



Verwerkersovereenkomst behorend bij de overeenkomst eDepot voor regio Westfriesland

Documentnummer: 2018-P023
Status: Definitief
Datum: 24 augustus 2018

Inhoudsopgave

ONDERGETEKENDEN:	3
OVERWEGEN DAT:	4
VERKLAREN TE ZIJN OVEREENGEKOMEN:	4
Artikel 1. Totstandkoming en looptijd.....	4
Artikel 2. Onderwerp van de Verwerkersovereenkomst	4
Artikel 3. Geheimhoudingsplicht	5
Artikel 4. Beveiliging en controle	5
Artikel 5. Kennisgeving van beveiligingsincidenten en datalekken	6
Artikel 6. Inschakelen derden.....	7
Artikel 7. Opslag van persoonsgegevens buiten Europees grondgebied	8
Artikel 8. Verzoeken van betrokkene.....	8
Artikel 9. Aansprakelijkheid	8
Artikel 10. Wijziging of beëindiging van de Verwerkersovereenkomst.....	9
Artikel 11. Teruggave, vernietiging persoonsgegevens en overdracht.....	10
Artikel 12. Slotbepalingen.....	10
ONDERTEKENING	11
BIJLAGE 1: OMSCHRIJVING VAN DE VERWERKING	12
BIJLAGE 2: BEVEILIGINGSMAATREGELEN	13

ONDERGETEKENDEN:

Het college van burgemeester en wethouders van de gemeente:

	Drechterland	Enkhuizen
KvK nummer:	37159718	37159077
Postadres:	Postbus 9, 1616 ZG, Hoogkarspel	Postbus 11, 1600 AA, Enkhuizen
Bezoekadres:	Raadhuisplein 1, Hoogkarspel	Hoogstraat 11, 1601 KT, Enkhuizen
	Hoorn	Koggenland
KvK nummer:	37159084	50582445
Postadres:	Postbus 603, 1620 AR, Hoorn	Postbus 21, 1633 ZG, Avenhorn
Bezoekadres:	Nieuwe Steen 1, 1625 HV, Hoorn	Middenhof 2, 1648 JG, De Goorn
	Medemblik	Opmeer
KvK nummer:	37159672	37159195
Postadres:	Postbus 45, 1687 ZG, Wognum	Postbus 199, 1715 ZK, Spanbroek
Bezoekadres:	Dick Ketlaan 21, 1687 CD, Wognum	Klaproos 1, 1716 VS, Opmeer
	Stede Broec	
KvK nummer:	37159550	
Postadres:	Postbus 20, 1610 AA, Bovenkarspel	
Bezoekadres:	De Middend 2, 1611 KW, Bovenkarspel	

Het dagelijks bestuur van:

	SED organisatie	Shared Service Center DeSom
KvK nummer:	62255002	59925736
Postadres:	Postbus 20, 1610 AA, Bovenkarspel	Postbus 45, 1687 ZG, Wognum
Bezoekadres:	De Middend 2, 1611 KW, Bovenkarspel	Dick Ketlaan 1, 1687 CD, Wognum
	WerkSaam Westfriesland	Westfries Archief
KvK nummer:	3714810	50152572
Postadres:	Postbus 566, 1620 AN, Hoorn	Postbus 603, 1620 AR, Hoorn
Bezoekadres:	Dampden 26, 1624 NR, Hoorn	Blauwe Berg 5 C, 1625 NT, Hoorn

te dezen rechtsgeldig vertegenwoordigd door de heer D. Dekema, directeur Westfries Archief, hierna te noemen: "Verwerkingsverantwoordelijke",

en

* (naam Leverancier), gevestigd en kantoorhoudende te *, te dezen rechtsgeldig vertegenwoordigd door *de heer/mevrouw * (naam), *(functie), hierna te noemen: "Verwerker",

gezamenlijk ook aan te duiden als "Partijen" en afzonderlijk als "Partij",

OVERWEGEN DAT:

- Verwerkingsverantwoordelijke en Verwerker een overeenkomst voor een eDepot voor de regio Westfriesland op *(datum) hebben gesloten, voor de periode 1 april 2019 tot 31 december 2022 hierna te noemen de “Hoofdovereenkomst”;
- Verwerker in het kader van de uitvoering van de Hoofdovereenkomst in opdracht van Verwerkingsverantwoordelijke persoonsgegevens verwerkt;
- Waar in deze verwerkersovereenkomst termen worden gebruikt die overeenstemmen met definities uit artikel 4 van de AVG, worden aan deze termen de betekenis van de definities uit de AVG toegekend.
- Verwerker hierbij wordt aangemerkt als ‘Verwerker’ in de zin van artikel 4 lid 8 van de Algemene Verordening Gegevensbescherming (hierna te noemen de ‘AVG’) en Verwerkingsverantwoordelijke als ‘Verwerkingsverantwoordelijke’ in de zin van artikel 4 lid 7 van de AVG;
- Partijen wensen hun afspraken over deze verwerking van persoonsgegevens door Verwerker vast te leggen in deze Verwerkersovereenkomst;
- Deze Verwerkersovereenkomst een integraal onderdeel is van de Hoofdovereenkomst.

VERKLAREN TE ZIJN OVEREENGEKOMEN:

Artikel 1. Totstandkoming en looptijd

1. Deze Verwerkersovereenkomst gaat in op het moment van ondertekening.
2. Deze Verwerkersovereenkomst is van kracht zolang Verwerker optreedt als Verwerker van de door Verwerkingsverantwoordelijke ter beschikking gestelde persoonsgegevens in het kader van de Hoofdovereenkomst.

Artikel 2. Onderwerp van de Verwerkersovereenkomst

1. Verwerker verwerkt persoonsgegevens in opdracht en volgens de instructies van Verwerkingsverantwoordelijke en niet meer dan noodzakelijk is voor het uitvoeren van de Hoofdovereenkomst. Deze verwerkingen vinden alleen plaats in het kader van en voor het doel zoals omschreven in de Hoofdovereenkomst.
2. Verwerkingsverantwoordelijke beschrijft deze verwerkingen, als bedoeld in artikel 28 lid 3 van de AVG. Deze beschrijving is opgenomen in Bijlage 1.
3. Het is Verwerker niet toegestaan persoonsgegevens van Verwerkingsverantwoordelijke aan aanvullende verwerkingen te onderwerpen, tenzij Verwerkingsverantwoordelijke hier voorafgaand aan de verwerking expliciet schriftelijke toestemming voor heeft gegeven met inachtneming van de van toepassing zijnde regelgeving.

4. Verwerker garandeert bij de verwerking van de persoonsgegevens zich te houden aan alle toepasselijke wet- en regelgeving, waaronder (maar niet uitsluitend) wet- en regelgeving betreffende de verwerking van persoonsgegevens. Hieronder valt ook het treffen van passende technische en organisatorische maatregelen, zodat de verwerking van persoonsgegevens aan deze wet- en regelgeving voldoet.
5. Verwerker stelt de Verwerkingsverantwoordelijke in staat om te voldoen aan wet- en regelgeving betreffende de verwerking van persoonsgegevens en verleent volledige medewerking, op het eerste verzoek van Verwerkingsverantwoordelijke.
6. Verwerker heeft geen zeggenschap over de ter beschikking gestelde persoonsgegevens. De Verwerker neemt geen beslissingen over ontvangst en gebruik van de persoonsgegevens, de verstrekking aan derden, tenzij dit voldoet aan de voorwaarden gesteld in artikel 6, en de duur van de opslag van gegevens. De zeggenschap over de persoonsgegevens ligt bij de Verwerkingsverantwoordelijke en niet bij de Verwerker.

Artikel 3. Geheimhoudingsplicht

1. Verwerker, personen in dienst van Verwerker, organisaties en/of personen werkzaam ten behoeve van Verwerker, zijn verplicht tot geheimhouding van de persoonsgegevens. Deze geheimhoudingsplicht is niet van toepassing als (en voor zover):
 - het verstrekken van de informatie aan derden, met inachtneming van de voorwaarden gesteld in artikel 6, logischerwijs noodzakelijk is om de opdracht van Verwerkingsverantwoordelijke en deze Verwerkersovereenkomst te kunnen uitvoeren,
 - Verwerker een wettelijke verplichting heeft om de informatie aan een derde te verstrekken.
2. Verwerker verplicht aantoonbaar personen in dienst van of werkzaam bij Verwerker deze geheimhoudingsplicht na te leven.

Artikel 4. Beveiliging en controle

1. Verwerker is verplicht voldoende en passende technische en organisatorische maatregelen te treffen om de persoonsgegevens te beveiligen tegen verlies, toegang door onbevoegden of tegen enige vorm van onrechtmatige verwerking, conform artikel 32 AVG.
2. Verwerker treft in ieder geval de maatregelen die zijn opgenomen in bijlage 2 bij deze Verwerkersovereenkomst.
3. Verwerker is verplicht om minimaal eens per *(jaar / twee jaar / drie jaar) een onderzoek te laten uitvoeren naar de opzet en bestaan van de verplichtingen in deze

Opmerking [PS1]: Als er sprake is van een verwerker die gevoelige of bijzondere persoonsgegevens verwerkt of om veel personen en de risico's zijn hoog, dan is het raadzaam om dit artikel op te nemen. Maak hierin ook een goede risico-afweging voor de keuze eens per 1, 2 of 3 jaar.

I.g.v. lage risico's (geen gevoelige persoonsgegevens, bijvb alleen naam en emailadres) dan volstaat lid 1 van dit artikel. Lid 3, 4 en 5 kunnen dan vervallen.

Verwerkersovereenkomst. Verwerker laat dit onderzoek uitvoeren door een onafhankelijke externe deskundige. Een afschrift van de Third Party Memorandum (TPM) met de bevindingen, wordt kosteloos aan Verwerkingsverantwoordelijke verstrekt. Indien Verwerker voldoet aan de genoemde maatregelen en dit kan aantonen door middel van een geldig ISO/IEC 27001/soort gelijk certificaat en bijbehorende verklaring van toepasselijkheid, welke door een onafhankelijk en extern geaccrediteerde auditor is afgegeven, volstaat dit ook;

4. Het onderzoek is voor rekening van de Verwerker.
5. Verwerker is verplicht de systemen, bestanden en documentatie voor dit onderzoek beschikbaar te houden.
6. Verwerkingsverantwoordelijke heeft het recht om altijd bij Verwerker een onderzoek uit te (laten) voeren om de naleving van deze Verwerkersovereenkomst, toepasselijke wet- en regelgeving en alles dat daarmee samenhangt, te controleren.
7. De kosten van het onderzoek benoemd in lid 7 zijn voor rekening van Verwerkingsverantwoordelijke. Als uit de controle blijkt dat Verwerker zich niet aan haar verplichtingen uit deze Verwerkersovereenkomst heeft gehouden, zijn de kosten van het onderzoek voor rekening van Verwerker.
8. Verwerker verleent medewerking aan het onderzoek en stelt alle voor het onderzoek relevante medewerkers en informatie, inclusief ondersteunende gegevens zoals systeemlogs, zo vroeg mogelijk (doch uiterlijk binnen twee weken na aankondiging van de controle door Verwerkingsverantwoordelijke) ter beschikking.
9. Het onderzoek mag niet tot vertraging leiden van de door Verwerker uit te voeren werkzaamheden in het kader van de Hoofdovereenkomst en de Verwerkersovereenkomst.
10. Verwerker stelt Verwerkingsverantwoordelijke zo spoedig mogelijk, doch uiterlijk binnen 5 werkdagen in kennis van de uitkomsten van de in dit artikel benoemde beveiligings- en controlewerkzaamheden.
11. Verwerker is verplicht om geconstateerde tekortkomingen, uit de in dit artikel benoemde onderzoeken, te verhelpen. De termijn waarbinnen de tekortkomingen verholpen moeten zijn, wordt bepaald door Verwerkingsverantwoordelijke.

Artikel 5. Kennisgeving van beveiligingsincidenten en datalekken

1. In het geval van een (vermoeden van):
 - een beveiligingslek (een tekortkoming in of inbreuk op de beveiliging van persoonsgegevens), en/of

- een datalek (een inbreuk zoals bedoeld in artikel 33 en 34 AVG) met betrekking tot de gegevens die Verwerker ten behoeve van Verwerkingsverantwoordelijke verwerkt of door een derde laat verwerken,
- die (mogelijk) nadelige gevolgen heeft voor betrokkene(n), garandeert Verwerker om Verwerkingsverantwoordelijke daarover onmiddellijk en uiterlijk binnen 24 uur na ontdekking van het lek te informeren. Verwerker verstrekt hiertoe alle gevraagde informatie in het formulier 'Nieuwe melding', te vinden in het Meldloket Datalekken op de website van de Autoriteit Persoonsgegevens. Verwerker stuurt deze informatie naar info@westfriesarchief.nl onder vermelding van de contractbeheerder en het contract. Verwerker garandeert dat de verstrekte informatie volledig, correct en accuraat is. Deze meldplicht geldt ongeacht de impact van het lek.
2. Indien Verwerker op het tijdstip van de melding niet over alle bovenstaande informatie beschikt, dan neemt Verwerker de beschikbare informatie in de melding op en stuurt de ontbrekende informatie zo spoedig mogelijk na. Verwerker neemt in de melding op wanneer de ontbrekende informatie beschikbaar wordt gesteld.
 3. Verwerker geeft, op het eerste verzoek van Verwerkingsverantwoordelijke, alle inlichtingen die Verwerkingsverantwoordelijke noodzakelijk acht om het lek te beoordelen en om het lek te melden aan de relevante autoriteiten en/of betrokkenen.
 4. Verwerker heeft een gedegen plan voor de omgang met en afhandeling van datalekken. Op verzoek van Verwerkingsverantwoordelijke geeft Verwerker inzage in het plan.
 5. Verwerker houdt een gedetailleerd logboek bij van alle beveiligingslekken en datalekken, ongeacht (mogelijke) nadelige gevolgen voor betrokkene(n), met de maatregelen die naar aanleiding van het lek zijn genomen. Verwerker verstrekt jaarlijks en op verzoek kosteloos een overzicht met beveiligings- en datalekken die betrekking hadden op de verwerkingen in het kader van de Hoofdovereenkomst.
 6. Indien de wet- en/of regelgeving dit vereist werkt Verwerker mee aan het informeren van de relevante autoriteiten en betrokkenen. Verwerkingsverantwoordelijke is verantwoordelijk voor het melden naar de relevante autoriteiten en betrokkenen.
 7. Verwerker neemt de oorzaak of oorzaken van het lek zo spoedig mogelijk weg en stelt alles in het werk om de gevolgen van het lek zoveel mogelijk te beperken en om herhaling te voorkomen.

Artikel 6. Inschakelen derden

1. Als Verwerker werkzaamheden in het kader van de Hoofdovereenkomst en Verwerkersovereenkomst overdraagt aan een derde, garandeert Verwerker dat deze derde partij alle verplichtingen uit deze Verwerkersovereenkomst op zich neemt en

nakomt. Verwerker staat in voor een correcte naleving van deze plichten door de door hem ingeschakelde derde. Verwerker is volledig aansprakelijk voor alle schade die de door hem ingeschakelde derde veroorzaakt. Verwerker blijft aanspreekpunt en verantwoordelijk voor de naleving van de bepalingen uit deze Verwerkersovereenkomst.

2. Op het eerste verzoek verstrekt Verwerker aan Verwerkingsverantwoordelijke een actueel overzicht met door hem ingeschakelde derden, zoals bedoeld in lid 1, en geeft inzicht in de door deze derden uitgevoerde werkzaamheden.

Artikel 7. Opslag van persoonsgegevens buiten Europees grondgebied

1. Verwerker is niet bevoegd tot verwerking en opslag van de persoonsgegevens buiten Europees grondgebied of bij een bedrijf waarvan de verwerking van persoonsgegevens (mede) onderhevig is aan de wettelijke regels van een land of gebiedsdeel buiten de Europese Unie.
2. Van deze bepaling mag alleen worden afgeweken met voorafgaande schriftelijke toestemming van de Verwerkingsverantwoordelijke en met inachtneming van de toepasselijke wet- en regelgeving ten aanzien van de doorgifte van persoonsgegevens naar landen buiten de Europese Unie.

Artikel 8. Verzoeken van betrokkene

1. Als een betrokkene een verzoek op grond van een wettelijke bepaling tot inzage, verbetering, aanvulling, wijziging of afscherming (in het gebruik) van zijn of haar gegevens richt aan Verwerker, verwijst Verwerker die betrokkene door naar Verwerkingsverantwoordelijke.
2. Verwerker verstrekt geen informatie aan een betrokkene (anders dan de doorverwijzing uit lid 1) zonder voorafgaande schriftelijke toestemming van Verwerkingsverantwoordelijke. Op verzoek van Verwerkingsverantwoordelijke verleent Verwerker direct zijn medewerking zodat Verantwoordelijk gehoor kan geven aan het verzoek van betrokkene zoals bedoeld in lid 1.

Artikel 9. Aansprakelijkheid

1. Verwerkingsverantwoordelijke kan Verwerker met betrekking tot deze Verwerkersovereenkomst aansprakelijk stellen voor:
 - alle aanspraken waarvoor Verwerker verantwoordelijk is en waarvoor Verwerkingsverantwoordelijke wordt aangesproken.
 - een maatregel opgelegd door de officieel bevoegde autoriteit aan Verwerkingsverantwoordelijke, waaronder begrepen een boete.

- alle kosten en schade die Verwerkingsverantwoordelijke maakt en heeft (daaronder begrepen de interne kosten) als gevolg van een beveiligingsincident of datalek als omschreven in artikel 5.

Verwerker kan alleen aansprakelijk worden gesteld:

- als de schade voortkomt uit het schenden van de wettelijke verplichtingen, andere toepasselijke regelgeving of verplichtingen uit deze Verwerkersovereenkomst en Hoofdovereenkomst betreffende de verwerking van persoonsgegevens,
 - voor zover en tot het bedrag dat de schade aan Verwerker of een door haar ingeschakelde derde kan worden toegerekend.
2. Indien Verwerker tekortschiet in de nakoming van de verplichtingen in deze Verwerkersovereenkomst kan Verwerkingsverantwoordelijke hem in gebreke stellen.
 3. Na ingebrekestelling komen Verwerker en verwerkersverantwoordelijke een redelijke termijn overeen waarbinnen verwerker alsnog haar verplichtingen nakomt.
 4. Indien nakoming binnen deze termijn uitblijft, is Verwerker in verzuim. Verwerker is onmiddellijk in verzuim als de nakoming van de verplichtingen, anders dan door overmacht, binnen de overeengekomen termijn, niet mogelijk is.
 5. Ongeacht de mogelijkheid tot beëindiging van de overeenkomst zoals bedoeld in artikel 10 lid 3 verbeurt verwerker in geval van verzuim per niet nagekomen verplichting een direct opeisbare een boete van € 500,-. Indien de hoogte van een eventueel aan de gemeente op te leggen boete door de Autoriteit Persoonsgegevens hoger is dan het boetebedrag op grond van vorenstaande, verbeurt verwerker de hoogte van de boete die door de Autoriteit Persoonsgegevens aan de gemeente is opgelegd.

Artikel 10. Wijziging of beëindiging van de Verwerkersovereenkomst

1. Partijen mogen deze Verwerkersovereenkomst wijzigen met wederzijdse instemming.
2. Verwerkingsverantwoordelijke en verwerker treden met elkaar in overleg over wijzigingen in deze verwerkersovereenkomst als een wijziging in regelgeving of een wijziging in de uitleg van regelgeving daartoe aanleiding geven.
3. Verwerkingsverantwoordelijke kan de Verwerkersovereenkomst en de Hoofdovereenkomst met onmiddellijke ingang en zonder rechterlijke tussenkomst beëindigen in geval van verzuim als bedoeld in artikel 9 lid 4 van deze Verwerkersovereenkomst. Verwerker kan geen aanspraak maken op enige vorm van schadevergoeding.
4. Bij het beëindigen van de Verwerkersovereenkomst met onmiddellijke ingang, wordt in

een brief de reden van beëindiging vermeld.

Artikel 11. Teruggave, vernietiging persoonsgegevens en overdracht

1. Verwerker verplicht zich om:
 - alle persoonsgegevens, kopieën en bewerkingen daarvan,
 - alle gegevensdragers waarop de persoonsgegevens, kopieën of bewerkingen daarvan, zijn of worden vastgelegd,direct, op het eerste verzoek van Verwerkingsverantwoordelijke en op het moment van beëindigen van de Verwerkersovereenkomst, te verstrekken aan Verwerkingsverantwoordelijke, te wissen of te vernietigen.
2. De Verwerkingsverantwoordelijke kan zo nodig nadere eisen stellen aan de wijze van beschikbaarstelling, waaronder eisen aan het bestandsformaat, dan wel vernietiging. Deze werkzaamheden moeten, binnen nader overeen te komen redelijke termijn, uitgevoerd worden. Hiervan wordt een verslag gemaakt en bewijs aangeleverd van de juistheid en volledigheid.
3. Verwerker verplicht zich om Verwerkingsverantwoordelijke direct te informeren als een faillissement of surséance van betaling dreigt, zodat Verwerkingsverantwoordelijke tijdig kan beslissen persoonsgegevens terug te vorderen voordat faillissement wordt uitgesproken.
4. Verwerker verleent alle medewerking aan de overdracht van de werkzaamheden met betrekking tot de verwerking van de persoonsgegevens aan Verwerkingsverantwoordelijke of een opvolgende Verwerker. Deze overdracht vindt plaats op een zodanige manier dat de continuïteit van de dienstverlening maximaal gewaarborgd blijft.
5. De verwerker zal altijd het recht op overdraagbaarheid van gegevens conform artikel 20 AVG waarborgen, zodanig dat er geen sprake is van verlies van functionaliteit of (delen van) de gegevens.
6. De kosten gemoeid met deze inspanningen van Verwerker komen voor rekening van Verwerker tenzij in de Hoofdovereenkomst is bepaald dat deze kosten voor Verwerkingsverantwoordelijke komen en op welke wijze de kosten worden berekend.

Artikel 12. Slotbepalingen

1. Bepalingen in deze Verwerkersovereenkomst die bestemd zijn om ook na het einde van deze Verwerkersovereenkomst van kracht te blijven, blijven na beëindiging van de Verwerkersovereenkomst van kracht. Hieronder behoren onder meer de bepalingen over de meldplicht, geheimhouding, teruggave, vernietiging en overdracht.

ONDERTEKENING

Voor akkoord Verwerkingsverantwoordelijke

Voor akkoord Verwerker

Datum :

Datum :

Handtekening :

Handtekening :

BIJLAGE 1: OMSCHRIJVING VAN DE VERWERKING

(uitwerking van artikel 2 lid 2)

Werkzaamheden verwerker	Het opnemen, bewaren, beschikbaar stellen en verstrekken van afschriften van (proces)informatie van archiefvormers in een digitale bewaarplaats om deze na de bewaartermijn te vernietigen of conform de overbrengingstermijn bepaald in artikel 12 van de Archiefwet openbaar raadpleegbaar te maken.
Soort persoonsgegevens	Gewone (art. 4.1. AVG) en bijzondere persoonsgegevens (art. 9.1 AVG)
Categorieën van betrokkenen	<ul style="list-style-type: none">▪ natuurlijke personen die een relatie met gemeente of een aan haar verbonden partij heeft en de informatie daarvan is gearhiveerd▪ natuurlijke personen, individueel of verbonden aan een particuliere instelling waarvan aan hen identificeerbare informatie wordt beheerd door het Westfries Archief▪ natuurlijke personen die de beschikbare informatie willen en mogen raadplegen
Archivering en vernietiging	Overheidsinformatie wordt niet langer bewaart dan is toegestaan op grond van Selectielijsten conform art. 2, 3, 4 en 5 van het Archiefbesluit. Informatie van particuliere burgers en instellingen wordt niet langer bewaart conform specifieke wetgeving en zoals overeengekomen met de archiefvormer of de aanbieder van de informatie.

BIJLAGE 2: BEVEILIGINGSMAATREGELEN

In deze bijlage zijn, in aanvulling op de bepalingen in de Verwerkersovereenkomst, de technische en organisatorische beveiligingsmaatregelen opgenomen die Verwerker in ieder geval heeft getroffen om een passend beschermingsniveau te waarborgen. Onderstaande opsomming neemt niet weg dat Verwerker aanvullende maatregelen dient te treffen als dat nodig is om een passend beveiligingsniveau te waarborgen.

De maatregelen zijn, indien van toepassing, voorzien van een verwijzing naar het betreffende BIG-nummer (Baseline Informatiebeveiliging Gemeenten, opgesteld door de VNG en KING).

BIG Nummer	titel	Maatregel verwerker
6.1.5.1	Geheimhoudingsovereenkomst	Medewerkers die te maken hebben met persoonsinformatie van de verwerkingsverantwoordelijke dienen een geheimhoudingsverklaring te ondertekenen. Hierbij wordt tevens vastgelegd dat na beëindiging van de functie, de betreffende persoon gehouden blijft aan die geheimhouding.
6.1.8.2	Onafhankelijke beoordeling van informatiebeveiliging	Periodieke beveiligingsaudits (minimaal eens per twee jaar) worden uitgevoerd volgens afspraken met de verwerkingsverantwoordelijke.
6.2.1.7	Identificatie van risico's die betrekking hebben op externe partijen	Over het naleven van de afspraken wordt jaarlijks gerapporteerd aan de verwerkingsverantwoordelijke.
6.2.3.1	Beveiliging behandelen in overeenkomsten met een derde partij	Maatregelen uit de verwerkersovereenkomst zijn geïmplementeerd.
7.2.2.1	Labeling en verwerking van informatie	De verwerker heeft maatregelen genomen zo dat niet geautoriseerden geen kennis kunnen nemen van persoonsgegevens.
8.1.1.2	Rollen en verantwoordelijkheden	Het personeel van de verwerker of derden moeten kennis hebben van de verantwoordelijkheden ten aanzien van de bewerking van de persoonsgegevens voor de verwerkingsverantwoordelijke.
8.1.2.1	Screening	Voor personen is een recente Verklaring Omtrent het Gedrag (VOG) vereist met punten die door de verwerkingsverantwoordelijke zijn aangedragen. Tenzij dit centraal in het contract geregeld is.
8.3.3.1	Blokkering van toegangsrechten	Toegangsrechten van medewerkers van de verwerker worden direct geblokkeerd als geen toegang voor de bewerking van de persoonsgegevens noodzakelijk is.
9.1.2.1	Fysieke toegangsbeveiliging	Toegang tot beveiligde zones of gebouwen waar persoonsgegevens van de verwerkingsverantwoordelijke zich bevinden is

BIG Nummer	titel	Maatregel verwerker
		alleen mogelijk na autorisatie daartoe.
9.1.3.1	Beveiliging van kantoren, ruimten en faciliteiten	Papieren documenten en mobiele gegevensdragers die persoonsgegevens of andere vertrouwelijke gegevens van de verwerkingsverantwoordelijke bevatten worden beveiligd opgeslagen.
10.3.1.1	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.
10.6.1.2	Maatregelen voor netwerken	Gegevensuitwisseling tussen vertrouwde en niet vertrouwde zones dient inhoudelijk geautomatiseerd gecontroleerd te worden op aanwezigheid van malware.
10.6.1.3	Maatregelen voor netwerken	Bij transport van vertrouwelijke informatie over niet vertrouwde netwerken tussen de verwerker en de verwerkingsverantwoordelijke, zoals over het internet, dient altijd geschikte encryptie te worden toegepast. Zie hiertoe 12.3.1.3.
10.6.2.1	Beveiliging van netwerkdiensten	Beveiligingskenmerken, niveaus van dienstverlening en beheer eisen 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 verwerker.
10.8.2.2	Uitwisselingsovereenkomsten	Verantwoordelijkheid en aansprakelijkheid in het geval van informatiebeveiligingsincidenten zijn beschreven, evenals procedures over melding van incidenten van de verwerker naar de verwerkingsverantwoordelijke.
10.8.3.1	Fysieke media die worden getransporteerd	De verwerker neemt maatregelen om vertrouwelijke informatie te beschermen, zoals: <ul style="list-style-type: none"> • Versleuteling. • Bescherming door fysieke maatregelen, zoals afgesloten containers. • Gebruik van verpakkingsmateriaal waaraan te zien is of getracht is het te openen • Persoonlijke aflevering. • Opsplitsing van zendingen in meerdere delen en eventueel verzending via verschillende routes.

BIG Nummer	titel	Maatregel verwerker
10.10.1.1	Aanmaken auditlogbestanden	Door de verwerker 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.
10.10.1.2	Aanmaken auditlogbestanden	<p>Een logregel bevat minimaal:</p> <ul style="list-style-type: none"> • Een tot een natuurlijk persoon herleidbare gebruikersnaam of ID. • De gebeurtenis (zie 10.10.2.1). • Waar mogelijk de identiteit van het werkstation of de locatie. • Het object waarop de handeling werd uitgevoerd. • Het resultaat van de handeling. • De datum en het tijdstip van de gebeurtenis.
10.10.1.3	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).
10.10.2.1	Controle van systeemgebruik	<p>De volgende gebeurtenissen worden in ieder geval opgenomen in de logging:</p> <ul style="list-style-type: none"> • 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. • Gebruik van functioneel beheerfuncties, zoals het wijzigingen van configuratie en instellingen, release van nieuwe functionaliteit, ingrepen in gegevenssets (waaronder databases). • Handelingen van beveiligingsbeheer, zoals het opvoeren en afvoeren gebruikers, toekennen en intrekken van rechten, wachtwoord reset, uitgifte en intrekken van cryptosleutels. • 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). • Verstoringen in het productieproces (zoals het vollopen van queues, systeemfouten, afbreken tijdens executie van programmatuur, het niet beschikbaar zijn van aangeroepen programmaonderdelen of systemen). • Handelingen van gebruikers, zoals goede en foute inlogpogingen, systeemtoegang, gebruik van online transacties en toegang tot bestanden door systeembeheerders.
10.10.3.3	Bescherming van informatie in logstanden	Logbestanden worden zodanig beschermd dat deze niet aangepast of gemanipuleerd kunnen worden.

BIG Nummer	titel	Maatregel verwerker
10.10.3.5	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 verwerkingsverantwoordelijke. Bij een (vermoed) informatiebeveiligingsincident is de bewaartermijn minimaal drie jaar.
10.10.6.1	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.
11.4.2.1	Authenticatie van gebruikers bij externe verbindingen.	Als externe toegang nodig is tot de persoonsgegevens van de verwerkingsverantwoordelijke door eigen personeel, of personeel van de verwerker, dienen geschikte authenticatie methodes te worden gebruikt.
11.4.5.5	Scheiding van netwerken	Zonering wordt ingericht met voorzieningen waarvan de functionaliteit is beperkt tot het strikt noodzakelijke (hardening van voorzieningen).
11.5.1.1	Beveiligde inlogprocedures	Toegang tot de persoonsgegevens van de verwerkingsverantwoordelijke wordt verleend op basis van twee-factor authenticatie.
11.5.1.2	Beveiligde inlogprocedures	Het wachtwoord wordt niet getoond op het scherm tijdens het ingeven. Er wordt geen informatie getoond die herleidbaar is tot de authenticatiegegevens.
11.5.1.3	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.
11.5.1.4	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.
11.5.1.5	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.
11.5.2.1	Gebruikersidentificatie en -authenticatie	Bij uitgifte van authenticatiemiddelen wordt minimaal de identiteit vastgesteld, evenals het feit dat de gebruiker recht heeft op het authenticatiemiddel.
11.5.3.1	Systemen voor wachtwoordbeheer	Er wordt automatisch gecontroleerd op goed gebruik van wachtwoorden (onder andere voldoende sterke wachtwoorden, regelmatige wijziging, directe wijziging van initieel wachtwoord).
11.5.5.1	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.
11.5.6.1	Beperking van verbindingstijd	De toegang voor onderhoud op afstand door een leverancier wordt alleen opengesteld op basis van een wijzigingsverzoek

BIG Nummer	titel	Maatregel verwerker
		of storingsmelding, met 2-factor authenticatie en tunneling.
11.6.1.1	Beperking van toegang tot informatie	In de soort toegangsregels wordt ten minste onderscheid gemaakt tussen lees- en schrijfbevoegdheden.
11.6.1.2	Beperking van toegang tot informatie	Managementsoftware heeft de mogelijkheid gebruikerssessies af te sluiten.
11.6.1.3	Beperking van toegang tot informatie	Bij extern gebruik vanuit een niet vertrouwde omgeving vindt sterke authenticatie (two-factor) van gebruikers plaats.
12.1.1.1	Analyse en specificatie van beveiligingseisen	In projecten ten behoeve van systemen voor de verwerkingsverantwoordelijke wordt een beveiligingsrisicoanalyse en maatregelbepaling opgenomen als onderdeel van het ontwerp. Ook bij wijzigingen worden de veiligheidsconsequenties meegenomen.
12.2.1.1	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.
12.2.2.1	Beheersing van interne gegevensverwerking	Er bestaan voldoende mogelijkheden om reeds ingevoerde gegevens te kunnen corrigeren door er gegevens aan te kunnen toevoegen.
12.2.3.1	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.
12.2.4.1	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).
12.3.1.1	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.
12.3.2.1	Sleutelbeheer	In het sleutelbeheer is minimaal aandacht besteed aan het proces, de actoren en hun verantwoordelijkheden.
12.4.1.1	Beheersing van operationele software	Alleen geautoriseerd personeel kan functies en software installeren of activeren.
12.5.1.1	Procedures voor wijzigingsbeheer	Er is aantoonbaar wijzigingsmanagement ingericht volgens gangbare best practices, zoals ITIL en voor applicaties ASL.
12.5.2.1	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 verwerkingsverantwoordelijke te niet doen.
12.5.4.1	Uitlekken van informatie	Op het grensvlak van een vertrouwde en een niet vertrouwde omgeving vindt content-scanning plaats.
12.5.4.2	Uitlekken van informatie	Er dient een proces te zijn om aan de verwerkingsverantwoordelijke te melden dat (persoons) informatie is uitgelekt. (zie 13.1.1)

BIG Nummer	titel	Maatregel verwerker
12.6.1.1	Beheersing van technische kwetsbaarheden	Er is een proces ingericht voor het beheer van technische kwetsbaarheden. Dit omvat minimaal het melden van incidenten aan de verwerkingsverantwoordelijke, het uitvoeren van periodieke penetratietests, het uitvoeren van risicoanalyses van kwetsbaarheden en patching van systemen en hardware.
13.1.1.1	Rapportage van informatiebeveiligingsgebeurtenissen	Er is een procedure voor het rapporteren van beveiligingsgebeurtenissen aan de verwerkingsverantwoordelijke 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.
13.1.1.4	Rapportage van informatiebeveiligingsgebeurtenissen	Alle beveiligingsincidenten worden vastgelegd in een systeem en geëscaleerd aan de verwerkingsverantwoordelijke.
13.1.1.5	Rapportage van informatiebeveiligingsgebeurtenissen	Vermissing of diefstal van apparatuur of media die gegevens van de verwerkingsverantwoordelijke kunnen bevatten wordt altijd ook aangemerkt als informatiebeveiligingsincident.
13.2.3.1	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.
15.1.3.1	Bescherming van bedrijfsdocumenten	De registraties van de verwerkingsverantwoordelijke behoren te worden beschermd tegen verlies, vernietiging en vervalsing, in overeenstemming met wettelijke en regelgevende eisen, contractuele verplichtingen en bedrijfsmatige eisen.
15.1.4.1	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.
15.1.6.1	Voorschriften voor het gebruik van cryptografische beheersmaatregelen	Er is vastgesteld aan welke overeenkomsten, wetten en voorschriften de toepassing van cryptografische technieken moet voldoen. Zie ook 12.3.
15.2.1.1	Naleving van beveiligingsbeleid en -normen	De verwerker 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 verwerker voor het toezicht op de uitvoering van het beveiligingsbeleid ten behoeve van de gegevens van de verwerkingsverantwoordelijke. Daarbij behoren ook periodieke beveiligingsaudits. Deze kunnen worden uitgevoerd door, of vanwege de verwerkingsverantwoordelijke.
15.2.2.1	Controle op technische naleving	Informatiesystemen van de verwerker ten behoeve van de verwerkingsverantwoordelijke worden regelmatig gecontroleerd op naleving van beveiligingsnormen. Dit kan door bijvoorbeeld kwetsbaarheidsanalyses en penetratietesten.