Verwerkersovereenkomst
voor […omschrijving]

gemeente Krimpen aan den IJssel – […naam Verwerker]

Inhoudsopgave

DE ONDERGETEKENDEN:

1. De gemeente Krimpen aan den IJssel, hierna te noemen: “Verwerkingsverantwoordelijke”, gevestigd te Raadhuisplein 2, 2922 AD Krimpen aan den IJssel, te dezen, krachtens het besluit van de burgemeester van [….datum], rechtsgeldig vertegenwoordigd door het hoofd van de afdeling [….naam afdeling], […. De heer/mevrouw] [….. voorletters + naam],

en

2. [...naam], hierna te noemen: “Verwerker”, statutair gevestigd te [...adres], ingeschreven in het handelsregister onder dossiernummer KvK […], te dezen rechtsgeldig vertegenwoordigd door [...functie], [...de heer/mevrouw] […voorletters + naam]

Hierna gezamenlijk te noemen: Partijen.

OVERWEGENDE DAT:

- Verwerkingsverantwoordelijke met Verwerker op [datum] de overeenkomst [NAAM overeenkomst] met betrekking tot […. Korte omschrijving opdracht] heeft gesloten, hierna te noemen “de Hoofdovereenkomst”;

- Verwerker in het kader van de uitvoering van de Hoofdovereenkomst persoonsgegevens, in de zin van artikel 4, onder a, van de Algemene verordening gegevensbescherming (AVG) verwerkt die afkomstig zijn van Verwerkingsverantwoordelijke of waarvoor Verwerkingsverantwoordelijke verantwoordelijk is;

- Het bepaalde in de voorgaande bullet laat onverlet dat opdrachtnemer (voor de uitvoering van de Hoofdovereenkomst) in het kader van de dienstverlening dossiers met daarin nadere gegevens van betrokkene(n) opbouwt. De opdrachtnemer (voor de uitvoering van de Hoofdovereenkomst) voor die gegevens is aan te merken als verwerkingsverantwoordelijke in de zin van de wet. De opdrachtnemer (voor de uitvoering van de Hoofdovereenkomst) garandeert dat de verwerking van persoonsgegevens op een rechtmatige wijze en in overeenstemming met de wet-, en regelgeving geschiedt.

- In de Hoofdovereenkomst is overeengekomen dat Verwerker de persoonsgegevens verwerkt in overeenstemming met het doel van de Hoofdovereenkomst behoudens afwijkende wettelijke verplichtingen;

- In de Hoofdovereenkomst is overeengekomen dat Verwerker zorg draagt voor de naleving van de voorwaarden die, met name op grond van de Wet bescherming persoonsgegevens (Wbp) en de wet- en regelgeving die deze wet per 25 mei 2018 zal vervangen; de Algemene verordening gegevensbescherming (AVG) en de bijbehorende Uitvoeringswet en de Wet basisregistratie personen, worden gesteld aan het verwerken van persoonsgegevens en een passend beveiligingsniveau;

- Partijen zijn overeengekomen dat ter uitwerking van het bepaalde in de Hoofdovereenkomst een aanvullende overeenkomst gesloten kan worden ter uitwerking van de bepalingen met betrekking tot het verwerken van persoonsgegevens en de beveiliging ervan;

- Het college van Burgemeester en Wethouders van de gemeente Krimpen aan den IJssel en/of de Burgemeester Verwerkingsverantwoordelijke is of zijn voor de verwerking van persoonsgegevens;

- De afdeling [NAAM afdeling] van de gemeente Krimpen aan den IJssel namens Verwerkingsverantwoordelijke belast is met het beheer van de bij Verwerker verwerkte persoonsgegevens voor zover die betrekking hebben op de gemeente Krimpen aan den IJssel;

- Partijen ter voldoening aan de AVG (in aanvulling op de Hoofdovereenkomst beschreven afspraken) in deze Verwerkersovereenkomst afspraken over het verwerken van de persoonsgegevens door Verwerker wensen vast te leggen;

- Partijen overeenkomen om bij het verwerken van deze persoonsgegevens de hierna volgende bepalingen in acht te nemen:

KOMEN OVEREEN:

ARTIKEL 1. DEFINITIES

1.1 Autoriteit Persoonsgegevens: de Autoriteit als bedoeld in artikel 51 van de AVG;

1.2 Bestand: elk gestructureerd geheel van persoonsgegevens, die volgens bepaalde criteria toegankelijk zijn, ongeacht of dit geheel gecentraliseerd of gedecentraliseerd is dan wel op functionele of geografische gronden is verspreid;

1.3 Betrokkene: de geïdentificeerde of identificeerbare natuurlijke persoon op wie een persoonsgegeven betrekking heeft;

1.4 Verwerker: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van Verwerkingsverantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen;

1.5 Bijlagen: aanhangsels bij deze Verwerkersovereenkomst, die onlosmakelijk deel uitmaken van deze Verwerkersovereenkomst.

1.6 Datalek: een inbreuk in verband met persoonsgegevens, zoals bedoeld in artikel 4 onder 12 van de AVG. Een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens;

1.7 Derde: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, niet zijnde de betrokkene, noch Verwerkingsverantwoordelijke, noch Verwerker, noch de persoon die onder rechtstreeks gezag van Verwerkingsverantwoordelijke of Verwerker gemachtigd zijn om de persoonsgegevens te verwerken.

1.8 Hoofdovereenkomst: de overeenkomst, waarin afspraken over de door Verwerker als opdrachtnemer te verrichten dienstverlening zijn gemaakt.

1.9 Normen en standaarden: de door Verwerkingsverantwoordelijke vastgestelde normen en standaarden ter zake van methoden, technieken, procedures, projecten, productiekenmerken en documentatievoorschriften welke bij de uitvoering van de werkzaamheden door Verwerker zullen worden gevolgd als vastgelegd in de Hoofdovereenkomst of in een bijlage bij deze Verwerkersovereenkomst.

1.10 Ontvanger: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, al dan niet een derde, aan wie/waaraan de persoonsgegevens worden verstrekt.

1.11 Persoonsgegeven: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon; 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;

1.12 TPM: third party mededeling: een verklaring die afgegeven wordt door een onafhankelijke auditpartij over de kwaliteit van de ICT dienstverlening en beheersing van de organisatie.

1.13 Verwerkingsverantwoordelijke: de natuurlijke persoon, rechtspersoon of het bestuursorgaan dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.

1.14 verwerking: een bewerking of een geheel van bewerkingen met betrekking tot 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, verspreiding, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens;

1.15 de Wet: de Wet bescherming persoonsgegevens (Wbp) en de wet- en regelgeving die deze wet per 25 mei 2018 zal vervangen; de Algemene verordening gegevensbescherming (AVG) en de bijbehorende Uitvoeringswet.

ARTIKEL 2. ONDERWERP EN DUUR VAN DEZE VERWERKERSOVEREENKOMST

2.1 De hierboven opgenomen Overwegingen maken integraal onderdeel uit van deze overeenkomst.

2.2 Deze Verwerkersovereenkomst vormt een onderdeel van de Hoofdovereenkomst. Ingevolge de Hoofdovereenkomst verricht Verwerker de navolgende dienstverlening: "XXXXXXXXXXXX" conform de in de Hoofdovereenkomst geformuleerde voorwaarden.

2.3 Deze Verwerkersovereenkomst heeft als doel dat Partijen voldoen aan hun wettelijke verplichtingen die voortvloeien uit de AVG, waaronder i) de verplichting van Verwerkingsverantwoordelijke om ervoor zorg te dragen dat Verwerker voldoende waarborgen biedt ten aanzien van de technische- en organisatorische beveiligingsmaatregelen en ii) de verplichting van Verwerkingsverantwoordelijke om te voldoen aan de verplichtingen die in het kader van de wet meldplicht datalekken zijn opgenomen in de AVG.

2.4 Deze Verwerkersovereenkomst is een onlosmakelijk onderdeel van de Hoofdovereenkomst en gaat in op het moment van ondertekening en duurt voort zolang Verwerker de beschikking heeft over persoonsgegevens of zeggenschap heeft over de wijze van door derden (subverwerker) verwerken van persoonsgegevens van Verwerkingsverantwoordelijke. Pas nadat Verwerker naar het oordeel van Verwerkingsverantwoordelijke genoegzaam heeft aangetoond dat hij heeft voldaan aan de verplichtingen als omschreven in artikel 3.10 van deze Verwerkersovereenkomst (vernietigen/ overdragen van persoonsgegevens aan Verwerkingsverantwoordelijke), eindigt deze Verwerkersovereenkomst.

2.5 Verplichtingen die naar hun aard bestemd zijn om ook na de beëindiging van deze Verwerkersovereenkomst voort te duren, blijven gelden. Tot deze verplichtingen behoren onder meer de bepalingen betreffende geheimhouding, aansprakelijkheid en boete en toepasselijk recht.

2.6 In het geval van tegenstrijdigheid tussen de bepalingen uit deze Verwerkersovereenkomst en de bepalingen van de Hoofdovereenkomst, dan zullen de bepalingen van deze Verwerkersovereenkomst leidend zijn.

2.7 De navolgende Bijlagen maken onlosmakelijk deel uit van deze Verwerkersovereenkomst:

Bijlage I	Omschrijving van te verwerken persoonsgegevens (dataset) en de te verrichten handelingen vanaf de start van de verwerking tot aan de vernietiging.
Bijlage II	De door Verwerker te implementeren technische beveiligingsnormen en standaards van Verwerkingsverantwoordelijke en de te nemen organisatorische beveiligingsmaatregelen.
Bijlage III	meldingsformulier beveiligingsincident/ datalek door Verwerker.
Bijlage IV	Lijst van subverwerkers (indien van toepassing)

ARTIKEL 3. VERPLICHTINGEN VERWERKER

3.1 Verwerker verbindt zich om alle persoonsgegevens die hij in het kader van de te verzorgen dienstverlening voor Verwerkingsverantwoordelijke verwerkt, zoals nader omschreven in Bijlage I, behoorlijk en zorgvuldig te verwerken. Het is Verwerker niet toegestaan om andere dan de in Bijlage I omschreven handelingen met de persoonsgegevens uit te voeren. Verwerker is verplicht om een register van verwerkingsactiviteiten als bedoeld in artikel 30, tweede lid, van de AVG bij te houden.

3.2 Verwerker verbindt zich om alle technische en organisatorische beveiligingsmaatregelen te nemen die Verwerkingsverantwoordelijke van een professioneel verwerker van persoonsgegevens mag verwachten, waaronder de maatregelen zoals omschreven in bijlage II. In bijlage II is tevens omschreven welke (groepen) van medewerkers van Verwerker toegang kunnen hebben tot welke persoonsgegevens en welke handelingen zij met de persoonsgegevens mogen en kunnen uitvoeren.

3.3 Verwerker verwerkt de persoonsgegevens slechts in opdracht en ten behoeve van Verwerkingsverantwoordelijke. De verwerking geschiedt in overeenstemming met de instructies en aanwijzingen van Verwerkingsverantwoordelijke en in overeenstemming met de toepasselijke wet- en regelgeving.

3.4 Verwerker heeft geen zeggenschap over de ter beschikking gestelde persoonsgegevens. Zo neemt hij geen beslissingen over ontvangst en gebruik van de gegevens, de verstrekking aan Derden en de duur van de opslag van gegevens. De zeggenschap over de persoonsgegevens verstrekt of hem ter beschikking gekomen onder de Hoofdovereenkomst en/of deze Verwerkersovereenkomst komt nimmer bij Verwerker te berusten.

3.5 Verwerker zal de persoonsgegevens, in een vorm die het mogelijk maakt de betrokkene te identificeren, niet langer bewaren dan strikt noodzakelijk in het kader van de uitvoering van de Hoofdovereenkomst.

Meldplicht datalekken en beveiligingsincidenten

3.6 Verwerker stelt Verwerkingsverantwoordelijke onmiddellijk – uiterlijk binnen twee uur - na het ontdekken van een mogelijke beveiligingsinbreuk of datalek op de hoogte door het sturen van een e-mail aan ciso@ijsselgemeenten.nl. Aan de e-mail zal Verwerker een volledig ingevulde Bijlage III toevoegen.

3.7 Verwerker zal het doen van meldingen aan de Autoriteit Persoonsgegevens overlaten aan Verwerkingsverantwoordelijke. Het is Verwerker niet toegestaan om namens Verwerkingsverantwoordelijke een melding bij de Autoriteit Persoonsgegevens te doen van een inbreuk op de beveiliging van de persoonsgegevens.

3.8 Verwerker stelt Verwerkingsverantwoordelijke in staat om binnen de wettelijke termijnen aan de wettelijke verplichtingen op grond van de AVG en in het bijzonder de verplichtingen inzake de melding van datalekken bij de Autoriteit Persoonsgegevens (artikel 33 AVG) te voldoen. Meer specifiek rusten op Verwerker ingeval van een mogelijk datalek de navolgende verplichtingen:

a. Verwerker overlegt alle benodigde gegevens voor de beoordeling van het datalek aan Verwerkingsverantwoordelijke;

b. Verwerker zal, in goed overleg met Verwerkingsverantwoordelijke, voor eigen rekening en risico alle noodzakelijke maatregelen nemen om de inbreuk te beëindigen en de schade die hieruit voortvloeit of kan vloeien te beperken;

c. Verwerker houdt Verwerkingsverantwoordelijke op de hoogte van de voortgang van het intern onderzoek, de ontwikkelingen rond het beveiligingsincident en de genomen of te nemen maatregelen;

d. Verwerker verleent de volledige medewerking indien Verwerkingsverantwoordelijke zelf onderzoek naar het datalek wenst uit te voeren;

e. Verwerker stelt Verwerkingsverantwoordelijke op de hoogte van de maatregelen die hij treft om de gevolgen van het incident te beperken en om een herhaling te voorkomen;

f. Verwerker verleent alle medewerking zodat Verwerkingsverantwoordelijke in staat is om betrokkene(n) in kennis te stellen;

g. Verwerker volgt de instructies van Verwerkingsverantwoordelijke op;

h. Verwerker voldoet aan de bindende aanwijzing van Autoriteit Persoonsgegevens, ook indien deze aan Verwerkingsverantwoordelijke wordt gegeven.

3.9 Verwerker beschikt over een gedegen plan van aanpak betreffende de omgang met en afhandeling van inbreuken en zal verwerkingsverantwoordelijke, op diens verzoek, inzage verschaffen in het plan. Verwerker stelt Verwerkingsverantwoordelijke op de hoogte van de materiele wijzigingen in het plan van aanpak.

3.10 Verwerker houdt een gedetailleerd logboek bij van alle (vermoedens van) inbreuken op de beveiliging, evenals de maatregelen die in vervolg op dergelijke inbreuken zijn genomen waarin minimaal de informatie als bedoeld in Bijlage III is opgenomen, en geeft daar op eerste verzoek van Verwerkingsverantwoordelijke inzage in.

<u>Gegevens ter beschikking stellen aan Verwerkingsverantwoordelijke</u>

3.11 Verwerker stelt op eerste schriftelijk verzoek van Verwerkingsverantwoordelijke aan hem onmiddellijk alle persoonsgegevens ter hand die in het kader van deze Verwerkersovereenkomst worden verwerkt. Hieronder worden mede begrepen kopieën en bewerkingen van persoonsgegevens. Een dergelijk verzoek kan door Verwerkingsverantwoordelijke worden gedaan gedurende de looptijd van de Verwerkersovereenkomst en op het moment dat de Hoofovereenkomst wordt beëindigd. Verwerkingsverantwoordelijke kan zo nodig eisen stellen aan de wijze van beschikbaarstelling van de persoonsgegevens, waaronder begrepen de eisen aan het bestandsformaat.

3.12 Verwerker zal te allen tijde de hiervoor beschreven dataportabiliteit waarborgen, zodanig dat er geen sprake is van verlies van functionaliteit of gedeelten van de gegevens. De uitvoering van de opdracht vindt verder op een zodanige wijze plaats dat de continuïteit van de dienstverlening maximaal gewaarborgd blijft, althans niet door handelen of nalaten van Verwerker wordt belemmerd. Verwerker is gehouden de na overdracht achtergebleven kopieën te vernietigen.

3.13 Het is Verwerker niet toegestaan persoonsgegevens aan anderen dan Verwerkingsverantwoordelijke te verstrekken, tenzij dit geschiedt op schriftelijk verzoek van Verwerkingsverantwoordelijke of met diens schriftelijke toestemming. Verwerker is verplicht schriftelijk te bevestigen dat een verstrekking heeft plaatsgevonden, waarbij hij exact de

verstrekte persoonsgegevens, de betrokkene, de Ontvanger en het moment van verstrekking dient te beschrijven.

3.14 Verwerker verbindt zich alle voor Verwerkingsverantwoordelijke verwerkte persoonsgegevens, waaronder kopieën en bewerkingen daarvan, alsmede alle gegevensdragers waarop deze zijn vastgelegd, op een door Verwerkingsverantwoordelijke nader te bepalen wijze over te dragen aan Verwerkingsverantwoordelijke en/of een opvolgende Verwerker binnen de door Verwerkingsverantwoordelijke aangegeven periode na het moment van beëindigen van de Hoofdovereenkomst of per een eerder moment wanneer Verwerkingsverantwoordelijke daar uitdrukkelijk om verzoekt. De overdracht vindt op een zodanige wijze plaats dat de continuïteit van de dienstverlening maximaal gewaarborgd blijft, althans niet door handelen of nalaten van Verwerker wordt belemmerd. Verwerker is gehouden alle na overdracht achtergebleven kopieën te vernietigen.

3.15 Indien Verwerkingsverantwoordelijke te kennen heeft gegeven dat er geen overdracht van de gegevens zal plaats hebben en/of gegevens niet langer noodzakelijk zijn voor de verwerkelijking van de doeleinden waarvoor zij worden verzameld of verwerkt en zullen zij door Verwerker worden vernietigd.

2 maanden voor de datum van vernietiging zal Verwerker een signaal geven aan Verwerkingsverantwoordelijke, dat de gegevens over 2 maanden worden vernietigd, Verwerkingsverantwoordelijke kan alsdan om haar moverende redenen besluiten dat een langere bewaartermijn noodzakelijk is.

Van de overdracht en/of vernietiging wordt door Verwerker een verslag gemaakt. Verwerkingsverantwoordelijke kan van de vernietiging een bewijs verlangen. De kosten van overdracht en/of vernietiging komen voor rekening van **< Verwerkingsverantwoordelijke /Verwerker >**

ARTIKEL 4 RECHTEN VAN BETROKKENEN

4.1 Verwerker informeert betrokkene voldoende over de wijze waarop persoonsgegevens worden verwerkt.

4.2 Verwerker stelt Verwerkingsverantwoordelijke te allen tijde in staat om binnen de wettelijke termijnen te voldoen aan de verplichtingen op grond van de AVG en meer in het bijzonder de rechten van betrokkenen, zoals, maar niet beperkt tot een verzoek om inzage, rectificatie, wissing, beperking, afscherming van persoonsgegevens.

4.3 In het geval dat een Betrokkene een verzoek tot inzage, zoals bedoeld in artikel 15 AVG, of rectificatie, wissing, beperking, afscherming, zoals bedoeld in hoofdstuk 3, afdeling 3 van de AVG , richt aan Verwerker, zal Verwerker het verzoek zelf afhandelen en Verwerkingsverantwoordelijke hierover direct informeren.

4.4 In het geval dat een Betrokkene een verzoek tot inzage, zoals bedoeld in artikel 15 AVG, of rectificatie, wissing, beperking, afscherming, zoals bedoeld in hoofdstuk 3, afdeling 3, richt aan Verwerkingsverantwoordelijke zal Verwerker daartoe op eerste verzoek van Verwerkingsverantwoordelijke zo spoedig mogelijk, doch uiterlijk binnen zeven werkdagen nadat het verzoek is gedaan aan Verwerkingsverantwoordelijke schriftelijk alle informatie verstrekken die Verwerkingsverantwoordelijke nodig mocht hebben om te kunnen voldoen aan de in artikel 14 van de AVG vervatte mededelingsplicht.

4.5 Verwerker zal op eerste verzoek van Verwerkingsverantwoordelijke persoonsgegevens rectificeren, wissen of overgaan tot een beperking van de verwerking. Verwerker zal aan dit verzoek voldoen binnen zodanige termijn dat Verwerkingsverantwoordelijke niet in overtreding is van het bepaalde in hoofdstuk 3, afdeling 3 en/of afdeling 4 van de AVG, doch in elk geval binnen vijf werkdagen nadat het verzoek door Verwerkingsverantwoordelijke is gedaan.

ARTIKEL 5. GEHEIMHOUDINGSPLICHT

5.1 Verwerker draagt er zorg voor dat alleen die Personen toegang tot de persoonsgegevens hebben die daartoe gezien hun functie bevoegd toe zouden moeten zijn.

5.2 Personen in dienst van, dan wel werkzaam ten behoeve van Verwerker, evenals Verwerker zelf, zijn verplicht tot geheimhouding met betrekking tot de persoonsgegevens waarvan zij kennis hebben kunnen nemen, tenzij een wettelijk voorschrift tot verstrekking verplicht. De medewerkers van Verwerker en van eventuele subverwerkers die door Verwerker worden ingeschakeld - die uit de aard van hun functie over de persoonsgegevens kunnen beschikken - tekenen hiertoe een geheimhoudingsverklaring.

5.3 Indien Verwerker op grond van een in Nederland en/of in de EU geldende wettelijke verplichting gegevens aan enige Derde dient te verstrekken, zal Verwerker de grondslag van het verzoek en de identiteit van de verzoeker verifiëren en zal Verwerker Verwerkingsverantwoordelijke onmiddellijk, voorafgaand aan de verstrekking, ter zake informeren, tenzij de relevante wettelijke bepalingen dit verbieden.

5.4 Verwerker is gehouden de persoonsgegevens te verwerken in landen binnen de Europese Unie (EU). Verwerker zal de gemeente desgevraagd op de hoogte stellen in welk land de gegevens worden bewerkt. Het is Verwerker niet toegestaan om persoonsgegevens, voor verwerking of anderszins waaronder opslag, uit te voeren naar landen buiten de EU of deze ter hand te stellen aan een vreemde mogendheid.

ARTIKEL 6. BEVEILIGINGSMAATREGELEN

6.1 Verwerker neemt alle passende technische en organisatorische beveiligingsmaatregelen om de persoonsgegevens die voor Verwerkingsverantwoordelijke worden verwerkt te beveiligen en beveiligd te houden tegen verlies of tegen enige vorm van onrechtmatig, onzorgvuldig, ondeskundig of ongeoorloofde verwerking. Voor “passende technische en organisatorische maatregen” en “een passend beveiligingsniveau” handelt Verwerker minimaal conform het richtsnoer “beveiliging van de persoonsgegevens” van de Autoriteit Persoonsgegevens en de Baseline Informatievoorziening Gemeenten (of de meest recente richtsnoeren indien de regelgeving hieromtrent wijzigt). Verwerker is voorts gehouden tot naleving van de beveiligingsnormen en standaarden van Verwerkingsverantwoordelijke, zoals beschreven in Bijlage II. Verwerker neemt steeds alle maatregelen die Verwerkingsverantwoordelijke van een professioneel handelend Verwerker van persoonsgegevens mag verwachten en zal de benodigde maatregelen treffen naar aanleiding van de plan-do-check-act-cyclus.

6.2 Verwerker rapporteert jaarlijks, voor het eerst op de datum één jaar na ingang van deze overeenkomst, aan Verwerkingsverantwoordelijke over de opzet en werking van het stelsel van maatregelen, procedures en incidenten, gericht op naleving van het bepaalde in deze Verwerkersovereenkomst. Deze rapportage betreft ook, indien van toepassing, de werkzaamheden van door hem ingeschakelde derden/subverwerkers.

6.3 Jaarlijks, voor het eerst op de datum één jaar na ingang van deze overeenkomst, dient Verwerker door middel van een interne- en externe pen- en hacktest, uitgevoerd door een daarin gespecialiseerde derde, aan te tonen dat de applicatie en de infrastructuur waarmee persoonsgegevens worden bewerkt voldoet aan de in deze Verwerkersovereenkomst gespecificeerde criteria. De resultaten van deze test dienen te worden overgelegd aan Verwerkingsverantwoordelijke. De kosten van de pen-en hacktest en de eventuele her-test worden door Verwerker gedragen.

6.4 Naast de jaarlijkse test zal Verwerker eveneens zijn volledige medewerking verlenen aan extra pen-en hacktesten indien Verwerkingsverantwoordelijke deze wenst te laten uitvoeren door een door hem geselecteerde partij, teneinde te bezien of de applicatie en de infrastructuur waarmee de persoonsgegevens worden bewerkt voldoet aan de in deze Verwerkersovereenkomst nader gespecificeerde criteria. De kosten van een pen- en hacktest en de eventuele her-test worden door Verwerkingsverantwoordelijke gedragen. De datum van uitvoering zal in onderling overleg tussen Verwerkingsverantwoordelijke en Verwerker worden bepaald.

6.5 Verwerker voert de uitkomsten van de pen- en hacktest en de naar aanleiding daarvan aangegeven aanbevelingen binnen de daartoe door Verwerkingsverantwoordelijke te bepalen termijn uit.

6.6 Verwerkingsverantwoordelijke is te allen tijde gerechtigd de verwerking van persoonsgegevens te doen controleren door middel van een audit. Verwerker is verplicht Verwerkingsverantwoordelijke of de - in opdracht van Verwerkingsverantwoordelijke- controlerende instantie toe te laten en alle medewerking te verlenen zodat de controle daadwerkelijk uitgevoerd kan worden. De met de audit gemoeide kosten zijn voor rekening van **<Verwerkingsverantwoordelijke/Verwerker>**. Verwerkingsverantwoordelijke zal de audit slechts (laten) uitvoeren na een voorafgaande schriftelijke melding aan Verwerker.

6.7 Verwerker verbindt zich om binnen een door Verwerkingsverantwoordelijke te bepalen termijn Verwerkingsverantwoordelijke, of de door Verwerkingsverantwoordelijke ingeschakelde derde, te voorzien van de verlangde informatie ten behoeve van de audit. Hierdoor kan Verwerkingsverantwoordelijke, of de door Verwerkingsverantwoordelijke

ingeschakelde derde, zich een oordeel vormen over de naleving door Verwerker van de Hoofdovereenkomst en/of deze Verwerkersovereenkomst.

6.8 Verwerker voert de aanbevelingen die voortvloeien uit een audit binnen de daartoe door Verwerkingsverantwoordelijke te bepalen redelijke termijn uit.

6.9 Verwerker zal na een verzoek daartoe door Verwerkingsverantwoordelijke kosteloos een TPM c.q. een verklaring van een onafhankelijke externe deskundige aan Verwerkingsverantwoordelijke verstrekken over de naleving van de overeengekomen technische en organisatorische beveiligingsmaatregelen.

6.10 Verwerkingsverantwoordelijke behoudt zich het recht voor om de Informatie-beveiligingsdienst voor Gemeenten danwel een andere Derde in te schakelen voor ondersteuning en advisering met betrekking tot in het kader van audits en/of in pen-en hacktest aangetroffen bevindingen. Verwerker stemt hiermee in.

ARTIKEL 7. INSCHAKELING DERDEN/SUBVERWERKERS

7.1 Verwerker is slechts gerechtigd de verwerking van persoonsgegevens geheel of ten dele uit te besteden aan derden (subverwerkers) na voorafgaande schriftelijke toestemming van Verwerkingsverantwoordelijke.

7.2 Verwerkingsverantwoordelijke kan aan de toestemming voorwaarden verbinden die dienen ter naleving van de verplichtingen uit deze Verwerkersovereenkomst. Verwerker dient in ieder geval contractueel verzekerd te hebben dat de derde (subverwerker) dezelfde verplichtingen als opgenomen in deze overeenkomst worden opgelegd. Dit betekent in ieder geval dat de derde (subverwerker) zich eveneens richt naar de instructies en aanwijzingen van Verwerkingsverantwoordelijke, tot geheimhouding is gehouden en de vereiste beveiligingsmaatregelen aangaande de gegevensverwerking en ICT-infrastructuur neemt. Verwerkingsverantwoordelijke dient in staat te worden gesteld toe te zien op de naleving van de afspraken van de derde (subverwerker) met Verwerker. Verwerker zal Verwerkingsverantwoordelijke op eerste verzoek inzage verschaffen in de overeenkomst(en) met derden, waarin deze verplichtingen zijn opgenomen.

7.3 Verwerker blijft te allen tijde aanspreekpunt en direct aansprakelijk en verantwoordelijk voor de naleving van de bepalingen uit de Hoofdovereenkomst en deze Verwerkersovereenkomst.

7.4 Verwerker houdt een actueel register bij van de door hem ingeschakelde subverwerkers waarin de identiteit, vestigingsplaats en een beschrijving van de werkzaamheden van deze derden/subverwerkers zijn opgenomen, alsmede eventuele door verwerkingsverantwoordelijke gestelde aanvullende voorwaarden. Dit register zal als Bijlage IV aan deze Verwerkersovereenkomst worden toegevoegd.

ARTIKEL 8. WIJZIGING VERWERKERSOVEREENKOMST

8.1 Indien zich naar het oordeel van één der Partijen gedurende de looptijd van de verwerkersovereenkomst wijzigingen in wet of regelgeving voordoen die van dien aard zijn dat de andere Partij naar maatstaven van redelijkheid en billijkheid ongewijzigde instandhouding van de Overeenkomst niet mag verwachten, zullen Partijen in overleg treden over de aanpassing van de Overeenkomst.

8.2 Aanvullingen op, dan wel wijzigingen van, deze Overeenkomst zijn voor de Partijen slechts bindend indien deze schriftelijk zijn bevestigd en vastgelegd in de vorm van een bijlage bij de Overeenkomst.

ARTIKEL 9. AANSPRAKELIJKHEID EN BOETEBEPALING

9.1 Indien Verwerker tekortschiet in de nakoming van de verplichtingen uit deze Verwerkersovereenkomst kan Verwerkingsverantwoordelijke hem in gebreke stellen. Ingebrekestelling geschiedt schriftelijk, waarbij aan Verwerker 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. Verwerker is echter onmiddellijk in gebreke als de nakoming van desbetreffende verplichting anders dan door overmacht, zoals gedefinieerd in de Hoofdovereenkomst, reeds blijvend onmogelijk is.

9.2 Verwerker is aansprakelijk voor alle schade of nadeel voortvloeiende uit het niet-nakomen van, of in strijd handelen met de bij of krachtens de AVG gegeven voorschriften en/of het niet-nakomen van, of in strijd handelen met het in deze Verwerkersovereenkomst bepaalde, onverminderd de aanspraken op grond van wettelijke regels. Verwerker is aansprakelijk voor schade of nadeel voor zover ontstaan door zijn werkzaamheid, daaronder begrepen ontstane inbreuken op de persoonlijke levenssfeer van betrokkenen. De aansprakelijkheid van Verwerker is, tenzij er sprak eis van opzet of grove schuld, beperkt tot het in de Hoofdovereenkomst overeengekomen bedrag.

9.3 Indien Verwerker enige van deze Verwerkersovereenkomst neergelegde verplichting niet of niet-tijdig nakomt en de Autoriteit Persoonsgegevens Verwerkingsverantwoordelijke dientengevolge een bestuurlijke boete oplegt, acht Verwerkingsverantwoordelijke Verwerker verantwoordelijk en zal Verwerkingsverantwoordelijke een contractuele boete ter hoogte van hetzelfde bedrag opleggen aan Verwerker. Deze boete is zonder rechterlijke tussenkomst, ingebrekestelling of aanmaning direct opeisbaar. Deze boete is niet vatbaar voor verrekening. Oplegging van deze boete laat alle andere rechten of vorderingen van Verwerkingsverantwoordelijke (inclusief o.a. het recht op nakoming, schadevergoeding) onverlet.

9.4 Indien Verwerker enige in artikel 5 (Geheimhoudingsplicht) en artikel 7 (inschakeling derden/subverwerkers) van deze Verwerkersovereenkomst genoemde verplichting niet of niet-tijdig nakomt, is Verwerker een boete verschuldigd van € 25.000,- per gebeurtenis. De boete is zonder rechterlijke tussenkomst, ingebrekestelling of aanmaning direct opeisbaar. De boete is niet vatbaar voor verrekening. De boete laat alle andere rechten of vorderingen, waaronder, doch niet uitsluitend, de vordering van Verwerkingsverantwoordelijke tot nakoming, een schriftelijke verklaring om zonder rechterlijke tussenkomst de overeenkomst eenzijdig geheel of gedeeltelijk te ontbinden en het recht op schadevergoeding onverlet.

ARTIKEL 10. TOEPASSELIJK RECHT

10.1 Op deze Verwerkersovereenkomst en op alle geschillen die eruit voortvloeien of ermee samenhangen is Nederlands recht van toepassing.

10.2 Partijen zullen trachten geschillen die ontstaan met betrekking tot de totstandkoming, inhoud dan wel uitvoering van deze Verwerkersovereenkomst eerst minnelijk op te lossen. Indien het geschil niet minnelijk wordt opgelost zal het bij uitsluiting worden voorgelegd aan de daartoe bevoegde rechter in het arrondissement Rotterdam.

Aldus in tweevoud opgemaakt en ondertekend te Krimpen aan den IJssel op [...datum].

Verwerker, **[...naam]**	Verwerkingsverantwoordelijke, **de gemeente**,
[...naam]	[...naam]

Bijlagen

I Omschrijving van te verwerken persoonsgegevens (dataset) en de te verrichten handelingen (van start tot vernietiging).

II De technische beveiligingsnormen en standaards van Verwerkingsverantwoordelijke, en de te nemen organisatorische beveiligingsmaatregelen, welke (groepen) van medewerkers van Verwerker hebben toegang tot welke persoonsgegevens en welke handelingen mogen deze medewerkers met de persoonsgegevens uitvoeren.

III Meldingsformulier beveiligingsincident/datalek door Verwerker.

IV Lijst van subverwerkers (indien van toepassing).

BIJLAGE I

TE VERWERKEN PERSOONSGEGEVENS EN DE TE VERRICHTEN HANDELINGEN

1. De specifieke diensten

Verwerker zal [omschrijf de dienstverlening XXXXXXXX] voor de gemeente Krimpen aan den IJssel verrichten.

2. Categorieën en soorten persoonsgegevens. (Graag aankruisen wat van toepassing is.)

	ja	nee
Naam		
gebootedatum		
geboorteplaats		
geslacht		
Postcode		
Huisnummer		
Huisletter		
Huisnummertoevoeging		
Straatnaam		
Plaatsnaam		
Telefoonnummer		
E-mail adres		
BSN nummer		
Ras of etnische afkomst		
Politieke opvattingen		
Religieuze of levensbeschouwelijke overtuigingen		
Lidmaatschap van een vakbond		
Genetisch of biometrisch met oog op unieke identificatie van een persoon		
gezondheidsgegevens		
Seksueel gedrag of seksuele gerichtheid		
Financiële-/economische gegevens		
Gegevens strafbare feiten		
IP adres		
Gebruikersnamen wachtwoorden en andere inloggegevens		
Overige(graag benoemen)		
-		
-		

3. Welke (groepen van) medewerkers van de Verwerker hebben toegang tot welke persoonsgegevens (in te vullen door Verwerker in autorisatieschema en goed te keuren door ICT)

4. Welke handelingen mogen deze medewerkers met de persoonsgegevens uitvoeren. (in te vullen door Verwerker en goed te keuren door ICT)

Autorisatieschema

Functie	**Systeem A**	**Systeem B**	**Systeem C**	**Systeem D**	**Systeem ect….**	
Functie A	-	-	-	-		
Functie B	X	X	X	X		
Functie C	-	-	-	-		
Functie D	X	X	X	X		
Functie Etc …..	-	-	-	-		

Toelichting autorisatieschema

Functie	**Opmerking bij autorisatieschema**
Functie A	Toegang i.v.m……..
Functie B	Toegang i.v.m……..
Functie C	Toegang i.v.m……..
Functie D	Toegang i.v.m……..
Functie Etc …..	Toegang i.v.m……..
	Toegang i.v.m……..
	Toegang i.v.m……..

BIJLAGE II

BEVEILIGING VAN PERSOONSGEGEVENS

Verwerkingsverantwoordelijke gaat daar waar het de beveiliging van persoonsgegevens betreft uit van de aanwezigheid van onderstaande documenten, maatregelen en/of procedures bij Verwerker:

• *Beleidsdocument voor informatiebeveiliging gebaseerd op de code voor informatiebeveiliging of de baseline informatiebeveiliging gemeenten*
Het beleidsdocument gaat expliciet in op de maatregelen die Verwerker treft om de verwerkte persoonsgegevens te beveiligen. Het document is goedgekeurd op bestuurlijk c.q. leidinggevend niveau en kenbaar gemaakt aan alle werknemers en relevante externe partijen.

• *Toewijzen van verantwoordelijkheden voor informatiebeveiliging*
Alle verantwoordelijkheden, zowel op sturend als op uitvoerend niveau, zijn duidelijk gedefinieerd en belegd.

• *Beveiligingsbewustzijn*
Verwerker en, voor zover van toepassing, ingehuurd personeel en externe gebruikers krijgen geschikte training en regelmatige bijscholing over het informatiebeveiligingsbeleid en de informatiebeveiligingsprocedures van de organisatie, voor zover relevant voor hun functie. Binnen de training en bijscholing wordt expliciet aandacht besteed aan de omgang met (bijzondere of anderszins gevoelige) persoonsgegevens.

• *Fysieke beveiliging en beveiliging van apparatuur*
IT-voorzieningen en apparatuur zijn fysiek beschermd tegen toegang door onbevoegden en tegen schade en storingen. De geboden bescherming is in overeenstemming met de vastgestelde risico's.

• *Toegangsbeveiliging*
Er zijn procedures om bevoegde gebruikers toegang te geven tot de informatiesystemen en -diensten die ze voor de uitvoering van hun taken nodig hebben en om onbevoegde toegang tot informatiesystemen te voorkomen. De procedures omvatten alle fasen in de levenscyclus van de gebruikerstoegang, van de eerste registratie van nieuwe gebruikers tot de uiteindelijke afmelding van gebruikers die niet langer toegang tot informatiesystemen en -diensten nodig hebben. Waar van toepassing wordt bijzondere aandacht besteed aan het beheren van toegangsrechten van gebruikers met extra ruime bevoegdheden, zoals systeembeheerders.

• *Logging en controle*
Activiteiten die gebruikers uitvoeren met persoonsgegevens worden vastgelegd in logbestanden. Hetzelfde geldt voor andere relevante gebeurtenissen, zoals pogingen om ongeautoriseerd toegang te krijgen tot persoonsgegevens en verstoringen die kunnen leiden tot verminking of verlies van persoonsgegevens. De logbestanden worden periodiek gecontroleerd op indicaties van onrechtmatige toegang of onrechtmatig gebruik van de persoonsgegevens en waar nodig wordt actie ondernomen.

Afhankelijk van de beveiligingscategorie gelden de onderstaande extra eisen:

Niveau	Authenticatie	Autorisatie	Monitoring	Beveiliging
Openbaar, risicoklasse 0	Geen	Geen	Geen	Geen
Bedrijfsvertrouwelijk, risicoklasse I	Authenticatie 'basis' vereist. Sessie-time-out na 15 min inactiviteit. Voor klant absolute sessie-time-out na 120 min. Identiteit blokkeren na 3 achtereenvolgende foutieve authenticatiepogingen. Authenticatie 'basis' nodig voor deblokkeren.	Autorisatie vereist (lid van organisatie).	Vastleggen herhaaldelijk foutieve authenticatie en tijdstip.[9] Monitoring-gegevens bewaren voor periode van 1/2 jaar.	Outputvalidatie. Versleuteling tijdens transport buiten netwerk via transportbeveiliging of berichtbeveiliging. Kopieën van gegevens moeten net zo goed beveiligd worden. Gegevens uit productieomgeving worden niet gebruikt in OTA omgevingen tenzij deze zijn geanonimiseerd en de gegevenseigenaar toestemming heeft gegeven.
Vertrouwelijk, risicoklasse II	Authenticatie 'midden' vereist. Sessie-time-out na 15 min inactiviteit. Voor klant absolute sessie-time-out na 120 min. Identiteit blokkeren na 3 achtereenvolgende foutieve authenticatiepogingen. Authenticatie 'midden' nodig voor deblokkeren.	Autorisatie vereist (specifieke rol).	Vastleggen herhaaldelijk foutieve authenticatie en tijdstip. Monitoring-gegevens bewaren voor periode van 2 jaar.	Outputvalidatie. Versleuteling tijdens transport en op tussenstations binnen en buiten netwerk via berichtbeveiliging. Kopieën van gegevens moeten minimaal net zo goed beveiligd worden. Aantal kopieën minimaliseren. Berichtbeveiliging. Gegevens uit productieomgeving worden niet gebruikt in OTA-omgevingen tenzij deze zijn geanonimiseerd en de gegevenseigenaar toestemming heeft gegeven.
Geheim, risicoklasse III	Authenticatie 'hoog' vereist. Sessie-time-out na 15 min inactiviteit. Voor klant absolute sessie-time-out na 120 min. Identiteit blokkeren na 3 achtereenvolgende foutieve authenticatiepogingen. Authenticatie 'hoog' nodig voor deblokkeren. Geen SSO toegestaan.	Autorisatie vereist (specifieke rol).	Vastleggen correcte en foutieve authenticatie en tijdstip. Monitoring-gegevens bewaren voor periode van 7 jaar.	Outputvalidatie. Versleuteling tijdens transport en op tussenstations via berichtbeveiliging. Versleutelde opslag van gegevens. Transport van gegevens minimaliseren. Alleen transport en opslag binnen vaste netwerk. Geen kopieën toegestaan behalve voor beschikbaarheid (back-up). Gegevens uit productieomgeving worden niet gebruikt in OTA-omgevingen tenzij deze zijn geanonimiseerd en de gegevenseigenaar toestemming heeft gegeven.

De authenticatieniveaus verwijzen naar het vereiste beveiligingsmechanisme:

Openbaar:	geen
Basis:	authenticatie gebaseerd op iets wat men weet (naam/wachtwoord).
Midden:	authenticatie gebaseerd op iets wat men weet en iets wat men heeft (bijv. een token, smartcard of certificaat).
Hoog:	authenticatie gebaseerd op eigenschap, bijvoorbeeld irisscan of vingerafdruk.

Bij datatransport is berichtbeveiliging te prefereren boven transportbeveiliging. Echter, transportbeveiliging kan in bepaalde gevallen eenvoudiger en/of goedkoper te implementeren zijn. Daarom is bij classificatieniveau ‘beschermd’ de keuze voor transportbeveiliging en berichtbeveiliging open gelaten. Bij ‘hoog’ en ‘absoluut’ is de classificatie zodanig dat berichtbeveiliging toegepast moet worden.

Het niveau van vertrouwelijkheid c.q. de risicoklasse wordt aan de hand van onderstaand schema bepaald:

Schema voor het bepalen van de risicoklasse

De onderlinge relatie tussen de risicoklassen is in onderstaand schema weergegeven.

Aard van de persoonsgegevens: *Hoeveelheid persoonsgegevens (aard en omvang)*	*Aard van de verwerking*	Persoonsgegevens	Bijzondere persoonsgegevens Conform artikel 16 WBP	Financieel en / of economische persoonsgegevens
Weinig persoonsgegevens	Lage complexiteit van verwerking	**Risicoklasse 0**	**Risicoklasse II**	**Risicoklasse II**
Veel persoonsgegevens	Hoge complexiteit van verwerking	**Risicoklasse I**	**Risicoklasse III**	

Deze overeenkomst valt binnen de categorie **<openbaar/bedrijfsvertrouwelijk/vertrouwelijk/geheim>.**

Igv. Catergorie geheim (risicoklasse III) gelden alle bepalingen van deze overeenkomst
Igv. Categorie vertrouwelijk (risicoklasse II) geldt artikel 6.9 van deze overeenkomst niet
Igv. Categorie bedrijfsvertrouwelijk (risicoklasse I) gelden de artikelen 6.6 tot en met 6.10 van deze overeenkomst niet
Igv. Categorie openbaar (risicoklasse 0) gelden de artikelen 6.3 tot en met 6.10 van deze overeenkomst niet

BIJLAGE III

MELDING BEVEILIGINGSINCIDENT/ DATALEK DOOR VERWERKER

Vragen formulier melding

0. Contact persoon bij Verwerker:

Vul onderstaande gegevens in	
Naam:	
Functie:	
Mobiele telefoon:	
E-mailadres:	

1. Is dit een vervolg op een eerdere melding?

Kies een van onderstaande opties:	**Maak een keuze**
a) Ja	
b) Nee	

2. Van wanneer dateert de oorspronkelijke melding?

(beantwoord deze vraag als u vraag 1 met ja hebt beantwoord)	**Invullen**
Datum:	

3. Wat is de strekking van de vervolgmelding?

(beantwoord deze vraag als u vraag 1 met ja hebt beantwoord, kies een van de volgende opties)	**Maak een keuze**
a) Toevoegen of wijzigen van informatie betreffende de eerdere melding	
b) Intrekking van de eerdere melding	

4. Wat is de reden van intrekking

(beantwoord deze vraag als u bij vraag 3 hebt gekozen voor optie b)	**Invullen**
De reden van intrekking is:	

5. Geef een samenvatting van het incident waarop de inbreuk op de beveiliging van persoonsgegevens zich heeft voorgedaan.

6. Van hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?

	Vul de aantallen in
a) Minimaal: (vul aan)	
b) Maximaal: (vul aan)	

7. Omschrijf de groep mensen van wie persoonsgegevens zijn betrokken bij de inbreuk.

8. Wanneer vond de inbreuk plaats?

Kies een van de volgende opties:	**Maak een keuze en vul in**
a) Op (datum)	
b) Tussen (begindatum periode en einddatum periode)	
c) Nog niet bekend	

Wanneer werd de inbreuk ontdekt?

Op (datum)

9. Wat is de aard van de inbreuk?

Reden	**U kunt meerdere mogelijkheden kiezen**
a) Lezen (vertrouwelijkheid)	Ja/nee
b) Kopiëren	Ja/nee
c) Veranderingen (integriteit)	Ja/nee
d) Verwijderen of vernietigen (beschikbaarheid)	Ja/nee
e) Diefstal	Ja/nee
f) Nog niet bekend	Ja/nee

10. Om welk type persoonsgegevens gaat het? U kunt hier meerdere mogelijkheden aankruisen.

Type persoonsgegeven	**U kunt meerdere mogelijkheden kiezen**
a) Naam adres en woongegevens	Ja/nee
b) Telefoonnummers	Ja/nee
c) E-mailadressen of andere adressen voor elektronische communicatie	Ja/nee
d) Toegangs- of identificatiegegevens (bijvoorbeeld inlognaam/wachtwoord of klantnummer)	Ja/nee
e) Financiële gegevens (bijvoorbeeld rekeningnummer, creditcardnummer)	Ja/nee
f) Burgerservicenummer (BSN)	Ja/nee
g) Paspoort kopieën of kopieën van andere legitimatiebewijzen	Ja/nee
h) Geslacht, geboortedatum en/of leeftijd	Ja/nee
i) Bijzondere persoonsgegevens (bijvoorbeeld godsdienst of levensovertuiging, politieke gezindheid, gezondheid, seksuele leven, lidmaatschep vakvereniging, strafrechtelijke gegevens en onrechtmatig/ hinderlijk gedrag met opgelegd verbod.	Ja/nee
j) Overige gegevens, namelijk (vul aan)	Ja/ nee. Zo ja welke,

11. Welke gevolgen kan de inbreuk hebben voor de persoonlijke levenssfeer van de betrokkene?`

Gevolgen	**U kunt meerdere mogelijkheden kiezen**
a) Stigmatisering of uitsluiting	Ja/nee
b) Schade aan de gezondheid	Ja/nee
c) Blootstelling aan (identiteits)fraude	Ja/nee
d) Blootstelling aan spam of phishing	Ja/nee
e) Anders, namelijk (vul aan)	Ja/nee

12. Welke technische en organisatorische maatregelen heeft uw organisatie getroffen om de inbreuk aan te pakken en om verdere inbreuk te voorkomen?

13. Wanner is het datalek gemeld aan Verwerkingsverantwoordelijke/Opdrachtgever?

	Invullen
Datum en tijdstip	

Contactpersoon Verwerkingsverantwoordelijke	Ja/nee
Melding is gedaan per:	Maak keuze, meerdere opties mogelijk
a) Telefoon	
b) E-mail	
c) Formulier	
d) Anders namelijk	

14. Zijn de persoonsgegevens, versleuteld, gehasht of op andere manier onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden?

Type persoonsgegeven	**Kies een van de opties en vul waar nodig aan**
a) Ja	
b) Nee	
c) Deels, namelijk (vul aan)	Ja/nee

15. Als de persoonsgegevens geheel of deels onbegrijpelijk of ontoegankelijk zijn gemaakt, op welke manier is dit dan gebeurd? (Beantwoord deze vraag als u bij vraag 14 gekozen heeft voor optie a) of optie c). Als u gebruik heeft gemaakt van encryptie, licht dan ook de wijze van versleutelen toe).

16. Is naar uw mening deze melding compleet?

Selecteer een van de onderstaande opties	**Maak uw keuze**
a) Ja, de vereiste informatie is verwerkt en er is geen vervolgmelding nodig	
b) Nee, er komt later een vervolgmelding met aanvullende informatie over deze inbreuk	

Afsluitend

Naam ondertekenaar Verwerker:	
Plaats:	
Datum:	
Handtekening	

Contactpersoon bij Verwerker

Naam:	
Functie:	
Mobiele telefoon:	
E-mail:	

FORMULIER MET SPOED BESCHIKBAAR STELLEN AAN:
Contactpersoon bij Verwerkingsverantwoordelijke:

Naam:	**Jan Wiegman**
Functie:	CISO
Mobiele telefoon:	010-2848989 (24 uur)
E-mail:	ciso@ijsselgemeenten.nl

Het formulier is door Verwerkingsverantwoordelijke ontvangen op:

Ondertekening

Verwerkingsverantwoordelijke	**Verwerker**
Naam:	**Naam:**
Functie:	**Functie:**
Datum:	**Datum:**

BIJLAGE IV

OMSCHRIJVING WERKZAAMHDEN TER UITWERKING VAN ARTIKEL 7 LID 4 VAN DE VERWERKERSOVEREENKOMST

Verwerker maakt bij de uitvoering van de opdracht gebruik van derden/subverwerkers die in deze Bijlage zijn vermeld. Verwerker zal deze Bijlage conform artikel 7 lid 4 van de Verwerkersovereenkomst bijwerken indien er wijzigingen plaatsvinden in de ingeschakelde derden/subverwerkers en deze lijst onverwijld ter beschikking stellen aan verwerkingsverantwoordelijke.

Partij 1	<naam>
Vestigingsplaats	
Inschrijvingsnummer handelsregister	
Beschrijving werkzaamheden	
Voorwaarden door Verwerkingsverantwoordelijke gesteld aan de toestemming	

Welke (groepen van) medewerkers van de subverwerker hebben toegang tot welke persoonsgegevens (in te vullen door Verwerker in autorisatieschema en goed te keuren door ICT)

Welke handelingen mogen deze medewerkers met de persoonsgegevens uitvoeren.
(in te vullen door Verwerker en goed te keuren door ICT)

Autorisatieschema

Functie	**Systeem A**	**Systeem B**	**Systeem C**	**Systeem D**	**Systeem ect.....**	
Functie A	-	-	-	-		
Functie B	X	X	X	X		
Functie C	-	-	-	-		
Functie D	X	X	X	X		
Functie Etc	-	-	-	-		

Toelichting autorisatieschema

Functie	**Opmerking bij autorisatieschema**
Functie A	Toegang i.v.m……..
Functie B	Toegang i.v.m……..
Functie C	Toegang i.v.m……..
Functie D	Toegang i.v.m……..
Functie Etc	Toegang i.v.m……..
	Toegang i.v.m……..
	Toegang i.v.m……..

Partij 2	<naam>
Vestigingsplaats	
Inschrijvingsnummer handelsregister	
Beschrijving werkzaamheden	
Voorwaarden door Verwerkingsverantwoordelijke gesteld aan de toestemming	

Welke (groepen van) medewerkers van de subverwerker hebben toegang tot welke persoonsgegevens (in te vullen door Verwerker in autorisatieschema en goed te keuren door ICT)

Welke handelingen mogen deze medewerkers met de persoonsgegevens uitvoeren.
(in te vullen door Verwerker en goed te keuren door ICT)

Autorisatieschema

Functie	**Systeem A**	**Systeem B**	**Systeem C**	**Systeem D**	**Systeem ect…..**	
Functie A	-	-	-	-		
Functie B	X	X	X	X		
Functie C	-	-	-	-		
Functie D	X	X	X	X		
Functie Etc …..	-	-	-	-		

Toelichting autorisatieschema

Functie	**Opmerking bij autorisatieschema**
Functie A	Toegang i.v.m……..
Functie B	Toegang i.v.m……..
Functie C	Toegang i.v.m……..
Functie D	Toegang i.v.m……..
Functie Etc …..	Toegang i.v.m……..
	Toegang i.v.m……..
	Toegang i.v.m……..