Model Bewerkersovereenkomst

INHOUD

Bewerkersovereenkomst Ooms Bouw en Ontwikkeling

Datum: 16 mei 2018

Contractpartijen:

1. Verantwoordelijke te weten Ooms Bouw en Ontwikkeling, statutair gevestigd te Scharwoude, vertegenwoordigd door PHJ Ooms.

hierna te noemen: **'Verantwoordelijke'**,

en

2. Verwerker te weten [STATUTAIRE NAAM], statutair gevestigd te [PLAATS], vertegenwoordigd door [NAAM EN/OF NAAM BESTUURDER]

hierna te noemen: **'Bewerker'**,

gezamenlijk aan te duiden als: **'Partijen'**;

Overwegende dat:

Partijen hebben op [DATUM] een Overeenkomst met betrekking tot [OMSCHRIJVING] gesloten. Ter uitvoering van deze Overeenkomst worden Persoonsgegevens verwerkt.
Verantwoordelijke hecht grote waarde aan het beschermen van deze Persoonsgegevens. Om die reden leggen Partijen in deze Bewerkersovereenkomst en de daarbij behorende bijlagen, 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 met betrekking tot het Datalek vast wat Bewerker wel en niet mag doen met de Persoonsgegevens.

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 mee 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 Bewerkersovereenkomst 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 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 Bewerkersovereenkomst

2.1 Deze Bewerkersovereenkomst treedt in werking op de datum waarop Partijen deze ondertekenen.

2.2 Deze Bewerkersovereenkomst is onderdeel van de Overeenkomst en zal gelden voor zolang de Overeenkomst duurt.

2.3 Indien de Overeenkomst eindigt, eindigt deze Bewerkersovereenkomst automatisch; de Bewerkersovereenkomst kan niet apart worden opgezegd.

2.4 Na beëindiging van deze Bewerkersovereenkomst zullen de lopende verplichtingen voor Bewerker, zoals het melden van Datalekken waarbij Persoonsgegevens van Verantwoordelijke betrokken zijn en de plicht tot geheimhouding blijven voortduren.

3. Verwerken Persoonsgegevens

3.1 Bewerker verwerkt alleen Persoonsgegevens in opdracht van Verantwoordelijke en Bewerker heeft geen zeggenschap over de Persoonsgegevens. Bewerker volgt instructies van Verantwoordelijke ten aanzien van de verwerking op en mag de Persoonsgegevens niet op een andere manier

verwerken, tenzij Verantwoordelijke Bewerker daar van tevoren toestemming of opdracht voor geeft.

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

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

3.4 Bewerker mag zonder voorafgaande schriftelijke toestemming van Verantwoordelijke geen andere personen of organisaties inschakelen bij het verwerken van de Persoonsgegevens.

3.5 Wanneer Bewerker met toestemming van Verantwoordelijke andere organisaties inschakelt, moeten zij minimaal voldoen aan de eisen die zijn opgenomen in deze Bewerkersovereenkomst.

3.6 Wanneer Verantwoordelijke een verzoek van een Betrokkene ontvangt ten aanzien van het uitoefenen van zijn of haar rechten, dan werkt Bewerker 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.

4. Beveiligen Persoonsgegevens

4.1 Bewerker zorgt ervoor dat de Persoonsgegevens voldoende worden beveiligd. Om verlies en onrechtmatige verwerkingen te voorkomen neemt Bewerker 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 daaromtrent wordt opgenomen in Bijlage 2.

4.3 Ter controle van de genomen beveiligingsmaatregelen zal Bewerker aan Verantwoordelijke ieder jaar een rapportage sturen waarin de genomen maatregelen staan en de eventuele aandachts- en/of verbeterpunten. Hiervoor brengt Bewerker geen kosten in rekening aan Verantwoordelijke.

4.4 Verantwoordelijke mag een audit laten uitvoeren om te bepalen of het verwerken van de Persoonsgegevens aan de wet en de afspraken uit deze Bewerkersovereenkomst voldoet. Bewerker verleent hierbij zijn medewerking. 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 Bewerker komen wanneer blijkt dat Bewerker zich niet aan de verplichtingen in deze Bewerkersovereenkomst houdt.

4.6 De controle op de algehele verwerking van Persoonsgegevens door Bewerker kan, naast de auditmogelijkheid, ook geschieden via zelfevaluatie door Bewerker. Bewerker zal hierbij aan Verantwoordelijke een rapport verstrekken waarin Bewerker aantoont dat hij voldoet aan de wet en de afspraken uit deze Bewerkersovereenkomst. Deze rapportage dient te worden ondertekend door een directielid binnen de organisatie van Bewerker.

4.7 Wanneer Partijen vinden dat een wijziging in de te nemen beveiligingsmaatregelen noodzakelijk is, treden Partijen in overleg over de wijziging daarvan. De kosten gemoeid met het wijzigen van de beveiligingsmaatregelen komen voor rekening van degene die de kosten maakt.

5. Exporteren Persoonsgegevens

5.1 Bewerker 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 Verantwoordelijke.

6. Geheimhouding

6.1 Bewerker zal de verstrekte Persoonsgegevens geheim houden, tenzij dit op basis van een wettelijke verplichting niet kan.

6.2 Bewerker zorgt dat zijn/haar 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 Bewerker Verantwoordelijke hierover informeren binnen een termijn van 24 uur overeenkomstig het proces volgend uit Bijlage 3, zodat Verantwoordelijke indien nodig een melding van het Datalek bij de Toezichthouder kan doen. De Bewerker zal niet op eigen initiatief melding van het Datalek doen bij de Toezichthouder.

7.2 Bewerker zal Verantwoordelijke op de hoogte houden van nieuwe ontwikkelingen rondom het Datalek, ook zal Bewerker de getroffen maatregelen om het Datalek te beperken en te beëindigen en een soortgelijk incident in de toekomst te kunnen voorkomen, overleggen aan Verantwoordelijke.

7.3 Bewerker mag geen melding van een Datalek aan de Toezichthouder doen, wanneer bij het Datalek Persoonsgegevens van Verantwoordelijke betrokken zijn. Ook mag Bewerker de Betrokkenen niet informeren over het Datalek. Deze verantwoordelijkheid ligt bij Verantwoordelijke.

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 Bewerker de verplichtingen uit deze Bewerkersovereenkomst niet nakomt, kan Verantwoordelijke Bewerker daarvoor aansprakelijk stellen.

8.2 Bewerker is aansprakelijk voor alle schade die Verantwoordelijke lijdt door het niet nakomen van de wet en de bepalingen uit deze Bewerkersovereenkomst, voor zover dit is ontstaan door de werkzaamheden van Bewerker.

8.3 Indien Bewerker de verplichtingen in deze Bewerkersovereenkomst overtreedt, is Bewerker aan *Verantwoordelijke een direct opeisbare boete verschuldigd gelijk aan de boet van overheidswege voor iedere overtreding en idem voor iedere dag dat Bewerker de overtreding begaat. Daarnaast behoudt Verantwoordelijke het recht om schadevergoeding te vorderen.* (optioneel)

8.4 Bewerker is aansprakelijk voor de aan Verantwoordelijke opgelegde bestuurlijke boete door de Toezichthouder als de schade het gevolg is van het onrechtmatig of nalatig handelen van Bewerker.

8.5 Verantwoordelijke is niet aansprakelijk voor aanspraken van Betrokkene of andere personen en

organisaties waar Bewerker de samenwerking mee is aangegaan of waarvan Bewerker Persoonsgegevens verwerkt, als dit het gevolg is van het onrechtmatig of nalatig handelen van Bewerker.

9. Teruggave Persoonsgegevens en bewaartermijn

9.1 Na het beëindigen van deze Bewerkersovereenkomst geeft Bewerker de Persoonsgegevens terug aan Verantwoordelijke.

9.2 De overgebleven Persoonsgegevens zal Bewerker vernietigen na verstrijken van de wettelijke bewaartermijn en/of op verzoek van Verantwoordelijke. Hierbij valt bijvoorbeeld te denken aan Persoonsgegevens die om belastingtechnische redenen bewaard moeten blijven.

10. Slotbepalingen

10.1 Deze Bewerkersovereenkomst is onderdeel van de Overeenkomst. Alle rechten en verplichtingen uit de Overeenkomst zijn daarom ook van toepassing op de Bewerkersovereenkomst.

10.2 Bij eventuele tegenstrijdigheden tussen de bepalingen in de Bewerkersovereenkomst en de Overeenkomst, gelden de bepalingen uit deze Bewerkersovereenkomst ten aanzien van de verwerking van Persoonsgegevens.

10.3 Afwijkingen van deze Bewerkersovereenkomst zijn slechts geldig wanneer Partijen dit samen schriftelijk afspreken.

Aldus door Partijen overeengekomen en ondertekend:

Verantwoordelijke:
Ondertekend voor en namens Ooms Bouw en Ontwikkeling
Naam:
Functie:
Datum en plaats:

Handtekening:

Bewerker:
Ondertekend voor en namens [STATUTAIRE NAAM]
Naam:
Functie:
Datum en plaats:

Handtekening:

Bijlage 1: Overzicht met verwerkingen van Persoonsgegevens en verwerkingsdoelen

Het onderstaande schema zal ingevuld moeten worden elke keer dat een Bewerkersovereenkomst 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 bewerker:	
Verwerkingsdoelen:	
Verantwoordelijke:	
Bewerker:	
Subbewerkers:	
Verwerkte Persoonsgegevens:	
Locatie verwerkingen:	
Bewaartermijn:	

Bijlage 2: Overzicht met beveiligingsmaatregelen

Overzicht van de beveiligingsnormen die de Verantwoordelijke aan de Bewerker oplegt.
Om vast te stellen wat passende beveiligingsmaatregelen zijn, moet een afweging worden gemaakt op basis van de risico's van de verwerking aan de hand van onder meer de volgende punten:

- Het soort Persoonsgegevens dat verwerkt wordt (normaal, bijzonder of gevoelig) en eventueel de daarbij behorende (risico)classificatie die de organisatie zelf aan de gegevens heeft gegeven. *Gaat het bijvoorbeeld om een naam of een e-mailadres, wat minder gevoelige Persoonsgegevens zijn, of gaat het om het verwerken van een BSN.*
- De hoeveelheid betrokkenen van wie gegevens worden verwerkt. *Hoe meer betrokkenen er zijn, hoe meer eisen er worden gesteld aan de beveiliging van de gegevens.*
- Het doel waarvoor gegevens worden verwerkt.
- De duur en de wijze waarop gegevens bewaard moeten worden.

Er kan vervolgens onderscheid gemaakt worden tussen organisatorische beveiligingseisen, zoals het voorkomen van diefstal van een laptop met daarop Persoonsgegevens uit de auto, en technische beveiligingseisen, zoals een uitgebreide IT-omgeving die beveiligd wordt tegen virussen en waar encryptie van de gegevens wordt toegepast. Van een grote organisatie wordt meer verwacht ten aanzien van de te nemen beveiligingseisen.

De onderstaande maatregelen zijn suggesties voor beveiligingsmaatregelen en de aanwezigheid hiervan kan een indicatie zijn van een gepast beveiligingsniveau.

Technische beveiligingsmaatregelen

☐ Up-to-date virusscanner op elke laptop, pc en tablet
☐ Beveiligde USB-sticks
☐ Accurate beveiliging medewerkerstelefoon
☐ Bitlocker toegangsmechanisme
☐ Unieke inlogcode en wachtwoord (regelmatig aanpassen)
☐ Versleutelde e-mail
☐ Geen onbeveiligde externe harde schijven
☐ Geen onbeveiligde back-ups maken
☐ Geen documenten op privélaptop opslaan

Organisatorische beveiligingsmaatregelen

☐ Clean desk policy
☐ Laptop niet onbemand achterlaten
☐ Laptop nooit achterlaten in de auto
☐ Privacy screens medewerkers
☐ Oude documenten op juiste manier vernietigen
☐ Zorgvuldig gebruik van USB-sticks

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 Bewerker namens de Verantwoordelijke 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, login-gegevens, cookies, IP-adressen of identificerende gegevens van computers of telefoons.

Hieronder vind je een aantal voorbeelden van beveiligingsincidenten die moeten worden gemeld bij de Autoriteit Persoonsgegevens.

- De website met login-gegevens 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 (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 je twijfelt, neem het zekere voor het onzekere en neem altijd contact op met de [invoeren naam contactpersoon of afdeling].

Waar meld je het beveiligingsincident?
Als je een beveiligingsincident hebt ontdekt, neem je direct contact op met de [invoeren naam contactpersoon of afdeling]:

Telefoon: 0229-547800
E-mail: Info@oomsbouw.nl

Geef in je e-mail beantwoording op de onderstaande vragen

Wij willen graag dat je de onderstaande vragen voor ons beantwoord. Deze vragen zijn gelijk aan de informatie die aan de Autoriteit Persoonsgegevens moet worden verstrekt.

De Kam coördinator kan je helpen met de beantwoording hiervan. 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 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.