Omgevingsdienst West-Holland

Verwerkersovereenkomst

Zaaknummer: 2018-074686
Kernmerk:
Contractnummer:

De ondergetekenden:

De gemeenschappelijke regeling Omgevingsdienst West-Holland,
gevestigd te Leiden, aan de Schipholweg 128,
rechtsgeldig vertegenwoordigd door M.E. Krul-Seen, directeur,
hierna te noemen : Opdrachtgever

en

<volledige naam en rechtsvorm contractant>,
statutair gevestigd te ……... en kantoorhoudende ……..,
hierbij rechtsgeldig vertegenwoordigd door de ……..…, ……..,
hierna te noemen: Opdrachtnemer,

Hierna gezamenlijk te noemen: **Partijen;**

OVERWEGENDE DAT:

-voor zover Opdrachtnemer Persoonsgegevens Verwerkt ten behoeve van Opdrachtgever in het kader van de Overeenkomst, Opdrachtgever zich krachtens artikel 4, onderdeel 7 en onderdeel 8, van de Verordening kwalificeert als verwerkingsverantwoordelijke voor de Verwerking van Persoonsgegevens en Opdrachtnemer als verwerker;

- Partijen in deze Verwerkersovereenkomst, zoals bedoeld in artikel 28, derde lid, van de Verordening, hun afspraken over de Verwerking van Persoonsgegevens door Opdrachtnemer wensen vast te leggen.

KOMEN OVEREEN:

Artikel 1 Definities

In deze verwerkersovereenkomst worden de hierna met een hoofdletter geschreven begrippen in de volgende betekenis gebruikt, onafhankelijk van de vraag of die begrippen in het enkelvoud of in het meervoud worden gebruikt en onafhankelijk van de vraag of dit woord als werkwoord dan wel als zelfstandig naamwoord wordt gebruikt:

a. AP: Autoriteit Persoonsgegevens;
b. Betrokkene: degene op wie een Persoonsgegeven betrekking heeft;
c. Opdrachtnemer: degene die ten behoeve van de Verantwoordelijke Persoonsgegevens verwerkt;
d. Overeenkomst: de Verwerkersovereenkomst met zaaknummer 2018-074686 tussen Opdrachtgever en Opdrachtnemer;
e. Functionaris: de functionaris voor gegevensbescherming als bedoeld in artikel 37 van de Verordening;
f. Persoonsgegeven: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon dat Opdrachtnemer op grond van de hoofdovereenkomst, zoals genoemd in artikel 3, eerste lid, van deze overeenkomst Verwerkt, of dient te Verwerken; 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;

g. Verwerking van persoonsgegevens: 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;
h. Verwerkersovereenkomst: deze overeenkomst inclusief overwegingen en bijbehorende bijlagen;
i. Verantwoordelijke: 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;
j. Verstrekken van persoonsgegevens: het bekend maken of ter beschikking stellen van persoonsgegevens;
k. Verordening: Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van de Richtlijn 95/46/EG (algemene verordening gegevensbescherming)

Artikel 2 Ingangsdatum en duur

1. Deze Verwerkersovereenkomst treedt in werking op het moment waarop deze door Partijen is ondertekend.
2. Deze Verwerkersovereenkomst eindigt nadat en voor zover Opdrachtnemer alle Persoonsgegevens overeenkomstig artikel 14 heeft gewist of terugbezorgd.
3. Geen van Partijen kan deze Verwerkersovereenkomst tussentijds opzeggen.

Artikel 3 Onderwerp overeenkomst

1. Deze Verwerkersovereenkomst regelt de Verwerking van Persoonsgegevens door Opdrachtnemer in het kader van de Overeenkomst.
2. De aard en het doel van de Verwerking, het soort Persoonsgegevens en de categorieën van Persoonsgegevens, Betrokkenen en ontvangers zijn in Bijlage 1 omschreven.
3. Opdrachtnemer garandeert de toepassing van passende technische en organisatorische maatregelen, opdat de Verwerking aan de vereisten van de Verordening voldoet en de bescherming van de rechten van de Betrokkene is gewaarborgd.
4. Opdrachtnemer garandeert te voldoen aan de vereisten van de toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens.

Artikel 4 Verwerking door Opdrachtnemer

1. Opdrachtnemer verwerkt de Persoonsgegevens uitsluitend in opdracht en op basis van instructies van Opdrachtgever behoudens afwijkende wettelijke voorschriften die op Opdrachtnemer van toepassing zijn.
2. Indien een instructie als bedoeld in het eerste lid naar het oordeel van Opdrachtnemer in strijd is met een wettelijk voorschrift inzake gegevensbescherming, stelt hij Opdrachtgever daarvan voorafgaand aan de Verwerking in kennis, tenzij een wettelijk voorschrift deze kennisgeving verbiedt.
3. Indien Opdrachtnemer op grond van een wettelijk voorschrift Persoonsgegevens dient te verstrekken, informeert hij Opdrachtgever onmiddellijk, en zo mogelijk voorafgaand aan de verstrekking.
4. Opdrachtnemer heeft geen zeggenschap over de ter beschikking gestelde Persoonsgegevens. De zeggenschap over de Persoonsgegevens berust te allen tijde bij Opdrachtgever. Dat betekent onder meer dat Opdrachtnemer geen zeggenschap heeft over ontvangst en gebruik van de Persoonsgegevens, de verstrekking aan derden en de duur van de opslag van de Persoonsgegevens.

5. Opdrachtnemer informeert Opdrachtgever onmiddellijk zodra hij kennis heeft genomen van onrechtmatige verwerkingen van persoonsgegevens of inbreuken op beveiligingsmaatregelen zoals genoemd in artikel 6.
6. Opdrachtnemer zal op eerste verzoek van Opdrachtgever en onder alle omstandigheden onmiddellijk en kosteloos alle Persoonsgegevens aan Opdrachtgever ter beschikking stellen en/of vernietigen.
7. Opdrachtnemer stelt Opdrachtgever te allen tijde in staat om binnen de wettelijke termijnen te voldoen aan de verplichtingen die op grond van de Verordening op Opdrachtgever rusten, waaronder het voldoen aan verzoeken om inzage, verbetering, aanvulling, verwijdering of afscherming van Persoonsgegevens en het uitvoeren van gehonoreerd aangetekend verzet.
8. Uitsluitend voor zover dat noodzakelijk is voor de nakoming van de Overeenkomst door Opdrachtnemer, verschaft Opdrachtnemer zijn werknemers toegang tot de Persoonsgegevens. De werknemers van Opdrachtnemer mogen slechts die handelingen met betrekking tot de Persoonsgegevens verrichten, die noodzakelijk zijn voor nakoming van de Overeenkomst door Opdrachtnemer.

Artikel 5 Geheimhoudingsplicht

1. De Persoonsgegevens hebben een vertrouwelijk karakter. Opdrachtnemer, werknemers van Opdrachtnemer en door Opdrachtnemer op de voet van artikel 11 ingeschakelde derden zijn verplicht om alle Persoonsgegevens waarvan zij kennis kunnen nemen geheim te houden. De verplichting tot geheimhouding geldt niet voor zover verstrekking van de Persoonsgegevens noodzakelijk is voor de nakoming van de Overeenkomst door Opdrachtnemer of een krachtens de wet gegeven voorschrift tot verstrekking verplicht. De medewerkers van Opdrachtnemer en door Opdrachtnemer op de voet van artikel 11 ingeschakelde derden tekenen hiertoe een geheimhoudingsverklaring.
2. Opdrachtnemer zal geen Persoonsgegevens aan een derde verstrekken zonder uitdrukkelijke schriftelijke toestemming van Opdrachtgever. Opdrachtgever kan aan de toestemming voorwaarden verbinden.
3. Indien Opdrachtnemer een verzoek van een derde ontvangt tot inzage of tot afgifte van (een deel van) de Persoonsgegevens, zal zij Opdrachtgever hiervan onmiddellijk, voorafgaand aan de verstrekking, in kennis stellen.
4. Indien een verstrekking dient plaats te vinden uit hoofde van een wettelijke verplichting, bevel of vordering van een gerechtelijke of bestuurlijke instantie, stelt Opdrachtnemer Opdrachtgever binnen 24 uur na ontvangst van een dergelijk bevel in kennis om Opdrachtgever in staat te stellen zo nodig tegen dat bevel een hem ter beschikking staand rechtsmiddel aan te wenden. Indien een dergelijke situatie zich voordoet, is Opdrachtnemer gehouden om alle door Opdrachtgever verzochte medewerking te verlenen, waaronder het verstrekken van alle informatie die Opdrachtgever nodig acht te hebben voor aanwending van voornoemd rechtsmiddel.

Artikel 6 Beveiligingsmaatregelen

1. Opdrachtnemer neemt alle passende technische en organisatorische maatregelen om Persoonsgegevens te beveiligen en beveiligd te houden tegen verlies of enige vorm van onrechtmatige Verwerking van persoonsgegevens, waaronder onzorgvuldig, ondeskundig of ongeoorloofd gebruik. De wijze van beveiliging wordt nader omschreven in Bijlage 2.
2. Opdrachtnemer erkent dat het waarborgen van een passend beveiligingsniveau voortdurend kan dwingen tot het treffen van aanvullende beveiligingsmaatregelen. Opdrachtnemer waarborgt een op het risico afgestemd beveiligingsniveau.
3. Indien en voor zover Opdrachtgever daarom uitdrukkelijk schriftelijk verzoekt, zal Opdrachtnemer aanvullende maatregelen treffen met het oog op de beveiliging van de Persoonsgegevens.
4. Opdrachtnemer Verwerkt Persoonsgegevens niet buiten de Europese Unie, tenzij hij daarvoor uitdrukkelijk schriftelijk toestemming heeft verkregen van Opdrachtgever en behoudens afwijkende wettelijke verplichtingen.
5. Opdrachtnemer verleent Opdrachtgever bijstand bij het doen nakomen van de verplichtingen uit hoofde van de artikelen 32 tot en met 36 van de Verordening.

Artikel 7. Informatieverplichting en audit

1. Opdrachtnemer stelt alle informatie ter beschikking die nodig is om aan te tonen dat de verplichtingen uit deze Verwerkersovereenkomst zijn en worden nagekomen.
2. Opdrachtgever is te allen tijde gerechtigd de Verwerking van Persoonsgegevens te (doen) controleren. Opdrachtnemer is verplicht Opdrachtgever of de controlerende instantie in opdracht van Opdrachtgever toe te laten en verplicht medewerking te verlenen zodat de audit naar de vraag of Opdrachtnemer in overeenstemming handelt met Verwerkersovereenkomst (waaronder de in bijlage 2 beschreven maatregelen), de Verordening en/of andere regelgeving waarin eisen aan het Verwerken van Persoonsgegevens worden gesteld, daadwerkelijk uitgevoerd kan worden. Opdrachtnemer verleent in dit verband binnen een redelijke termijn alle door Opdrachtgever verlangde medewerking, waaronder begrepen, maar niet uitsluitend:
    - het verschaffen van alle door Opdrachtgever gevraagde informatie en inlichtingen;
    - het verlenen van toegang aan Opdrachtgever en/of een door Opdrachtgever ingeschakelde derde tot de locaties van Opdrachtnemer;
    - het verlenen van toegang aan Opdrachtgever en/of een door Opdrachtgever ingeschakelde derde tot de systemen van Opdrachtnemer;
    - het beschikbaar stellen van het personeel van Opdrachtnemer voor het geven van een toelichting aan de Opdrachtgever en/of een door de Opdrachtgever ingeschakelde derde.
3. De Opdrachtgever zal de audit slechts (laten) uitvoeren na een voorafgaande schriftelijke melding aan Opdrachtnemer.
4. Binnen een redelijke termijn na uitvoering van de audit zal door of namens de Opdrachtgever verslag worden gedaan van de audit. Opdrachtnemer is gehouden de in het verslag gedane aanbevelingen binnen de in het verslag vermelde termijn uit te voeren. Uitvoering van de in het verslag gedane aanbevelingen binnen de gestelde termijn, doet niet af aan het recht van de Opdrachtgever om zijn schade op Opdrachtnemer te verhalen en aanspraak te maken op de in artikel 10 beschreven boete.
5. De Opdrachtgever draagt ervoor zorg dat de door hem ingeschakelde derde verplicht is tot geheimhouding tegenover derden van alle informatie betreffende de audit, waaronder de bevindingen van de audit.
6. De kosten van de ingeschakelde derde komen voor rekening van de Opdrachtgever, tenzij uit de audit blijkt dat Opdrachtnemer in strijd handelt met Verwerkersovereenkomst, de Verordening of andere regelgeving waarin eisen worden gesteld aan het verwerken van Persoonsgegevens. In dat geval komen de kosten van de ingeschakelde derde voor rekening van Opdrachtnemer. De kosten die het uitvoeren van de audit meebrengt voor de eigen organisaties van de Opdrachtgever en Opdrachtnemer zijn voor eigen rekening.
7. ***<OPTIONEEL>*** Opdrachtnemer verstrekt met een frequentie van eenmaal per […], uiterlijk op [datum] aan Opdrachtgever een verklaring van een onafhankelijke externe deskundige, waarin deze een oordeel geeft over de genoemde naleving.

Artikel 9 Meldplicht datalekken en beveiligingsincidenten

1. Opdrachtnemer informeert de Opdrachtgever onverwijld en in ieder geval binnen 24 uur na de eerste ontdekking, over alle inbreuken op de beveiliging alsmede andere incidenten die op grond van wetgeving moeten worden gemeld aan een toezichthouder of betrokkene, onverminderd de verplichting om de gevolgen van dergelijke inbreuken en incidenten zo snel mogelijk ongedaan te maken dan wel te beperken. Deze meldplicht behelst tevens ten minste informatie over wat de (vermeende) oorzaak is van het lek, wat het (vooralsnog bekende en/of te verachten) gevolg is en wat de (voorgestelde) oplossing is.
2. Opdrachtnemer zal het doen van meldingen aan de toezichthouder(s) overlaten aan de Opdrachtgever.
3. Opdrachtnemer dient de Opdrachtgever alle noodzakelijke informatie, medewerking en toegang te verlenen om de Opdrachtgever in staat te stellen zo spoedig mogelijk de oorzaak en de omvang van de inbreuk of het incident vast te stellen en Betrokkenen adequaat te informeren.
4. Indien sprake is van een inbreuk op de beveiliging of een ander incident, neemt Opdrachtnemer, al dan niet in opdracht van Opdrachtgever, zo spoedig mogelijk alle

maatregelen om de inbreuk of het incident te herstellen, de gevolgen ervan te beperken en verdere inbreuken of incidenten te voorkomen. Opdrachtnemer is in dit kader verplicht om alle bevelen van Opdrachtgever op te volgen, waaronder het bevel tot vernietiging of het ter beschikking stellen van de Persoonsgegevens aan de Opdrachtgever.
5. Zolang de inbreuk of het incident voortduurt, informeert Opdrachtnemer Opdrachtgever iedere 24 uur in ieder geval over de status en de aard van de inbreuk of het incident, de geconstateerde en de vermoedelijke gevolgen, de instanties waar meer informatie over de inbreuk of het incident kan worden verkregen en de aanbevolen maatregelen om de negatieve gevolgen te beperken.
6. Opdrachtnemer houdt een gedetailleerd logboek bij van alle inbreuken op de beveiliging, evenals de maatregelen die in het vervolg op dergelijke inbreuken zijn genomen en geeft daar op eerste verzoek van Opdrachtgever inzage in.

Artikel 10 Verzoeken van Betrokkenen

1. Opdrachtnemer dient Opdrachtgever in kennis te stellen van alle verzoeken met betrekking tot inzage in de Persoonsgegevens die rechtstreeks van een Betrokkene zijn ontvangen. Opdrachtnemer geeft aan een dergelijk verzoek alleen gevolg indien Opdrachtgever Opdrachtnemer daartoe schriftelijk opdracht heeft gegeven. Deze inzage wordt alleen via Opdrachtgever verschaft.
2. Opdrachtnemer verleent Opdrachtgever haar volledige medewerking om (i) inzage in hun Persoonsgegevens te laten krijgen, (ii) Persoonsgegevens te laten verwijderen of te corrigeren, en/of (iii) aan te laten tonen dat de Persoonsgegevens verwijderd of gecorrigeerd zijn indien zij incorrect zijn of, indien Opdrachtgever het standpunt van betrokkene bestrijdt, vast te leggen dat Betrokkene zijn Persoonsgegevens als incorrect beschouwt.

Artikel 11 Aansprakelijkheid

1. Indien Opdrachtnemer tekortschiet in de nakoming van de verplichting uit deze verwerkersovereenkomst kan Opdrachtgever hem in gebreke stellen. Opdrachtnemer is echter onmiddellijk in gebreke als de nakoming van desbetreffende verplichting anders dan door overmacht binnen de overeengekomen termijn, reeds blijvend onmogelijk is. Ingebrekestelling geschiedt schriftelijk, waarbij aan Opdrachtnemer een redelijke termijn wordt gegund om alsnog haar verplichtingen na te komen. Deze termijn is een fatale termijn. Indien nakoming binnen deze termijn uitblijft, is verwerker in verzuim.
2. Opdrachtnemer is aansprakelijk op grond van het bepaalde in artikel 82 AVG, voor schade of nadeel voortvloeiende uit het niet nakomen van deze verwerkersovereenkomst, daaronder begrepen wanneer bij de verwerking niet wordt voldaan aan de specifiek tot Opdrachtnemer gerichte verplichtingen van de AVG, of buiten de rechtmatige instructies van Opdrachtgever is gehandeld.
3. Opdrachtnemer vrijwaart Opdrachtgever voor schade of nadeel voor zover ontstaan door werkzaamheid van Opdrachtnemer.
4. Indien Opdrachtnemer een in deze verwerkersovereenkomst neergelegde verplichting niet of niet-tijdig nakomt en de toezichthouder Opdrachtgever dientengevolge een bestuurlijke boete oplegt, is Opdrachtnemer aansprakelijk en zal Opdrachtgever een contractuele boete ter hoogte van hetzelfde bedrag opleggen aan Opdrachtnemer. Deze boete is niet vatbaar voor verrekening en opschorting en laat de rechten van verwerkingsverantwoordelijken op nakoming en schadevergoeding onverlet.

Artikel 12 Inschakeling derden

1. Opdrachtnemer is slechts gerechtigd de uitvoering van de werkzaamheden geheel of ten dele uit te besteden aan derden na voorafgaande schriftelijke toestemming van Opdrachtgever.
2. Opdrachtgever kan aan de schriftelijke toestemming voorwaarden verbinden, op het gebied van geheimhouding en ter naleving van de verplichtingen uit deze Verwerkersovereenkomst.
3. Opdrachtnemer blijft in deze gevallen te allen tijde aanspreekpunt en verantwoordelijk voor de naleving van bepalingen uit deze Verwerkersovereenkomst.

Artikel 13 Wijziging

Wijziging van deze Verwerkersovereenkomst kan slechts schriftelijk plaatsvinden middels een door een beide partijen geaccordeerd voorstel.

Artikel 14 Terugbezorgen of wissen Persoonsgegevens

1. Na afloop van de Overeenkomst draagt Opdrachtnemer, naar gelang de keuze van Opdrachtgever, zorg voor het terugbezorgen aan Opdrachtgever of het wissen van alle Persoonsgegevens. Opdrachtnemer verwijdert kopieën, behoudens afwijkende wettelijke voorschriften.
2. ***<OPTIONEEL>***Opdrachtnemer [wist of retourneert] de Persoonsgegevens binnen [aantal] [dagen/weken] na afloop van de Overeenkomst, bij gebreke waarvan Opdrachtnemer een boete verschuldigd is van €[bedrag] per dag, met een maximum van €[bedrag].
3. ***<OPTIONEEL>*** Persoonsgegevens worden in de door Opdrachtgever aangegeven vorm en op de door Opdrachtgever aangegeven wijze terugbezorgd.
4. ***<OPTIONEEL>*** De Persoonsgegevens worden als volgt terugbezorgd: [bestandsformaat] [wijze] [adres].

Artikel 16 Overdracht rechten en plichten

De rechten en verplichtingen uit deze Verwerkersovereenkomst kunnen door Opdrachtnemer niet aan derden worden overgedragen zonder de voorafgaande schriftelijke toestemming van de Opdrachtgever.

Artikel 18 Toepasselijk recht en geschillen

1. Op deze Verwerkersovereenkomst en op alle geschillen die daaruit voortvloeien of daarmee samenhangen is Nederlands recht van toepassing.
2. Alle geschillen voortvloeiende uit of samenhangende met deze Verwerkersovereenkomst zullen uitsluitend worden voorgelegd aan de bevoegde rechter te Den Haag

Aldus overeengekomen en in tweevoud ondertekend,

Opdrachtgever Omgevingsdienst West-Holland Opdrachtnemer

Datum: ……-……-…… Datum: ……-……-……

Bijlage 1: omschrijving werkzaamheden ter uitwerking van artikel 3

1. De werkzaamheden van Opdrachtnemer (de verleende diensten en de bijbehorende verwerking). zoals:

- Hosting bestaande uit activiteiten zoals…
- Back-ups maken en restoren
- Applicatiebeheer bestaande uit activiteiten zoals…
- Technisch beheer bestaande uit activiteiten zoals…
- Database beheer bestaande uit activiteiten zoals…
- Helpdesk bestaande uit activiteiten zoals…
- Communicatievoorziening (zoals berichtenverkeer)
- Archiefbeheer
- Vernietiging van gegevensdragers
- Printing, scanning, kopiëren (lease van Multifunctionals)
- Inhoudelijke werkzaamheden die namens Opdrachtgever worden uitgevoerd zoals:
    1. Voeren salarisadministratie
    2. Uitvoeren bepaalde taken

2. Omschrijving van de werkzaamheden van de derden (subOpdrachtnemers) als deze er zijn, als bedoeld in artikel 12.

Werkzaamheden zoals:

- Hosting bestaande uit activiteiten zoals…
- Back-ups maken en restoren
- Applicatiebeheer bestaande uit activiteiten zoals…
- Technisch beheer bestaande uit activiteiten zoals…
- Database beheer bestaande uit activiteiten zoals…
- Helpdesk bestaande uit activiteiten zoals…
- Communicatievoorziening (zoals berichtenverkeer
- Onderhoud aan multifunctionals

3. Categorieën personen en soorten persoonsgegevens, zoals:

- Bijzondere persoonsgegevens zoals bedoeld in artikel 9 en 10 van de Verordening. Het gaat hierbij om persoonsgegevens over iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging en om strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag. Het BSN valt ook onder bijzondere persoonsgegevens.
- Gegevens over de financiële of economische situatie van de betrokkene. Hieronder vallen bijvoorbeeld gegevens over (problematische) schulden, salaris- en betalingsgegevens.
- (Andere) gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene. Hieronder vallen bijvoorbeeld gegevens over gokverslaving, prestaties op school of werk of relatieproblemen.
- Gebruikersnamen, wachtwoorden en andere inloggegevens. De mogelijke gevolgen voor betrokkenen hangen af van de verwerkingen en van de persoonsgegevens waar de inloggegevens toegang toe geven. Bij de afweging moet worden betrokken dat veel mensen wachtwoorden hergebruiken voor verschillende verwerkingen.
- Gegevens die kunnen worden misbruikt voor (identiteits)fraude. Het gaat hierbij onder meer om kopieën van identiteitsbewijzen en om het Burgerservicenummer (bsn).

Bijlage 2: beschrijving beveiliging ter uitwerking van artikel 6 lid 1

Normenstelsel
De informatiebeveiliging vindt plaats volgende algemeen erkende normen, namelijk NEN7510, NEN/ISO 27001, PCI/DSS.

De toereikendheid van de informatiebeveiliging blijkt uit :

a. Certificering;
b. Periodieke externe controles zoals audits;
c. Een rapportage met conclusie over de bevindingen van de auditor
d. Eigen controles of eigen mededelingen.

Uit de certificering of periodieke externe controles, uit de audits of uit de eigen controles blijkt of kan afgeleid wordt dat de beveiliging voldoet aan of gelijkwaardig is met de genoemde maatregelen in bijlage 3.

Bijlage 3 Beveiligingsmaatregelen Opdrachtnemer

Nr.	Titel	Maatregel Opdrachtnemer
1.	Geheimhoudingsverklaring	Medewerkers die te maken hebben met persoonsinformatie van de verantwoordelijke dienen een geheimhoudingsverklaring te ondertekenen. Hierbij wordt tevens vastgelegd dat na beëindiging van de functie, de betreffende persoon gehouden blijft aan de geheimhouding.
2.	Onafhankelijke beoordeling van informatiebeveiliging	Periodieke beveiligingsaudits (minimaal eens per twee jaar) worden uitgevoerd volgens bevindingen t.a.v. de Verwerking van Persoonsgegevens van de Verantwoordelijke en worden aan Verantwoordelijke gerapporteerd, indien mogelijk in combinatie met rapportage zoals genoemd in artikel 7 van deze overeenkomst.
3.	Beveiliging behandelen in overeenkomsten met een derde partij	Maatregelen uit Verwerkersovereenkomst zijn geïmplementeerd.
	Identificatie van risico's die betrekking hebben op externe partijen	Over het naleven van de afspraken wordt op schriftelijk verzoek gerapporteerd aan de verantwoordelijke.
4.	Labeling en verwerking van informatie	Opdrachtnemer heeft maatregelen genomen zo dat niet geautoriseerden geen kennis kunnen nemen van persoonsgegevens
5.	Rollen en verantwoordelijkheden	Het personeel van Opdrachtnemer of derden moeten kennis hebben van de verantwoordelijkheden ten aanzien van de bewerking van de persoonsgegevens voor de verantwoordelijke.
6.	Screening	Voor personen is een recente Verklaring Omtrent het Gedrag (VOG) vereist, tenzij dit centraal in het contract geregeld is.
7.	Blokkering van toegangsrechten	Toegangsrechten van medewerkers van Opdrachtnemer worden direct geblokkeerd als geen toegang voor de bewerking van de persoonsgegevens noodzakelijk is.
8.	Fysieke toegangsbeveiliging	Toegang tot beveiligde zones of gebouwen waar persoonsgegevens van de verantwoordelijke zich bevinden is alleen mogelijk na autorisatie daartoe.
9.	Beveiliging van kantoren, ruimten en faciliteiten	Papieren documenten en mobiele gegevensdragers die persoonsgegevens of andere vertrouwelijke gegevens van de verantwoordelijke bevatten worden beveiligd opgeslagen.
10.	Capaciteitsbeheer	De ICT-voorzieningen voldoen aan het voor de dienst overeengekomen niveau van beschikbaarheid. Er worden voorzieningen geïmplementeerd om de beschikbaarheid van componenten te bewaken (bijvoorbeeld de controle op aanwezigheid van een component en metingen die het gebruik van een component vaststellen). Op basis van voorspellingen van het gebruik wordt actie genomen om tijdig de benodigde uitbreiding van capaciteit te bewerkstelligen. Op basis van een risicoanalyse wordt bepaald wat de beschikbaarheidseis van een ICT-voorziening is en wat de impact bij uitval is. Afhankelijk daarvan worden maatregelen bepaald zoals automatisch werkende mechanismen om uitval van (fysieke) ICT-voorzieningen, waaronder verbindingen op te vangen.
11.	Maatregelen voor netwerken	Gegevensuitwisseling tussen vertrouwde en niet vertrouwde zones dient inhoudelijk geautomatiseerd gecontroleerd te worden op aanwezigheid van malware.
12.	Maatregelen voor netwerken	Bij transport van vertrouwelijke informatie over niet vertrouwde netwerken tussen de Opdrachtnemer en de verantwoordelijke, zoals over het internet, dient altijd geschikte encryptie te worden toegepast.
13	Beveiliging van netwerkdiensten	Beveiligingskenmerken, niveaus van dienstverlening en beheereisen voor alle netwerkdiensten behoren te worden geïdentificeerd en opgenomen in elke overeenkomst voor

		netwerkdiensten, zowel voor diensten die intern worden geleverd als voor uitbestede diensten door een Opdrachtnemer.
14.	Uitwisselingsovereenkomsten	Verantwoordelijkheid en aansprakelijkheid in het geval van informatiebeveiligingsincidenten zijn beschreven, evenals procedures over melding van incidenten van de Opdrachtnemer naar de verantwoordelijke.
15.	Fysieke media die worden getransporteerd	De Opdrachtnemer neemt maatregelen om vertrouwelijke informatie te beschermen, zoals: a. Versleuteling; b. Bescherming door fysieke maatregelen, zoals afgesloten containers; c. Gebruik van verpakkingsmateriaal waaraan te zien is of getracht is het te openen; d. Persoonlijke aflevering; e. Opsplitsing van zendingen in meerdere delen en eventueel verzending via verschillende routes.
16.	Aanmaken auditlogbestanden	Door de Opdrachtnemer worden rapportages van logbestanden gemaakt die periodiek worden beoordeeld. Deze periode dient te worden gerelateerd aan de mogelijkheid van misbruik en de schade die kan optreden.
17.	Aanmaken auditlogbestanden	Een logregel bevat minimaal: f. Een tot een natuurlijk persoon herleidbare gebruikersnaam of ID; g. De gebeurtenis (zie nr. 19.); h. Waar mogelijk de identiteit van het werkstation of de locatie; i. Het object waarop de handeling werd uitgevoerd; j. Het resultaat van de handeling; k. De datum en het tijdstip van de gebeurtenis.
18	Aanmaken auditlogbestanden	In een logregel wordt in geen geval gevoelige gegevens opgenomen. Dit betreft onder meer gegevens waarmee de beveiliging doorbroken kan worden (zoals wachtwoorden, inbelnummers, et cetera).
19	Controle van systeemgebruik	De volgende gebeurtenissen worden in ieder geval opgenomen in de logging: l. Gebruik van technische beheerfuncties, zoals het wijzigingen van configuratie of instelling: uitvoeren van een systeemcommando, starten en stoppen, uitvoering van een back-up of restore. m. Gebruik van functioneel beheerfuncties, zoals het wijzigingen van configuratie en instellingen, release van nieuwe functionaliteit, ingrepen in gegevenssets (waaronder databases). n. Handelingen van beveiligingsbeheer, zoals het opvoeren en afvoeren gebruikers, toekennen en intrekken van rechten, wachtwoord reset, uitgifte en intrekken van cryptosleutels. o. Beveiligingsincidenten (zoals de aanwezigheid van malware, testen op vulnerabilities, foutieve inlogpogingen, overschrijding van autorisatiebevoegdheden, geweigerde pogingen om toegang te krijgen, het gebruik van niet operationele systeemservices, het starten en stoppen van security services). p. Verstoringen in het productieproces (zoals het vollopen van queues, systeemfouten, afbreken tijdens executie van programmatuur, het niet beschikbaar zijn van aangeroepen programmaonderdelen of systemen). q. Handelingen van gebruikers, zoals goede en foute inlogpogingen, systeemtoegang, gebruik van online transacties en toegang tot bestanden door

		systeembeheerders.
20.	Bescherming van informatie in logestanden	Logbestanden worden zodanig beschermd dat deze niet aangepast of gemanipuleerd kunnen worden.
21.	Bescherming van informatie in logestanden	De beschikbaarheid van loginformatie is gewaarborgd binnen de termijn waarin loganalyse noodzakelijk wordt geacht, met een minimum van drie maanden, conform de wensen van de verantwoordelijke. Bij een (vermoed informatiebeveiligingsincident is de bewaartermijn minimaal drie jaar.
22.	Synchronisatie van systeemklokken	Er worden maatregelen genomen om er voor te zorgen dat de logbestanden die verzameld worden aan elkaar te relateren zijn, op basis van het tijdstip waarin ze zijn opgetreden.
23.	Authenticatie van gebruikers bij externe verbindingen.	Als externe toegang nodig is tot de persoonsgegevens van de verantwoordelijke door eigen personeel, of personeel van de Opdrachtnemer, dienen geschikte authenticatie methodes te worden gebruikt
24.	Scheiding van netwerken	Zonering wordt ingericht met voorzieningen waarvan de functionaliteit is beperkt tot het strikt noodzakelijke (hardening van voorzieningen).
	Beveiligde inlogprocedures	Toegang tot de persoonsgegevens van de verantwoordelijke wordt verleend op basis van twee-factor authenticatie.
25.	Beveiligde inlogprocedures	Het wachtwoord wordt niet getoond op het scherm tijdens het ingeven. Er wordt geen informatie getoond die herleidbaar is tot de authenticatiegegevens.
	Beveiligde inlogprocedures	Voorafgaand aan het aanmelden wordt aan de gebruiker een melding getoond dat alleen geautoriseerd gebruik is toegestaan voor expliciet door de organisatie vastgestelde doeleinden.
26.	Beveiligde inlogprocedures	Bij een succesvol loginproces wordt de datum en tijd van de voorgaande login of loginpoging getoond. Deze informatie kan de gebruiker enige informatie verschaffen over de authenticiteit en/of misbruik van het systeem.
27.	Beveiligde inlogprocedures	Nadat voor een gebruikersnaam 3 keer een foutief wachtwoord gegeven is, wordt het account minimaal 10 minuten geblokkeerd. Indien er geen lock-out periode ingesteld kan worden, dan wordt het account geblokkeerd totdat de gebruiker verzoekt deze lock-out op te heffen of het wachtwoord te resetten.
28.	Gebruikersidentificatie en -authenticatie	Bij uitgifte van authenticatiemiddelen wordt minimaal de identiteit vastgesteld, evenals het feit dat de gebruiker recht heeft op het authenticatiemiddel.
29.	Systemen voor wachtwoordbeheer	Er wordt automatisch gecontroleerd op goed gebruik van wachtwoorden (onder andere voldoende sterke wachtwoorden, regelmatige wijziging, directe wijziging van initieel wachtwoord).
30.	Time-out van sessies	De periode van inactiviteit van een werkstation is vastgesteld op maximaal 15 minuten. Daarna wordt de PC vergrendeld. Bij remote desktop sessies geldt dat na maximaal 15 minuten inactiviteit de sessie verbroken wordt.
31.	Beperking van verbindingstijd	De toegang voor onderhoud op afstand door een leverancier wordt alleen opengesteld op basis van een wijzigingsverzoek of storingsmelding, met 2-factor authenticatie en tunneling.
32.	Beperking van toegang tot informatie	In de soort toegangsregels wordt ten minste onderscheid gemaakt tussen lees- en schrijfbevoegdheden.
33.	Beperking van toegang tot informatie	Managementsoftware heeft de mogelijkheid gebruikerssessies af te sluiten.
34.	Beperking van toegang tot informatie	Bij extern gebruik vanuit een niet vertrouwde omgeving vindt sterke authenticatie (two-factor) van gebruikers plaats.
35.	Analyse en specificatie van Beveiligingseis en	In projecten ten behoeve van systemen voor de verantwoordelijke wordt een beveiligingsrisicoanalyse en maatregelbepaling opgenomen als onderdeel van het ontwerp. Ook bij wijzigingen worden de

		veiligheidsconsequenties meegenomen.
36.	Validatie van invoergegevens	Er moeten controles worden uitgevoerd op de invoer van gegevens. Daarbij wordt minimaal gecontroleerd op grenswaarden, ongeldige tekens, onvolledige gegevens, gegevens die niet aan het juiste format voldoen, toevoegen van parameters (SQL-Injectie) en inconsistentie van gegevens.
37.	Beheersing van interne gegevensverwerking	Er bestaan voldoende mogelijkheden om reeds ingevoerde gegevens te kunnen corrigeren door er gegevens aan te kunnen toevoegen.
38.	Integriteit van berichten	Er behoren eisen en geschikte beheersmaatregelen te worden vastgesteld en geïmplementeerd, voor het bewerkstelligen van authenticiteit en het beschermen van integriteit van berichten in toepassingen.
39.	Validatie van uitvoergegevens	De uitvoerfuncties van programma's maken het mogelijk om de volledigheid en juistheid van de gegevens te kunnen vaststellen (bijvoorbeeld door check-sums).
40.	Beleid voor het gebruik van cryptografische beheersmaatregelen	De gebruikte cryptografische algoritmen voor versleuteling zijn als open standaard gedocumenteerd en zijn door onafhankelijke betrouwbare deskundigen getoetst.
41..	Sleutelbeheer	In het sleutelbeheer is minimaal aandacht besteed aan het proces, de actoren en hun verantwoordelijkheden.
42..	Beheersing van operationele software	Alleen geautoriseerd personeel kan functies en software installeren of activeren.
43.	Procedures voor wijzigingsbeheer	Er is aantoonbaar wijzigingsmanagement ingericht volgens gangbare best practices, zoals ITIL en voor applicaties ASL.
44..	Technische beoordeling van toepassingen na wijzigingen in het besturingssysteem	Van aanpassingen (zoals updates) aan softwarematige componenten van de technische infrastructuur wordt vastgesteld dat deze de juiste werking van de technische componenten niet in gevaar brengen en de beveiliging zoals afgesproken met de verantwoordelijke te niet doen.
45.	Uitlekken van informatie	Er dient een proces te zijn om aan de verantwoordelijke te melden dat (persoons) informatie is uitgelekt. Zie rapportage van informatiebeveiligingsgebeurtenissen. nrs. 38 – 40.
46.	Uitlekken van informatie	Er dient een proces te zijn om aan de verantwoordelijke te melden dat (persoons) informatie is uitgelekt. (zie 38)
47.	Beheersing van technische kwetsbaarheden	Er is een proces ingericht voor het beheer van technische kwetsbaarheden. Dit omvat minimaal het melden van incidenten aan de verantwoordelijke, het uitvoeren van periodieke penetratietests, het uitvoeren van risicoanalyses van kwetsbaarheden en patching van systemen en hardware.
48.	Rapportage van informatiebeveiligingsgebeurtenissen	Er is een procedure voor het rapporteren van beveiligingsgebeurtenissen aan de verantwoordelijke vastgesteld, in combinatie met een reactie- en escalatieprocedure voor incidenten, waarin de handelingen worden vastgelegd die moeten worden genomen na het ontvangen van een rapport van een beveiligingsincident.
49.	Rapportage van informatiebeveiligingsgebeurtenissen	Alle beveiligingsincidenten worden vastgelegd in een systeem en geëscaleerd aan de verantwoordelijke.
50.	Rapportage van informatiebeveiligingsgebeurtenissen	Vermissing of diefstal van apparatuur of media die gegevens van de verantwoordelijke kunnen bevatten wordt altijd ook aangemerkt als informatiebeveiligingsincident.
51.	Verzamelen van bewijsmateriaal	Voor een vervolgprocedure naar aanleiding van een beveiligingsincident behoort bewijsmateriaal te worden verzameld, bewaard en gepresenteerd in overeenstemming met de voorschriften voor bewijs die voor het relevante rechtsgebied zijn vastgelegd.
52.	Bescherming van bedrijfsdocumenten	De registraties van de verantwoordelijke behoren te worden beschermd tegen verlies, vernietiging en vervalsing, in overeenstemming met wettelijke en regelgevende eisen, contractuele verplichtingen en bedrijfsmatige eisen.

53.	Bescherming van gegevens en Geheimhouding van persoonsgegevens	De bescherming van gegevens en privacy behoort te worden bewerkstelligd in overeenstemming met relevante wetgeving, voorschriften en indien van toepassing contractuele bepalingen.
54.	Voorschriften voor het gebruik van cryptografische beheersmaatregelen	Er is vastgesteld aan welke overeenkomsten, wetten en voorschriften de toepassing van cryptografische technieken moet voldoen.
55.	Naleving van beveiligingsbeleid en -normen	De Opdrachtnemer is verantwoordelijk voor uitvoering en beveiligingsprocedures en toetsing daarop (onder andere de jaarlijkse in control verklaring). Conform deze Verwerkersovereenkomst en andere contractuele eisen zorgt de Opdrachtnemer voor het toezicht op de uitvoering van het beveiligingsbeleid ten behoeve van de gegevens van de verantwoordelijke. Daarbij behoren ook periodieke beveiligingsaudits. Deze kunnen worden uitgevoerd door, of vanwege de verantwoordelijke.
46.	Controle op technische naleving	Informatiesystemen van de Opdrachtnemer ten behoeve van de verantwoordelijke worden regelmatig gecontroleerd op naleving van beveiligingsnormen. Dit kan door bijvoorbeeld kwetsbaarheidsanalyses en penetratietesten.