

VERWERKERSOVEREENKOMST

ONDERGETEKENDEN

1. De N.V. SRO, gevestigd te [postcode] Amersfoort, aan de [adres en huisnummer], geregistreerd in het handelsregister van de Kamer van Koophandel onder nummer [nummer], te deze rechtsgeldig vertegenwoordigd door de heer drs. M.C. Bloemsma, in diens hoedanigheid van directeur, hierna te noemen: **'Verwerkingsverantwoordelijke'**;

EN

2. De [rechtsvorm] [Statutaire Naam], gevestigd te [postcode] [plaats], aan de [adres en huisnummer], geregistreerd in het handelsregister van de Kamer van Koophandel onder nummer [nummer], te deze rechtsgeldig vertegenwoordigd door [de heer/mevrouw] [Naam], in diens hoedanigheid van [functie], hierna te noemen: **'Verwerker'**;

Hierna ieder voor zich aan te duiden als **'Partij'** en gezamenlijk aangeduid als **'Partijen'**.

OVERWEGENDE DAT:

- i. Verwerkingsverantwoordelijke en Verwerker op [datum] de in Bijlage 1 opgenomen overeenkomst [naam en titel overeenkomst] zijn aangegaan, inhoudende dat Verwerker diensten voor Verwerkingsverantwoordelijke zal verrichten, verder te noemen: **'Hoofdovereenkomst'**;
- ii. Verwerkingsverantwoordelijke beschikt over Persoonsgegevens in de zin van artikel 4 lid 1 van de Algemene Verordening Gegevensbescherming (verder te noemen: **'AVG'**), welke Persoonsgegevens door Verwerkingsverantwoordelijke aan Verwerker ter beschikking zijn gesteld en Verwerker ter uitvoering van de Hoofdovereenkomst in opdracht en ten behoeve van Verwerkingsverantwoordelijke verwerkt;
- iii. Het doel en omschrijving van de verwerking van Persoonsgegevens nader worden gespecificeerd in Bijlage 2 bij deze Verwerkersovereenkomst (verder te noemen: **'Overeenkomst'**);

- iv. Verwerker slechts met toestemming van Verwerkingsverantwoordelijke gerechtigd is de verwerking van Persoonsgegevens krachtens de Hoofdovereenkomst en deze Overeenkomst, door een Sub-Verwerker te doen verrichten;
- v. Verwerker aan door hem ingeschakelde Sub-Verwerker tenminste dezelfde verplichtingen zal opleggen als voortkomend uit deze Overeenkomst en zal toezien op de naleving daarvan door Sub-Verwerker;
- vi. Partijen middels deze Overeenkomst de afspraken met betrekking tot de verwerking van Persoonsgegevens in het kader van de Hoofdovereenkomst wensen vast te leggen.

PARTIJEN KOMEN HET VOLGENDE OVEREEN:

Artikel 1 Definities

- 1.1 De in deze Overeenkomst gebruikte woorden of formuleringen hebben de volgende betekenis:
 - a. **AVG**: Algemene Verordening Gegevensbescherming (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 over de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en over het vrije verkeer van die gegevens (en tot intrekking van Richtlijn 95/46/EG).
 - b. **Betrokkene**: degene op wie een Persoonsgegeven betrekking heeft.
 - c. **Datalek**: 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 verstuurde, opgeslagen of op andere wijze verwerkte gegevens (artikel 4 sub 12 AVG).
 - d. **Diensten**: [omschrijving diensten] die Verwerker aan Verwerkingsverantwoordelijke levert uit hoofde van de Hoofdovereenkomst.
 - e. **Hoofdovereenkomst**: de in Bijlage 1 opgenomen overeenkomst van [datum] tussen Partijen, die betrekking heeft op het verrichten van Diensten door Verwerker in opdracht en ten behoeve van Verwerkingsverantwoordelijke.
 - f. **Overeenkomst**: deze Verwerkersovereenkomst;
 - g. **Persoonsgegevens**: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon in de zin van artikel 4 lid 1 AVG.

- h. **Sub-Verwerker:** iedere niet-ondergeschikte derde partij die door Verwerker is ingeschakeld bij de verwerking van Persoonsgegevens, niet zijnde personeel van de Verwerker.
- i. **Verwerker:** een natuurlijk persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die Persoonsgegevens verwerkt ten behoeve van de Verwerkingsverantwoordelijke.
- j. **Verwerkingsverantwoordelijke:** een natuurlijk 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 bepaalt.

1.2 Naast bovenstaande begrippen, afkortingen en definities worden in deze Verwerkersovereenkomst ook de begrippen en de daarbij behorende definities van artikel 4 van de AVG verstaan.

Artikel 2 Onderwerp, duur en samenhang met Hoofdovereenkomst

- 2.1 Deze Overeenkomst heeft als doel dat Partijen voldoen aan hun wettelijke verplichtingen die voortvloeien uit de AVG, waaronder:
 - a. de verplichting van Verwerkingsverantwoordelijke om ervoor zorg te dragen dat Verwerker voldoende waarborgen biedt ten aanzien van de technische- en organisatorische beveiligingsmaatregelen, en
 - b. de verplichting van Verwerkingsverantwoordelijke om te voldoen aan de verplichtingen die in het kader van de Wet Meldplicht Datalekken zijn opgenomen in de AVG.
- 2.2 Deze Overeenkomst is van toepassing op de diensten verleend uit hoofde van de Hoofdovereenkomst en is een onlosmakelijk onderdeel van de Hoofdovereenkomst.
- 2.3 Deze Overeenkomst is van kracht vanaf de datum van de Hoofdovereenkomst en duurt voort zolang Verwerker de beschikking heeft over persoonsgegevens, dan wel de zeggenschap heeft over de wijze waarop door Sub-Verwerkers persoonsgegevens van Verwerkingsverantwoordelijke worden verwerkt. Indien de verleende Diensten ook na de beëindiging van de Hoofdovereenkomst moeten worden voortgezet, bijvoorbeeld door een exit-regeling, dan zijn de bepalingen van deze Overeenkomst blijvend van kracht op deze verdere levering van Diensten voor de gehele duur van de feitelijke samenwerking. De bepalingen inzake geheimhouding overleven de beëindiging van de samenwerking.

- 2.4 Deze Overeenkomst eindigt pas nadat Verwerker naar het oordeel van Verwerkingsverantwoordelijke genoegzaam heeft aangetoond dat hij heeft voldaan aan de verplichtingen als omschreven in artikel 6 lid 3 van deze Overeenkomst.
- 2.5 Voor zover enige bepaling van deze Overeenkomst, die betrekking heeft op de verwerking van Persoonsgegevens, in strijd is met hetgeen in de Hoofdovereenkomst is bepaald, prevaleert hetgeen in deze Overeenkomst is bepaald.

Artikel 3 Beëindiging Hoofdovereenkomst

- 3.1 In het geval de Hoofdovereenkomst is beëindigd zal Verwerker, ter vrije keuze van Verwerkingsverantwoordelijke, de mogelijkheid bieden tot de in het kader van de Hoofdovereenkomst verwerkte Persoonsgegevens te vernietigen of terug te leveren, tenzij anders overeengekomen in de Hoofdovereenkomst.
- 3.2 Verwerker zal hangende de keuze van Verwerkingsverantwoordelijke de Persoonsgegevens blijven bewaren. Verwerker is niet gerechtigd om zonder uitdrukkelijke instructie van Verwerkingsverantwoordelijke, de Persoonsgegevens te vernietigen.
- 3.3 Het terug leveren van de Persoonsgegevens geschiedt in een algemeen leesbaar en deugdelijk gedocumenteerd bestandsformaat.
- 3.4 Ongeacht het voorgaande:
- a. is Verwerker gerechtigd om de gegevens te bewaren indien wetgeving haar daartoe verplicht;
 - b. zal Verwerker informatie met betrekking tot inbreuken, zoals bedoeld in artikel 10 van deze Overeenkomst, tenminste tot één (1) jaar na beëindiging van de Hoofdovereenkomst bewaren.

Artikel 4 Verwerking persoonsgegevens

- 4.1 Verwerker verbindt zich om alle Persoonsgegevens die hij uitsluitend in het kader van de Hoofdovereenkomst voor Verwerkingsverantwoordelijke verwerkt, behoorlijk en zorgvuldig en slechts in opdracht en ten behoeve van Verwerkingsverantwoordelijke te verwerken, in overeenstemming met de instructies en aanwijzingen van Verwerkingsverantwoordelijke en in overeenstemming met de toepasselijke wet- en regelgeving.

- 4.2 Verwerker zal de Persoonsgegevens niet voor enig ander doel verwerken dan zoals door Verwerkingsverantwoordelijke in de Hoofdovereenkomst is vastgesteld. Indien Verwerker op grond van toepasselijke wet- of regelgeving verplicht is om anders te handelen, stelt Verwerker voorafgaand aan de verwerking, Verwerkingsverantwoordelijke in kennis van dat wettelijk voorschrift, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt.
- 4.3 De in opdracht van Verwerkingsverantwoordelijke te verwerken Persoonsgegevens blijven eigendom van de Verwerkingsverantwoordelijke en/of de betreffende Betrokkene. Verwerker heeft geen zeggenschap over en is niet verantwoordelijke voor de ter beschikking gestelde Persoonsgegevens. Verwerker neemt geen beslissingen over ontvangst en gebruik van de gegevens, de verstrekking aan Derde(n) en de duur van de opslag van gegevens. De zeggenschap over en de verantwoordelijkheid voor de Persoonsgegevens verstrekt of hem ter beschikking gekomen onder deze Overeenkomst komt nimmer bij Verwerker te berusten.
- 4.4 Verwerkingsverantwoordelijke zal Verwerker op de hoogte stellen van de verwerkingsdoeleinden voor zover deze niet reeds in de Hoofdovereenkomst dan wel in deze Overeenkomst zijn genoemd. Verwerkingsverantwoordelijke staat er voor in dat de Betrokkene zijn/haar toestemming heeft verleend voor het verwerken van zijn/haar Persoonsgegevens.
- 4.5 De aard en de doeleinden van de verwerking, evenals het soort Persoonsgegevens en de categorieën van Betrokkenen die door Verwerker namens Verwerkingsverantwoordelijke worden verwerkt, staan nader uitgewerkt in Bijlage 2, bij gebreke waarvan de verwerking is beperkt tot de werkzaamheden die noodzakelijk zijn voor de uitvoering van de Hoofdovereenkomst.

Artikel 5 Verplichtingen van Verwerker

- 5.1 Verwerker dient zorg te dragen voor de naleving van de voorwaarden die op grond van de toepasselijke wet- en regelgeving worden gesteld aan het verwerken van Persoonsgegevens. De verplichtingen van Verwerker die uit deze Overeenkomst en/of toepasselijke wet- en regelgeving voortvloeien, gelden ook voor diegenen die Persoonsgegevens verwerken onder het gezag van Verwerker, waaronder begrepen maar niet beperkt tot werknemers en Sub-Verwerkers. Verwerker schaft enkel toegang tot de Persoonsgegevens aan haar werknemers en Sub-Verwerkers voor zover dit nodig is voor het verrichten van de diensten uit hoofde van de Hoofdovereenkomst.

- 5.2 Verwerker mag uitsluitend na voorafgaande schriftelijke toestemming van Verwerkingsverantwoordelijke een Sub-Verwerker inschakelen bij de uitvoering van de Verwerkersovereenkomst. Verwerkingsverantwoordelijke kan aan de toestemming voorwaarden verbinden, die dienen ter naleving van de verplichtingen uit deze Overeenkomst.
- 5.3 Verwerker zal aan de door hem ingeschakelde Sub-Verwerker tenminste dezelfde verplichtingen opleggen als voor hemzelf uit deze Overeenkomst en de wet voortvloeien en ziet toe op de naleving daarvan door Sub-Verwerker. De betreffende afspraken met Sub-Verwerker zullen schriftelijk worden vastgelegd. Verwerker zal Verwerkingsverantwoordelijke op eerste verzoek daartoe afschrift verstrekken van deze Sub-Verwerkersovereenkomst(en). Verwerker dient in ieder geval contractueel verzekerd te hebben dat de Sub-Verwerker:
- a. zich eveneens richt naar de instructies en aanwijzingen van de Verwerkingsverantwoordelijke;
 - b. tot geheimhouding is gehouden, en;
 - c. de vereiste beveiligingsmaatregelen aangaande de verwerking van Persoonsgegevens en ICT-infrastructuur neemt.
- 5.4 Verwerkingsverantwoordelijke dient in staat te worden gesteld toe te zien op de naleving van de afspraken van de Sub-Verwerker met Verwerker. Verwerker blijft in deze gevallen te allen tijde aanspreekpunt en verantwoordelijk voor de naleving van de bepalingen uit de Hoofdovereenkomst en deze Overeenkomst door de Sub-Verwerker.

Artikel 6 Gegevensverstrekking

- 6.1 Verwerker stelt Verwerkingsverantwoordelijke in kennis van alle verzoeken met betrekking tot de verwerking van Persoonsgegevens die rechtstreeks van een Betrokkene zijn ontvangen.
- 6.2 Verwerker zal te allen tijde op eerste schriftelijk verzoek van Verwerkingsverantwoordelijke onmiddellijk alle met betrekking tot de Hoofdovereenkomst relevante Persoonsgegevens ter hand stellen. Het is Verwerker niet toegestaan Persoonsgegevens aan anderen dan Verwerkingsverantwoordelijke te verstrekken, tenzij dit geschiedt op schriftelijk verzoek van Verwerkingsverantwoordelijke of met diens schriftelijke toestemming. Verwerker is verplicht schriftelijk te bevestigen dat een verstrekking heeft plaatsgevonden,

waarbij hij exact de verstrekte Persoonsgegevens, de Betrokkene, de ontvanger en het moment van verstrekking dient te beschrijven.

- 6.3 Verwerker verbindt zich alle met de Hoofdovereenkomst samenhangende Persoonsgegevens, kopieën en bewerkingen daarvan, alsmede alle gegevensdragers waarop deze zijn vastgelegd, op een door Verwerkingsverantwoordelijke nader te bepalen wijze over te dragen aan Verwerkingsverantwoordelijke en/of een opvolgende Verwerker, binnen de door Verwerkingsverantwoordelijke aangegeven periode na het moment van beëindigen van de Hoofdovereenkomst of per een eerder moment wanneer Verwerkingsverantwoordelijke daar uitdrukkelijk om verzoekt. Verwerker is gehouden de na overdracht achtergebleven kopieën te vernietigen.
- 6.4 Van de overdracht en gevraagde vernietiging wordt door Verwerker een verslag gemaakt. Verwerkingsverantwoordelijke kan van de vernietiging een bewijs verlangen. De kosten van overdracht en vernietiging komen volledig voor de rekening van Verwerkingsverantwoordelijke.

Artikel 7 Geheimhouding en vertrouwelijkheid

- 7.1 Op alle persoonsgegevens die Verwerker van Verwerkingsverantwoordelijke ontvangt in het kader van de Hoofdovereenkomst, rust een geheimhouding ten opzichte van Derden. Verwerker zal deze informatie niet voor een ander doel gebruiken dan waarvoor Verwerker deze heeft gekregen, zelfs niet wanneer deze informatie in een zodanige vorm is gebracht zodat deze niet tot Betrokkenen herleidbaar is.
- 7.2 Verwerker zal de Persoonsgegevens tegenover derden geheim houden en zal deze niet openbaar maken, anders dan voor zover noodzakelijk voor het uitvoeren van de Hoofdovereenkomst, dan wel voor zover een wettelijk voorschrift of rechterlijk bevel Verwerker tot mededeling c.q. verstrekking verplicht.
- 7.3 Indien Verwerker op grond van een in Nederland en/of in de Europese Unie (EU) geldende wettelijke verplichting Persoonsgegevens dient te verstrekken, zal Verwerker de grondslag van het verzoek en de identiteit van de verzoeker verifiëren en zal Verwerker Verwerkingsverantwoordelijke onmiddellijk, voorafgaand aan de verstrekking, ter zake informeren, tenzij de relevante wettelijke bepalingen dit verbieden.
- 7.4 Verwerker is gehouden de Persoonsgegevens te verwerken in landen binnen de EU. Verwerker zal Verwerkingsverantwoordelijke desgevraagd op de hoogte stellen in

welk land de Persoonsgegevens worden verwerkt. Het is Verwerker niet toegestaan om Persoonsgegevens voor verwerking of anderszins uit te voeren naar landen buiten de EU of deze ter hand te stellen aan een vreemde mogendheid.

- 7.5 Verwerker staat er voor in en garandeert dat werknemers, Sub-Verwerkers en alle overige natuurlijke personen die handelen onder zijn gezag en toegang hebben tot de persoonsgegevens eveneens onder dezelfde voorwaarden geheimhouding zullen betrachten ten aanzien van voornoemde informatie.

Artikel 8 Beveiligingsmaatregelen

- 8.1 Verwerker neemt alle passende technische en organisatorische maatregelen om de Persoonsgegevens die voor Verwerkingsverantwoordelijke worden verwerkt te beveiligen en beveiligd te houden tegen verlies of enige vorm van onzorgvuldige, ondeskundige, ongeoorloofde of onrechtmatige verwerking. Deze maatregelen, gespecificeerd in Bijlage 3, garanderen een passend beveiligingsniveau gelet op de gevoelige aard van de Persoonsgegevens die Verwerker verwerkt. Verwerker is voorts gehouden tot naleving van de normen en standaards van Verwerkingsverantwoordelijke, zoals beschreven in de Hoofdovereenkomst en neemt steeds alle maatregelen die Verwerkingsverantwoordelijke van een professioneel handelende Verwerker van Persoonsgegevens mag verwachten.
- 8.2 Verwerker erkent dat beveiligingseisen voortdurend veranderen en dat een effectieve beveiliging frequente evaluatie en regelmatige verbetering van verouderde beveiligingsmaatregelen vereist en staat er niet voor in dat de beveiliging onder alle omstandigheden doeltreffend is. Verwerker zal daarom de maatregelen zoals geïmplementeerd op basis van dit artikel periodiek evalueren en, waar nodig, de maatregelen verbeteren om te blijven voldoen aan de verplichtingen onder dit artikel

Artikel 9 Audit

- 9.1 Verwerkingsverantwoordelijke is gerechtigd naleving van de hiervoor onder artikel 8 genoemde beveiligingsmaatregelen in verband met de verwerkingsactiviteiten die onder deze Overeenkomst vallen, te (laten) onderzoeken (verder te noemen '**Audit**'). Verwerker is verplicht Verwerkingsverantwoordelijke of de, in opdracht van Verwerkingsverantwoordelijke, controlerende instantie toe te laten en alle medewerking te verlenen zodat de Audit daadwerkelijk uitgevoerd kan worden.

- 9.2 Verwerkingsverantwoordelijke zal de Audit slechts (laten) uitvoeren na een voorafgaande schriftelijke melding aan Bewerker. Indien Verwerkingsverantwoordelijke de Audit laat uitvoeren door een controlerende instantie, dan dient deze naar het redelijk oordeel van beide Partijen neutraal en deskundig te zijn. Verwerkingsverantwoordelijke draagt zorg dat de controlerende instantie tot geheimhouding van haar bevindingen tegenover derden is verplicht.
- 9.3 Verwerker verbindt zich om binnen een door Verwerkingsverantwoordelijke te bepalen termijn Verwerkingsverantwoordelijke, of de door Verantwoordelijke ingeschakelde controlerende instantie, te voorzien van de verlangde informatie ten behoeve van de Audit. Hierdoor kan Verwerkingsverantwoordelijke, of de door Verwerkingsverantwoordelijke ingeschakelde controlerende instantie, zich een oordeel vormen over de naleving door Verwerker van de Hoofdovereenkomst en deze Overeenkomst.
- 9.4 Verwerkingsverantwoordelijke zal Verwerker een exemplaar van het rapport van de Audit verstrekken. Indien het rapport tot aanbevelingen leidt, garandeert Verwerker de aangegeven aanbevelingen ter verbetering die voortvloeien uit de Audit binnen de daartoe door Verwerkingsverantwoordelijke te bepalen redelijke termijn uit te voeren.
- 9.5 Indien een uitdrukkelijk omschreven beveiliging in de Hoofdovereenkomst dan wel in deze Overeenkomst ontbreekt, zal Verwerker zich inspannen dat de beveiliging zal voldoen aan een niveau dat, gelet op de stand van de techniek, de gevoeligheid van de Persoonsgegevens en de aan het treffen van de beveiliging verbonden kosten, niet onredelijk is.
- 9.6 De met de Audit gemoeide kosten, vergoedingen en onkosten met inbegrip van redelijke door Verwerker gemaakte interne kosten, zijn volledig voor de rekening van Verwerkingsverantwoordelijke, tenzij uit de audit blijkt dat er sprake is van een aan Verwerker toerekenbare tekortkoming in de nakoming van diens verplichtingen voortvloeiende uit de Hoofdovereenkomst, deze Overeenkomst of toepasselijke wet- en regelgeving op het gebied van bescherming van Persoonsgegevens.

Artikel 10 Meldplicht inbreuk (datalek)

- 10.1 Partijen informeren elkaar over iedere inbreuk op Persoonsgegevens, volgens de specificatie opgenomen in Bijlage 4, met bijvoorbeeld de vernietiging, het verlies, de

wijziging of de ongeoorloofde verstrekking van of ongeoorloofde toegang tot Persoonsgegevens tot gevolg.

- 10.2 Partijen verlenen alle noodzakelijke informatie zonder onredelijke vertraging, doch in ieder geval binnen de in de toepasselijke wet- en regelgeving opgenomen termijnen, zodra daarvan kennis is genomen. Indien en voor zover het niet mogelijk is om alle informatie gelijktijdig te verstrekken, kan de informatie zonder onredelijke vertraging in stappen worden verstrekt.
- 10.3 Niettegenstaande het voorgaande, stellen Partijen elkaar onmiddellijk, doch uiterlijk binnen vierentwintig (24) uur, na het ontdekken van een mogelijke beveiligingsinbreuk of datalek op de hoogte door het sturen van een bericht aan de primaire contactpersoon van de andere Partij, zoals opgenomen in Bijlage 4. Het bericht bevat in ieder geval:
- a. de aard van de inbreuk, wat de bekende en/of te verwachten gevolgen zijn en wat de (voorgestelde) oplossing is, waar mogelijk onder vermelding van de categorieën van Betrokkenen en bij benadering het aantal Betrokkenen in kwestie;
 - b. de naam van de organisatie en contactpersoon inclusief contactgegevens zoals e-mailadres en telefoonnummer waar meer informatie kan worden verkregen en indien van toepassing ook de naam en de contactgegevens van de functionaris voor gegevensbescherming;
 - c. de dag en het tijdstip waarop de mogelijke beveiligingsinbreuk of het mogelijke datalek is geconstateerd;
 - d. de maatregelen die zijn voorgesteld of genomen om de inbreuk aan te pakken, waaronder de maatregelen ter beperking van eventuele nadelige gevolgen daarvan;
 - e. enige andere informatie die nodig is op basis van de toepasselijke wet- en regelgeving.
- 10.4 Het is Verwerker niet toegestaan om namens Verwerkingsverantwoordelijke een melding bij de AP te doen van een inbreuk op de beveiliging van de Persoonsgegevens. Verwerkingsverantwoordelijke stelt Verwerker per omgaande op de hoogte van het melding-nummer bij AP.
- 10.5 Verwerker stelt Verwerkingsverantwoordelijke in staat om aan de wettelijke verplichtingen betreffende de melding krachtens artikel 33 AVG te voldoen. Meer specifiek rusten op Verwerker ingeval van een mogelijk datalek de navolgende verplichtingen:

- a. Verwerker legt alle benodigde gegevens voor de beoordeling van het datalek aan Verwerkingsverantwoordelijke over;
- b. Verwerker houdt Verwerkingsverantwoordelijke op de hoogte van de voortgang van het intern onderzoek en de ontwikkelingen rond het beveiligingsincident;
- c. Verwerker verleent de volledige medewerking indien Verwerkingsverantwoordelijke zelf onderzoek naar het datalek wenst uit te voeren;
- d. Verwerker stelt Verwerkingsverantwoordelijke op de hoogte van de maatregelen die hij treft om de gevolgen van het incident te beperken en om een herhaling te voorkomen;
- e. Verwerker verleent alle medewerking zodat Verwerkingsverantwoordelijke in staat is om Betrokkene(n) in kennis te stellen;
- f. Verwerker volgt de instructies van Verwerkingsverantwoordelijke op, en;
- g. Verwerker voldoet aan de bindende aanwijzing van de toezichthoudende autoriteit, ook indien deze aan Verwerkingsverantwoordelijke wordt gegeven.

10.6 Voor zover het datalek een beveiligingsincident betreft bij Verwerker, zal Verwerker op eigen kosten en voor eigen rekening ervoor zorgdragen dat de beveiligingsmaatregelen aangepast worden zodat in het vervolg een dergelijke beveiligingsincident c.q. datalek wordt voorkomen.

Artikel 11 Rechten van betrokkenen

- 11.1 Verwerker stelt Verwerkingsverantwoordelijke te allen tijde in staat om binnen de wettelijke termijnen te voldoen aan de verplichtingen op grond van de AVG en meer in het bijzonder de rechten van Betrokkenen.
- 11.2 Verwerker zal daartoe op eerste verzoek van Verwerkingsverantwoordelijke zo spoedig mogelijk, doch uiterlijk binnen zeven (7) werkdagen nadat het verzoek is gedaan aan Verwerkingsverantwoordelijke schriftelijk alle informatie verstrekken die Verwerkingsverantwoordelijke nodig mocht hebben om te kunnen voldoen aan de in artikel 15 tot en met artikel 22 AVG vervatte rechten van Betrokkenen.
- 11.3 Verwerker zal tevens op eerste verzoek van Verwerkingsverantwoordelijke, Persoonsgegevens verbeteren, aanvullen, verwijderen of afschermen alsook een gehonoreerd aangetekend verzet uitvoeren. Verwerker zal aan dit verzoek voldoen binnen zodanige termijn dat Verwerkingsverantwoordelijke niet in overtreding is van

de in artikel 12 AVG genoemde termijn, doch in elk geval binnen tien (10) werkdagen nadat het verzoek door Verwerkingsverantwoordelijke is gedaan.

- 11.4 In het geval dat een Betrokkene zich rechtstreeks tot Verwerker wendt en een beroep op diens rechten doet, dan zal Verwerker het beroep van Betrokkene op diens rechten zelf afhandelen en Verwerkingsverantwoordelijke hiervan binnen zeven (7) werkdagen nadat Betrokkene zich bij Verwerker op diens rechten heeft beroepen hiervan op de hoogte stellen. Alle hieruit voortvloeiende kosten komen volledig voor de rekening van Verwerkingsverantwoordelijke.

Artikel 12 Aansprakelijkheid

- 12.1 Indien Verwerker enig in artikel 8 en/of artikel 10 van deze Overeenkomst neergelegde verplichting niet of niet-tijdig nakomt en de toezichthoudende autoriteit Verwerkingsverantwoordelijke als gevolg daarvan een boete oplegt, dan wordt Verwerker daarvoor aansprakelijk geacht en zal Verwerkingsverantwoordelijke betaling van de opgelegde boete, ter hoogte van hetzelfde bedrag, van Verwerker vorderen. Deze boete is zonder rechterlijke tussenkomst, ingebrekestelling of aanmaning direct opeisbaar. Deze boete is niet vatbaar voor verrekening. Het vorderen van deze boete laat alle andere rechten of vorderingen van Verwerkingsverantwoordelijke, inclusief onder andere het recht op nakoming en/of schadevergoeding, onverlet.
- 12.2 Indien Verwerker tekortschiet in de nakoming van enige andere verplichting uit deze Overeenkomst kan Verwerkingsverantwoordelijke hem in gebreke stellen. Verwerker is echter onmiddellijk in gebreke als de nakoming van desbetreffende verplichting anders dan door overmacht zoals gedefinieerd in de Hoofdovereenkomst binnen de overeengekomen termijn reeds blijvend onmogelijk is. Ingebrekestelling geschiedt schriftelijk, waarbij aan Verwerker een redelijke termijn wordt gegund om alsnog zijn verplichtingen na te komen. Deze termijn is een fatale termijn. Indien nakoming binnen deze termijn uitblijft, is Verwerker in verzuim.
- 12.3 Verwerker is niet aansprakelijk voor schade en/of nadeel die/dat het gevolg is van het niet naleven van de AVG en/of overige toepasselijke wet- en/of regelgeving op het gebied van bescherming van Persoonsgegevens door Verwerkingsverantwoordelijke. Verwerker is uitsluitend aansprakelijk voor schade of nadeel die het rechtstreekse gevolg is van (een samenhangende serie van) toerekenbare tekortkomingen voortvloeiende uit of verband houdend met het niet-nakomen van, of in strijd handelen met deze Overeenkomst en/of toepasselijke wet-

en regelgeving aan haar zijde, onverminderd de aanspraken op grond van wettelijke regels. Verwerker is aansprakelijk voor schade of nadeel voor zover ontstaan door haar werkzaamheid. Verwerker is tevens aansprakelijk voor alle schade of nadeel voortvloeiende uit de door haar werkzaamheid ontstane inbreuken op de persoonlijke levenssfeer van betrokkenen.

- 12.4 De aansprakelijkheid van Verwerker voor directe schade is beperkt tot het bedrag dat volgens de aansprakelijkheidsverzekeraar van Verwerker voor het betreffende geval wordt uitgekeerd, vermeerderd met het eventueel door Verwerker uit hoofde van de verzekering te dragen eigen risico. Indien, om welke reden dan ook, de aansprakelijkheidsverzekeraar niet tot uitkering overgaat, is de aansprakelijkheid van Verwerker beperkt tot het bedrag van het voor de uitvoering van de Hoofdovereenkomst in rekening gebrachte jaarhonorarium.
- 12.5 Onder directe schade wordt uitsluitend verstaan alle schade bestaande uit:
- a. schade direct toegebracht aan stoffelijke zaken (zaakschade);
 - b. redelijke en aantoonbare kosten om Verwerker er toe te manen deze Overeenkomst (weer) degelijk na te komen;
 - c. redelijke kosten ter vaststelling van de oorzaak en de omvang van de schade voor zover betrekking hebbende op de directe schade zoals hier bedoeld is, en;
 - d. redelijke en aantoonbare kosten die Verwerkingsverantwoordelijke heeft gemaakt ter voorkoming of beperking van de directe schade zoals in dit artikel bedoeld.
- 12.6 De aansprakelijkheid van Verwerker voor indirecte schade is uitgesloten. Onder indirecte schade wordt verstaan alle schade die geen directe schade is en daarmee in ieder geval, maar niet beperkt tot, gevolgschade, gederfde winst, gemiste besparingen, verminderde goodwill, schade door bedrijfsstagnatie, schade door het niet behalen van marketingdoeleinden, schade verband houdende met het gebruik van door Verwerkingsverantwoordelijke voorgeschreven gegevens of databestanden, of verlies, verminking of vernietiging van gegevens of databestanden.
- 12.7 Verwerker vrijwaart Verwerkingsverantwoordelijke tegen aanspraken van Betrokkene(n), in verband met het toerekenbaar tekort schieten van Verwerker in de nakoming van deze Overeenkomst of overtreding door Verwerker van enige toepasselijke wet- en/of regelgeving op het gebied van bescherming van Persoonsgegevens.

- 12.8 De in dit artikel bedoelde uitsluitingen en beperkingen komen te vervallen indien en voor zover de schade het gevolg is van opzet of bewuste roekeloosheid van Verwerker, haar werknemers of de door haar ingeschakelde Sub-Verwerker.
- 12.9 Iedere vordering tot schadevergoeding door Verwerkingsverantwoordelijke tegen Verwerker die niet gespecificeerd en expliciet is gemeld, vervalt door het enkele verloop van twaalf (12) maanden na het ontstaan van de vordering.
- 12.10 Verwerker zal zich gedurende de Verwerkersovereenkomst adequaat verzekerd hebben en houden voor aansprakelijkheid conform dit artikel. De verzekeringsvoorwaarden hiertoe kunnen op verzoek worden ingezien.

Artikel 13 Boetebepaling

- 13.1 Indien Verwerker toerekenbaar tekortschiet in de nakoming van diens verplichtingen uit deze Overeenkomst, is Verwerker zonder rechterlijke tussenkomst, ingebrekestelling of aanmaning een direct opeisbare boete verschuldigd van € 1.000,00 (zegge: duizend Euro) voor elke tekortkoming alsmede een boete van € 500,00 (zegge: vijfhonderd Euro) voor elke dag dat de tekortkoming voortduurt. De boete is niet vatbaar voor verrekening.
- 13.2 De boete laat onverlet alle andere rechten of vorderingen, waaronder, doch niet uitsluitend, de vordering van Verwerkingsverantwoordelijke tot nakoming en/of het recht op schadevergoeding. Betaling van de boete ontslaat de Verwerker niet van zijn verplichting tot deugdelijke nakoming van deze Overeenkomst.

Artikel 14 Wijziging Overeenkomst

- 14.1 Wijzigingen op deze Overeenkomst en/of de bijlagen zijn alleen geldig voor zover deze schriftelijk zijn vastgelegd en zijn ondertekend door beide Partijen.
- 14.2 Indien één of meer bepalingen van deze Overeenkomst niet rechtsgeldig blijkt te zijn, zal deze Overeenkomst voor het overige van kracht blijven. Partijen zullen over de bepalingen welke niet rechtsgeldig zijn overleg plegen, teneinde een vervangende regeling te treffen die wel rechtsgeldig is en zoveel mogelijk aansluit bij de strekking van de te vervangen regeling.

Artikel 15 Rechts- en forumkeuze

15.1 Op deze Overeenkomst en alle hieruit voortvloeiende verbintenissen is uitsluitend Nederlands recht van toepassing.

15.2 Alle geschillen voortvloeiende of samenhangende met deze Overeenkomst en/of de hieruit voortvloeiende verbintenissen zullen uitsluitend worden voorgelegd aan de bevoegde rechter te Utrecht.

Aldus door Partijen opgemaakt en in tweevoud ondertekend op [datum] te [plaats].

N.V. SRO

Voor deze

drs. M.C. Bloemsma RA

directeur

[Statutaire Naam]

Voor deze

[de heer/mevrouw naam]

[functie]

Bijlage 1 Hoofdovereenkomst

Deze Overeenkomst is van toepassing op de Diensten die worden verleend uit hoofde van de Hoofdovereenkomst tussen de Verwerkingsverantwoordelijke en Verwerker, met de volgende kenmerken:

Datum	Titel	Omschrijving

Bijlage 2 Verwerking Persoonsgegevens

Onderstaande gegevens betreffen de specificatie van Persoonsgegevens, het doel van verwerking en de Betrokkenen die ten behoeve van de onder Bijlage 1 genoemde Hoofdovereenkomst worden verwerkt.

Doel van de verwerking	[invullen]
Toelichting	[invullen]
Categorie gegevens	[invullen]
Categorie betrokkenen	[invullen]
Categorie Persoonsgegevens (*)	• Geslacht • Naam (voornamen, tussenvoegsel, achternaam) • Adres (straat, huisnummer, huisnummertoevoeging) • Woonplaats en postcode • Telefoonnummer • E-mailadres • Inschrijving nieuwsbrief
Categorie ontvangers	[invullen]
Bewaartermijn	[invullen]

[(*) Deze lijst bevat voorbeelden van persoonsgegevens. Deze lijst moet worden aangevuld door Verwerkingsverantwoordelijke.]

Verwerker, garandeert maatregelen die persoonsgegevens beschermt tegen ongeoorloofde of onrechtmatige verwerking en tegen verlies, vernietiging of beschadiging van data. De getroffen beveiligingsmaatregelen ten tijde van de totstandkoming van deze overeenkomst zijn onderstaand opgenomen en worden periodiek geëvalueerd en zo nodig geactualiseerd.

Technische beveiligingsmaatregelen (*)

Technische voorzieningen die erop zijn gericht om verlies of onrechtmatige verwerking van persoonsgegevens te voorkomen of beperken dan wel de ernst van de gevolgen daarvan zo beperkt mogelijk te houden.

De volgende maatregelen zijn van kracht:

- Versleutelde communicatie persoonsgegevens;
- Twee factor authenticatie voor toegang tot persoonsgegevens;
- Logging van toegang en mutaties;
- Aanwezigheid van firewalls, virusscanners en software tegen malware-aanvallen op serverniveau;
- Dagelijkse back-up;
- Beveiligde server enkel benaderbaar vanuit vastgestelde ip-adressen;
- Toegang tot database enkel op basis van accountnaam, wachtwoord en sms-verificatie;
- Systemen alleen benaderbaar via een beveiligde verbinding door middel van encryptie data;
- Wachtwoorden bij accounts worden opgeslagen als hash-code en daarmee onherkenbaar gemaakt;
- Gebruikers hebben alleen toegang tot persoonsgegevens binnen eigen projecten.

Organisatorische beveiligingsmaatregelen (*)

Beveiligingsmaatregelen die er voor zorgen dat persoonsgegevens alleen toegankelijk zijn voor die personen binnen de organisatie die de gegevens nodig hebben voor de uitvoering van hun taken.

De volgende maatregelen zijn van kracht:

- De servers van Verwerker en/of de door Verwerker ingeschakelde Sub-Verwerker zijn ondergebracht in een Nederlands datacenter die ISO27001 en NEN7510 gecertificeerd is.
- Iedere computer voorzien van inlogbeveiliging, virusscanners, software tegen malwareaanvallen en een versleutelde harde schijf;
- Interne netwerk voorzien van firewall;
- Beperking tot toegang privacy gevoelige informatie, enkel beschikbaar voor (service) medewerkers die deze toegang nodig hebben voor de werkzaamheden;
- Geheimhoudingsverklaring voor iedere medewerker, inclusief externen (freelance);
- Verwerkersovereenkomsten met leveranciers;
- Het creëren van informatieveiligheidsbewustzijn onder medewerkers;
- Bij uitdiensttreding van een medewerker treedt de procedure in werking voor het ontszeggen van toegang tot bedrijfsgevoelige informatie en persoonsgegevens;
- Duidelijke protocollen en procedures voor het tijdig en doeltreffend behandelen van informatiebeveiligingsincidenten en zwakke plekken in de beveiliging.

[(*) Deze lijsten bevat voorbeelden van technische en organisatorische maatregelen. Deze lijst moet worden aangevuld door Verwerkingsverantwoordelijke en Verwerker.]

Bijlage 4 Procedure Meldplicht Datalekken

Contactpersonen

De contactpersoon van Verwerkingsverantwoordelijke inzake meldplicht datalekken is:

Organisatie:	
Contactpersoon:	
Functie:	
Telefoon:	
E-mail:	

De contactpersoon van Verwerker inzake meldplicht datalekken is:

Organisatie:	
Contactpersoon:	
Functie:	
Telefoon:	
E-mail:	

Bij het melden van een datalek worden de volgende gegevens verstrekt:

1. Gegevens over het datalek

Wat is de aard van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest?

Selecteer een van de opties	JA	NEE
Apparaat, gegevensdrager (bijv. USB-stick) en/of papier met persoonsgegevens kwijtgeraakt of gestolen		
Brief of postpakket met persoonsgegevens kwijtgeraakt of geopend retour ontvangen		
Hacking, malware (bijv. ransomware) en/of phishing		
Persoonsgegevens bij oud papier gezet		
Persoonsgegevens nog aanwezig op afgedankt apparaat of op afgedankte gegevensdrager (bijv. USBstick)		
Persoonsgegevens per ongeluk gepubliceerd		

Persoonsgegevens van verkeerde klant getoond in klantportaal		
Persoonsgegevens verstuurd of afgegeven aan verkeerde ontvanger		
Anders, namelijk:		

Geef een samenvatting van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest (tekstuele toelichting).

Vond de inbreuk plaats in een verwerking die is uitbesteed aan een andere organisatie?

Selecteer een van de opties		JA	NEE
Organisatie:			
Contactpersoon:			
Functie:			
Telefoon:			
E-mail:			

Van minimaal hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?

Van maximaal hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?

Omschrijf de groep mensen van wie persoonsgegevens zijn betrokken bij de inbreuk.

--

Is bekend wanneer de inbreuk was?

Selecteer een van de opties	JA	NEE
Bekend		

Is de exacte datum bekend wanneer de inbreuk was?

Selecteer een van de opties	JA	NEE
Bekend		

Exacte datum waarop de inbreuk was

dd/mm/jjjj

Startdatum van de periode waarbinnen de inbreuk was

dd/mm/jjjj

Einddatum van de periode waarbinnen de inbreuk was

dd/mm/jjjj

Wanneer werd de inbreuk ontdekt?

dd/mm/jjjj

2. Wat is de aard van de inbreuk?

Selecteer één of meerdere opties	JA	NEE
Lezen (vertrouwelijkheid)		
Kopiëren		
Veranderen (integriteit)		
Verwijderen of vernietigen (beschikbaarheid)		
Diefstal		
Nog niet bekend		

3. Om welk type persoonsgegevens gaat het?

Selecteer één of meerdere opties en geef, indien van toepassing, een toelichting:	JA	NEE
Naam-, adres- en woonplaatsgegevens		
Telefoonnummers		
E-mailadressen of andere adressen voor elektronische communicatie		
Toegangs- of identificatiegegevens		
Financiële gegevens		
Burgerservicenummer (BSN)		
Paspoortkopieën of kopieën van andere legitimatiebewijzen		
Geslacht, geboortedatum en/of leeftijd		

4. Bijzondere persoonsgegevens

Selecteer één of meerdere opties en geef, indien van toepassing, een toelichting:	JA	NEE
Over iemands godsdienst of levensovertuiging		
Over iemands ras		
Over iemands politieke gezindheid		
Over iemands gezondheid		
Over iemands seksuele leven		
Over het lidmaatschap van een vakvereniging		
Strafrechtelijke persoonsgegevens		
Over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag		
Overige / onbekend, namelijk:		

5. Welke gevolgen kan de inbreuk hebben voor de persoonlijke levenssfeer van de betrokkenen?

Selecteer één of meerdere opties	JA	NEE
Stigmatisering of uitsluiting		
Schade aan de gezondheid		
Blootstelling aan (identiteits)fraude		
Blootstelling aan spam of phishing		
Andere gevolgen, namelijk:		