Inserve
e info@inserve.nl
t +31 (0) 485 - 21 18 35
kvk 17265861

Verwerkersovereenkomst

v1.0 - 9 november 2020

Indien Inserve bij de uitvoering van de Overeenkomst ten behoeve van de Verwerkingsverantwoordelijke persoonsgegevens verwerkt, zijn naast de Algemene Voorwaarden en ter voldoening aan het bepaalde in artikel 28 lid 3 AVG bepaalde, de onderstaande voorwaarden van toepassing.

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, gebruikte, 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 Wij deze ondertekenen.

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 de verwerker, zoals het melden van Datalekken, waarbij de Persoonsgegevens van de verwerkingsverantwoordelijke betrokken zijn, en de plicht tot geheimhouding blijven voortduren.

3. Verwerken Persoonsgegevens

3.1 De Verwerker verwerkt alleen Persoonsgegevens in opdracht van de Verwerkingsverantwoordelijke en heeft geen zeggenschap over de Persoonsgegevens. De Verwerker volgt de instructies van de Verwerkingsverantwoordelijke hierover op en mag de Persoonsgegevens niet op een andere manier verwerken, tenzij de Verwerkingsverantwoordelijke daar van te voren toestemming of opdracht voor geeft aan de Verwerker.

3.2 In Bijlage 1 wordt opgenomen welke Persoonsgegevens de Verwerker precies zal verwerken en voor welke verwerkingsdoeleinden.

3.3 De Verwerker houdt zich aan de wet en verwerkt de gegevens op een behoorlijke, zorgvuldige en transparante wijze.

3.4 De Verwerker mag zonder voorafgaande schriftelijke toestemming van de Verwerkingsverantwoordelijke geen andere personen of organisaties inschakelen bij het verwerken van de Persoonsgegevens.

3.5 Wanneer de Verwerker met toestemming van de Verwerkingsverantwoordelijke andere organisaties inschakelt, moeten zij minimaal voldoen aan de eisen die zijn opgenomen in deze Verwerkersovereenkomst.

3.6 Wanneer de Verwerkingsverantwoordelijke een verzoek krijgt van een Betrokkene die zijn of haar privacy rechten wil uitoefenen, werkt de Verwerker daar zo snel mogelijk, maar uiterlijk binnen een termijn van 30 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 de Verwerkingsverantwoordelijke de Verwerker verzoekt om informatie te geven, dan zal Verwerker de informatie verstrekken die de Verwerkingsverantwoordelijke nodig heeft voor het uitvoeren van een Gegevensbeschermingseffectbeoordeling. De Verwerkingsverantwoordelijke heeft dit nodig om in te kunnen schatten wat het risico van de Verwerking is die de Verwerker namens de Verwerkingsverantwoordelijke uitvoert.

4. Beveiligen van Persoonsgegevens

4.1 De Verwerker zorgt ervoor dat de Persoonsgegevens voldoende beveiligd zijn. Om verlies en onrechtmatige verwerkingen te voorkomen neemt de Verwerker 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 nemen Wij op in bijlage 2.

4.3 De Verwerkingsverantwoordelijke mag een inspectie of audit bij de Verwerker laten uitvoeren om te bepalen of het verwerken van de Persoonsgegevens aan de wet en de afspraken uit deze Verwerkersovereenkomst voldoet. Hierbij zal de Verwerker medewerking verlenen, waaronder het toegang verlenen tot gebouwen en databases en het ter beschikking stellen van alle relevante informatie.

4.4 De kosten voor de uitvoering van deze audit zullen voor rekening van de Verwerker komen wanneer blijkt dat de Verwerker zich niet aan de verplichtingen in deze Verwerkersovereenkomst houdt.

4.5 De controle op de algehele verwerking van Persoonsgegevens door de verwerker kan, naast de audit mogelijkheid, ook gebeuren via zelfevaluatie. De Verwerker zal hierbij aan de Verwerkingsverantwoordelijke een rapport verstrekken waarin de Verwerker aantoont dat de Verwerker voldoet aan de wet en de afspraken uit deze Verwerkersovereenkomst.

4.6 Wanneer een van ons vindt dat een wijziging in de te nemen beveiligingsmaatregelen noodzakelijk is, treden Wij in overleg over de wijziging daarvan. De kosten voor het wijzigen van de beveiligingsmaatregelen komen voor de rekening van degene die de kosten maakt.

5. Exporteren Persoonsgegevens

5.1 De Verwerker 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 de Verwerkingsverantwoordelijke.

6. Geheimhouding

6.1 De Verwerker houdt de Persoonsgegevens welke worden verwerkt voor de Verwerkingsverantwoordelijke geheim, tenzij dit op basis van een wettelijke verplichting niet mogelijk is.

6.2 De Verwerker zorgt ervoor dat ook zijn personeel en 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 de Verwerker, de Verwerkingsverantwoordelijke hierover informeren binnen 36 uur per e-mail en de informatie verstrekken die is aangegeven in Bijlage 3, zodat de Verwerkingsverantwoordelijke indien nodig een melding bij de Toezichthouder kan doen.

7.2 Na de melding van een Datalek door de Verwerker aan de Verwerkingsverantwoordelijke, wordt de Verwerkingsverantwoordelijke op de hoogte gehouden van nieuwe ontwikkelingen rondom het Datalek en de maatregelen die Verwerker heeft 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 is niet toegestaan dat de Verwerker een melding van een Datalek doet aan de Toezichthouder en ook mag de Verwerker de Betrokkenen niet informeren over het Datalek. Dit is de verantwoordelijkheid van de Verwerkingsverantwoordelijke.

7.4 Eventuele kosten die gemaakt worden om het Datalek op te lossen en in de toekomst te kunnen voorkomen, komen voor rekening van degene die de kosten maakt.

8. Aansprakelijkheid

8.1 Als de Verwerker zijn verplichtingen uit deze Verwerkersovereenkomst niet nakomt, kan de Verwerkingsverantwoordelijke de Verwerker daarvoor aansprakelijk stellen tot maximaal 2.000 Euro.

8.2 De Verwerker is aansprakelijk voor schade geleden door het niet nakomen van de wet en de bepalingen uit deze Verwerkersovereenkomst, voor zover dit is ontstaan door de werkzaamheden van de Verwerker.

9. Teruggave Persoonsgegevens en bewaartermijn

9.1 Na het beëindigen van deze Verwerkersovereenkomst geeft de Verwerker de Persoonsgegevens terug. Eventuele achter gebleven Persoonsgegevens moet de Verwerker op een zorgvuldige en veilige manier vernietigen.

9.2 De Persoonsgegevens die de Verwerker verwerkt volgens deze Verwerkersovereenkomst worden vernietigd na verstrijken van de wettelijke bewaartermijn en/of op verzoek van mij. Een wettelijke bewaartermijn is er bijvoorbeeld wanneer de Verwerker de Persoonsgegevens moet bewaren om belastingtechnische redenen.

10. Slotbepalingen

10.1 Deze Verwerkersovereenkomst is onderdeel van de Overeenkomst. Alle rechten en verplichtingen uit de Overeenkomst 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.

10.3 Afwijkingen van deze Verwerkersovereenkomst zijn slechts geldig wanneer Wij dit samen schriftelijk afspreken.

Bijlage 1: Overzicht met verwerkingen van persoonsgegevens en verwerkingsdoelen

Het onderstaande schema zal ingevuld moeten worden elke keer dat een Verwerkersovereenkomst wordt gesloten. Het geeft een volledig overzicht van de persoonsgegevens die verwerkt zullen worden. Dit maakt het makkelijker om aan te kunnen tonen waar, door wie en voor welk doel de persoonsgegevens worden verwerkt.

Beschrijving verwerkingsactiviteiten door Verwerker:	Onderhoud, ontwikkeling en leveren van Software as a Service
Verwerkingsdoelen:	Ondersteunen van de software
Verwerkingsverantwoordelijke:	Opdrachtgever
Verwerker:	Inserve
Sub verwerkers:	Cyberfusion
Verwerkte Persoonsgegevens:	Gewone persoonsgegevens
Bewaartermijn:	7 jaar voor facturen Overige persoonsgegevens volgens afspraak klant
Locatie verwerkingen:	Boxmeer

Bijlage 2: Beveiligingsmaatregelen

Mens

- Apparatuur moet vergrendeld worden bij verlaten werkplek.
- Er mag geen data of documenten worden opgeslagen op niet-versleutelde externe opslag (o.a. USB sticks).
- Er moeten veilige wachtwoorden gebruikt worden.
- Er mogen geen wachtwoorden gedeeld of gebruikt worden op onbeheerde apparaten.
- Wachtwoorden worden in een wachtwoordenkluis bewaard.
- Er is een datalekprotocol aanwezig.
- Gevoelige data moet altijd versleuteld of afgeschermd zijn.
- Toegang tot de servers mag alleen onder beveiligde verbindingen en waar mogelijk met twee-factor authenticatie.
- De bewaartermijn van gegevens wordt procesmatig gemonitord.

Techniek

- Voor externe verbindingen worden alleen veilige protocollen gebruikt (SSL, SFTP, SSH).
- Niet gebruikte poorten worden dichtgezet.
- Versies van gebruikte software worden zoveel mogelijk verborgen.
- De online omgeving wordt dagelijks automatisch gescand op kwetsbaarheden volgens het ISO27001 protocol.
- Er wordt maandelijks een rapport uitgebracht door een externe partij over de kwetsbaarheid van de server en applicaties met aanbevelingen. Deze aanbevelingen moeten zo spoedig mogelijk uitgevoerd worden.
- De servers zijn redundant uitgevoerd en staan in Ede, Nederland.
- Back-ups worden ieder uur op de fileserver in Arnhem, Nederland geplaatst.
- De klant heeft de mogelijkheid om dagelijks een eigen backup te ontvangen van de database en bestanden op een eigen SFTP locatie.

Partners

- De hosting is ondergebracht bij Cyberfusion. Zij heeft haar eigen beveiligingsmaatregelen, waaronder een Clean Desk Policy, E-mail Policy, Router and Switch Security Policy en Server Security Policy.
- De servers zijn ondergebracht in de datacenters van Tuxis. Zij heeft geen toegang tot de data. Tuxis heeft haar eigen maatregelen: https://www.tuxis.nl/policies/
- De enige partijen die toegang hebben tot de servers en data zijn Inserve en Cyberfusion. Indien het nodig is om externe ontwikkelaars toegang te geven, mag dit alleen als er een geheimhoudingsbeding met een boeteclausule en een verwerkersovereenkomst is gesloten.
- Toegang aan personen wordt verleend tot enkel de persoonsgegevens die zij nodig hebben voor de uitoefening van hun werkzaamheden.

Bijlage 3: Proces rondom het melden van Datalekken en de te verstrekken informatie

Wat is een beveiligingsincident en wanneer moet dit gemeld worden?

Een datalek is een beveiligingsincident waarbij Persoonsgegevens, die de Verwerker namens de Verwerkingsverantwoordelijke beheert, mogelijk verloren zijn gegaan of onbedoeld toegankelijk waren voor derden. Het gaat om gegevens die te koppelen zijn aan deze personen, zoals, maar niet beperkt tot, namen, adressen, telefoonnummers, e-mailadressen, log in gegevens, cookies, IP adressen of identificerende gegevens van computers of telefoons.

Hieronder staan 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.
- Salarisstroken van medewerkers zijn per ongeluk naar verkeerde personen gestuurd.
- 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 je op basis van bovenstaande niet zeker weet of er sprake is van een beveiligingsincident, stel je jezelf in ieder geval alvast de volgende vragen als hulpmiddel:

- Is er een technisch of fysiek beveiligingsprobleem?
- Gaat het probleem over de beveiliging van Persoonsgegevens? Ook IP-adressen, telefoonnummers of identificerende gegevens, bijvoorbeeld van hardware, kunnen hieronder vallen.
- Gaat het om gevoelige gegevens zoals ras, gezondheidsgegevens, informatie over iemands financiële situatie, zoals salaris of gegevens waar (identiteits)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?

Waar meld je het beveiligingsincident?

Als de Verwerker een beveiligingsincident heeft ontdekt, neemt de Verwerker direct contact op met:

Naam contactpersoon Verwerkingsverantwoordelijke: [contactpersoon]

TEL: [telefoonnummer]
E-MAIL: [emailadres]

Geef in je e-mail beantwoording op de onderstaande vragen. Deze vragen zijn gelijk aan de informatie die aan de Autoriteit Persoonsgegevens moet worden verstrekt. Gaarne de vragen zo volledig mogelijk en schriftelijk beantwoorden.

1. Geef een samenvatting van het beveiligingslek / beveiligingsincident / datalek: wat is er gebeurd? Vermeld hier ook de naam van het betrokken systeem.
2. Welke typen persoonsgegevens zijn betrokken bij het beveiligingsincident? Zoals, maar niet beperkt tot, naam, adres, e-mailadres, IP-nummer, Burgerservicenummer, pasfoto en ieder ander tot een persoon te herleiden gegeven.
3. Van hoeveel personen zijn de persoonsgegevens betrokken bij het beveiligingsincident? Geef a.u.b. een minimum en maximum aantal personen.
4. Omschrijving van de groep personen om wiens gegevens het gaat. Geef aan of het gaat om medewerkersgegevens, gegevens van internetgebruikers. Bijzondere aandacht verdienen gegevens van een kwetsbare groepen personen, zoals kinderen.
5. 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?
6. Wat is de oorzaak (root cause) van het beveiligingsincident? Heeft u een idee hoe het beveiligingsincident heeft kunnen ontstaan?
7. Op welke datum of in welke periode heeft het beveiligingsincident plaats kunnen vinden? Geef dit a.u.b. zo specifiek mogelijk aan.