerker enkel Subverwerkers aanstelt om Persoonsgegevens in het kader van VIP te verwerken na uitdrukkelijke, specifieke goedkeuring van het Vlaams Datanutsbedrijf.

2.9 MACHTIGINGEN EN PROTOCOLLEN

Partijen spreken af dat in geval een machtiging aangevraagd moet worden of een protocol afgesloten moet worden, het (DPO-team van het) Vlaams Datanutsbedrijf optreedt als coördinator en facilitator van de werkzaamheden, met dien verstaande dat alle Partijen bij de procedure betrokken worden. Het Vlaams Datanutsbedrijf is als coördinator en facilitator bevoegd de machtigingsaanvragen en protocollen te onderhandelen en te ondertekenen.

Zoals bepaald in artikel 83, §6, eerste lid Kaderdecreet zal het Vlaams Datanutsbedrijf protocollen afsluiten met de Federatie van Notarissen en het Beroepsinstituut van Vastgoedmakelaars voorafgaand het beschikbaar stellen van het product.

2.10 HET VERRICHTEN VAN EEN GEGEVENSBESCHERMINGSEFFECTBEOORDELING

De Verwerking door de Partijen die valt onder deze Overeenkomst, vergt het opstellen van een gegevensbeschermingseffectbeoordeling conform artikel 35 AVG. Deze wordt verricht door alle Partijen gezamenlijk, zij het dat de Partijen, vanuit overwegingen inzake efficiëntie, overeenkomen dat het Vlaams Datanutsbedrijf hierbij het initiatief neemt. Als zodanig kan het Vlaams Datanutsbedrijf de risico's die zich kunnen stellen als gevolg van de Verwerking, identificeren en omschrijven, alsook, aan de Verwerker de maatregelen voorstellen en opleggen die nodig zijn om die risico's te beheren en te beheersen.

Indien noodzakelijk, ondersteunt de andere Partij het Vlaams Datanutsbedrijf met het opmaken van een gegevensbeschermingseffectbeoordeling, waar mogelijk, door het overhandigen van de technische en organisatorische maatregelen waar zij over beschikken.

Conform artikel 36 AVG zullen Partijen de toezichthoudende autoriteit voorafgaand raadplegen indien uit de gegevensbeschermingseffectbeoordeling blijkt dat de Verwerking een hoog risico zou opleveren.

2.11 WERKWIJZE BIJ EEN DATALEK

Partijen verbinden zich ertoe om elkaar zonder onredelijke vertraging op de hoogte te stellen van elke Inbreuk in verband met persoonsgegevens die impact heeft op de andere Partij of op beide Partijen. In voorkomend geval verschaffen de Partijen elkaar alle informatie die ze nuttig of nodig achten om de beveiligingsmaatregelen te optimaliseren en die nodig is om een eventuele melding bij de toezichthoudende autoriteit of aan de Betrokkenen in orde te brengen (in overeenstemming met de artikelen 33 en 34 van de AVG).

Deze informatie bevat minstens volgende elementen:

- De aard van het Datalek, waar mogelijk onder vermelding van de categorieën van Betrokkenen en persoonsgegevensregisters in kwestie en, bij benadering, het aantal Betrokkenen en persoonsgegevensregisters in kwestie;
- De naam en de contactgegevens van de DPO of een ander contactpunt waar meer informatie kan worden verkregen;
- De waarschijnlijke gevolgen van de inbreuk in verband met Persoonsgegevens;
- De maatregelen die de Partij heeft voorgesteld of genomen om de Inbreuk in verband met persoonsgegevens aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.

Het Vlaams Datanutsbedrijf, zal zonder onredelijke vertraging, en indien mogelijk uiterlijk 72 uur, na het vaststellen van een Inbreuk in Verband met Persoonsgegevens een melding doen bij de toezichthoudende autoriteit in overeenstemming met artikel 33 van de AVG. Het Vlaams Datanutsbedrijf zal AJH onmiddellijk op de hoogte stellen van de melding aan de toezichthoudende autoriteit.

Alle Partijen zullen samenwerken met de toezichthoudende autoriteit in verband met eventuele verzoeken om informatie en assistentie in verband met deze melding.

Het Vlaams Datanutsbedrijf meldt eveneens, indien nodig, het Datalek ook aan de Betrokkenen overeenkomstig artikel 34 van de AVG. De Partijen zullen samenwerken om de nodige informatie tijdig aan de Betrokkenen te verstrekken.

2.12 CONTACTEN MET TOEZICHTHOUDERS

De contacten met de toezichthoudende autoriteit verlopen in eerste instantie via de DPO van het Vlaams Datanutsbedrijf.

Betreft het een vraag of verzoek in het kader van de opvolging van een klacht die door de Betrokkene bij de toezichthoudende autoriteit is ingediend, wordt de vraag of het verzoek voor overleg overgemaakt aan de Partij tegen wie de klacht is ingediend.

Betreft het een vraag of een verzoek in het kader van het beheer van het VIP-platform, wordt de vraag of het verzoek behandeld door het Vlaams Datanutsbedrijf. In voorkomend geval verschaft AJH op vraag van het Vlaams Datanutsbedrijf alle informatie die ze nuttig of nodig acht om de vraag of het verzoek te behandelen.

2.13 VERTROUWELIJKHEID

De Partijen verbinden zich er uitdrukkelijk toe het vertrouwelijk karakter en de beveiliging van de Persoonsgegevens die zij in het kader van deze Overeenkomst verwerken, te waarborgen.

De Partijen waken erover dat alle Medewerker(s) of aangestelde(n) die toegang hebben tot de Persoonsgegevens, contractueel en/of statutair tot vertrouwelijkheid gebonden zijn.

De Partijen zien erop toe dat Medewerker(s) of aangestelde(n) enkel toegang verkrijgen tot Persoonsgegevens verwerkt in het Vastgoedinformatieplatform op basis van het noodzakelijkheidsbeginsel ("*need-to-know*"-principe).

De Partijen voorkomen dat door middel van functie- en rollenscheiding een combinatie van toegangsrechten zou kunnen leiden tot ongeautoriseerde handelingen of niet-toegelaten toegang tot Persoonsgegevens door Medewerker(s) of aangestelde(n).

De verplichting tot vertrouwelijkheid blijft gelden na beëindiging van de Overeenkomst.

2.14 TECHNISCHE EN ORGANISATORISCHE MAATREGELEN

Partijen nemen elk voor de Verwerking waarvoor zij verantwoordelijk zijn gepaste technische en organisatorische maatregelen in overeenstemming met artikel 32 van de AVG om de Persoonsgegevens en de Verwerking ervan te beveiligen tegen vernietiging, verlies, vervalsing, niet toegelaten verspreiding of toegang en elke andere vorm van onrechtmatige Verwerking.

Partijen komen overeen dat het Vlaams Datanutsbedrijf als operationeel beheerder verantwoordelijk is voor de uitvoering van de technische en organisatorische maatregelen op het VIP en de ondersteunende infrastructuur. De specifieke maatregelen die genomen moeten worden, zijn opgenomen in Bijlage 2 die aan deze Overeenkomst is toegevoegd.

Op éénvoudig verzoek van één van de Partijen, bezorgen de andere Partijen extra verduidelijking over de technische en organisatorische maatregelen aan de desbetreffende DPO.

De Partijen zullen minstens eenmaal per jaar de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de Verwerking, testen, beoordelen en evalueren. Indien nodig zullen de technische en organisatorische maatregelen worden geactualiseerd.

2.15 PLAATS VAN DE VERWERKING EN DOORGIFTE

Partijen komen overeen dat de Verwerkingen van de Persoonsgegevens enkel binnen de EER zal gebeuren. Het Vlaams Datanutsbedrijf neemt de taak op zich om daarover te waken jegens de (Sub)Verwerker(s).

2.16 AANSPRAKELIJKHEID

Partijen zijn elk aansprakelijk voor de schade die het gevolg is van inbreuken op de AVG door de Verwerking die zij uitvoeren in het kader van deze Overeenkomst.

De aansprakelijkheid van Partijen is beperkt zoals voorzien in de verwerkingsopdracht, zonder evenwel afbreuk te doen aan artikel 82 van de AVG.

2.17 CONTACT

Elke Partij duidt een contactpunt aan voor de aangelegenheden met betrekking tot de Verwerking van Persoonsgegevens in het kader van deze Overeenkomst (hierna: de "SPOC"). Wanneer een SPOC gedurende de looptijd van deze Overeenkomst zou wijzigen, moet dit gemeld worden aan de Partijen, zonder dat evenwel aanpassing van deze Overeenkomst noodzakelijk is. De contactgegevens van de contactpunten worden opgenomen in Bijlage 1 van deze Overeenkomst.

2.18 INWERKINGTREDING

De Overeenkomst treedt in werking na ondertekening door beide Partijen.

2.19 DUUR

De Overeenkomst is van onbepaalde duur.

2.20 TOEPASSELIJK RECHT EN BEVOEGDE RECHTBANK

In geval van betwisting is het Belgische recht van toepassing en zijn de hoven en rechtbanken van het gerechtelijk arrondissement Brussel, bevoegd.

2.21 DEELBAARHEID

Indien een bepaling van deze Overeenkomst geheel of gedeeltelijk ongeldig of niet-afdwingbaar wordt geacht, wordt deze (voor zover deze ongeldig of niet-afdwingbaar is) als scheidbaar beschouwd en wordt de geldigheid van de andere bepalingen van deze Overeenkomst niet aangetast.

De Partijen zullen vervolgens te goeder trouw onderhandelen om de ongeldige, onwettige of nietige bepaling te vervangen door een geldige bepaling die zoveel als mogelijk de gevolgen heeft van de ongeldige, onwettige of nietige bepaling.

2.22 ENIGE OVEREENKOMST EN WIJZIGINGEN

De Overeenkomst omvat de volledige afspraken tussen de Partijen met betrekking tot het onderwerp en de beoogde verplichtingen in deze Overeenkomst, en vervangt hierbij alle eerdere afspraken, voorstellen, onderhandelingen, overeenkomsten, toezeggingen en verklaringen, hetzij mondeling hetzij schriftelijk.

De bepalingen van onderhavige Overeenkomst kunnen uitsluitend bij een door vertegenwoordigingsbevoegde personen van beide Partijen ondertekend geschrift worden aangepast, gewijzigd, aangevuld of ingeperkt. De aanpassingen, wijzigingen, aanvullingen of inperkingen treden slechts in werking vanaf de datum van ondertekening ervan, tenzij wanneer anders uitdrukkelijk en schriftelijk wordt overeengekomen.

Deze Overeenkomst werd elektronisch opgesteld en ondertekend.

Voor het Vlaams Datanutsbedrijf

Voor het Agentschap Justitie en
Handhaving

Ps

Björn De Vidts
CEO
Vlaams Datanutsbedrijf (Athumi)

Bob Van den Broeck
Administrateur-generaal
Agentschap Justitie en Handhaving

Bijlagen:

- Bijlage 1: Contactgegevens
- Bijlage 2: Technische en organisatorische maatregelen
- Bijlage 3: Verwerkersovereenkomst

BIJLAGE 1 CONTACTGEGEVENS

	Vlaams Datanutsbedrijf	AJH
Contactpersoon	Sammy Parmentier	Tia Cormon
Naam + functie	Business unit lead Real estate	Data Protection Officer AJH
Email	Sammy.parmentier@athumi.eu	
DPO	privacy@athumi.eu	Dpo.ajh@vlaanderen.be
Email		

BIJLAGE 2 TECHNISCHE EN ORGANISATORISCHE MAATREGELEN

1. Veiligheidskader

Het Vlaams Datanutsbedrijf maakt gebruik van de informatieclassificatie van de Vlaamse overheid en het informatieveiligheidsbeheerssysteem van het Vlaams Datanutsbedrijf, op basis van de ISO 27001-norm als kompas voor het implementeren van de nodige technische en organisatorische maatregelen om het beveiligingsniveau van de verwerking te waarborgen.

1	Informatie die toegankelijk mag zijn voor iedereen . Bij een incident met de betrokken informatie is de impact of materiele schade verwaarloosbaar of onbestaand .
2	Informatie die slechts beperkt toegankelijk is op basis van organisatorische criteria. Bij een incident met de betrokken informatie is de impact of materiele schade minimaal .
3	Informatie die slechts toegankelijk mag zijn voor een beperkte groep van gebruikers. Bij een incident met de betrokken informatie is de impact of materiele schade belangrijk .
4	Informatie die slechts toegankelijk mag zijn voor een beperkte groep gebruikers. Bij een incident is de impact van directe, indirecte materiële en immateriële schade ernstig .
5	Informatie die slechts toegankelijk mag zijn aan een zeer select aantal gebruikers . Bij een incident is de impact van directe, indirecte materiële en immateriële schade bedreigend, voor het voortbestaan van de organisatie of personen en hun vrijheden.

De classificatie die van toepassing is, is de op één na hoogste classificatie die uit de inventaris van alle geïdentificeerde Persoonsgegevens kan afgeleid worden. Het is die classificatie die de informatieclassificatie van het volledige platform bepaalt. De gegevens die via het Vastgoedinformatieplatform verwerkt worden, zijn na analyse volgens dit model ingedeeld in informatieklasse 4.

Om de beschikbaarheid, integriteit en vertrouwelijkheid van de Persoonsgegevens tijdens de verwerking te garanderen worden, op basis van deze indeling, de hierna beschreven technische en organisatorische veiligheidsmaatregelen genomen.

2. Organisatorische veiligheidsmaatregelen

De Partijen treffen in ieder geval ten minste volgende organisatorische en technische beveiligingsmaatregelen:

- Een informatieveiligheidsbeleid hebben;
- Een DPO aangewezen hebben;
- Een informatieveiligheidscel aangesteld te hebben;
- Een procedure m.b.t. de behandeling van Datalekken te hebben;
- De medewerkers van de Partij, incl. ingehuurd of tijdelijk personeel en eventuele derde partijen die rechtstreeks of onrechtstreeks betrokken zijn bij de uitvoering van de opdracht zijn

- Gehouden zijn tot een confidentialiteitsplicht, die wettelijk en/of contractueel is opgelegd;
- Ingelicht zijn omtrent de regels van de AVG;
- De informatieveiligheidsinstructies hebben die ze moeten respecteren;
- Het (lokale) netwerk van de organisatie beveiligd is opgezet, o.m. door een actieve firewall;
- De e-mailtoepassing wordt beveiligd, minstens door een virusscanner

De Partijen zijn verantwoordelijk voor het uitvoeren van gepaste maatregelen op de toestellen onder hun beheer. De aangestelde administrators verstrekken lokale Medewerkers de benodigde rechten en toegang, waarbij zij het principe van minimale toegang toepassen. Alleen Medewerkers die toegang nodig hebben tot het loket om hun taken uit te voeren, krijgen deze rechten toegewezen.

(a) Op niveau van het Vlaams Datanutsbedrijf

- Er is een functionaris voor gegevensbescherming aangesteld. De functionaris voor gegevensbescherming controleert of de Verwerkingen gebeuren in overeenstemming met de bepalingen van de Toepasselijke Gegevensbeschermingswetgeving en met de verwerkersopdracht.
- Het Vlaams Datanutsbedrijf beschikt over een informatieveiligheidsbeleid en –plan.
- Conform de AVG:
 - Wordt een geheimhoudingsverklaring ondertekend door alle relevante interne en externe Medewerkers, inclusief Subverwerkers;
 - Is er een incidentenbeheerprocedure opgesteld en naar alle relevante Medewerkers gecommuniceerd;
 - Zijn er procedures opgesteld en gecommuniceerd naar alle relevante Medewerkers met betrekking tot volgende aspecten:
 - Recht van inzage,
 - Recht op rectificatie,
 - Recht op gegevenswissing,
 - Recht op beperking van de verwerking,
 - Recht op overdraagbaarheid van de persoonsgegevens,
 - Recht van bezwaar;
- Maatregelen zijn getroffen voor de fysieke beveiliging van de omgeving.
- Is een register van verwerkingsactiviteiten opgesteld zoals bedoeld in art 30 AVG.

(b) Op niveau Vastgoedinformatieplatform

- Conform de AVG:
 - Beschikt de privacylogging over een auditfunctionaliteit die toegankelijk is voor de functionaris voor gegevensbescherming van Athumi.
 - Processen zijn geïmplementeerd met betrekking tot het toegangsbeheer, het loggingsbeheer, het security event management.
 - Is er een register van verwerkingsactiviteiten opgesteld;
 - Beschikt de privacylogging over een auditfunctionaliteit die toegankelijk is voor de functionaris voor gegevensbescherming.

- Processen zijn uitgeschreven en geïmplementeerd met betrekking tot het toegangsbeheer, het loggingsbeheer, het security event management.
- In lijn met de Overeenkomst zijn verplichtingen inzake de Verwerking van Persoonsgegevens contractueel vastgelegd met de respectieve Subverwerkers.
- Het Vastgoedinformatieplatform is uitvoering gedocumenteerd voor interne doeleinden op Confluence, Azure Devops en SharePoint.

3. Technische veiligheidsmaatregelen

Logging en Monitoring

Voor het monitoren en analyseren van applicaties en infrastructuur wordt gebruik gemaakt van een uitgebreide observability omgeving die het Vlaams Datanutsbedrijf in staat stelt om metrics, logs en traces te verzamelen, te visualiseren en te analyseren. Dit bevordert een diepgaand inzicht in systeemgedrag en helpt bij het snel identificeren en onderzoeken van informatiebeveiligingsgebeurtenissen die tot een informatiebeveiligingsincident kunnen leiden of nadat een incident zich heeft voorgedaan.

Loggegevens worden beveiligd opgeslagen en overgedragen, leestoegang tot loggegevens is beperkt tot bevoegde gebruikers om integriteit en vertrouwelijkheid te waarborgen.

Retentieperiodes worden door applicatieteams ingesteld conform het beleid dat Athumi hiervoor toepast.

Audit en Compliance Logging

Een aparte infrastructuur met onveranderbare opslag garandeert dat logdata gedurende een langere periode bewaard (10 jaar) en beveiligd blijven om de integriteit en vertrouwelijkheid te waarborgen.

Leestoegang tot deze logs is strikt gecontroleerd en gelogd en is strikt beperkt tot geautoriseerde personen na goedkeuring door de DPO.

Security Information and Event Management (SIEM)

De SIEM-oplossing stelt het Vlaams Datanutsbedrijf in staat om op een centrale manier logs en beveiligingssignalen te verzamelen, te analyseren en op te volgen.

Dankzij deze opzet kunnen de securityteams van het Vlaams Datanutsbedrijf dreigingen sneller detecteren, incidenten beter opvolgen en zorgt het Vlaams Datanutsbedrijf voor continue monitoring en compliance van de IT-omgeving.

Cryptografie en Sleutelbeheer

Data wordt zowel in opslag als tijdens overdracht en gebruik (confidential compute) versleuteld om vertrouwelijkheid te waarborgen.

Encryptiesleutels worden zorgvuldig beheerd door een strikt beperkt aantal bevoegde medewerkers gebruik makend van infrastructuur die voldoet aan FIPS 140-2 Level 3.

IT-dienstverleners hebben geen toegang tot het sleutelbeheer. Het Vlaams Datanutsbeheer heeft volledige controle over de accounts die de sleutels beheren en voert sleutelbeheer volledig zelf uit. Daarnaast worden er logs bijgehouden van toegang en gebruik van sleutels om integriteit en controleerbaarheid te waarborgen.

Toegangsbeveiliging

Authenticatie van bevoegde personen (zowel standaard gebruikers als geprivilegieerde gebruikers) verloopt via VO Toegangsbeheer (ACM/IDM) en stelt aanvullende multi-factor authenticatie (MFA) verplicht.

Functioneel noodzakelijke toegangsrechten worden vanuit een Least Privileged principe toegewezen aan individueel identificeerbare persoonlijke gebruikersaccounts.

Het Least privileged principe wordt bewaakt door een aangestelde toegangsbeheerder volgens het functiescheidingsprincipe waarbij de persoon die de rechten “bewaakt” niet dezelfde is dan deze die ze “inricht”.

Bij indiensttreding, job-rotatie en uitdiensttreding wordt een gestandaardiseerde procedure toegepast voor het toekennen en ontnemen van toegangen.

Netwerkbeveiliging

Er is voorzien in de scheiding tussen niet-productieomgevingen en productieomgevingen met strikte netwerksegmentatie.

Standaard Azure DDoS-bescherming op infrastructuurniveau is voorzien. Voor de productieomgeving maakt het Vlaams Datanutsbedrijf aanvullend gebruik van de Azure DDoS Protection Service. Deze service biedt specifieke bescherming voor het publieke IP-adres tegen DDoS-aanvallen, met applicatiespecifieke drempels.

Enkel TLS versleuteld inkomende verkeer wordt toegelaten. Inkomend verkeer wordt gefilterd via een firewall en gevalideerd voordat het de interne infrastructuur bereikt. Intern verkeer is beveiligd met netwerkregels en certificaten. Gegevensopslagsegmenten zijn alleen toegankelijk via compute-segmenten en niet rechtstreeks vanaf het internet. Uitgaand verkeer wordt eveneens gecontroleerd om te waarborgen dat alleen geautoriseerd verkeer de omgeving verlaat.

Er wordt gebruik gemaakt van Azure Firewall Standard.

Back-up en Herstel

Back-ups van data en infrastructuur worden planmatig uitgevoerd en zijn versleuteld en geografisch redundant opgeslagen. In geval van uitval of rampen kan de volledige omgeving snel worden hersteld naar een andere regio, met minimale dataverlies (RPO) en vastgelegde hersteltijden (RTO) afgestemd met de productteams.

Het testen van de Back-up en Herstel procedures wordt planmatig opgenomen binnen de Applicatie beheer teams.

Endpoint (malware) Protection

Het Vlaams Datanutsbedrijf beveiligt de Cloud omgeving en systemen met Microsoft Defender-tools die continu monitoren en kwetsbaarheden opsporen. Cloud Security Posture Management (CSPM) controleert automatisch de beveiligingsinstellingen en geeft aanbevelingen voor verbeteringen, terwijl Cloud Workload Protection (CWP) zich richt op de beveiliging van applicaties en data. Beveiligingswaarschuwingen worden direct doorgestuurd naar het team voor snelle opvolging, zodat de systemen en gegevens optimaal beschermd blijven.

Voor Blob/File storage is Microsoft defender for storage geactiveerd. Deze service doet een scan op bekende malware en verdachte content op de inhoud van de storage. Hierbij wordt gebruik gemaakt van Microsoft Threat Intelligence and Microsoft Defender Antivirus.

BIJLAGE 3 VERWERKERSOVEREENKOMST

Deze bijlage geldt voor de Verwerkingsactiviteiten betreffende de Verwerkingen omschreven in artikel 2.2.1 van de Overeenkomst waarbij het agentschap Justitie en Handhaving optreedt als Verwerkingsverantwoordelijke en het Vlaams Datanutsbedrijf als Verwerker.

In deze bijlage wordt verwezen naar het agentschap Justitie en Handhaving als 'Verwerkingsverantwoordelijke' en het Vlaams Datanutsbedrijf als 'Verwerker'.

AFDELING I – ALGEMENE ARTIKELS

ARTIKEL 1 - TOEPASSINGSGEBIED

- a. Deze artikels zijn van toepassing op de verwerking van persoonsgegevens als gespecificeerd in artikel 2.2.1 van de Overeenkomst. Deze artikels laten de verplichtingen die op de Verwerkingsverantwoordelijke rusten krachtens de AVG onverlet.
- b. De in deze bijlage in hoofdletter geschreven woorden, afkortingen, begrippen en verduidelijkingen worden begrepen zoals gedefinieerd in de AVG en artikel 1 van de Overeenkomst.

ARTIKEL 2 - ONVERANDERLIJKHEID VAN DE ARTIKELS

- a. Aanvullingen en wijzigingen van de artikels uit deze Verwerkersovereenkomst dienen schriftelijk te gebeuren, door middel van een addendum dat als bijlage aan deze Verwerkersovereenkomst zal worden gehecht.

ARTIKEL 3 - INTERPRETATIE

- a. Indien een artikel uit deze Verwerkersovereenkomst geheel of gedeeltelijk ongeldig, onwettig of nietig zou worden verklaard, tast dit op geen enkele wijze de geldigheid, wettigheid en toepasbaarheid van de andere artikels aan.

ARTIKEL 4 – HIËRARCHIE

- a. In geval van tegenstrijdigheid tussen de artikels uit deze Verwerkersovereenkomst en de artikels van gerelateerde overeenkomsten tussen de partijen prevaleren deze artikels uit deze Verwerkersovereenkomst.

AFDELING II – VERPLICHTINGEN VAN PARTIJEN

ARTIKEL 5 – BESCHRIJVING VAN DE VERWERKING(EN)

- a. De bijzonderheden van de verwerkingen, en met name de categorieën persoonsgegevens en de doeleinden van de verwerking(en) waarvoor de persoonsgegevens namens de Verwerkingsverantwoordelijke worden verwerkt, zijn gespecificeerd in artikel 2.2 van de Overeenkomst.

ARTIKEL 6 – VERPLICHTINGEN VAN DE PARTIJEN

6.1 INSTRUCTIES

- a. De Verwerker verwerkt persoonsgegevens uitsluitend op basis van schriftelijke instructies van de Verwerkingsverantwoordelijke binnen het specifiek doel of doeleinde van de verwerking, zoals beschreven in artikel 2.2 van de Overeenkomst, tenzij een op de Verwerker van toepassing zijnde wettelijke bepaling hem tot verwerking verplicht. In dat geval stelt de Verwerker de Verwerkingsverantwoordelijke, voorafgaand aan de verwerking, in kennis van dat wettelijk voorschrift, tenzij de wetgeving dit om gewichtige redenen van algemeen belang verbiedt. De Verwerkingsverantwoordelijke kan ook tijdens de verwerking van persoonsgegevens steeds verdere instructies geven.
- b. De Verwerker stelt de Verwerkingsverantwoordelijke onmiddellijk in kennis als de instructies van de Verwerkingsverantwoordelijke inbreuk maken op de AVG of de toepasselijke gegevensbeschermingsbepalingen van de Unie of de lidstaten.

6.2 DUUR VAN DE VERWERKING VAN PERSOONSGEGEVENS

- a. Verwerking door de Verwerker vindt slechts plaats tot het Besluit tot toevoeging van het product maatregelenregister voor overdracht in werking treedt.

6.3 BEVEILIGING VAN DE VERWERKING

- a. De Verwerker treft ten minste de in bijlage 2 gespecificeerde technische en organisatorische maatregelen om de beveiliging van de persoonsgegevens te waarborgen. Dit houdt onder meer in dat de gegevens worden beschermd tegen een inbreuk op de beveiliging die leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of ongeoorloofde toegang tot de gegevens, hetzij per ongeluk hetzij onrechtmatig. Bij de beoordeling van het passende beveiligingsniveau houden de partijen naar behoren rekening met de stand van de techniek, de uitvoeringskosten, de aard, de reikwijdte, de context en de doeleinden van de verwerking en de risico's voor de Betrokkenen.

6.4 VERTROUWELIJKHEID

- a. De Verwerker verleent zijn personeel slechts toegang tot de persoonsgegevens die worden verwerkt voor zover dat strikt noodzakelijk is voor de uitvoering, het beheer en de monitoring

van de overeenkomst. De Verwerker waarborgt dat de gemachtigde personen zich ertoe hebben verbonden vertrouwelijkheid in acht te nemen of door een passende wettelijke verplichting van vertrouwelijkheid zijn gebonden. Op verzoek legt de Verwerker het model van vertrouwelijkheidsclausule of -overeenkomst die de gemachtigde personen ondertekenen of de vertrouwelijkheidsplicht waartoe ze al gebonden zijn ingevolge een wettelijke verplichting, voor aan de Verwerkingsverantwoordelijke.

6.5 DOCUMENTATIE EN NALEVING

- a. De Verwerker stelt de Verwerkingsverantwoordelijke alle informatie ter beschikking die nodig is om aan te tonen dat is voldaan aan de in deze artikels vastgestelde verplichtingen die rechtstreeks voortvloeien uit de AVG. Op verzoek van de Verwerkingsverantwoordelijke staat de Verwerker ook regelmatig, of indien er aanwijzingen van niet-naleving zijn, audits toe van de onder deze artikels vallende verwerkingsactiviteiten en draagt de Verwerker aan die audits bij.
- b. De Verwerkingsverantwoordelijke kan ervoor kiezen de audit zelf uit te voeren of een onafhankelijke auditor daartoe opdracht te geven. De audits kunnen ook inspecties in de bedrijfsruimten of fysieke faciliteiten van de Verwerker omvatten en worden, in voorkomend geval, tijdig aangekondigd. De Verwerkingsverantwoordelijke zal de Verwerker een exemplaar van het rapport van audit verstrekken binnen 10 werkdagen.
- c. De partijen stellen de in dit artikel bedoelde informatie, met inbegrip van de resultaten van eventuele audits, op verzoek van de Verwerkingsverantwoordelijke en/of de toezichthoudende autoriteit(en) zelf, ter beschikking van de bevoegde toezichthoudende autoriteit(en).

6.6 GEBRUIK VAN SUBVERWERKERS

- a. De Verwerker heeft algemene toestemming van de Verwerkingsverantwoordelijke om subverwerkers van de overeengekomen lijst, zoals omschreven in bijlage 4, in dienst te nemen. De Verwerker stelt de Verwerkingsverantwoordelijke ten minste 10 werkdagen van tevoren specifiek schriftelijk in kennis van beoogde veranderingen van die lijst door middel van de toevoeging of vervanging van subverwerkers, samen met de benodigde informatie vermeld in bijlage 4, zodat de Verwerkingsverantwoordelijke voldoende tijd krijgt om bezwaar tegen die veranderingen te maken voordat de subverwerker(s) in dienst wordt/worden genomen. De Verwerker verstrekt de Verwerkingsverantwoordelijke de informatie die deze nodig heeft om zijn recht om bezwaar te maken uit te oefenen. De lijst van door de Verwerkingsverantwoordelijke erkende subverwerkers is opgenomen in bijlage 4. De partijen zorgen ervoor dat bijlage 4 steeds is bijgewerkt.
- b. Wanneer de Verwerker een subverwerker in dienst neemt voor de uitvoering van specifieke verwerkingen (namens de Verwerkingsverantwoordelijke), doet zij dit door middel van een overeenkomst die de subverwerker dezelfde verplichtingen inzake gegevensbescherming oplegt als die welke op grond van deze artikels aan de Verwerker worden opgelegd. De Verwerker zorgt ervoor dat de subverwerker voldoet aan de verplichtingen die krachtens deze artikels en de AVG op de Verwerker rusten. De Verwerker blijft ten opzichte van de Verwerkingsverantwoordelijke volledig verantwoordelijk voor de uitvoering van de verplichtingen van de subverwerker overeenkomstig zijn overeenkomst met de Verwerker. De

Verwerker stelt de Verwerkingsverantwoordelijke in kennis van elk verzuim van de subverwerker om zijn contractuele verplichtingen na te komen.

ARTIKEL 7 – BIJSTAND AAN DE VERWERKINGSVERANTWOORDELIJKE

- a. De Verwerker stelt de Verwerkingsverantwoordelijke onverwijld in kennis van elk verzoek dat hij van de Betrokkene heeft ontvangen. De Verwerker antwoordt niet zelf op het verzoek, tenzij de Verwerkingsverantwoordelijke daartoe toestemming heeft gegeven.
- b. De Verwerker staat de Verwerkingsverantwoordelijke bij, bij het vervullen van zijn verplichtingen om te reageren op verzoeken van Betrokkenen tot uitoefening van hun rechten, en houdt daarbij rekening met de aard van de verwerking. Bij het nakomen van zijn verplichtingen uit hoofde van de punten a) en b) volgt de Verwerker de instructies van de Verwerkingsverantwoordelijke.
- c. De Verwerker heeft niet alleen de verplichting de Verwerkingsverantwoordelijke bij te staan overeenkomstig artikel 7, punt b), maar staat de Verwerkingsverantwoordelijke ook bij, bij het waarborgen van de naleving van de volgende verplichtingen, waarbij rekening wordt gehouden met de aard van de gegevensverwerking en de informatie waarover de Verwerker beschikt:
 1. de verplichting om een beoordeling uit te voeren van het effect van de beoogde verwerkingen op de bescherming van persoonsgegevens (een “gegevensbeschermingseffectbeoordeling”) wanneer een bepaalde soort verwerking waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen;
 2. de verplichting om de bevoegde toezichthoudende autoriteit(en) voorafgaand aan de verwerking te raadplegen wanneer uit een gegevensbeschermingseffectbeoordeling blijkt dat de verwerking een hoog risico zou opleveren indien de Verwerkingsverantwoordelijke geen maatregelen neemt om dat risico te beperken;
 3. de verplichting om ervoor te zorgen dat persoonsgegevens accuraat en actueel zijn, door de Verwerkingsverantwoordelijke onverwijld in te lichten wanneer de Verwerker ervan kennis heeft gekregen dat de gegevens die hij verwerkt onjuist of achterhaald zijn;
 4. de verplichtingen in artikel 32 AVG omtrent de beveiliging van de verwerking.

ARTIKEL 8 – KENNISGEVING VAN EEN INBREUK IN VERBAND MET PERSOONSGEGEVENS

- a. In het geval van een inbreuk in verband met persoonsgegevens werkt de Verwerker samen met de Verwerkingsverantwoordelijke en staat hij hem bij zodat de Verwerkingsverantwoordelijke kan voldoen aan zijn verplichtingen uit hoofde van de artikelen 33 en 34 AVG, indien van toepassing, waarbij rekening wordt gehouden met de aard van de verwerking en de informatie waarover de Verwerker beschikt.

8.1 INBREUK IN VERBAND MET GEGEVENS DIE DOOR DE VERWERKINGSVERANTWOORDELIJKE WORDEN VERWERKT

- a. In geval van een inbreuk in verband met persoonsgegevens die door de Verwerkingsverantwoordelijke worden verwerkt, staat de Verwerker de Verwerkingsverantwoordelijke bij:
1. bij het zonder onredelijke vertraging melden van de inbreuk in verband met persoonsgegevens aan de bevoegde toezichthoudende autoriteit(en) nadat de Verwerkingsverantwoordelijke er kennis van heeft gekregen, indien relevant/(tenzij het onwaarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen);
 2. bij het verkrijgen van onderstaande informatie die overeenkomstig artikel 33, lid 3 AVG in de kennisgeving van de Verwerkingsverantwoordelijke moet worden vermeld. Indien en voor zover al deze informatie niet op hetzelfde moment kan worden verstrekt, bevat de oorspronkelijke kennisgeving de dan beschikbare informatie en wordt verdere informatie vervolgens onverwijld verstrekt zodra deze beschikbaar is;
 3. bij het naleven, overeenkomstig artikel 34 AVG, van de verplichting om de Betrokkene de inbreuk in verband met persoonsgegevens onverwijld mee te delen, wanneer de inbreuk in verband met persoonsgegevens waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen.

8.2 INBREUK IN VERBAND MET GEGEVENS DIE DOOR DE VERWERKER WORDEN VERWERKT

- a. In geval van een inbreuk in verband met persoonsgegevens die door de Verwerker worden verwerkt, stelt de Verwerker, nadat hij kennis heeft gekregen van de inbreuk, de Verwerkingsverantwoordelijke daarvan onverwijld en uiterlijk binnen 24 uur na kennisname van de inbreuk in kennis. Deze kennisgeving bevat ten minste informatie overeenkomstig artikel 33, lid 3 en 4 AVG. Indien en voor zover al deze informatie niet op hetzelfde moment kan worden verstrekt, bevat de oorspronkelijke kennisgeving de dan beschikbare informatie en wordt verdere informatie vervolgens onverwijld verstrekt zodra deze beschikbaar is.

ARTIKEL 9 – AANSPRAKELIJKHEID

- a. Onverminderd de artikels opgenomen in de opdrachtdocumenten die betrekking hebben op de overheidsopdracht in het kader waarvan persoonsgegevens worden verwerkt en deze Verwerkersovereenkomst wordt gesloten, is de Verwerker volledig aansprakelijk ten aanzien van de Verwerkingsverantwoordelijke voor de schade die voortvloeit uit een handeling of een nalatigheid wanneer bij de verwerking niet is voldaan aan de specifiek tot de Verwerkers gerichte verplichtingen van de AVG, dan wel uit een handeling of nalatigheid buiten dan wel in strijd met de rechtmatige instructies van de Verwerkingsverantwoordelijke.

ARTIKEL 10 – NIET-NALEVING VAN DE ARTIKELS EN BEËINDIGING

- a. Onverminderd eventuele artikels van de AVG kan de Verwerkingsverantwoordelijke, ingeval de Verwerker zijn verplichtingen uit hoofde van deze artikels niet nakomt, de Verwerker opdracht geven de verwerking van persoonsgegevens op te schorten totdat de Verwerker aan deze artikels voldoet of de overeenkomst beëindigen. Wanneer de Verwerker om welke reden dan ook niet aan deze artikels kan voldoen, stelt hij de Verwerkingsverantwoordelijke daarvan onverwijld in kennis.
- b. Indien de Verwerkingsverantwoordelijke aandringt op naleving van de instructies, nadat de Verwerker hem er overeenkomstig bepaling 6.1, punt b) van in kennis heeft gesteld dat zijn

instructies inbreuk maken op de toepasselijke wettelijke vereisten, heeft de Verwerker het recht de overeenkomst op te zeggen, voor zover deze de verwerking van persoonsgegevens overeenkomstig deze bepalingen betreft.

- c. Na beëindiging van de overeenkomst, dan wel na afloop van de verwerkingsopdracht, indien deze later plaatsvindt, wist de Verwerker, naar keuze van de Verwerkingsverantwoordelijke, alle persoonsgegevens die namens de Verwerkingsverantwoordelijke zijn verwerkt en bevestigt hij tegenover de Verwerkingsverantwoordelijke dat hij dit heeft gedaan, of zendt hij alle persoonsgegevens terug aan de Verwerkingsverantwoordelijke en verwijdert hij bestaande kopieën, tenzij het Unierecht of het lidstatelijke recht de opslag van de persoonsgegevens voorschrijft. Totdat de persoonsgegevens zijn gewist of teruggegeven, blijft de Verwerker ervoor zorgen dat deze artikels worden nageleefd.
- d. Deze Verwerkersovereenkomst is onderworpen aan het Belgisch recht. Alle geschillen in verband met deze Verwerkersovereenkomst zullen worden voorgelegd aan de bevoegde rechter in het arrondissement waar de Verwerkingsverantwoordelijke gevestigd is.

BIJLAGE 4 (SUB)VERWERKER(S)

Subverwerker	Beschrijving van de Verwerkingsactiviteiten door de Subverwerker	Categorieën van Persoonsgegevens	Vindt er een gegevensdoorgifte naar derde landen plaats? Indien ja, welke maatregelen zijn er genomen in het licht van hoofdstuk V AVG?	Heeft de Verwerker met de Subverwerker een overeenkomst gesloten op grond van art. 28 AVG?
<p>Naam : Digitaal Vlaanderen, Adres: Havenlaan 88/b, 1000 Brussel Data Protection Officer: privacy@digitaal.vlaanderen.be;</p>	<p>- Gebruik van Veiligheidsbouwstenen voor de toegangscontrole tot het Vastgoedinformatieplatform</p>	<p>- Contact- en identificatiegegevens - Identificatienummer van het Rijksregister/KBO-nummer - Vastgoedinformatie - Gegevens in het kader van stedenbouwkundige- en milieumisdrijven en -inbreuken - Financiële gegevens</p>	<p><input checked="" type="checkbox"/> Neen. <input type="checkbox"/> Ja, in/naar de volgende landen:</p>	<p><input checked="" type="checkbox"/> Ja. <input type="checkbox"/> Neen, want:</p>
<p>Naam: Microsoft Adres: Microsoft Ireland Operations, Ltd. One Microsoft Place South County Business Park Leopardstown Dublin 18, D18 P521, Ireland</p>	<p>Hosting (Azure Cloud Services) van het Vastgoedinformatieplatform dat er onder meer voor zorgt dat gegevens uit centrale authentieke bronnen (open-data) automatisch worden opgehaald. Lokale besturen vullen de vastgoedinlichtingen verder aan met de eigen lokale vastgoedinformatie. Opslag van de vastgoedinlichtingen gebeurt eveneens op deze omgeving.</p>	<p>- Contact- en identificatiegegevens - Vastgoedinformatie - Gegevens in het kader van stedenbouwkundige- en milieumisdrijven en -inbreuken - Financiële gegevens - Identificatienummer van het Rijksregister/KBO-nummer.</p>	<p><input type="checkbox"/> Neen. <input checked="" type="checkbox"/> Ja, in/naar de volgende landen: Gelet op het feit dat Microsoft een Amerikaanse cloudprovider is, is het mogelijk dat er in zeldzame gevallen een doorgifte van persoonsgegevens kan plaatsvinden naar de Verenigde Staten. Indien deze doorgifte zou plaatsvinden dan verloopt dit volgens de modaliteiten</p>	<p><input checked="" type="checkbox"/> Ja. <input type="checkbox"/> Neen, want:</p>

			opgenomen in artikel 3.10 van deze Overeenkomst.	
<p>Eviden Belgium NV Da Vincilaan 5 1930 Zaventem</p> <p>Aanspreekpunt DPO: Jo.vercammen@eviden.com</p>	<p>De Verwerker staat in voor het beheer van het clearing house platform die de verwerking op zich neemt van de clearing en settlement van alle financiële transacties gekoppeld aan producten van het VIP platform. Er worden geen vastgoedinlichtingen opgeslagen bij deze verwerker, alleen de financiële transacties</p>	<ul style="list-style-type: none"> - Financiële gegevens - Identificatienummer van het Rijksregister/KBO-nummer. 	<p><input checked="" type="checkbox"/> Neen.</p> <p><input type="checkbox"/> Ja, in/naar de volgende landen:</p>	<p><input checked="" type="checkbox"/> Ja.</p> <p><input type="checkbox"/> Neen, want:</p>
<p>CCV Belgium Ter Waarde 50 8900 Ieper</p> <p>Data Protection Officer (CCV groep) : fg@lumengroup.nl</p>	<p>De Verwerker staat in voor een financiële ontzorging door de retributies te innen voor naam en voor rekening voor de partijen ingeval er betaald wordt via een payment service provider. Ingeval de aanvrager van vastgoedinformatie online (contant) betaalt via een payment serviceprovider worden er persoonsgegevens verwerkt voor deze finaliteit.</p>	<ul style="list-style-type: none"> - Contact- en identificatiegegevens - Identificatienummer van het Rijksregister/KBO-nummer - Financiële gegevens 	<p><input checked="" type="checkbox"/> Neen.</p> <p><input type="checkbox"/> Ja, in/naar de volgende landen:</p>	<p><input checked="" type="checkbox"/> Ja.</p> <p><input type="checkbox"/> Neen, want:</p>