Bijlage gegevensverwerking (de verwerkingsovereenkomst) Versie 1.0 incl. bijlagen 1a t/m 1c D.D. 23 mei 2018

Partij A: Risico-Consult NL "verder te noemen RC" en Partij B: Zijnde de Opdrachtgever "verder te noemen OG" zoals genoemd in de getekende offerte c.q. het opdracht formulier hebben een overeenkomst met betrekking tot daarin genoemde zaken gesloten. Ter uitvoering van deze Overeenkomst worden Persoonsgegevens verwerkt. Partij OG heeft door acceptatie van de offerte c.q. het opdrachtformulier deze verwerkersovereenkomst ook van toepassing verklaart.
OG hecht grote waarde aan het beschermen van de persoonsgegevens welke hij aan RC verstrekt, daarom is RC verantwoordelijk voor de gegevens die RC gaat verwerken en leggen zij dat in deze Verwerkersovereenkomst en de daarbij behorende bijlagen 1a t/m 1c vast wat RC wel en niet mag doen met de Persoonsgegevens, te weten:

1. Overzicht met verwerkingen van persoonsgegevens en verwerkingsdoelen
2. Overzicht met beveiligingsmaatregelen
3. Proces rondom het melden van Datalekken en de te verstrekken informatie

1. Definities:
De hierna en hiervoor gebruikte begrippen volgen uit de Algemene Verordening Gegevensbescherming en hebben de volgende betekenis:
1.1 Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de 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
1.2 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;
1.3 Verwerkingsverantwoordelijke: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen ("**Verantwoordelijke**");
1.4 Verwerker: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt ("**Bewerker**");
1.5 Betrokkene: geïdentificeerde of identificeerbaar natuurlijk persoon op wie de verwerkte persoonsgegeven betrekking hebben;
1.6 Verwerkersovereenkomst: deze overeenkomst inclusief de bijlagen ("**Bewerkersovereenkomst**");
1.7 Overeenkomst: de hoofdovereenkomst waar deze Verwerkersovereenkomst uit voortvloeit;
1.8 Inbreuk in verband met persoonsgegevens: 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 gegevens ("**Datalek**");
1.9 Gegevensbeschermingseffectbeoordeling: het uitvoeren van een beoordeling, voorafgaand aan het uitvoeren van de verwerking, van het effect van de beoogde verwerkingsactiviteiten op de bescherming van de persoonsgegevens.
1.10 Toezichthoudende autoriteit: een onafhankelijke overheidsinstantie verantwoordelijk voor het toezicht op de naleving van de wet in verband met de verwerking van Persoonsgegevens. In Nederland is dit de Autoriteit Persoonsgegevens;

2. Totstandkoming, duur en beëindiging van deze Verwerkersovereenkomst
2.1 Deze Verwerkersovereenkomst treedt in werking op de datum waarop partij OG de offerte of het opdracht formulier ondertekend.
2.2 Deze Verwerkersovereenkomst is onderdeel van de Overeenkomst en zal gelden voor zolang de Overeenkomst duurt.
2.3 Indien de Overeenkomst eindigt, eindigt deze Verwerkersovereenkomst automatisch; de Verwerkersovereenkomst kan niet apart worden opgezegd.
2.4 Na beëindiging van deze Verwerkersovereenkomst zullen de lopende verplichtingen voor RC zoals het melden van Datalekken, waarbij de Persoonsgegevens van OG betrokken zijn, en de plicht tot geheimhouding blijven voortduren.

3. Verwerken Persoonsgegevens

3.1 RC mag alleen persoonsgegevens verwerken in opdracht van het bedrijf of de persoon die de opdracht heeft verstrekt c.q. de offerte heeft getekend en heeft geen zeggenschap over de Persoonsgegevens. RC volgt de gegeven instructies hierover op en mag de persoonsgegevens niet op een andere manier verwerken, tenzij RC daar van te voren toestemming of opdracht heeft gekregen.
3.2 In Bijlage 1a wordt opgenomen welke Persoonsgegevens RC zal verwerken en waarvan de verwerkingsdoeleinden zijn om de in de offerte c.q opdracht formulier opgenomen opdracht uit te voeren.
3.3 RC houdt zich aan de wet en verwerkt de gegevens op een behoorlijke, zorgvuldige en transparante wijze.
3.4 RC mag zonder voorafgaande schriftelijke toestemming van OG geen andere personen of organisaties inschakelen bij het verwerken van de Persoonsgegevens.
3.5 Wanneer RC met toestemming van OG andere organisaties inschakelt, moeten zij minimaal voldoen aan de eisen die zijn opgenomen in deze Verwerkersovereenkomst.
3.6 Wanneer OG een verzoek krijg van een Betrokkene die zijn of haar privacy rechten wil uitoefenen, werkt RC daar binnen een termijn van 14 dagen aan mee. Deze rechten bestaan uit een verzoek om inzage, verbetering, aanvulling, verwijdering of afscherming, bezwaar maken tegen de verwerking van de persoonsgegevens en een verzoek tot overdraagbaarheid van de eigen Persoonsgegevens.
3.7 Wanneer OG RC verzoekt om OG informatie te geven, dan zal RC de informatie verstrekken die OG nodig heeft voor het uitvoeren van een Gegevensbeschermingseffectbeoordeling. OG heeft dit dan nodig om in te kunnen schatten wat het risico van de Verwerking is die RC namens OG uitvoert.

4. Beveiligen van Persoonsgegevens

4.1 RC zorgt ervoor dat de Persoonsgegevens voldoende beveiligt zijn. Om verlies en onrechtmatige verwerkingen te voorkomen neem RC passende technische en organisatorische maatregelen.
4.2 Deze maatregelen zijn afgestemd op het risico van de verwerking. Een overzicht van deze maatregelen en het beleid daarover wordt opgenomen in bijlage 1b.
4.3 OG mag een inspectie of audit in de organisatie van RC laten uitvoeren om te bepalen of het verwerken van de Persoonsgegevens aan de wet en de afspraken uit deze Verwerkersovereenkomst voldoet. Hierbij zal RC medewerking verlenen, waaronder het toegang verlenen tot gebouwen en databases en het ter beschikking stellen van alle relevante informatie.
4.5 De kosten voor de uitvoering van deze audit zullen voor rekening van OG komen ook wanneer blijkt dat RC zich niet aan de verplichtingen in deze Verwerkersovereenkomst houdt.
4.6 De controle op de algehele verwerking van Persoonsgegevens door RC kan, naast de audit mogelijkheid, ook gebeuren via zelfevaluatie. RC zal hierbij aan OG een rapport verstrekken waarin RC verklaart dat deze voldoet aan de wet en de afspraken uit deze Verwerkersovereenkomst. Deze rapportage dient te worden ondertekend door de eigenaar van RC.
4.7 Wanneer een van partijen vindt dat een wijziging in de te nemen beveiligingsmaatregelen noodzakelijk is, treden partijen in overleg over de wijziging daarvan. De kosten voor het wijzigen van de beveiligingsmaatregelen komen voor de rekening van OG.

5. Exporteren Persoonsgegevens

5.1 RC mag geen Persoonsgegevens laten verwerken door andere personen of organisaties buiten de Europese Economische Ruimte (EER), zonder daarvoor voorafgaande schriftelijke toestemming te hebben verkregen van OG.

6. Geheimhouding

6.1 RC zal verstrekte Persoonsgegevens geheim houden, tenzij dit op basis van een wettelijke verplichting niet mogelijk is.
6.2 RC zal ervoor zorgen ingeschakelde hulppersonen zich aan deze geheimhouding houden, door een geheimhoudingsplicht in de (arbeids-) contracten op te nemen.

7. Datalekken

7.1 In geval van een ontdekking van een mogelijk Datalek zal RC OG hierover informeren binnen 24 uur en hem de informatie verstrekken die is aangegeven in Bijlage 1c, zodat OG indien nodig een melding bij de Toezichthouder kan doen.
7.2 Na de melding van een Datalek aan OG, zal RC OG op de hoogte houden van nieuwe ontwikkelingen rondom het Datalek en de maatregelen die RC hebt getroffen om de omvang van het Datalek te beperken en te beëindigen en een soortgelijk incident in de toekomst te kunnen voorkomen.

7.3 Het niet toegestaan dat RC een melding van een Datalek doet aan de Toezichthouder en ook mag RC de Betrokkenen niet informeren over het Datalek. Dit is OG zijn verantwoordelijkheid.
7.4 Eventuele kosten die gemaakt worden om het Datalek op te lossen en in de toekomst te kunnen voorkomen, komen voor rekening van OG.

8. Aansprakelijkheid
8.1 Als RC zijn verplichtingen uit deze Verwerkersovereenkomst niet nakomt, stelt OG RC daarvoor aansprakelijk.
8.2 RC is aansprakelijk voor alle schade geleden door het niet nakomen van de wet en de bepalingen uit deze Verwerkersovereenkomst, voor zover dit is ontstaan door zijn werkzaamheden.
8.3 Indien RC de verplichtingen in deze Verwerkersovereenkomst overtreedt, is RC aan OG een direct opeisbare boete verschuldigd van € 50,-- voor iedere overtreding. Daarnaast behoud OG het recht om schadevergoeding te vorderen. dit alles te samen tot maximaal 20% van de waarde van de opdracht of dat deel van de opdracht waarop de overtreding van toepassing is.
8.4 RC is aansprakelijk voor 1 % van de de aan OG opgelegde bestuurlijke boete door de Toezichthouder als de geleden schade het gevolg is van jouw onrechtmatig of nalatig handelen.
8.5 OG is niet aansprakelijk voor aanspraken van Betrokkenen of andere personen en organisaties waar RC de samenwerking mee is aangegaan of waarvan RC Persoonsgegevens verwerkt, als dit het gevolg is van jouw onrechtmatig of nalatig handelen.
8.6 Voor artikel 8.1 tot 8.5 te samen is het maximaal te vorderen bedrag maximaal 20% van de waarde van de verstrekte opdracht of dat deel van de opdracht waarop de overtreding van toepassing is.

9.Teruggave Persoonsgegevens en bewaartermijnen opdrachten
9.1 Na het beëindigen van deze Verwerkersovereenkomst geeft RC de Persoonsgegevens terug. Eventuele achter gebleven Persoonsgegevens zal RC op een zorgvuldige en veilige manier vernietigen.
9.2 De Persoonsgegevens die RC verwerkt volgens deze Verwerkersovereenkomst zal RC vernietigen na verstrijken van de wettelijke bewaartermijn en de termijn zoals genoemd in de privacyverklaring. Een wettelijke bewaartermijn voor OG is bijvoorbeeld wanneer RC de Persoonsgegevens moet bewaren om belastingtechnische redenen.
9.3 RC zal na de teruggave en/of vernietiging van de Persoonsgegevens schriftelijk aan OG verklaren dat RC de Persoonsgegevens niet langer heeft.

10. Slotbepalingen
10.1 Deze Verwerkersovereenkomst is onderdeel van de getekende Opdracht formulier of offerte met de daarbij behorende voorwaarden. Alle rechten en verplichtingen uit de Overeenkomst of offerte zijn daarom ook van toepassing op de Verwerkersovereenkomst.
10.2 Bij eventuele tegenstrijdigheden tussen de bepalingen in de Verwerkersovereenkomst en de Overeenkomst, gelden de bepalingen uit deze Verwerkersovereenkomst of voorwaarden welke het minst nadelig zijn voor RC.
10.3 Afwijkingen van deze Verwerkersovereenkomst zijn slechts geldig wanneer dit samen schriftelijk af gesproken is.
10.4 Op deze Verwerkersovereenkomst en werkzaamheden is het Nederlandse recht van toepassing.
10.5 Over eventuele geschillen tussen ons bepaald de rechter in de rechtbank binnen het gebied waar RG zijn bedrijf gevestigd is.

Bijlage 1a Overzicht met verwerkingen van persoonsgegevens en verwerkingsdoelen
Beschrijving verwerkingsactiviteiten door Verwerker: activiteiten zoals opgenomen in de offerte c.q. het opdrachtformulier.
Verwerkingsdoelen: het beoordelen van risico factoren die het bedrijf van OG zouden kunnen bedreigen en het geven van daarop afgestemde risico beperkende adviezen en het uitvoeren van implementatie hiervan. Deze kunnen zowel organisatorisch als duurzaam inzetbare adviezen zijn maar ook fysiek van aard. Tevens zijn er persoonsgegevens nodig voor communicatie met OG, eventuele aangewezen personeelsleden en facturatie.
Verwerkingsverantwoordelijke: OG
Verwerker: RC
Sub verwerkers: n.v.t. of indien OG hier opdracht toe geeft
Verwerkte Persoonsgegevens: NAW gegevens, telefoonnummers, e-mailadressen, banknummers van Opdrachtgever en personeels gegevens welke noodzakelijk zijn om de onderliggende stukken te produceren. BTW nummer en KvK nummer van Opdrachtgever
Locatie verwerkingen: bij OG en RC op Locatie
Bewaartermijn: 8 jaar na het boekjaar waarin de laatste opdracht heeft plaatsgevonden dit ivm geldigheid duur van sommige duurzaam inzetbare adviezen en de bewaartermijn van 7 jaren van de belastingdienst.

Bijlage 1b: Overzicht met beveiligingsmaatregelen
Mocht OG van mening zijn dat er extra maatregelen nodig zijn zal hij dat voor ondertekenen van de offerte c.q. het opdracht formulier aan RC mededelen. RC behoudt zich het recht voor de overeenkomst dan te ontbinden of de extra kosten door te berekenen dit naar keuze van OG.

Beveiligingsmaatregelen getroffen door RC zijn:

- ✓ Up to date virusscanner
- ✓ Geen USB-sticks
- ✓ Unieke inlogcode en wachtwoord voor websites waar RC van gebruik maakt.
- ✓ Twee traps authentificatie
- ✓ Geen onbeveiligde back ups maken
- ✓ Laptop niet onbemand achterlaten
- ✓ Laptop nooit achterlaten in de auto
- ✓ Oude documenten worden op juiste manier vernietigd met papiervernietiger

Bijlage 1c: Proces rondom het melden van Datalekken en de te verstrekken informatie
Wat is een beveiligingsincident en wanneer moet dit gemeld worden?
Hieronder een aantal voorbeelden van beveiligingsincidenten die moeten worden gemeld bij de Autoriteit Persoonsgegevens.

- ✓ De website met logingegevens is gehackt of is toegankelijk voor derden.
- ✓ Verlies van een laptop of USB-stick met persoonsgegevens.
- ✓ Brieven of e-mails worden naar een verkeerd adres gestuurd.
- ✓ Een aanval van een hacker op het ICT systeem.
- ✓ Een verloren of gestolen telefoon waar persoonsgegevens op aanwezig zijn.

Wat te doen bij twijfel?
Als RC op basis van bovenstaande niet zeker weet of er sprake is van een beveiligingsincident, stelt RC zichzelf in ieder geval alvast de volgende vragen als hulpmiddel:

- ✓ Is er een technisch of fysiek beveiligingsprobleem?
- ✓ Gaat het probleem over de beveiliging van Persoonsgegevens?
- ✓ Gaat het om gevoelige gegevens zoals ras, gezondheidsgegevens, informatie over iemands financiële
- ✓ situatie, zoals salaris of gegevens waar (identiteit)fraude mee kan worden gepleegd, zoals een
- ✓ Burgerservicenummer.
- ✓ Zijn er grote hoeveelheden persoonsgegevens onbedoeld toegankelijk geworden voor derden?
- ✓ Gaat het om gegevens van kwetsbare groepen zoals kinderen?
- ✓ Worden de persoonsgegevens beheerd door een leverancier?

Ook wanneer RC twijfelt, neemt hij het zekere voor het onzekere en neem altijd contact op met de OG waar hij het beveiligingsincident meld?
Hierbij zal RC beantwoording op de onderstaande vragen proberen te geven.

- ✓ Een samenvatting van het beveiligingslek / beveiligingsincident / datalek: wat is er gebeurd?
- ✓ Hij vermeld hierbij ook de naam van het betrokken systeem.
- ✓ Welke typen persoonsgegevens zijn betrokken bij het beveiligingsincident?
- ✓ Van hoeveel personen zijn de persoonsgegevens betrokken bij het beveiligingsincident?
- ✓ Waarbij hij een minimum en maximum aantal personen zal trachten te noemen.
- ✓ Omschrijving groep personen om wiens gegevens het gaat.
- ✓ Zijn de contactgegevens van de betrokken personen bekend?
- ✓ Het kan zijn dat betrokkenen geïnformeerd moeten worden over het datalek, kunnen we deze personen in
- ✓ dat geval bereiken?
- ✓ Wat is de oorzaak (root cause) van het beveiligingsincident?
- ✓ Op welke datum of in welke periode heeft het beveiligingsincident plaats kunnen vinden?