

Bijlage 9

Aanbestedingsleidraad VvE-aanpak Energie Diensten Centrum - kenmerk 21356



PROVINCIE  UTRECHT

**Concept Gegevensuitwisselingsovereenkomst
Verwerkingsverantwoordelijke – Verwerkingsverantwoordelijke**

inzake de verwerking van persoonsgegevens bij de uitvoering van de Opdracht
Overeenkomst 
inzake de VvE aanpak Energie Diensten Centrum
tussen

de Provincie Utrecht

en



PARTIJEN

1. De publiekrechtelijke rechtspersoon, de Provincie Utrecht, gevestigd aan de Archimedeslaan 6, 3584 BA te Utrecht, te dezen krachtens volmacht van de Commissaris van de Koning, rechtsgeldig vertegenwoordigd door mr. drs. A.G. Knol-van Leeuwen, Algemeen directeur/ Provinciesecretaris en handelend ter uitvoering van het Organisatiebesluit Provincie Utrecht 2004 juncto Mandaatbesluit secretaris, hierna te noemen: de Provincie Utrecht

EN

2. XXX, gevestigd aan de XXX te XX, bekend onder KvK-nummer: XX te dezen rechtsgeldig vertegenwoordigd door XXX, functie XX, hierna te noemen: Opdrachtnemer

hierna nader aan te duiden als **"de Provincie en Opdrachtnemer"** hierna tezamen aan te duiden als **"Partijen"**

NEMEN IN OVERWEGING:

- (A) Partijen hebben op XX de overeenkomst met kenmerk XX of NAAM, hierna **"Overeenkomst"** gesloten met betrekking tot de dienstverlening omtrent de VvE aanpak Energie Diensten Centrum t.b.v. verduurzaming van Verenigingen van Eigenaren (VvE's). Ter uitvoering van de Overeenkomst wisselen partijen Persoonsgegevens uit.
- (B) Partijen wensen in overeenstemming met de AVG en andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens hun rechten en plichten ten aanzien van de Verwerking van Persoonsgegevens van Betrokkenen Schriftelijk vast te leggen in deze Gegevensuitwisselingsovereenkomst.
- (C) In het kader van de uitvoering van Overeenkomst worden Persoonsgegevens verwerkt. Beide Partijen kwalificeren hiervoor als verwerkingsverantwoordelijke in overeenstemming met het Toepasselijke Recht, hetgeen betekent dat Partijen elk afzonderlijk of gezamenlijk de doeleinden en de middelen van de verwerking van de Persoonsgegevens bepalen.
- (D) Als (gezamenlijk) verwerkingsverantwoordelijken zullen Partijen een regeling in de zin van artikel 26 van de Algemene Verordening Gegevensbescherming (hierna: **"AVG"**) moeten treffen met betrekking tot de verwerking van de Persoonsgegevens en hun respectieve rollen en verantwoordelijkheden voor de nakoming van hun verplichtingen uit hoofde van het Toepasselijke Recht, in het bijzonder met betrekking tot hun verantwoordelijkheden jegens elkaar en hun rollen en verplichtingen ten aanzien van de Betrokkenen, waaronder hun informatieverplichtingen en de uitoefening van de rechten van de Betrokkenen;
- (E) In deze Gegevensuitwisselingsovereenkomst wensen Partijen hun afspraken met betrekking tot de verwerking van de Persoonsgegevens in het kader van deze overeenkomst in overeenstemming met het Toepasselijk Recht te bepalen. Deze Gegevensuitwisselingsovereenkomst vormt een aanvulling op en is een Bijlage bij de Overeenkomst met kenmerk XX.

KOMEN HIERBIJ OVEREEN EN STELLEN VAST:

Artikel 1.

Definities

1.1 In deze overeenkomst worden de volgende begrippen gehanteerd:

AVG

De Algemene Verordening Gegevensbescherming (EU 2016/679);

Betrokkene

De persoon op wie de Persoonsgegevens betrekking hebben;

Datalek(ken)

Een inbreuk op de beveiliging die resulteert in een (mogelijke) accidentele of onwettige vernietiging, verlies, wijziging, niet-geautoriseerde vrijgave van of toegang tot de Persoonsgegevens die worden doorgegeven, opgeslagen of anderszins verwerkt;

Persoonsgegevens(s)

Elk gegeven met betrekking tot een geïdentificeerde of identificeerbare levende natuurlijke persoon, zoals bedoeld in het Toepasselijke Recht, die door een Partij of haar onderaannemers wordt verwerkt in verband met de uitvoering van het Programma van Eisen (hierna "PvE") ;

Overeenkomst

De hoofdovereenkomst die tussen Verwerkingsverantwoordelijken is gesloten en op grond waarvan Persoonsgegevens ten behoeve van de uitvoering van deze overeenkomst worden verwerkt.

Toepasselijke Recht

De wet(en) of enige andere (lokale) regelgeving, met inbegrip van maar niet beperkt tot de AVG en de bijbehorende lokale implementaties, de EU-regels inzake e-privacy en de bijbehorende lokale implementaties, en richtlijnen of beleidslijnen, instructies of aanbevelingen van enige bevoegde overheidsinstantie die van toepassing zijn op de verwerking van de Persoonsgegevens, met inbegrip van alle wijzigingen, herzieningen, aanpassingen of andere latere versies van deze wet(ten) en (lokale) regelgeving;

Verwerkingsactiviteiten

De (uit te voeren) verwerking van Persoonsgegevens door de betreffende Partij.

Gegevensuitwisselingsovereenkomst

De onderhavige overeenkomst inclusief Bijlagen.

Sub-verwerker

Een andere verwerker, waaronder maar niet beperkt tot groepsmaatschappijen, zustermaatschappijen, dochtermaatschappijen en hulpleveranciers, die Verwerker inschakelt om voor rekening van de Verwerkingsverantwoordelijke specifieke verwerkingsactiviteiten te verrichten.

Verwerker

Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/ dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt;

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, zoals bedoeld in artikel 4.2 AVG.

Artikel 2. Onderwerp van deze overeenkomst

- 2.1** In verband met de uitvoering van de Verwerkingsactiviteiten is elke Partij een (gezamenlijke en/of zelfstandige) verwerkingsverantwoordelijke voor de verwerking van Persoonsgegevens en kwalificeren zij dienovereenkomstig in relatie tot de (een deel van de) Verwerkingsactiviteiten als gezamenlijke verwerkingsverantwoordelijke en/of als zelfstandige verwerkingsverantwoordelijke, zoals bepaald in het Toepasselijke Recht.
- 2.2** Elke Partij verwerkt de Persoonsgegevens in overeenstemming met het Toepasselijke Recht. Partijen zullen elkaar alle informatie verschaffen die redelijkerwijs noodzakelijk is om aan te tonen dat voldaan wordt aan de relevante eisen van het Toepasselijke Recht.

Artikel 3. Verwerking van de persoonsgegevens

- 3.1** **Bijlage A** bij deze Gegevensuitwisselingsovereenkomst bevat een beschrijving van de (gezamenlijk en afzonderlijke) Verwerkingsactiviteiten die door elke Partij worden verricht en hun respectieve rollen ten opzichte van elkaar en hun verantwoordelijkheden ten aanzien van de Betrokkenen.
- 3.2** Rekening houdend met de aard van de gegevensverwerking en de aan Partijen ter beschikking staande informatie, zullen Partijen elkaar alle redelijkerwijs noodzakelijke bijstand verlenen bij het aantoonbaar nakomen van de op Partijen rustende verplichtingen onder het Toepasselijke Recht, in het bijzonder de verplichtingen ter zake van de beveiliging van Persoonsgegevens, privacy by design en by default, kennisgevings- en documentatieverplichtingen in verband met Datalekken en de uitvoering van gegevens beschermingseffect beoordelingen, alsmede het laten uitvoeren van een voorafgaande raadpleging door (een) bevoegde overheidsinstantie(s).
- 3.3** In het bijzonder zal Opdrachtnemer:
 - a) De verwerking van de Persoonsgegevens opnemen in haar verwerkingsregister;
 - b) De Persoonsgegevens niet verwerken op een wijze die onverenigbaar is met de doeleinden van de verwerking, zoals uiteengezet in **Bijlage A** van de Gegevensuitwisselingsovereenkomst, tenzij de Provincie hier na voorafgaand overleg uitdrukkelijk schriftelijk mee instemt;
 - c) De Persoonsgegevens niet langer verwerken dan noodzakelijk is voor de uitvoering van de doeleinden, zoals uiteengezet in **Bijlage A** van deze Gegevensuitwisselingsovereenkomst.

Artikel 4.

Nakoming rechten van betrokkenen en informatieplicht

- 4.1** In het kader van deze overeenkomst is Opdrachtnemer aangewezen als de Partij die verantwoordelijk is voor het informeren van de Betrokkenen. Opdrachtnemer zal de Betrokkenen tijdig informeren over de verwerking van de Persoonsgegevens van de Betrokkenen, inclusief over de essentie van deze Gegevensuitwisselingsovereenkomst, in overeenstemming met de informatieverplichtingen krachtens het Toepasselijke Recht. Partijen zullen met elkaar samenwerken en alle redelijkerwijs noodzakelijke informatie en bijstand verstrekken zodat beide Partijen hun verplichtingen onder het Toepasselijke Recht als (gezamenlijk) verwerkingsverantwoordelijke kunnen nakomen indien een Betrokkene zijn rechten onder het Toepasselijke Recht uitoefent.
- 4.2** Uitvoeren rechten van betrokkenen en klachten
- a) Om een uniforme werkwijze en communicatie te bewerkstelligen worden verzoeken met betrekking tot de rechten van Betrokkenen of overige klachten omtrent de naleving van het Toepasselijke Recht ontvangen door Opdrachtnemer en vervolgens afgestemd met zowel privacyfunctionarissen van Opdrachtnemer als met privacyfunctionarissen van de Provincie via privacy@provincie-utrecht.nl;
 - b) Aangezien het recht op inzage, correctie en verwijdering geen absoluut recht betreft, onderzoeken de privacyfunctionarissen gezamenlijk of er sprake is van een uitzonderingsgrond en of het verzoek daadwerkelijk uitvoerbaar is, alvorens het verzoek te honoreren;
 - c) Partijen verlenen onverwijld, ten minste binnen twee weken, medewerking aan de privacyfunctionarissen ten behoeve van de uitvoering van het verzoek of de klacht.
- 4.3** Aan de hand van de aard van het verzoek wordt gezamenlijk door de privacyfunctionarissen bepaald welke Partij deze afhandelt.
- 4.4** Onverminderd hun verplichtingen uit deze Gegevensuitwisselingsovereenkomst, erkennen dat Partijen dat aan de Betrokkenen hun rechten uit hoofde van het Toepasselijke Recht jegens Partijen niet kunnen worden ontzegd.

Artikel 5.

Beveiligingsmaatregelen

- 5.1** Partijen zullen passende technische en organisatorische maatregelen treffen om Persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. De maatregelen genomen door Opdrachtnemer zijn opgenomen in **Bijlage B** bij deze Gegevensuitwisselingsovereenkomst. De bedoelde maatregelen die Opdrachtnemer treft dienen dusdanig te zijn dat ook de Provincie voldoet aan de AVG in het kader van de doeleinden van deze overeenkomst.
- 5.2** De Provincie heeft het recht om Opdrachtnemer naar redelijkheid en billijkheid te instrueren om aanvullende beveiligingsmaatregelen te nemen en Opdrachtnemer zal deze aanvullende beveiligingsmaatregelen implementeren binnen een in onderling overleg vastgestelde redelijke termijn.
- 5.3** Partijen staan ervoor in dat de technische en organisatorische maatregelen:
- a) Passend zijn, rekening houdend met de stand van de techniek, de kosten van de tenuitvoerlegging, 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;
 - b) Dusdanig worden vastgesteld en toegepast dat Partijen ter zake van de Verwerkingsactiviteiten steeds in overeenstemming handelen met het Toepasselijke Recht.

- c) Partijen of door Opdrachtnemer ingeschakelde derden zullen, indien dat door de Provincie wenselijk wordt geacht, een audit laten doen naar de naleving door Opdrachtnemer en de door haar ingeschakelde derden van deze overeenkomst en meer specifiek naar de technische en organisatorische maatregelen, tenzij Opdrachtnemer en eventuele ingeschakelde derden (Verwerkers) door middel van een geldige certificering, die periodiek door een geaccrediteerde instelling wordt getoetst, hebben aangetoond de gemaakte afspraken na te komen.
- d) Partijen zullen elkaar op de hoogte brengen van de uitkomsten van de audit. Hierdoor kan de Provincie zich een oordeel vormen over de naleving door Opdrachtnemer van deze overeenkomst. De Provincie, of de door de Provincie in dit verband ingeschakelde derde, is gehouden alle informatie betreffende deze controles vertrouwelijk te behandelen.

Artikel 6. Melden van Datalekken

- 6.1 Zodra een van de Partijen een Datalek detecteert of redelijkerwijs vermoedt dat een Datalek zich heeft voorgedaan, stelt zij de andere Partij hiervan zonder onnodige vertraging, en in ieder geval binnen 24 uur, in kennis na detectie of vermoeden van een Datalek. Deze kennisgeving door Opdrachtnemer zal geschieden per e-mail aan het e-mailadres: datalek@provincieutrecht.nl. Deze kennisgeving door Provincie zal geschieden per email aan het e-mailadres: XXX
- 6.2 De kennisgeving zal informatie bevatten over:
 - a) Het tijdstip van aanvang van de beveiligingsinbreuk;
 - b) De aard en de omvang van de beveiligingsinbreuk;
 - c) Bij welke dienst en/of deel van het systeem de beveiligingsinbreuk heeft plaatsgevonden;
 - d) De verwachte hersteltijd;
 - e) Aard en omvang van betrokken databestanden;
 - f) De mogelijke consequenties van de inbreuk voor degene op wie de persoonsgegevens betrekking hebben, alsmede een voorstel ter voorkoming van mogelijke schade en andere negatieve consequenties; en
 - g) Welke maatregelen zijn genomen om de beveiligingsinbreuk te beëindigen.
- 6.3 Opdrachtnemer stelt de bevoegde overheidsinstanties en/of Betrokkenen tijdig in kennis van een Datalek zoals vereist door het Toepasselijke Recht, na overleg met en schriftelijke goedkeuring van de Provincie voor zover dit overleg en deze goedkeuring een tijdige kennisgeving(en) van het Datalek zoals vereist door het Toepasselijke Recht niet in de weg zou staan. Opdrachtnemer verstrekt de Provincie zonder onnodige vertraging na het indienen van een dergelijke kennisgeving een kopie of kopieën van de aan een overheidsinstantie en/of de Betrokkenen voorgelegde kennisgeving(en) van een Datalek. Waar nodig zal Opdrachtnemer in overleg met en met voorafgaande schriftelijke goedkeuring van Provincie, een door haar gedane melding van een Datalek bijwerken, wijzigen of intrekken op redelijk verzoek van de Provincie en/of indien vereist onder het Toepasselijke Recht.
- 6.4 Partijen documenteren alle informatie met betrekking tot het Datalek, met inbegrip van de gevolgen ervan en eventuele herstelmaatregelen die zijn genomen.
- 6.5 Partijen zullen elkaar alle redelijkerwijs te verwachten assistentie verlenen en alle noodzakelijke of door de andere Partij gevraagde informatie met de ander delen, opdat elke Partij, indien van toepassing, haar (mogelijk) getroffen Betrokkenen en/of de relevante overheidsinstanties of toezichthouders die bevoegd zijn om te oordelen over de verwerking van de Persoonsgegevens, tijdig kan informeren over het Datalek en in staat wordt gesteld om naleving aan de meldplichten inzake Datalekken onder het Toepasselijke Recht aan te tonen en conform het Toepasselijke Recht te documenteren. Partijen zullen met elkaar in

overleg treden over de wijze waarop en wanneer de Betrokkenen en, indien van toepassing, in overeenstemming met het Toepasselijke Recht worden geïnformeerd.

Artikel 7. **Inschakeling onderaannemers**

- 7.1** Indien een onderaannemer die kwalificeert als een Verwerker naar Toepasselijke Recht betrokken is bij de verwerking van de Persoonsgegevens voor een Partij of voor beide Partijen, zal de betreffende Partij of, indien van toepassing beide Partijen met de Verwerker een schriftelijke overeenkomst sluiten in overeenstemming met de vereisten van artikel 28 AVG. Partijen blijven, indien zij een onderaannemer inschakelen voor de verwerking van Persoonsgegevens, volledig verantwoordelijk en aansprakelijk voor de nakoming van de hen rustende verplichtingen uit hoofde van het Toepasselijke Recht.

Artikel 8. **Geheimhouding**

- 8.1** Partijen zullen de Persoonsgegevens uitsluitend inzichtelijk maken voor personen in dienst van dan wel opdrachtnemers voor zover dit noodzakelijk is voor de uitvoering van de verplichtingen van iedere Partij voor de werkzaamheden/Overeenkomst, Verwerkingsactiviteiten, en voor het overige geheim houden, tenzij anders vereist door het Toepasselijke Recht.
- 8.2** Partijen zullen de in deze Gegevensuitwisselingsovereenkomst neergelegde verplichtingen, waaronder de beveiligings- en geheimhoudingsverplichtingen, opleggen aan hun Personeel en/of opdrachtnemers indien deze Werknemers en/of opdrachtnemers toegang hebben tot of anderszins betrokken zijn bij de verwerking van de Persoonsgegevens en niet gebonden zijn aan een passende wettelijke geheimhoudingsverplichting. Partijen zullen ervoor zorgdragen dat het Personeel en/of door hen ingeschakelde opdrachtnemers aan deze verplichtingen voldoen

Artikel 9. **Doorgifte en opslag van persoonsgegevens**

- 9.1** Doorgifte en opslag van persoonsgegevens vindt niet plaats buiten de Europese Unie (EU) of de Europese Economische Ruimte (EER).
- 9.2** Onverminderd eventuele andere rechten, zijn Partijen gerechtigd om de doorgifte van de Persoonsgegevens op te schorten of te beëindigen zonder aansprakelijk te zijn voor kosten of schade als gevolg van een dergelijke opschorting of beëindiging.

Artikel 10. **Aansprakelijkheid**

- 10.1** Elke Partij is verantwoordelijk en aansprakelijk voor elke verwerking van Persoonsgegevens voor haar eigen doeleinden als zelfstandige verwerkingsverantwoordelijke, waaronder begrepen Verwerkingsactiviteiten die niet in **Bijlage A** zijn opgenomen, zoals verwerkingen die voorafgaand aan en/of plaatsvinden na de verwerkingen die in **Bijlage A** zijn beschreven, of verwerkingen waarvoor een Partij in **Bijlage A** als zelfstandige verwerkingsverantwoordelijke is aangemerkt, en elke andere verwerking waarvoor een Partij onder het Toepasselijke Recht als zelfstandige verwerkingsverantwoordelijke kwalificeert.
- 10.2** Opdrachtnemer vrijwaart en stelt de Provincie schadeloos met betrekking tot alle aanspraken van derden, alle schade van de Provincie en aan de Provincie opgelegde boetes door toezichthouders, ontstaan of geleden wegens een schending van het Toepasselijke Recht gerelateerd aan de verwerking

van de Persoonsgegevens die aan Opdrachtnemer, of aan haar Personeel of aan de door haar ingeschakelde derden en/of onderaannemers kan worden toegerekend.

- 10.3** Partijen zullen elkaar volledig vrijwaren en schadeloos stellen ter zake van eventuele schade, claims, procedures, sancties, boetes, maatregelen en andere kosten van (de zijde van) de ander en derden, waaronder uitdrukkelijk – maar niet uitsluitend – begrepen toezichthouders zoals de Toezichthoudende autoriteit en Betrokkenen, gebaseerd op of voortvloeiend uit de uitvoering, schending en/of niet-naleving door de ander (inclusief door haar ingeschakelde (rechts)personen, waaronder – maar niet beperkt tot – Medewerkers, Verwerkers en/of Sub-verwerkers) van voorschriften bij of krachtens de AVG of andere wet- en, regelgeving, de Overeenkomst en/of deze overeenkomst.

Artikel 11. Evaluatie, duur en beëindiging overeenkomst

- 11.1** De duur van de Gegevensuitwisselingsovereenkomst is gelijk aan de duur van de Overeenkomst. De Gegevensuitwisselingsovereenkomst is niet los van de Overeenkomst te beëindigen. Bij beëindiging van de Overeenkomst eindigt de Gegevensuitwisselingsovereenkomst van rechtswege.
- 11.2** Verplichtingen welke naar hun aard bestemd zijn om ook na ontbinding van deze overeenkomst voort te duren blijven na beëindiging van de overeenkomst gelden. Tot deze bepalingen behoren onder meer de bepalingen betreffende geheimhouding en aansprakelijkheid.

Artikel 12. Slotbepalingen

- 12.1** Afwijkingen van deze overeenkomst zijn slechts bindend voor zover zij schriftelijk tussen Partijen zijn overeengekomen.
- 12.2** Alvorens Partijen een geschil voorleggen aan de bevoegde rechter, spannen Partijen zich tot het uiterste in om deze geschillen in onderling overleg op te lossen.
- 12.3** Alle uit deze overeenkomst voortvloeiende en/of daarmee verband houdende geschillen zullen, indien deze niet in onderling overleg kunnen worden opgelost, worden voorgelegd aan de daartoe bevoegde rechter van de Rechtbank Midden-Nederland, locatie Utrecht.

Aldus vastgesteld en ondertekend op:

Namens de Provincie Utrecht,
Voor akkoord:
de commissaris van de Koning,
Namens deze,

Namens **Naam Opdrachtnemer**,

.....
mr. drs. A.G. Knol-van Leeuwen
Algemeen directeur/ Provinciesecretaris
Datum:

.....
Naam
Functie
Datum:

Bijlage A

Overzicht van de Verwerkingsactiviteiten

Voorwerp en aard van de verwerking	Doeleinden waarvoor de gegevens worden verwerkt	Duur van de verwerking	Categorieën Betrokkenen	Persoonsgegevens	Rol Partij	Bewaar termijn	Respectievelijke verantwoordelijkheden van de Partij(en) met betrekking tot: 1)Melden van datalekken bij overheidsinstanties en Betrokkenen; 2)Informatieverplichtingen jegens Betrokkenen; 3)Het afhandelen van verzoeken van Betrokkenen
Documentbeheer	Vastleggen, inlezen, raadpleging, archivering en opslaan van documenten	Duur van de overeenkomst	Medewerkers Provincie, Opdrachtnemer en Betrokkenen	NAW van VvE Emailadres contactperso(o)n(en) Telefoonnummer contactperso(o)n(en) Energietabel of energetische staat woning/VvE Aangevraagde subsidies en leningen	Verwerkers verantwoordelijke		1, 2, 3
Registratie klantcontact helpdesk in CRM-systeem	Monitoring en optimaliseren dienstverlening	Duur van de overeenkomst	Medewerkers Opdrachtnemer en Betrokkenen	NAW Emailadres Telefoonnummer	Verwerkers verantwoordelijke		1, 2, 3
Registratie status begeleidings-traject VvE in CRM-systeem	Monitoring en optimaliseren dienstverlening	Duur van de overeenkomst	Medewerkers Opdrachtnemer en Betrokkenen	NAW van VvE Emailadres contactperso(o)n(en) Telefoonnummer contactperso(o)n(en) Energietabel of energetische staat woning/VvE Aangevraagde subsidies en leningen			
Registratie en oplossen klachten	Oplossen klachten van Betrokkenen	Duur van de overeenkomst	Medewerkers Opdrachtnemer en Betrokkenen	NAW Emailadres Telefoonnummer	Verwerkers verantwoordelijke		1, 2, 3

Bijlage B:

Overzicht beveiligingsmaatregelen Opdrachtnemer

Opdrachtnemer neemt alle passende technische en organisatorische maatregelen om Persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige Verwerking. Opdrachtnemer dient in ieder geval voor de beveiligingsmaatregelen uit het onderstaande overzicht aan te geven of de desbetreffende maatregel is geïmplementeerd aangevuld met een verklaring/uitleg. Opdrachtnemer is vrij om zelf maatregelen toe te voegen aan het overzicht.

	Beschrijving beveiligingsmaatregel	Aanwezig ja/nee	Verklaring/uitleg Opdrachtnemer
1.	Opdrachtnemer heeft een autorisatie proces en geeft aan op welke wijze rechten worden toegekend, gecontroleerd en ingetrokken.		
2.	Opdrachtnemer maakt gebruik van Multi-Factor Authenticatie (MFA) en geeft aan hoe toegang tot systemen en data is geregeld en of generieke accounts worden gebruikt en waarvoor.		
3.	Opdrachtnemer maakt gebruik van marktconforme encryptie en geeft aan op welke wijze, waar en met welke algoritmes dit wordt toegepast en hoe men encryptie marktconform houdt.		
4.	Opdrachtnemer heeft een vastgestelde incident management procedure en geeft aan hoe deze werkt in het geval van een security incident.		
5.	Opdrachtnemer maakt gebruik van logging en monitoring en geeft aan hoe dit in zijn werk gaat, met name de wijze waarop met alerts omgegaan wordt, en hoelang en op welke wijze logging wordt bewaard.		
6.	Opdrachtnemer heeft een vastgesteld patch managementbeleid en geeft aan op welke wijze welke type patches, met name kritieke/security patches, worden		

	afgehandeld en hoe en hoe vaak gecontroleerd wordt op patches/fixes.		
7.	Opdrachtnemer heeft een system hardening beleid en geeft aan hoe dit in zijn werk gaat.		
8.	Opdrachtnemer heeft een screening beleid en geeft aan op welke wijze en wanneer screening wordt ingezet.		
9.	Opdrachtnemer heeft een security awareness programma en legt uit wat er onderdeel is van dit programma, inclusief tijdslijnen en herhaling van training.		
10.	Opdrachtnemer gebruikt anti-malware, anti-phishing systemen en geeft aan welke producten gebruikt worden en waar.		
11.	Opdrachtnemer houdt zich aan internationale standaarden, zoals bijvoorbeeld de OWASP, voor het ontwikkelen van veilige software en geeft aan welke standaarden dat zijn.		
12.	Opdrachtnemer heeft een back-up beleid en geeft aan op welke termijnen welke type back-ups worden gemaakt en hoe herstel procedures worden getest.		
13.	Opdrachtnemer geeft aan hoe omgegaan wordt met de instellingen van Cloud omgevingen en op welke wijze de beveiligingsinstellingen hiervan door verwerker worden gemanaged.		
14.	Opdrachtnemer geeft aan indien zij gebruik maakt van anonimisatie en/of pseudonimisatie technieken, hoe deze tot stand komen en waarvoor deze worden ingezet.		
15	Opdrachtnemer geeft aan indien er nog andere van belang zijnde securitymaatregelen en/of processen zijn die zij heeft inzake de bescherming van persoonsgegevens, waarbij per maatregel/proces een uitleg vereist is.		
16			

