

VERWERKERSOVEREENKOMST

[Format hoog risico]

TUSSEN

Stichting Zuyd Hogeschool

EN

[NAAM BEDRIJF]

DE ONDERGETEKENDEN:

Stichting Zuyd Hogeschool, gevestigd aan Nieuw Eyckholt 300 te Heerlen, Kamer van Koophandel nummer 14060995 en rechtsgeldig vertegenwoordigd door **[naam en functie]** (hierna: “**Zuyd**”);

en

<NAAM BEDRIJF>, gevestigd aan **<ADRES>** te **<PLAATS>**, Kamer van Koophandel nummer **<KVK>** en rechtsgeldig vertegenwoordigd door **[naam en functie]** (hierna: “**Verwerker**”);

Hierna gezamenlijk te noemen: “**Partijen**” en individueel te noemen “**Partij**”;

NEMEN HET VOLGENDE IN AANMERKING:

- Partijen hebben op **<DATUM>** een overeenkomst gesloten met kenmerk **<KENMERK VAN DE OVEREENKOMST>** met betrekking tot **<ONDERWERP VAN DE OVEREENKOMST>**. Ter uitvoering van de Overeenkomst verwerkt Verwerker ten behoeve van Zuyd Persoonsgegevens;
- In het kader van het uitvoeren van de Overeenkomst is **<NAAM LEVERANCIER>** aan te merken als Verwerker in de zin van de AVG en is Zuyd aan te merken als Verwerkingsverantwoordelijke in de zin van de AVG;
- Partijen wensen zorgvuldig en in overeenstemming met de AVG en andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens om te gaan met de Persoonsgegevens die ter uitvoering van de Overeenkomst verwerkt (zullen) worden;
- Partijen wensen in overeenstemming met de AVG en andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens hun rechten en plichten ten aanzien van de Verwerking van Persoonsgegevens van Betrokkenen Schriftelijk vast te leggen in deze Verwerkersovereenkomst.

EN ZIJN ALS VOLGT OVEREENGEKOMEN:

ARTIKEL 1. DEFINITIES

In deze Verwerkersovereenkomst hebben de met hoofdletter geschreven begrippen de in dit artikel opgenomen betekenis. Waar de definitie in dit artikel in het enkelvoud is opgenomen, wordt ook het meervoud daaronder begrepen en vice versa, tenzij uitdrukkelijk anders vermeld of uit de context anders blijkt.

1.1 AVG: de 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).

1.2 Betrokkene: de geïdentificeerde of identificeerbare natuurlijke persoon op wie de Persoonsgegevens betrekking hebben, zoals bedoeld in artikel 4 onder 1) AVG.

1.3 Bijlage: een bijlage bij deze Verwerkersovereenkomst, die een integraal onderdeel vormt van deze Verwerkersovereenkomst.

1.4 Bijzondere categorieën Persoonsgegevens: Persoonsgegevens in verband met ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, het lidmaatschap van een vakbond, 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, zoals bedoeld in artikel 9 AVG.

1.5 Derde: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, niet zijnde de Betrokkene, noch Zuyd, noch de Verwerker, noch de personen die onder rechtstreeks gezag van Zuyd of de Verwerker gemachtigd zijn om Persoonsgegevens te verwerken, zoals bedoeld in artikel 4 onder 10) AVG.

1.6 Dienst: de op grond van de Overeenkomst te leveren dienst(en) door Verwerker aan Zuyd.

1.7 Inbreuk in verband met Persoonsgegevens: een (vermoeden van een) inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte Persoonsgegevens, zoals bedoeld in artikel 4 onder 12) AVG.

1.8 Medewerker: de door Verwerker ingeschakelde werknemers en andere personen waarvan de werkzaamheden onder zijn verantwoordelijkheid vallen en die worden ingeschakeld door Verwerker ter uitvoering van de Overeenkomst.

1.9 Ontvanger: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, al dan niet een Derde, aan wie/waaraan de Persoonsgegevens worden verstrekt, zoals bedoeld in artikel 4 onder 9) AVG.

1.10 Overeenkomst: de overeenkomst die tussen Zuyd en Verwerker is gesloten en op grond waarvan Verwerker Persoonsgegevens ten behoeve van de uitvoering van deze overeenkomst voor Zuyd verwerkt, zoals bedoeld in de considerans van deze verwerkersovereenkomst.

1.11 Persoonsgegeven: alle informatie over een 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, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische,

culturele of sociale identiteit van die natuurlijke persoon, zoals bedoeld in artikel 4 onder 1) AVG.

1.12 DPIA: de privacy impact assessment (gegevensbeschermingseffectbeoordeling) die vóór de Verwerking ten aanzien van het effect van de beoogde verwerkingsactiviteiten op de bescherming van Persoonsgegevens wordt uitgevoerd, zoals bedoeld in artikel 35 AVG.

1.13 Schriftelijk: op schrift gesteld of langs de elektronische weg, zoals bedoeld in artikel 6:227a van het Burgerlijk Wetboek.

1.14 Sub-verwerker: een andere verwerker, waaronder maar niet beperkt tot groepsmaatschappijen, zustermaatschappijen, dochtermaatschappijen en hulpleveranciers, die Verwerker inschakelt om voor rekening van Zuyd specifieke verwerkingsactiviteiten te verrichten.

1.15 Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens: de toepasselijke wet- en regelgeving en/of (nadere) verdragen, verordeningen, richtlijnen, besluiten, beleidsregels, instructies en/of aanbevelingen van een bevoegde overheidsinstantie betreffende de Verwerking van Persoonsgegevens, tevens omvattende toekomstige wijziging hiervan en/of aanvulling hierop, inclusief lidstaatrechtelijke uitvoeringswetten van de AVG en de Telecommunicatiewet.

1.16 Toezichthoudende autoriteit: één of meer onafhankelijke overheidsinstanties die verantwoordelijk is of zijn voor het toezicht op de toepassing van de AVG, teneinde de grondrechten en fundamentele vrijheden van natuurlijke personen in verband met de Verwerking van hun Persoonsgegevens te beschermen en het vrije verkeer van Persoonsgegevens binnen de Unie te vergemakkelijken, zoals bedoeld in artikel 4 onder 21) en artikel 51 AVG. In Nederland is dit de Autoriteit Persoonsgegevens.

1.17 Verwerkersovereenkomst: de onderhavige overeenkomst inclusief Bijlagen, zoals bedoeld in artikel 28 lid 3 AVG.

1.18 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, zoals bedoeld in artikel 4 onder 2) AVG.

1.19 Verwerkingsverantwoordelijke: een natuurlijk persoon of rechtspersoon, een overheidsinstantie, een dienst of ander orgaan die/dat alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.

ARTIKEL 2. VOORWERP VAN DE VERWERKERSOVEREENKOMST

2.1 De Verwerkersovereenkomst vormt een aanvulling op de Overeenkomst en vervangt eventuele eerder gemaakte afspraken tussen Partijen ten aanzien van de Verwerking van Persoonsgegevens. Bij tegenstrijdigheid tussen de bepalingen uit de

Verwerkersovereenkomst en de Overeenkomst, prevaleren de bepalingen uit de Verwerkersovereenkomst.

2.2 De bepalingen uit de Verwerkersovereenkomst gelden voor alle Verwerkingen die plaatsvinden ter uitvoering van de Overeenkomst. Verwerker brengt Zuyd onverwijld op de hoogte indien Verwerker reden heeft om aan te nemen dat Verwerker niet langer aan de Verwerkersovereenkomst kan voldoen.

2.3 Zuyd geeft Verwerker opdracht en instructies om de Persoonsgegevens te verwerken namens Zuyd. De instructies van Zuyd zijn nader omschreven in de Verwerkersovereenkomst en de Overeenkomst inclusief eventuele bijlagen. Zuyd kan naar redelijkheid Schriftelijk aanvullende of afwijkende instructies geven.

2.4 Verwerker verwerkt de Persoonsgegevens uitsluitend in opdracht van Zuyd en op basis van de instructies van Zuyd. Verwerker verwerkt de Persoonsgegevens uitsluitend voor zover de Verwerking noodzakelijk is ter uitvoering van de Overeenkomst, nimmer ten eigen nutte, ten nutte van Derden en/of voor reclamadoeleinden c.q. andere doeleinden, tenzij een op Verwerker van toepassing zijnde Unierechtelijke of lidstaatrechtelijke bepaling Verwerker tot Verwerking verplicht. In dat geval stelt Verwerker Zuyd voorafgaand aan de Verwerking Schriftelijk op de hoogte van deze bepaling, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt.

2.5 Verwerker en Zuyd leven de AVG en andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens na. Verwerker stelt Zuyd onmiddellijk in kennis indien naar mening van Verwerker een instructie van Zuyd inbreuk oplevert op de AVG en/of andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens.

2.6 Indien Verwerker in strijd met de Verwerkersovereenkomst en/of de AVG en/of andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens het doel en/of de middelen van de Verwerking van Persoonsgegevens bepaalt, wordt Verwerker voor die Verwerkingen als (mede) Verwerkingsverantwoordelijke beschouwd.

ARTIKEL 3. VERWERKING VAN PERSOONSGEGEVENS

3.1 Partijen leggen in Bijlage A vast welke Verwerkingen de Verwerker in opdracht van Zuyd uitvoert. Verwerker is uitsluitend tot de in Bijlage A gespecificeerde Verwerkingen gerechtigd.

ARTIKEL 4. VERLENEN VAN BIJSTAND EN MEDEWERKING

4.1 Verwerker verleent Zuyd alle benodigde bijstand en medewerking bij het doen nakomen van de op Partijen rustende verplichtingen op grond van de AVG en andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens ten

behoefte van de uitvoering van de Overeenkomst. Verwerker verleent Zuyd in ieder geval bijstand met betrekking tot:

- (i) De beveiliging van Persoonsgegevens;
- (ii) Het uitvoeren van controles en audits;
- (iii) Het uitvoeren van DPIA's;
- (iv) Voorafgaande raadpleging van de Toezichthoudende autoriteit;
- (v) Het voldoen aan verzoeken van de Toezichthoudende autoriteit of een andere overheidsinstantie;
- (vi) Het voldoen aan verzoeken van Betrokkenen;
- (vii) Het melden van Inbreuken in verband met Persoonsgegevens.

4.2 Onder het verlenen van bijstand en medewerking met betrekking tot het voldoen aan verzoeken van Betrokkenen, worden in ieder geval de volgende verplichtingen voor Verwerker verstaan:

4.2.1 Verwerker neemt alle redelijke maatregelen om ervoor te zorgen dat Betrokkene zijn rechten kan uitoefenen.

4.2.2 Indien een Betrokkene met betrekking tot de uitvoering van zijn rechten direct contact opneemt met Verwerker, dan gaat Verwerker hier – behoudens uitdrukkelijke andersluidende instructie van Zuyd – niet (inhoudelijk) op in, maar bericht Verwerker dit onverwijld aan Zuyd met een verzoek om nadere instructies.

4.2.3 Indien Verwerker de Dienst rechtstreeks aanbiedt aan Betrokkene, is Verwerker verplicht om Betrokkene namens Zuyd te informeren over de Verwerking van de Persoonsgegevens van Betrokkene op een wijze die in overeenstemming is met de rechten van Betrokkene.

4.3 Onder het verlenen van bijstand en medewerking met betrekking tot het voldoen aan verzoeken van de Toezichthoudende autoriteit of een andere overheidsinstantie, worden in ieder geval de volgende verplichtingen voor Verwerker verstaan:

4.3.1 Indien Verwerker een verzoek of een bevel van een Nederlandse en/of buitenlandse overheidsinstantie ontvangt met betrekking tot Persoonsgegevens, waaronder maar niet beperkt tot een verzoek van de Toezichthoudende autoriteit, informeert Verwerker Zuyd onverwijld, voor zover dat wettelijk is toegestaan. Bij de behandeling van het verzoek of bevel neemt Verwerker alle instructies van Zuyd in acht en verleent Verwerker alle redelijkerwijs benodigde medewerking aan Zuyd.

4.3.2 Indien het Verwerker wettelijk is verboden om te voldoen aan zijn verplichtingen op grond van artikel 4.3.1, behartigt Verwerker de redelijke belangen van Zuyd. Hieronder wordt in ieder geval verstaan:

4.3.2.1 Verwerker laat juridisch toetsen in hoeverre: (i) Verwerker wettelijk verplicht is om aan het verzoek of bevel te voldoen; en (ii) het Verwerker daadwerkelijk is verboden om aan zijn verplichtingen jegens Zuyd op grond van artikel 4.3.1 te voldoen.

4.3.2.2 Verwerker werkt alleen mee aan het verzoek of bevel indien Verwerker hiertoe wettelijk verplicht is en waar mogelijk maakt Verwerker (in rechte) bezwaar tegen het verzoek of bevel of het verbod om Zuyd hierover te informeren of de instructies van Zuyd op te volgen.

4.3.2.3 Verwerker verstrekt niet meer Persoonsgegevens dan strikt noodzakelijk om aan het verzoek of bevel te voldoen.

4.3.2.4 Verwerker onderzoekt indien sprake is van doorgifte in de zin van artikel 9 de mogelijkheden om te voldoen aan de artikelen 44 tot en met 46 AVG.

ARTIKEL 5. TOEGANG TOT PERSOONSgegevens

5.1 Verwerker beperkt de toegang tot Persoonsgegevens aan Medewerkers, Sub-verwerkers, Derden en andere Ontvangers van Persoonsgegevens tot een noodzakelijk minimum.

5.2 Verwerker verschaft uitsluitend toegang aan die Medewerkers voor wie ter uitvoering van de Overeenkomst deze toegang tot Persoonsgegevens noodzakelijk is.

5.3 Verwerker verschaft Sub-verwerkers geen toegang tot Persoonsgegevens zonder voorafgaande algemene of specifieke Schriftelijke toestemming van Zuyd. Algemene Schriftelijke toestemming voor het inschakelen van Sub-verwerkers is slechts verleend indien dit expliciet in Bijlage A is opgenomen. Specifieke toestemming voor het inschakelen van Sub-verwerkers is slechts verleend aan Sub-verwerkers die in Bijlage A zijn gespecificeerd.

5.4 Verwerker licht Zuyd in geval van algemene Schriftelijke toestemming voor het inschakelen van Sub-verwerkers uiterlijk drie (3) maanden voorafgaand aan beoogde veranderingen inzake de toevoeging, vervanging of wijziging van Sub-verwerker(s), Schriftelijk in, waarbij Zuyd de mogelijkheid wordt geboden tegen deze veranderingen bezwaar te maken binnen uiterlijk een (1) maand. Partijen treden hierop in onderhandeling.

5.5. De algemene of specifieke toestemming van Zuyd voor het inschakelen Sub-verwerkers laat de verplichtingen voor Verwerker voortvloeiende uit de Verwerkersovereenkomst, waaronder maar niet beperkt tot artikel 9, onverlet. Zuyd kan zijn algemene of specifieke Schriftelijke toestemming voor het inschakelen van Sub-verwerkers intrekken, indien Verwerker niet of niet langer voldoet aan de verplichtingen uit de Verwerkersovereenkomst, de AVG en/of andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens.

5.6 De Sub-verwerkers die Verwerker inschakelt ter uitvoering van de Overeenkomst, zijn opgenomen in Bijlage A.

5.7 Verwerker legt de in de Verwerkersovereenkomst opgenomen verplichtingen op aan de door Verwerker ingeschakelde (rechts)personen, waaronder maar niet beperkt tot Sub-verwerkers door middel van een schriftelijke overeenkomst. Verwerker garandeert dat de tot het verwerken van de Persoonsgegevens gemachtigde personen en andere Ontvangers van Persoonsgegevens zich ertoe hebben verbonden vertrouwelijkheid in acht te nemen of door een passende wettelijke verplichting van vertrouwelijkheid zijn gebonden.

5.8 Verwerker brengt Zuyd onverwijld op de hoogte indien Verwerker en/of door Verwerker ingeschakelde (rechts)personen, waaronder maar niet beperkt tot Medewerkers en/of Sub-verwerkers, in strijd handelen met de Verwerkersovereenkomst en/of de met Verwerker gesloten Schriftelijke overeenkomst zoals bedoeld in artikel 5.7.

5.9 Verwerker verstrekt op verzoek van Zuyd bewijs van de Schriftelijke overeenkomst tussen Verwerker en de door Verwerker ingeschakelde Sub-verwerkers.

5.10 Verwerker blijft ten aanzien van Zuyd volledig verantwoordelijk en volledig aansprakelijk voor het nakomen van de verplichtingen door de door Verwerker ingeschakelde (rechts)personen, waaronder maar niet beperkt Sub-verwerkers, voortvloeiende uit de AVG en/of andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens en de verplichtingen voortvloeiende uit de Overeenkomst en de Verwerkersovereenkomst.

ARTIKEL 6. BEVEILIGING

6.1 Verwerker treft passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen, opdat de Verwerking aan de vereisten van de AVG en andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens voldoet en de bescherming van de rechten van Betrokkenen is gewaarborgd. Verwerker treft hiertoe tenminste de technische en organisatorische maatregelen die zijn opgenomen in Bijlage B.

6.2 Bij de beoordeling van het passende beveiligingsniveau houdt Verwerker rekening met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, vooral als gevolg van de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens, hetzij per ongeluk hetzij onrechtmatig.

6.3 Verwerker legt zijn beveiligingsbeleid Schriftelijk vast. Op verzoek van Zuyd verschafft Verwerker bewijs van het beveiligingsbeleid van Verwerker.

6.4 Het aansluiten bij een goedgekeurde gedragscode als bedoeld in artikel 40 AVG of een goedgekeurd certificeringsmechanisme als bedoeld in artikel 42 AVG kan worden gebruikt als element om aan te tonen dat de in dit artikel bedoelde vereisten worden nageleefd.

6.5 Het is Zuyd toegestaan om (onaangekondigde) kwetsbaarheidsanalyses en pentesten uit te voeren binnen de grenzen van de contractuele overeenkomst en wetgeving.

ARTIKEL 7. AUDIT

7.1 Verwerker is verplicht periodiek een onafhankelijke, externe deskundige een audit te laten uitvoeren ten aanzien van de organisatie van Verwerker, teneinde aan te tonen dat Verwerker aan het bepaalde in de Verwerkersovereenkomst, de AVG en andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens voldoet.

7.2 Verwerker verricht tenminste een keer per twee jaar een periodieke audit, zoals bedoeld in artikel 7.1.

7.3 Verwerker is enkel niet gehouden tot het verrichten van een periodieke audit zoals bedoeld in artikel 7.1, indien uitdrukkelijk in Bijlage A is opgenomen dat Verwerker niet gehouden is tot het verrichten van een periodieke audit.

7.4 Verwerker is verplicht de bevindingen van de onafhankelijke, externe deskundige, op verzoek aan Zuyd ter beschikking te stellen in de vorm van een verklaring, waarin de deskundige een oordeel geeft over de kwaliteit van de door Verwerker getroffen technische en organisatorische beveiligingsmaatregelen met betrekking tot de Verwerkingen die Verwerker ten behoeve van Zuyd verricht.

7.5 Zuyd heeft het recht om op zijn verzoek éénmaal per jaar een audit te laten uitvoeren door een door Zuyd gemachtigde (rechts)persoon, ten aanzien van de organisatie van Verwerker, teneinde aan te tonen dat Verwerker aan het bepaalde in de Verwerkersovereenkomst, de AVG en andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens voldoet.

7.6 De kosten van de periodieke audit komen voor rekening van Verwerker. De kosten van de audit op verzoek van Zuyd komen voor rekening van Zuyd, tenzij uit de bevindingen van de audit blijkt dat Verwerker de bepalingen uit de Verwerkersovereenkomst en/of de AVG en/of andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens niet is nagekomen. Deze bepaling laat de overige rechten van Zuyd, waaronder het recht op schadevergoeding, onverlet.

7.7 Indien tijdens een audit wordt vastgesteld dat Verwerker niet aan het bepaalde in de Verwerkersovereenkomst en/of de AVG en/of andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens voldoet, neemt Verwerker onverwijld alle redelijkerwijs noodzakelijke maatregelen om te zorgen dat Verwerker hieraan alsnog voldoet. De bijbehorende kosten komen voor rekening van Verwerker.

7.8 Op verzoek van Zuyd geeft verwerker inzage in de resultaten van de meest recente penetratietest. Indien verwerker geen penetratietesten uitvoert of laat uitvoeren, dan heeft Zuyd het recht maximaal eenmaal per twee jaar op eigen kosten een penetratietest uit te (laten) voeren op het betrokken systeem. Indien Zuyd dit voornemens is, dan

treedt Zuyd minimaal twee maanden voor het uitvoeren van de penetratietest in overleg met de verwerker.

ARTIKEL 8. INBREUK IN VERBAND MET PERSOONSgegevens

8.1 Verwerker informeert Zuyd zonder onredelijke vertraging en uiterlijk binnen 24 uur na kennisneming, over een Inbreuk in verband met Persoonsgegevens of een redelijk vermoeden van een Inbreuk in verband met Persoonsgegevens. Verwerker informeert Zuyd via de contactpersoon en de contactgegevens van Zuyd zoals opgenomen in het meest recente formulier datalekken van de Autoriteit Persoonsgegevens, welke te vinden is op de website van de Autoriteit Persoonsgegevens. Verwerker garandeert dat de verstrekte informatie volledig, correct en accuraat is.

8.2 Indien en voor zover het voor Verwerker niet mogelijk is om alle informatie gelijktijdig te verstrekken, kan de informatie zonder onredelijke vertraging en uiterlijk binnen 24 uur na het ontdekken, in stappen worden verstrekt aan Zuyd.

8.3 Verwerker heeft adequaat beleid en adequate procedures ingericht om Inbreuken in verband met Persoonsgegevens in een zo vroeg mogelijk stadium te detecteren, Zuyd hierover uiterlijk binnen 24 uur te informeren, hierop adequaat en onmiddellijk te reageren, (verdere) onbevoegde kennisneming, wijziging, en verstrekking dan wel anderszins onrechtmatige Verwerking te voorkomen of te beperken en herhaling hiervan te voorkomen. Op verzoek van Zuyd verschaft Verwerker informatie over en inzage in dit door Verwerker ingerichte beleid en deze door Verwerker ingerichte procedures.

8.4 Verwerker houdt Schriftelijk een register bij van alle Inbreuken in verband met Persoonsgegevens die betrekking hebben op of verband houden met de (uitvoering van de) Overeenkomst, met inbegrip van de feiten omtrent de Inbreuk in verband met Persoonsgegevens, de gevolgen daarvan en de getroffen corrigerende maatregelen. Op verzoek van Zuyd verschaft Verwerker Zuyd een afschrift van dit register.

ARTIKEL 9. DOORGIFTE VAN PERSOONSgegevens

9.1 Persoonsgegevens mogen enkel worden doorgegeven aan landen buiten de EER of internationale organisaties indien sprake is van een passend beschermingsniveau, in overeenstemming wordt gehandeld met artikelen 44 tot en met 49 AVG, de standaardcontractbepalingen zoals bedoeld in het *UITVOERINGSBESLUIT (EU) 2021/914 VAN DE COMMISSIE van 4 juni 2021 betreffende standaardcontractbepalingen voor de doorgifte van persoonsgegevens naar derde landen overeenkomstig Verordening (EU) 2016/679 van het Europees Parlement en de Raad*, zijn ondertekenend en Zuyd hiervoor specifieke Schriftelijke toestemming heeft verleend. Deze specifieke Schriftelijke toestemming is slechts verleend indien dit is opgenomen in Bijlage A. Verwerker is uitsluitend gerechtigd tot deze in Bijlage A gespecificeerde doorgiften aan derde landen of internationale organisaties, tenzij een op Verwerker van toepassing zijnde Unierechtelijke of lidstaatrechtelijke bepaling Verwerker tot Verwerking

verplicht. In dat geval stelt Verwerker Zuyd voorafgaand aan de Verwerking Schriftelijk op de hoogte van deze bepaling, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt.

ARTIKEL 10. VERTROUWELIJKHEID VAN PERSOONSGEGEVENS

10.1 Alle Persoonsgegevens worden als vertrouwelijke gegevens gekwalificeerd en dienen als zodanig te worden behandeld.

10.2 Partijen houden alle Persoonsgegevens geheim en maken deze op geen enkele wijze verder intern of extern bekend, behalve voor zover:

- (i) Bekendmaking en/of verstrekking van de Persoonsgegevens in het kader van de uitvoering van de Overeenkomst of Verwerkersovereenkomst noodzakelijk is;
- (ii) Enig voorschrift van dwingend Unie- of lidstatelijk recht of een daarop gebaseerde rechterlijke uitspraak van een bevoegde rechtbank, of een geldende internationale overeenkomst Partijen tot bekendmaking, verstrekking en/of doorgifte van die Persoonsgegevens verplicht, waarbij Partijen hetgeen is bepaald in artikel 4 in acht nemen;
- (iii) Bekendmaking en/of verstrekking van die Persoonsgegevens geschiedt met voorafgaande Schriftelijke toestemming van Zuyd.

10.3 Overtreding van artikel 10.1 en/of artikel 10.2 wordt beschouwd als een Inbreuk in verband met Persoonsgegevens.

ARTIKEL 11. AANSPRAKELIJKHEID

11.1 Een Partij kan geen beroep doen op een aansprakelijkheidsbeperking, die is opgenomen in de Overeenkomst of andere tussen Partijen bestaande overeenkomst of regeling, ten aanzien van een door de andere Partij ingestelde:

- a. verhaalsactie op grond van artikel 82 AVG; of
- b. schadevergoedingsactie uit hoofde van de Verwerkersovereenkomst, indien en voor zover de actie bestaat uit verhaal van een aan de Toezichthoudende autoriteit betaalde geldboete die geheel of gedeeltelijk toerekenbaar is aan de andere Partij.

Het bepaalde in dit artikel laat onverlet de rechtsmiddelen die de aangesproken Partij op grond van de geldende wet- of regelgeving ter beschikking staat.

11.2 Iedere Partij is verplicht de andere Partij zonder onnodige vertraging op de hoogte te stellen van een (mogelijke) aansprakelijkstelling of het (mogelijk) opleggen van een boete door de Toezichthoudende autoriteit, beiden in verband met de Verwerkersovereenkomst. Iedere Partij is in redelijkheid verplicht de andere Partij informatie te verstrekken en/of ondersteuning te verlenen ten behoeve van het voeren van verweer tegen een (mogelijke) aansprakelijkstelling of boete, zoals bedoeld in de

vorige volzin. De Partij die informatie verstrekt en/of ondersteuning verleent, is gerechtigd om eventuele redelijke kosten dienaangaande in rekening te brengen bij de andere Partij, Partijen informeren elkaar zo veel mogelijk vooraf over deze kosten.

ARTIKEL 12. WIJZIGING

12.1 Verwerker is verplicht Zuyd onmiddellijk te informeren over voorgenomen wijzigingen in de Dienst, (de uitvoering van) de Overeenkomst en (de uitvoering van) de Verwerkersovereenkomst die betrekking hebben op de Verwerking van Persoonsgegevens. Hieronder wordt in ieder geval verstaan:

- (i) Wijzigingen die invloed (kunnen) hebben op de te verwerken (categorieën) Persoonsgegevens;
- (ii) Wijziging van de middelen waarmee de Persoonsgegevens worden verwerkt;
- (iii) Het inschakelen van andere Sub-verwerkers;
- (iv) Wijziging in de doorgifte van Persoonsgegevens aan derde landen en/of internationale organisaties.

12.2 Indien een wijziging met betrekking tot de Verwerking van Persoonsgegevens of een audit daartoe aanleiding geeft, treden Partijen op eerste verzoek van Zuyd in overleg over het wijzigen van de Verwerkersovereenkomst.

12.3 Verwerker is pas gerechtigd tot het uitvoeren van een wijziging in de Dienst, een wijziging in (de uitvoering van) de Overeenkomst, een wijziging in (de uitvoering van) de Verwerkersovereenkomst indien Zuyd daaraan voorafgaand Schriftelijk toestemming voor deze wijziging(en) heeft gegeven.

12.4 Wijzigingen die betrekking hebben op de Verwerking van Persoonsgegevens mogen nooit tot gevolg hebben dat Zuyd niet kan voldoen aan de AVG en/of andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens.

12.5 In geval van nietigheid of vernietigbaarheid van één of meer bepalingen van de Verwerkersovereenkomst, blijven de overige bepalingen onverkort van kracht.

ARTIKEL 13. DUUR EN BEËINDIGING

13.1 De duur van de Verwerkersovereenkomst is gelijk aan de duur van de Overeenkomst. De Verwerkersovereenkomst is niet los van de Overeenkomst te beëindigen. Bij beëindiging van de Overeenkomst eindigt de Verwerkersovereenkomst van rechtswege en vice versa.

13.2 Zuyd is gerechtigd de Verwerkersovereenkomst op te zeggen, indien Verwerker niet voldoet of niet langer kan voldoen aan de Verwerkersovereenkomst en/of de AVG en/of andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens, zonder dat Verwerker aanspraak maakt op enige schadevergoeding.

Bij de opzegging neemt Zuyd een redelijke opzegtermijn in acht, tenzij de omstandigheden onmiddellijke opzegging rechtvaardigen.

13.3 Binnen een maand nadat de Overeenkomst eindigt, vernietigt en/of retourneert Verwerker alle Persoonsgegevens en/of draagt Verwerker deze over aan Zuyd en/of een andere door Zuyd aan te wijzen partij, naar gelang de keuze van Zuyd. Alle bestaande (overige) kopieën van Persoonsgegevens, zich al dan niet bevindende bij door Verwerker ingeschakelde (rechts)personen, waaronder maar niet beperkt tot Medewerkers en/of Sub-verwerkers, worden hierbij aantoonbaar permanent verwijderd, tenzij opslag van de Persoonsgegevens Unierechtelijk of lidstaatrechtelijk is verplicht.

13.4 Verwerker bevestigt op verzoek van Zuyd Schriftelijk dat Verwerker aan alle verplichtingen uit artikel 13.3 heeft voldaan.

13.5 Verwerker draagt de kosten voor vernietiging, retournering en/of overdracht van de Persoonsgegevens. Zuyd kan nadere eisen stellen aan de wijze van vernietiging, retournering en/of overdracht van de Persoonsgegevens, waaronder eisen aan het bestandsformaat.

13.6 Verplichtingen uit de Verwerkersovereenkomst die naar hun aard bestemd zijn om na beëindiging van de Verwerkersovereenkomst voort te duren, blijven na beëindiging van de Verwerkersovereenkomst voortduren.

ARTIKEL 14. TOEPASSELIJK RECHT EN GESCHILLENBESLECHTING

14.1 De Verwerkersovereenkomst en de uitvoering daarvan worden beheerst door Nederlands recht.

14.2 Alle geschillen, die tussen Partijen ontstaan in verband met de Verwerkersovereenkomst, zullen worden voorgelegd aan de bevoegde rechter in de plaats waar Zuyd gevestigd is.

Aldus in tweevoud opgesteld en ondertekend,

Stichting Zuyd Hogeschool

<NAAM BEDRIJF>

____/____/____

____/____/____

Datum

Datum

Plaats

Plaats

Naam

Naam

Handtekening

Handtekening

Bijlage A: Specificatie van de Verwerking van Persoonsgegevens

Versie: 01; datum laatste wijziging: XX-XX-XXXX

Omschrijving van de Verwerking

(in te vullen door Zuyd)

Doeleinden van de Verwerking

(in te vullen door Zuyd)

Categorieën Betrokkenen

(in te vullen door Zuyd)

(categorieën) Persoonsgegevens

(in te vullen door Zuyd)

Frequentie verrichten van audit

(in te vullen door Zuyd)

--

Bewaartermijn van de Persoonsgegevens of de criteria om die vast te stellen
(enkel invullen indien van toepassing)
(in te vullen door Zuyd)

--

De persoonsgegevens worden opgeslagen in de volgende landen:
(in te vullen door verwerker)

--

Sub-verwerkers

Zuyd heeft Verwerker [aankruisen wat van toepassing is door Zuyd]:

- ☐ Algemene toestemming gegeven voor het inschakelen van Sub-verwerkers.
- ☐ Specifieke toestemming gegeven voor het inschakelen van de hierna opgenomen Sub-verwerkers:

Sub-verwerker die door Verwerker wordt ingeschakeld voor het Verwerken van Persoonsgegevens	(categorie) Persoonsgegevens die Sub-verwerker verwerkt	Soort Verwerking	Land van Verwerking	Vestigings-land Sub-verwerker

Doorgiften buiten de EU

Zuyd heeft Verwerker specifieke toestemming gegeven voor de hierna opgenomen doorgiften aan derde landen of internationale organisaties (in te vullen door Zuyd).

Beschrijving doorgifte	Entiteit die de Persoonsgegevens doorgeeft + land	Entiteit die de Persoonsgegevens ontvangt + land	Doorgifte-mechanisme

Contactgegevens

Algemene contactgegevens	Naam	Functie	E-mail adres	Telefoonnummer
Zuyd (in te vullen door Zuyd)				
Verwerker (in te vullen door verwerker)				

Contactgegevens bij Inbreuk in verband met Persoonsgegevens	Naam	Functie	E-mail adres	Telefoonnummer
Zuyd	Computer Security Incident Response Team (CSIRT)	Computer Security Incident Response Team	csirt@zuyd.nl	+31454006090
Verwerker (in te vullen door verwerker)				

Bijlage B: Beveiligingsmaatregelen [invullen door verwerker]

Versie: 01; datum laatste wijziging: XX-XX-XXXX

De verwerker garandeert dat passende technische en organisatorische maatregelen zijn getroffen opdat zijn verwerkingen aan de vereisten van de AVG voldoen en de rechten van de betrokkenen zijn gewaarborgd.

Normen informatiebeveiliging

Verwerker verplicht zich desgevraagd tegenover Zuyd aan te tonen op welke wijze hij passende technische en organisatorische maatregelen heeft genomen om te waarborgen dat de verwerkingen plaatsvinden in overeenstemming met de AVG en het gestelde in deze Verwerkersovereenkomst. De voorkeur is dat Verwerker is aangesloten bij een goedgekeurde gedragscode als bedoeld in artikel 40 AVG of een goedgekeurd certificeringsmechanisme als bedoeld in artikel 42 AVG.

Het is Zuyd toegestaan om (onaangekondigde) kwetsbaarheidsanalyses en pentesten uit te voeren binnen de grenzen van de contractuele overeenkomst en wetgeving.

Technische en organisatorische maatregelen, met inbegrip van technische en organisatorische maatregelen om de beveiliging van de gegevens te waarborgen

Beschrijving van de door de verwerker(s) genomen technische en organisatorische beveiligingsmaatregelen (met inbegrip van eventuele relevante certificeringen) om een passend beveiligingsniveau te waarborgen, rekening houdend met de aard, de reikwijdte, de context en het doel van de verwerking, alsmede met de risico's voor de rechten en vrijheden van natuurlijke personen.

Certificaten waarover (Sub)verwerker beschikt

Certificaten	Certificaat Scope	Geldigheidsduur certificaat

Door ondertekening van de Verwerkersovereenkomst verklaart Verwerker te voldoen aan bovengenoemde normen en beveiligingsmaatregelen en te beschikken over de aangegeven certificaten.

Indien de verwerker **niet** over een geldig certificaat beschikt, geef dan hieronder aan welke beveiligingsmaatregelen genomen worden en **licht deze indien van toepassing toe**. Beschikt de verwerker wel over een geldig certificaat dan hoeven onderstaande maatregelen niet ingevuld te worden.

1.1 Beleid en organisatie

Nr.	Vraag	Antwoord	Toelichting verplicht bij geen "ja"	ISO 27002
1.1.1	Zijn de taken en verantwoordelijkheden met betrekking tot informatiebeveiliging gedefinieerd, vastgelegd in documentatie en toegewezen?	☐ Ja ☐ Nee ☐ Nog niet ☐ N.v.t.		6.1.1
1.1.2	Maakt informatiebeveiliging een integraal onderdeel uit van het projectbeheer	☐ Ja ☐ Nee ☐ Nog niet ☐ N.v.t.		6.1.5
1.1.3	Is er een vastgesteld beleid voor het veilig gebruik van mobiele apparatuur?	☐ Ja ☐ Nee ☐ Nog niet ☐ N.v.t.		6.2.1.1

1.1.4	Is er een vastgesteld beleid voor het gebruik van cryptografische beheersmaatregelen?	☐ Ja ☐ Nee ☐ Nog niet ☐ N.v.t.		10.1.1.1
1.1.5	Zijn er tools of applicaties aanwezig waarmee het beleid voor het gebruik van cryptografische beheersmaatregelen wordt geïmplementeerd?	☐ Ja ☐ Nee ☐ Nog niet ☐ N.v.t.		10.1.1.2
1.1.6	Hanteert jullie organisatie een vastgesteld beleid voor veilig informatietransport dat geïmplementeerd is door middel van procedures en/of beheersmaatregelen?	☐ Ja ☐ Nee ☐ Nog niet ☐ N.v.t.		13.2.1
1.1.7	Zijn er overeenkomsten vastgesteld om veilig informatietransport met externe partijen te borgen?	☐ Ja ☐ Nee ☐ Nog niet ☐ N.v.t.		13.2.2
1.1.8	Zijn de relevante beveiligingseisen en -aspecten opgenomen in leveranciersovereenkomsten?	☐ Ja ☐ Nee ☐ Nog niet ☐ N.v.t.		15.1.2
1.1.9	Zijn de verantwoordelijkheden (incl. die van de directie) en procedures bij informatiebeveiligingsincidenten vastgesteld ten behoeve van een snelle, doeltreffende en ordelijke response?	☐ Ja ☐ Nee ☐ Nog niet ☐ N.v.t.		16.1.1
1.1.10	Worden informatiebeveiligingsgebeurtenissen gerapporteerd?	☐ Ja ☐ Nee ☐ Nog niet ☐ N.v.t.		16.1.2
1.1.11	Zijn er in overeenstemming met wettelijke, regelgevende, contractuele en bedrijfseisen maatregelen vastgesteld om registraties van informatie te beschermen tegen verlies, vernietiging, vervalsing, onbevoegde toegang / vrijgave?	☐ Ja ☐ Nee ☐ Nog niet ☐ N.v.t.		18.1.3
1.1.12	Zijn er maatregelen bijvoorbeeld privacy-beleid en geschikte procedures vastgesteld, gedocumenteerd en gecommuniceerd om de privacy en bescherming van persoonsgegevens te waarborgen in overeenstemming met de relevante wet- en regelgeving?	☐ Ja ☐ Nee ☐ Nog niet ☐ N.v.t.		18.1.4

1.2 Personeel, studenten en gasten

Nr.	Vraag	Antwoord	Toelichting verplicht bij geen "ja"	ISO 27002
1.2.1	Zijn de verantwoordelijkheden van medewerkers, contractanten en de organisatie zelf, vermeld in de contractuele overeenkomst?	☐ Ja ☐ Nee ☐ Nog niet ☐ N.v.t.		7.1.2
1.2.2	Zijn de eisen voor vertrouwelijkheids- of geheimhoudingsovereenkomsten betreffende het beschermen van informatie vastgesteld, gedocumenteerd, en worden deze regelmatig beoordeeld?	☐ Ja ☐ Nee ☐ Nog niet ☐ N.v.t.		13.2.4
1.2.3	Bestaat er voor medewerkers en contractanten een procedure om waargenomen of vermeende beveiligingsincidenten in de informatiebeveiliging tijdig te rapporteren?	☐ Ja ☐ Nee ☐ Nog niet ☐ N.v.t.		16.1.3

1.3 Ruimten en apparatuur

Nr.	Vraag	Antwoord	Toelichting verplicht bij geen "ja"	ISO 27002
1.3.1	Zijn er formele procedures die regelen hoe media op een veilige en beveiligde manier verwijderd moeten worden als ze niet langer nodig zijn?	☐ Ja ☐ Nee ☐ Nog niet ☐ N.v.t.		8.3.2
1.3.2	Is er een fysiek toegangsbeveiligingsbeleid om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt tot beveiligde gebieden?	☐ Ja ☐ Nee ☐ Nog niet ☐ N.v.t.		11.1.2
1.3.3	Zijn er fysieke beveiligingsmaatregelen ontworpen en geïmplementeerd voor kantoren, ruimten en faciliteiten?	☐ Ja ☐ Nee ☐ Nog niet ☐ N.v.t.		11.1.3
1.3.4	Wordt apparatuur onderhouden om de continue beschikbaarheid en integriteit ervan te kunnen waarborgen?	☐ Ja ☐ Nee ☐ Nog niet ☐ N.v.t.		11.2.4
1.3.5	Apparaten die opslagmedia bevatten, worden getoetst/gecheckt om ervoor te zorgen dat gevoelige gegevens en gelicenseerde software zijn verwijderd of veilig zijn overschreven voordat ze worden weggegooid of hergebruikt.	☐ Ja ☐ Nee ☐ Nog niet ☐ N.v.t.		11.2.7

1.4 Continuïteit

Nr.	Vraag	Antwoord	Toelichting verplicht bij geen "ja"	ISO 27002
1.4.1	Zijn er beheersmaatregelen tegen malware opgesteld en geïmplementeerd?	☐ Ja ☐ Nee ☐ Nog niet ☐ N.v.t.		12.2.1.1
1.4.2	Worden er regelmatig back-up kopieën van informatie, software en systemen gemaakt conform Zuyd backup beleid?	☐ Ja ☐ Nee ☐ Nog niet ☐ N.v.t.		12.3.1.1
1.4.3	Worden gemaakte back-ups regelmatig getest conform Zuyd backup beleid?	☐ Ja ☐ Nee ☐ Nog niet ☐ N.v.t.		12.3.1.2
1.4.4	Wordt informatie over technische kwetsbaarheden van informatiesystemen tijdig gesignaleerd en geëvalueerd, en worden aan de hand hiervan passende maatregelen genomen om risico's aan te pakken?	☐ Ja ☐ Nee ☐ Nog niet ☐ N.v.t.		12.6.1
1.4.5	Worden informatiebeveiligingsgebeurtenissen beoordeeld en wordt geoordeeld of deze moeten worden geclassificeerd als informatiebeveiligingsincidenten?	☐ Ja ☐ Nee ☐ Nog niet ☐ N.v.t.		16.1.4

1.5 Vertrouwelijkheid en Integriteit

Nr.	Vraag	Antwoord	Toelichting verplicht bij geen "ja"	ISO 27002
1.5.1	Zijn er procedures die regelen dat medewerkers en contractanten alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn?	☐ Ja ☐ Nee ☐ Nog niet ☐ N.v.t.		9.1.2
1.5.2	Is er een registratie- en afmeldingsprocedure geïmplementeerd voor de toewijzing van toegangsrechten?	☐ Ja ☐ Nee ☐ Nog niet ☐ N.v.t.		9.2.1
1.5.3	Is er een procedure vastgesteld voor het beheer van speciale toegangsrechten?	☐ Ja ☐ Nee ☐ Nog niet ☐ N.v.t.		9.2.3
1.5.4	Wordt het gebruik van geheime authenticatie-informatie door medewerkers en contractanten geborgd?	☐ Ja ☐ Nee ☐ Nog niet ☐ N.v.t.		9.3.1
1.5.5	Is er een beveiligde inlogprocedure voor de toegang tot systemen en toepassingen?	☐ Ja ☐ Nee ☐ Nog niet ☐ N.v.t.		9.4.2
1.5.6	Is er een vastgesteld beleid met betrekking tot het gebruik, de bescherming en de levensduur van cryptografische sleutels?	☐ Ja ☐ Nee ☐ Nog niet ☐ N.v.t.		10.1.2.1
1.5.7	Zijn er maatregelen opgesteld om de netwerken en systemen te beveiligen, beheren en beschermen?	☐ Ja ☐ Nee ☐ Nog niet ☐ N.v.t.		13.1.1
1.5.8	Zijn groepen van informatiediensten, -gebruikers en -systemen op netwerken van elkaar gescheiden?	☐ Ja ☐ Nee ☐ Nog niet ☐ N.v.t.		13.1.3

1.6 Controle en Logging

Nr.	Vraag	Antwoord	Toelichting verplicht bij geen "ja"	ISO 27002
1.6.1	Worden logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, gemaakt, bewaard en regelmatig beoordeeld?	☐ Ja ☐ Nee ☐ Nog niet ☐ N.v.t.		12.4.1
1.6.2	Worden de activiteiten van systeembeheerders en operators vastgelegd, en de logbestanden bewaard en regelmatig beoordeeld?	☐ Ja ☐ Nee ☐ Nog niet ☐ N.v.t.		12.4.3
1.6.3	Zijn er procedures opgesteld voor het identificeren, verzamelen, verkrijgen en bewaren van informatie die als bewijs kan dienen bij informatiebeveiligingsincidenten?	☐ Ja ☐ Nee ☐ Nog niet ☐ N.v.t.		16.1.7
1.6.4	Worden de informatiesystemen regelmatig beoordeeld op naleving van de technische beleidsregels en normen?	☐ Ja ☐ Nee ☐ Nog niet ☐ N.v.t.		18.2.3