

Verwerkersovereenkomst Tangram

1. Algemeen

- 1.1 De bepalingen uit de Overeenkomst zijn onverkort van toepassing op de Verwerkersovereenkomst. Deze verwerkersovereenkomst vormt een integraal onderdeel van de Overeenkomst. Voor zover er in de Overeenkomst bepalingen omtrent de verwerking van persoonsgegevens zijn opgenomen, prevaleren de bepalingen uit deze Verwerkersovereenkomst.
- 1.2 De klant is ten aanzien van de verwerking van persoonsgegevens in het kader van de Overeenkomst verwerkingsverantwoordelijke in de zin van artikel 4(7) van de Algemene verordening gegevensbescherming ("AVG") aan te merken en Tangram als verwerker in de zin van artikel 4(8) AVG.
- 1.3 Begrippen uit de AVG zoals "verwerken", "persoonsgegevens", "verwerkingsverantwoordelijke" en "verwerker" hebben de betekenis die daaraan is gegeven in de AVG.

2. VERWERKING PERSOONSGEGEVENS

- 2.1 De categorieën van Betrokkenen en soorten Persoonsgegevens die door Verwerker worden verwerkt en het doel van die verwerking zijn opgenomen in **Bijlage 1**.
- 2.2 Verwerker zal de Persoonsgegevens die aan haar bekend worden uitsluitend verwerken op basis van schriftelijke instructies van Verwerkingsverantwoordelijke en enkel in het kader van de uitvoering van de Overeenkomst, tenzij een op Verwerker van toepassing zijnde Unierechtelijke of lidstaatrechtelijke bepaling hem tot verwerking verplicht. In dat geval stelt Verwerker Verwerkingsverantwoordelijke, voorafgaand aan de verwerking, in kennis van dat wettelijk voorschrift, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt.

- 2.3 Verwerker heeft geen zeggenschap over het doel en middelen van de verwerking van Persoonsgegevens. Niets in deze Verwerkersovereenkomst is bedoeld om op enigerlei wijze zeggenschap ten aanzien van de Persoonsgegevens aan Verwerker over te dragen.

- 2.4 Het is Verwerker niet toegestaan de Persoonsgegevens:

- 2.4.1 voor eigen doeleinden te verwerken;
- 2.4.2 voor andere of verdergaande doeleinden te verwerken dan redelijkerwijs nodig in het kader van de uitvoering van de Overeenkomst;
- 2.4.3 aan derden te verstrekken voor zover dat niet is toegestaan op basis van de Overeenkomst en/of de Verwerkersovereenkomst en/of op grond van een dwingendrechtelijke bepaling op grond waarvan Verwerker verplicht is Persoonsgegevens aan (toezichthoudende of opsporings-) autoriteiten te verstrekken.

3. NALEVING WET- EN REGELGEVING

- 3.1 Partijen zullen zich gedragen overeenkomstig de op enig moment geldende bepalingen van de AVG en toekomstige (Europese) wet- en regelgeving op het gebied van verwerking van persoonsgegevens. Indien toekomstige wet- en regelgeving noopt tot aanpassing van de Verwerkersovereenkomst, zullen Partijen in overleg treden teneinde nieuwe afspraken te maken waardoor de strekking van deze Verwerkersovereenkomst zo veel mogelijk wordt gehandhaafd.
- 3.2 Verwerker verleent Verwerkingsverantwoordelijke medewerking bij de uitvoering van een Data Protection Impact Assessment, althans voor zover dat

- mogelijk is in verband met de hem ter beschikking staande informatie en de aard van de verwerking. De redelijke kosten die deze medewerkingsplicht met zich meebrengt voor Verwerker worden door Verwerkingsverantwoordelijke gedragen.
- 3.3 Indien en voor zover Verwerkingsverantwoordelijke op grond van wet- en regelgeving gehouden is om aan een toezichthoudende autoriteit informatie te verstrekken over het verwerken van Persoonsgegevens, dan zal Verwerker op eerste verzoek van Verwerkingsverantwoordelijke alle redelijkerwijs verzochte medewerking verlenen aan Verwerkingsverantwoordelijke, zodat deze informatie beschikbaar komt en de toezichthoudende autoriteit naar behoren kan worden geïnformeerd.
- 4. GEHEIMHOUDING**
- 4.1 Verwerker is verplicht de Persoonsgegevens geheim te houden en zal waarborgen dat de tot het verwerken van de Persoonsgegevens gemachtigde personen zich ertoe hebben verbonden vertrouwelijkheid in acht te nemen.
- 4.2 Ook na de beëindiging van deze Verwerkersovereenkomst blijft deze geheimhoudingsplicht bestaan, behalve voor zover het informatie betreft die reeds publiekelijk bekend is geworden, anders dan ten gevolge van een schending van de voormelde geheimhoudingsplicht.
- 5. BEVEILIGINGSMATREGELEN VERWERKER**
- 5.1 Verwerker treft passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen, die onder meer de in **Bijlage 2** genoemde maatregelen omvatten.
- 5.2 Er wordt bij het bepalen van de maatregelen door Verwerker rekening gehouden 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.
- 5.3 Bij de beoordeling van het passende beveiligingsniveau wordt door Verwerker met name rekening gehouden met de verwerkingsrisico's, 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.
- 5.4 Verwerker treft maatregelen om ervoor te zorgen dat iedere natuurlijke persoon die handelt onder het gezag van de Verwerker en toegang heeft tot de Persoonsgegevens, deze slechts in opdracht van de Verwerkingsverantwoordelijke verwerkt, tenzij een Unierechtelijke of lidstaatrechtelijke bepaling Verwerker tot verwerking verplicht.
- 6. TOEZICHT DOOR VERWERKINGSVERANTWOORDELIJKE**
- 6.1 Verwerker voorziet Verwerkingsverantwoordelijke op diens verzoek van de noodzakelijke informatie waardoor Verwerkingsverantwoordelijke een oordeel kan vormen over de naleving door Verwerker van het bepaalde in artikelen 2, 4, 5, 7 en 10 van deze Verwerkersovereenkomst.
- 6.2 Verwerkingsverantwoordelijke heeft het recht om de naleving van de verplichtingen van Verwerker in artikelen 2, 4, 5, 7 en 10 van deze Verwerkersovereenkomst door een onafhankelijke deskundige te laten vaststellen die aan geheimhouding is gebonden. Verwerker zal aan de audit meewerken en alle voor de audit redelijkerwijs relevante informatie zo tijdig mogelijk ter beschikking stellen. De kosten

- van audits die in opdracht van Verwerkingsverantwoordelijke zijn uitgevoerd, worden door Verwerkingsverantwoordelijke gedragen, tenzij blijkt dat Verwerker haar verplichtingen niet voldoende is nagekomen in welk geval Verwerker de kosten zal dragen.
- 6.3 Indien uit het auditrapport van de onafhankelijke deskundige blijkt dat de door Verwerker getroffen maatregelen en voorzieningen niet in voldoende mate voldoen aan deze Verwerkersovereenkomst zal Verwerker onverwijld de nodige maatregelen treffen om hier alsnog aan te voldoen.
- 7. MELDPLICHT DATALEKKEN**
- 7.1 Verwerker informeert Verwerkingsverantwoordelijke onverwijld, zodra zij constateert dat een inbreuk in verband met de Persoonsgegevens heeft plaatsgevonden. Deze informatieverstrekking is zodanig dat Verwerkingsverantwoordelijke in staat is om aan haar verplichtingen op grond van artikel 33 en artikel 34 AVG te voldoen.
- 7.2 Verwerker zal Verwerkingsverantwoordelijke steeds volledig op de hoogte houden over de voortgang van het herstel en alle relevante ontwikkelingen aangaande de inbreuk als bedoeld in artikel 7.1 en de gevolgen daarvan. Verwerker zal alle maatregelen nemen die redelijkerwijze van haar kunnen worden verwacht om de nadelige gevolgen van de inbreuk als bedoeld in artikel 7.1 in voorkomend geval te herstellen dan wel zoveel mogelijk te beperken.
- 7.3 Het is Verwerker niet toegestaan om in het kader van een inbreuk als bedoeld in artikel 7.1 te communiceren met Betrokkene(n) en/of toezichthoudende autoriteit(en) anders dan op instructie van Verwerkingsverantwoordelijke, dan wel met

haar uitdrukkelijke en expliciete toestemming.

8. SUB-VERWERKERS

- 8.1 Verwerker verkrijgt hierbij toestemming om gedurende de looptijd van de Overeenkomst delen van de verwerking van de Persoonsgegevens uit te besteden aan andere verwerkers, zoals omschreven in **Bijlage 1**.
- 8.2 Verwerker licht de Verwerkingsverantwoordelijke in over beoogde veranderingen inzake de toevoeging of vervanging van sub-verwerkers, waarbij de Verwerkingsverantwoordelijke de mogelijkheid wordt geboden binnen 30 dagen tegen deze veranderingen bezwaar te maken.
- 8.3 Verwerker waarborgt dat alle door hem ingeschakelde sub-verwerkers die een rol spelen bij de uitvoering van de Overeenkomst de verplichtingen zoals vervat in deze Verwerkersovereenkomst na zullen leven, met name de verplichting afdoende garanties met betrekking tot het toepassen van passende technische en organisatorische maatregelen te bieden om zo een equivalent beschermingsniveau van de Persoonsgegevens te waarborgen.

9. VERZOEKEN VAN BETROKKENEN

- 9.1 Verwerkingsverantwoordelijke heeft op grond van de AVG verplichtingen tegenover de Betrokkenen, zoals ten aanzien van het verstrekken van informatie, het geven van inzage in, het rectificeren en verwijderen van Persoonsgegevens. Verwerker zal – indien mogelijk – medewerking verlenen aan de door Verwerkingsverantwoordelijke na te komen verplichtingen. Verwerker behoudt zich het recht voor om zijn reguliere uurtarief in rekening te brengen bij Verwerkingsverantwoordelijke voor diens medewerking.

- 9.2 Indien een Betrokkene met betrekking tot de uitvoering van zijn rechten onder de AVG direct contact opneemt met Verwerker, dan gaat Verwerker hier niet (inhoudelijk) op in, maar bericht dit onverwijld aan Verwerkingsverantwoordelijke.

10. INTERNATIONAAL VERKEER

- 10.1 Verwerker draagt er zorg voor dat iedere verwerking van Persoonsgegevens welke door of namens Verwerker met inbegrip van de door haar ingeschakelde derden wordt verricht in verband met het uitvoeren van de Overeenkomst binnen de Europese Economische Ruimte (EER) plaats zal vinden of naar of vanuit landen die een gewaarborgd beschermingsniveau bieden in overeenstemming met de AVG.
- 10.2 Zonder de voorafgaande schriftelijke toestemming van Verwerkingsverantwoordelijke mag Verwerker derhalve geen Persoonsgegevens doorgeven naar of opslaan in een land of organisatie buiten de EER of Persoonsgegevens toegankelijk maken vanuit een niet-EER land, tenzij dat land of organisatie een gewaarborgd beschermingsniveau biedt of een op de Verwerker van toepassing zijnde Unierechtelijke of lidstaatrechtelijke bepaling hem tot verwerking verplicht. In dat geval stelt de Verwerker de Verwerkingsverantwoordelijke, voorafgaand aan de verwerking, in kennis van dat wettelijk voorschrift, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt.

11. GARANTIE EN VRIJWARING

- 11.1 Verwerkingsverantwoordelijke garandeert dat de gegevensverwerking in overeenstemming met toepasselijke wet- en regelgeving plaatsvindt. Dit betekent in ieder geval dat Verwerkingsverantwoordelijke garandeert dat hij het recht heeft om de gegevens te (laten)

verzamelen en hij gerechtigd is tot het (laten) verwerken van deze gegevens.

- 11.2 Verwerkingsverantwoordelijke vrijwaart Verwerker voor schade en kosten ten gevolge van eventuele aanspraken van derden, waaronder uitdrukkelijk begrepen Betrokkene(n) en toezichthoudende autoriteiten (zoals de Autoriteit Persoonsgegevens), verbandhoudende met of voortvloeiende uit een onrechtmatige verwerking en/of andere schending van de AVG en/of de Verwerkersovereenkomst die aan de Verwerkingsverantwoordelijke kan worden toegerekend.

12. AANSPRAKELIJKHEID

- 12.1 Verwerker staat in voor een correcte naleving van de verplichtingen uit de Verwerkersovereenkomst. Deze Verwerkersovereenkomst maakt integraal onderdeel uit van de Overeenkomst tussen Verwerkingsverantwoordelijke en Verwerker en de (totale) aansprakelijkheid van Verwerker is (daarmee) beperkt conform het bepaalde in de Overeenkomst en/of algemene voorwaarden.

13. LOOPTIJD VERWERKERSOVEREENKOMST

- 13.1 Deze Verwerkersovereenkomst treedt in werking op het moment van inwerkingtreding van de Overeenkomst en wordt aangegaan voor de looptijd van de Overeenkomst.
- 13.2 Zodra de Overeenkomst wordt beëindigd of eindigt, om welke reden dan ook, blijft onderhavige Verwerkersovereenkomst van kracht zolang er door Verwerker Persoonsgegevens worden verwerkt, waarna deze Verwerkersovereenkomst van rechtswege eindigt.
- 13.3 Na afloop van deze Verwerkersovereenkomst zal Verwerker, op eerste verzoek en naar keuze van de Verwerkingsverantwoordelijke, alle Persoonsgegevens wissen of deze aan hem

terugbezorgen.

Verwerkingsverantwoordelijke dient zijn keuze uiterlijk twee (2) weken voor beëindiging van de Verwerkersovereenkomst aan Verwerker kenbaar te maken. Indien Verwerker deze keuze niet tijdig ontvangt, is Verwerker gerechtigd om de Persoonsgegevens te wissen.

- 13.4 Verwerker behoudt uitsluitend een kopie van de Persoonsgegevens indien deze daartoe

op grond van een dwingende wetsbepaling is verplicht.

14. SLOTBEPALING

- 14.1 Wijzigingen van en aanvullingen op onderhavige Verwerkersovereenkomst zijn slechts geldig indien zij schriftelijk tussen Partijen zijn overeengekomen.
- 14.2 Op deze Verwerkersovereenkomst is uitsluitend Nederlands recht van toepassing.

BIJLAGE 1 OVERZICHT PERSOONSGEGEVENS EN SUBVERWERKERS

TANGRAM

De Klant maakt gebruik van een van of meerdere onderstaande diensten:

Dienst: Online Sollicitatie formulier (TIS)

Aard van de verwerking

Verwerking van sollicitatie gegevens ten behoeve van een gerichte sollicitatie of arbeidsbemiddeling.

Soort Persoonsgegevens

NAW gegevens, Telefoonnummer, E-mailadres, Sociale media profielen, Persoonlijke kenmerken, Opleiding en vorming, Beroep en betrekking, Website gedrag (ip-nummer).

Categorieën van betrokkenen

Sollicitanten.

Doeleinden van de verwerking

Gegevens worden verstrekt in het kader van een sollicitatie of arbeidsbemiddeling.

Dienst: Hosted Database

Aard van de verwerking

Verwerking van sollicitatie gegevens ten behoeve van een gerichte sollicitatie of arbeidsbemiddeling.

Soort Persoonsgegevens

NAW gegevens, Telefoonnummer, E-mailadres, Sociale media profielen, Persoonlijke kenmerken, Opleiding en vorming, Beroep en betrekking, Website gedrag (ip-nummer). Mogelijke opslag van bijzondere persoonsgegevens als BSN, kopie identiteitsbewijs.

Categorieën van betrokkenen

Sollicitanten, Contactpersonen opdrachtgevers.

Doeleinden van de verwerking

Gegevens worden verstrekt in het kader van een sollicitatie of arbeidsbemiddeling.

Dienst: TIS Manager/ Online Dashboard

Aard van de verwerking

Verwerking van sollicitatie gegevens ten behoeve van een gerichte sollicitatie.

Soort Persoonsgegevens

NAW gegevens, Telefoonnummer, E-mailadres, Sociale media profielen, Persoonlijke kenmerken, Opleiding en vorming, Beroep en betrekking.

Categorieën van betrokkenen

Sollicitanten.

Doeleinden van de verwerking

Gegevens worden verstrekt in het kader van een sollicitatie.

Goedgekeurde subverwerkers

Naam en contactgegevens subverwerker	KvK-nummer	Uitbestede verwerkingen	Toepassing
Micros Internetdiensten B.V. Oostplein 426 3061 CH Rotterdam	24299825	..	Werving en selectie, relatiebeheer, klant- en contractadministratie
Textkernel BV Nieuwendammerkade 26A-5 1022 AB Amsterdam	59663863	Verwerking CV gegevens	Werving en selectie
Flipbase B.V. Tingietersweg 99 2031 ER Haarlem	69080860	Verwerking beeldmateriaal	Video solliciteren

Duur van de verwerking

Gedurende de looptijd van de verwerkersovereenkomst.

BIJLAGE 2 SPECIFICATIE VAN BEVEILIGING

Technische en organisatorische beveiligingsmaatregelen TANGRAM

A. Algemene informatie over getroffen beveiligingsmaatregelen:

- Er is een informatiebeveiligingsbeleid opgesteld, waarin de best practices rondom informatiebeveiliging zijn opgenomen. Het informatiebeveiligingsprogramma is van toepassing op de gehele IT-infrastructuur, met strenge wachtwoordregels, firewalls en antivirusbescherming.
- Verwerkingsactiviteiten worden gedocumenteerd, verantwoordelijkheden zijn duidelijk toegewezen en periodieke beoordelingen van gegevensbescherming worden uitgevoerd om naleving te waarborgen.
- Systemen worden regelmatig bijgewerkt en gepatcht, met actuele virusbescherming en kwetsbaarheidsscans om misbruik te voorkomen.
- Werknemers van Tangram hebben een arbeidsovereenkomst met geheimhoudingsovereenkomst getekend. Regelmatige training over AVG-vereisten, best practices voor gegevensbescherming en informatiebeveiliging wordt aan alle medewerkers gegeven, om een cultuur van naleving te bevorderen.
- Persoonsgegevens worden uitsluitend verwerkt wanneer dat strikt noodzakelijk is voor de levering van specifieke diensten, zonder overbodige of irrelevante informatie te verzamelen.
- Persoonsgegevens worden uitsluitend verwerkt door goedgekeurde subverwerkers waarmee een verwerkersovereenkomst is afgesloten, die minimaal hetzelfde niveau van bescherming persoonsgegevens bieden als Tangram.
 - Tangram heeft een Verwerkersovereenkomst met de Subverwerkers: Micros Internetdiensten voor de hosting, Textkernel voor de CV extractie en Flipbase voor de video solliciteren.
- Persoonsgegevens worden alleen bewaard zolang dit noodzakelijk is voor het vastgestelde doel.
- Indien Tangram persoonsgegevens ontvangt in de vorm van een back-up ten behoeve van het oplossen van een software-incident of voor gegevensconversie, worden deze in een afgeschermd netwerk segment opgeslagen waar alleen de direct betrokkenen toegang toe hebben. De gegevens worden direct vernietigd zodra het niet langer noodzakelijk is om de gegevens te bewaren.
- Gedocumenteerde plannen waarborgen de continuïteit van de dienstverlening, met jaarlijkse tests om de effectiviteit te controleren.

B. Maatregelen om te zorgen dat uitsluitend bevoegd personeel toegang heeft tot de Persoonsgegevens:

- Tangram hanteert een autorisatie- en rechten structuur op basis van een gebruikersrol. Alleen medewerkers met de juiste gebruikersrol hebben toegang tot persoonsgegevens.
- Toegang tot het datacenter wordt uitsluitend verleend aan bevoegd personeel.

C. Maatregelen om de Persoonsgegevens te beschermen tegen verlies of wijziging en tegen ongevoegde of onrechtmatige verwerking, toegang of openbaarmaking:

- Gegevens worden opgeslagen in een Europees datacenter dat ISO 27001-gecertificeerd is. Het datacenter is 24/7 beveiligd, zowel elektronisch als fysiek.
- Werknemers van Tangram en haar subverwerkers hebben uitsluitend op afstand toegang tot de servers met verplichte 2-factor authenticatie.
- Logboeken van toegang tot servers worden bijgehouden en regelmatig gecontroleerd om ongeautoriseerde handelingen op te sporen.
- Een robuust back-upsysteem waarborgt de integriteit en beschikbaarheid van gegevens, met een getest noodherstelplan.

D. Maatregelen voor opsporen van zwakke plekken en incidentenbeheer:

- Extended Detection and Response (XDR) in combinatie met een 24/7 Security Operations Center (SOC), detecteert verdachte activiteiten en blokkeert ongeoorloofde toegang.
- Periodiek worden door externe partijen penetratietesten uitgevoerd op de hosted webapplicaties. Eventuele bevindingen worden doorgevoerd in de applicatie.
- Er bestaat een vastgesteld protocol voor het reageren op datalekken. De respons op incidenten omvat gedocumenteerde procedures voor het identificeren, onderzoeken en oplossen van beveiligingsinbreuken en datalekken.