Themablad Bewerkersovereenkomst NOM Keur

Onderwerp	**Themablad Bewerkersovereenkomst NOM Keur**
Datum	15 december 2015
Versie	versie 1.04
Auteurs	Marten Witkamp
Auteursrechten	© Copyright 2016 door Vereniging De BredeStroomversnelling Dit document mag vrij gebruikt en zonder toestemming gedeeld worden. Het is bedoeld als integraal onderdeel van een Nul op de Meter Afnameovereenkomst.
Aantal pagina's	12 pagina's inclusief deze
Deelnemers	Ard Jan Dunnik (Brinkhof) Gerrit-Jan Zwenne (Brinkhof) Lucas Wolthuis Scheeres

Standaard bewerkersovereenkomst voor de verwerking van gegevens die betrekking hebben op de bewoners van Nul op de Meter Keur woningen, ter naleving van de regels die van toepassing zijn op de verwerking van persoonsgegevens.

A. CONTRACTANTEN:

1. _____ , statutair gevestigd te _____, KvK-nummer _____, hierbij rechtsgeldig vertegenwoordigd door _____, hierna te noemen 'Afnemer';

   en

2. _____, statutair gevestigd te _____, KvK-nummer _____, hierbij rechtsgeldig vertegenwoordigd door _____, hierna te noemen 'Leverancier;

B. NEMEN IN AANMERKING:

1. Vanaf 25 mei 2018 is de EU Verordening 2016/679 ("Verordening") van toepassing, waarmee de huidige Wet bescherming persoonsgegevens ("Wbp") komt te vervallen. Dit betreft wet- en regelgeving die van toepassing is op de verwerking van persoonsgegevens.

2. De Afnemer verwerkt of laat persoonsgegevens verwerken van diverse betrokkenen in verband met zijn zakelijke activiteiten en is daarom in het kader van de Wbp alsmede de Verordening een Verantwoordelijke – de term Afnemer wordt hier gehanteerd om coherentie binnen de Afnameovereenkomst te bewerkstelligen;

3. De Leverancier verwerkt persoonsgegevens in opdracht van de Afnemer en is daarom in het kader van de Wbp alsmede de Verordening een Bewerker – de term Leverancier wordt hier gehanteerd om coherentie binnen de Afnameovereenkomst te bewerkstelligen;

4. De Afnemer wenst gebruik te maken van de diensten van de Leverancier om persoonsgegevens voor hem te verwerken;

5. In overeenstemming met Artikel 14 van de Wbp alsmede artikel 28 van de Verordening willen de Afnemer en Leverancier afspraken vastleggen in deze bewerkersovereenkomst.

C. **DE PARTIJEN KOMEN HET VOLGENDE OVEREEN:**

1. DEFINITIES EN INTERPRETATIE

1.1 In deze bewerkersovereenkomst hebben we de volgende woorden en zinnen de volgende betekenis toegekend:

"Afnameovereenkomst": De overeenkomst tussen Afnemer en Leverancier, waarvan deze bewerkersovereenkomst integraal onderdeel uitmaakt;

"Betrokkene": Degene op wie een persoonsgegeven betrekking heeft. In deze bewerkersovereenkomst betreft dat de huurder, die een huurovereenkomst met energieprestatie is aangegaan met Afnemer;

"Bewerker": diegene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt. In deze bewerkersovereenkomst betreft dat Leverancier die is ingeschakeld door Afnemer.

"Datalek": Een inbreuk op de beveiligingsmaatregelen die kan leiden tot een aanzienlijke kans op ernstige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens;

"Persoonsgegevens": Elk gegeven betreffende een geïdentificeerde of direct of indirect identificeerbare natuurlijke persoon;

"Verantwoordelijke": De natuurlijke persoon, rechtspersoon of ieder ander die allen of tezamen met anderen het doel en de middelen van de verwerking van Persoonsgegevens vaststelt. In deze bewerkersovereenkomst betreft dat Afnemer (een verhuurder), die een huurovereenkomst met energieprestatie heeft met de Betrokkene (een huurder).

2. DOELEINDEN VAN VERWERKING

2.1 Leverancier verbindt zich om, onder de voorwaarden in deze bewerkersovereenkomst, in opdracht van Afnemer Persoonsgegevens te verwerken zoals benodigd voor uitvoering van de Afnameovereenkomst. Deze verwerking zal

uitsluitend plaatsvinden in het kader van de volgende doelstellingen:

- Het door Afnemer kunnen voldoen aan de wettelijke verplichting de huurder jaarlijks inzicht te geven in de prestaties van de woning.
- Het door Afnemer kunnen beoordelen of de woning voldoet aan de afgesproken prestatie-eisen.
- Het door Leverancier aan de verhuurder kunnen rapporteren over de prestaties van de woningen.
- Het door Leverancier kunnen beoordelen of de Nul op de Meter woning naar behoren werkt.
- Het door Leverancier aan de bewoner verschaffen van inzicht in het effect van diens gedrag op de beschikbare energiebundel en daarmee de jaarafrekening.
- Het door Leverancier kunnen uitvoeren en optimaliseren van beheers- en onderhoudsdiensten.
- Het door Leverancier kunnen verbeteren van diens Nul op de Meter producten door inzicht in geanonimiseerde prestatie- en gebruiksdata (onderzoek en ontwikkeling),

2.2 Leverancier zal de gegevens niet voor enige ander doel verwerken dan zoals door Afnemer middels deze bewerkersovereenkomst dan wel anderszins schriftelijk is overeengekomen.

3. VERPLICHTINGEN VAN LEVERANCIER (BEWERKER)

3.1 Leverancier verwerkt Persoonsgegevens uitsluitend op basis van schriftelijke afspraken met Afnemer. Leverancier stelt Afnemer onmiddellijk in kennis indien naar zijn mening een instructie resulteert in een inbreuk op van toepassing zijnde regelgeving. Ten aanzien van de in artikel 2 genoemde verwerkingen zal Leverancier zorgdragen voor de naleving van de toepasselijke wet- en regelgeving, waaronder in ieder geval begrepen de wet- en regelgeving op het gebied van de bescherming van Persoonsgegevens.

3.2 Leverancier zal Afnemer, op diens verzoek, informeren over de door hem in het kader van deze bewerkingsovereenkomst genomen maatregelen.

3.3 De verplichtingen van Leverancier uit hoofde van deze bewerkersovereenkomst gelden ook voor degenen die Persoonsgegevens verwerken onder het gezag van Leverancier, waaronder inbegrepen de werknemers van Leverancier en eventuele onderaannemers, zoals nader gespecificeerd in Artikel 9.

3.4 Leverancier draagt er voor zorg dat zij namens Afnemer de verwerking van Persoonsgegevens in het kader van de Afnameovereenkomst meldt bij de Autoriteit Persoonsgegevens, en verleent, voor zover mogelijk, bijstand bij een gegevensbescherming effectbeoordeling dan wel voorafgaande raadpleging van de Autoriteit Persoonsgegevens, voor zover de van toepassing zijnde wet deze verplichtingen oplegt aan Afnemer.

3.5 Leverancier zal passende technische en organisatorische beveiligingsmaatregelen nemen met betrekking tot de te verrichten verwerking om de Persoonsgegevens te beveiligen tegen verlies, onnodige verzameling of tegen enige vorm van onrechtmatige verwerking (zoals onbevoegde kennisname, aantasting, wijziging, of verstrekking van Persoonsgegevens).

3.6 Leverancier mag uitsluitend Persoonsgegevens verwerken buiten de Europese Economische Ruimte, indien zij toestemming heeft van Afnemer, alsmede voldoende waarborgen worden geboden voor een passend beveiligingsniveau, zoals vereist door de wet.

3.7 Rekening houdend met de aard van de verwerking, verleent Leverancier met passende technische en organisatorische maatregelen bijstand aan Afnemer, voor zover mogelijk, bij het vervullen van diens plicht om verzoeken om uitoefening van de wettelijke rechten van de Betrokkene te beantwoorden.

3.8 Leverancier stelt alle informatie ter beschikking aan Afnemer voor zover Afnemer deze nodig heeft om te voldoen aan wettelijke of contractuele verplichtingen die meebrengen dat Afnemer aantoont dat zij voldoet aan de wet- en regelgeving die van toepassing is op verwerking van Persoonsgegevens.

4. VERPLICHTINGEN VAN AFNEMER (VERANTWOORDELIJKE)

4.1 Afnemer garandeert dat de inhoud, het gebruik en de opdracht tot de verwerkingen van Persoonsgegevens zoals bedoeld in deze bewerkersovereenkomst, niet

onrechtmatig is en geen inbreuk maakt op enig recht van derden.

5. VERTROUWELIJKHEID

5.1 Leverancier is gehouden tot geheimhouding van Persoonsgegevens waarvan zij kennisneemt, behoudens voor zover enig wettelijk voorschrift haar tot mededeling verplicht of uit haar taak de noodzaak tot mededeling voortvloeit.

5.2 Leverancier waarborgt dat de tot het verwerken van Persoonsgegevens gemachtigde personen zich ertoe hebben verbonden vertrouwelijkheid in acht te nemen of door een passende wettelijke verplichting van vertrouwelijkheid zijn gebonden.

5.3 Niets in deze Overeenkomst mag de partijen beletten te voldoen aan alle wettelijke verplichtingen opgelegd door een regelgever of de rechtbank. Beide partijen zullen, waar mogelijk samen, praten over een passend antwoord op elk verzoek van een regelgever of de rechtbank voor openbaarmaking van informatie.

6. MELDPLICHT DATALEK

6.1 Leverancier zal in het geval van een geconstateerd of vermoed Datalek:

- Onmiddellijk alle maatregelen treffen die redelijkerwijs van Leverancier mogen worden verwacht om de nadelige gevolgen van het Datalek voor de Verwerking van de Persoonsgegevens te beperken of op te heffen;
- Onmiddellijk alle maatregelen treffen die redelijkerwijs van Leverancier mogen worden verwacht om de ongunstige gevolgen van het Datalek voor Betrokkenen te beperken of op te heffen;
- Afnemer zo snel als redelijkerwijs mogelijk is, maar niet later dan één werkdag na de ontdekking van het Datalek, informeren over de aard van het Datalek, de mogelijke impact van het Datalek op Afnemer en/of de Betrokkene(n), alsmede de maatregelen die Leverancier heeft genomen of voornemens is te nemen om de beveiliging te corrigeren en/of de gevolgen te beperken;
- Samenwerken met Afnemer om de oorzaak van het Datalek te onderzoeken, alsmede om de omvang of de gevolgen voor de

Verwerking van de Persoonsgegevens en de gevolgen voor de Betrokkenen vast te stellen; en

- Zo spoedig mogelijk alle maatregelen nemen die Afnemer nodig acht om herhaling van het incident te voorkomen of tekortkomingen in de beveiliging van de Persoonsgegevens op te heffen.

6.2 Afnemer zal in het geval van een geconstateerd of vermoed Datalek:

- De Autoriteit Persoonsgegevens, indien van toepassing, informeren over de aard van het Datalek, de mogelijke impact van het Datalek op de Betrokkene(n), alsmede de maatregelen die Leverancier heeft genomen of voornemens is te nemen om de beveiliging te corrigeren en/of de gevolgen te beperken;
- De Betrokkenen, indien van toepassing, informeren over de aard van het Datalek, de mogelijke impact van het Datalek op de Betrokkene(n), alsmede de maatregelen die Leverancier heeft genomen of voornemens is te nemen om de beveiliging te corrigeren en/of de gevolgen te beperken;

6.3 Leverancier vrijwaart Afnemer, indien blijkt dat het redelijkerwijs in het vermogen van de Leverancier had gelegen om het Datalek te voorkomen, van alle directe kosten en schade als gevolg van het Datalek, waaronder in ieder geval begrepen:

- Een boete opgelegd aan Afnemer wegens het niet tijdig melden van het Datalek voor zover dit niet tijdig melden toe te rekenen is aan de Leverancier;
- Een boete opgelegd aan Afnemer wegens een tekortkoming in de maatregelen ter beveiliging van de Persoonsgegevens voor zover deze tekortkoming is toe te rekenen aan de Leverancier;
- De kosten van het door Afnemer inschakelen van deskundigen op het gebied van informatiebeveiliging om het Datalek te onderzoeken en corrigerende maatregelen voor te stellen;
- De kosten van de melding aan de bevoegde toezichthouder(s) die Afnemer op grond van de toepasselijke wet- en regelgeving moet doen;
- De kosten van de melding aan de Betrokkene(n) die Afnemer op grond van de toepasselijke wet- en regelgeving moet doen;

- De kosten van de maatregelen die Afnemer voorstelt aan Betrokkene(n) om de gevolgen van het Datalek te beperken, voor zover die kosten voor rekening van Afnemer komen.

6.4 Leverancier zal Afnemer direct informeren als de Autoriteit Persoonsgegevens toegang tot de Persoonsgegevens vraagt of de Autoriteit Persoonsgegevens maatregelen neemt tegen Leverancier, tenzij Leverancier deze informatie op grond van wetgeving niet mag geven.

7. OMGANG MET BETROKKENE (HUURDER)

7.1 Leverancier zal Afnemer op verzoek alle medewerking verlenen in geval van een klacht of vraag van een Betrokkene, dan wel onderzoeken of inspecties door de Autoriteit Persoonsgegevens.

7.2 Als Leverancier rechtstreeks of via Afnemer een verzoek van een Betrokkene om inzage, correctie of verwijdering van zijn of haar Persoonsgegevens ontvangt, informeert Leverancier Afnemer binnen twee werkdagen over de ontvangst van het verzoek.

7.3 Leverancier voert per omgaande alle instructies uit die Afnemer aan Leverancier geeft als gevolg van een verzoek tot inzage, correctie of verwijdering van Persoonsgegevens door Betrokkene.

8. ONDERAANNEMING

8.1 Waar Leverancier een sub-contractant zijn verplichtingen uit hoofde van deze schriftelijke overeenkomst oplegt, gelden dezelfde verplichtingen met betrekking tot de veiligheid van de verwerking op de sub-contractant zoals Leverancier zijn opgelegd krachtens deze bewerkersovereenkomst.

8.2 Leverancier neemt geen andere Bewerker (sub-contractant) in dienst zonder voorafgaande specifieke schriftelijke toestemming van Afnemer.

8.3 Ter voorkoming van twijfel, waar de sub-contractant haar verplichtingen voortgekomen uit een overeenkomst voor de onderaanneming niet nakomt, blijft Leverancier verantwoordelijk naar Afnemer voor de vervulling van haar verplichtingen uit hoofde van deze bewerkersovereenkomst.

9. TERMIJN EN BEËINDIGING

9.1 Deze bewerkersovereenkomst blijft volledig van kracht voor zo lang Leverancier Persoonsgegevens verwerkt uit naam van Afnemer, dat wil zeggen voor de duur van de beheer- en onderhoudsperiode zoals beschreven in bijlage 6 van de Afnameovereenkomst.

9.2 Binnen twee weken na de beëindiging van deze bewerkersovereenkomst wordt van Leverancier, op verzoek van Afnemer verwacht dat:

a) Hij voldoet aan enige andere overeenkomst gemaakt tussen de partijen betreffende de teruggave of vernietiging van gegevens, of
b) Alle Persoonsgegevens die Afnemer doorgegeven heeft aan Leverancier, en/of de gegevens die Leverancier namens Afnemer heeft verzameld voor verwerking onherroepelijk worden geanonimiseerd.

10. CONTROLE EN BORGING

10.1 Leverancier laat aan Afnemer jaarlijks weten wanneer de meest recente audit (Third Party Memorandum) inzake de informatiebeveiliging rondom de betreffende Persoonsgegevens is uitgevoerd en wat daaruit de belangrijkste conclusies waren. Leverancier zet zich in om een dergelijke audit tenminste elke drie jaar uit te laten voeren.

10.2 Afnemer behoudt zich het recht voor om steekproeven te nemen inzake de informatiebeveiliging rondom de Persoonsgegevens bij de Leverancier. Afnemer zal

een controle tenminste 48 uur van te voren aankondigen. De kosten van de controle zijn voor rekening van Afnemer, tenzij de controle aan het licht brengt dat Leverancier zich niet aan haar verplichtingen op grond van de overeenkomst heeft gehouden, in welk geval de kosten van de controle voor rekening van Leverancier zijn.

10.3 Rapportage, audit en controle in de zin van dit artikel richten zich in elk geval op de procedures rondom de autorisaties, de logbestanden, de opslag van gegevensdragers en de wijze waarop Persoonsgegevens worden verstrekt.

11. TOEPASSELIJK RECHT

11.1 Deze overeenkomst zal worden beheerst door en geïnterpreteerd volgens Nederlands recht.

D. ONDERTEKENING

Deze overeenkomst is integraal onderdeel van de te ondertekenen Afnameovereenkomst en hoeft daarom niet apart te worden ondertekend.

TOELICHTING BIJ DE BEWERKERSOVEREENKOMST

1. Wettelijke vereisten

1.1 De Leverancier zal ten aanzien van de verwerking van persoonsgegevens, namens de Afnemer, toepasselijke wet- en regelgeving identificeren en daaraan voldoen door maatregelen te treffen. Op de verwerking van persoonsgegevens is de Wet bescherming persoonsgegevens van toepassing. Vanaf 25 mei 2018 komt deze wet te vervallen en is de EU Verordening 2016/679 van toepassing.

2. Praktische beveiligingsmaatregelen

2.1 Met inachtneming van haar verplichtingen uit hoofde van clausule 3.5 met betrekking tot de verwerking van persoonsgegevens namens de Afnemer implementeert de Leverancier minimaal de volgende soorten veiligheidsmaatregelen:

- Beleidsdocument voor informatiebeveiliging
  Een beleidsdocument is de basis voor het kwaliteitsmanagementsysteem.

- Toewijzing en vastlegging van verantwoordelijkheden voor informatiebeveiliging
  Het benoemen van een officier voor informatiebeveiliging (Functionaris Gegevensbescherming) zorgt ervoor dat iemand hiervoor aanspreekbaar is.

- Bewustwording, opleiding en training voor informatiebeveiliging
  Meer dan de helft van de informatiebeveiligingsincidenten wordt veroorzaakt door mensen binnen de eigen organisatie. Informatiebeveiliging is voor 80% het werk van mensen en voor 20% het nemen van technische maatregelen. Daarmee is het creëren van bewustzijn en organiseren van kennis en trainingen een belangrijke voorwaarde voor een succesvol informatiebeveiligingsbeleid.

- Maatregelen tegen kwaadaardige programmatuur
  De huidige ”operating”-systemen, het internet en de vele communicatiemogelijkheden maken applicaties en ermee opgeslagen informatie makkelijk benaderbaar voor gewenst gebruik, maar tevens voor ongewenst gebruik en daarmee privacyschending.

- Toegangsbeveiliging
  Toegangsbeveiliging houdt onder meer in dat er een geformuleerd beleid is, waarin wordt aangegeven wie er toegang heeft en op welke wijze het beleid wordt gerealiseerd. Met wachtwoorden moet voorzichtig worden omgegaan.

- Ontwikkelen en implementeren van continuïteitsvoorzieningen en -plannen
  Er moet een plan van aanpak zijn m.b.t. de werkwijze bij het wegvallen van de continuïteit (bijvoorbeeld goede "back-ups", snel vervangende apparatuur en software).

- Intellectueel eigendom
  Gebruik uitsluitend geregistreerde programmatuur. Maak het ongeautoriseerd installeren van programmatuur onmogelijk.

- Beveiliging van bedrijfsdocumenten
  Er moet een procedure worden opgesteld voor elektronische opslag van gegevens, waarbij rekening moet worden gehouden met het de beperkte technische levensduur van elektronische opslagmedia. De elektronische opslagmedia moeten regelmatig worden herzien, opdat toegankelijkheid tot gearchiveerde gegevens wordt gewaarborgd.

- Naleving beveiligingsbeleid
  80% van de beveiligingsincidenten wordt veroorzaakt door mensen. Zonder het organiseren van een vorm van (sociale) controle door een bevoegde zullen mensen zich minder houden aan de regels.

- Het rapporteren van beveiligingsincidenten
  Zonder rapportage van incidenten zal er niets kunnen worden geleerd en aangepast binnen de organisatie. Het rapporteren van (bijna) ongelukken behoort tot het reguliere professionele handelen. Rapportages dienen te worden gedaan aan de hiertoe bevoegde persoon van Afnemer.

Bovenstaande maatregelen worden als urgent aangemerkt en dienen altijd te zijn ingericht bij de Leveranciers. Op basis van risicoanalyse door zowel Afnemer als Leverancier wordt vastgesteld welke aanvullende maatregelen getroffen dienen te worden zodat een goed beveiligingsbeleid bereikt wordt en de Wbp en andere voor Nul op de Meter relevante standaarden in acht genomen worden. In principe dienen deze maatregelen te zijn geïmplementeerd voordat wordt begonnen met de uitwisseling van persoonsgegevens.