Verwerkersovereenkomst <naam van uw organisatie> en <naam verwerker>

Verwerkersovereenkomst van <naam van uw organisatie> met de <naam verwerker> verwerker.

Partijen,

<volledige naam van uw organisatie, NAW gegevens> verder te noemen **verwerkingsverantwoordelijke**, ten deze rechtsgeldig vertegenwoordigd door de heer/mevrouw <naam en positie vertegenwoordiger van de organisatie>,

en

<naam + rechtsvorm (bijvoorbeeld een B.V.) verwerker>, gevestigd te <adres en postcode>, ingeschreven in het handelsregister van de Kamer van Koophandel onder nummer <KvK nummer>, verder te noemen **verwerker**, ten deze rechtsgeldig vertegenwoordigd door <de heer/mevrouw <naam directeur> in zijn/haar functie als <functie>,

verklaren te zijn overeengekomen een verwerkersovereenkomst als bedoeld in artikel 14, tweede lid, van de Wbp c.q. artikel 28, derde lid, van de AVG, tussen de verwerkingsverantwoordelijke en de verwerker, zoals hierna weergegeven. Waar in deze verwerkersovereenkomst termen worden gebruikt die overeenstemmen met definities uit artikel 1 Wbp, wordt aan deze termen de betekenis van de definities uit de Wbp toegekend.

**Definities**

**Artikel 1**

Waar in deze verwerkersovereenkomst termen worden gebruikt die overeenstemmen met definities uit artikel 4 AVG, wordt aan deze termen de betekenis van de definities uit de AVG toegekend. In aanvulling daarop gelden de volgende definities:

* 1. **AP:**

De Autoriteit Persoonsgegevens.

* 1. **AVG:**

Verordening (EU) 2016/679 van het Europees parlement en de Raad van 27 april 2016 (de Algemene Verordening Gegevensbescherming).

* 1. **Bijlagen:**

Aanhangsels bij deze verwerkersovereenkomst, die integraal deel uitmaken van deze verwerkersovereenkomst.

* 1. **BRP:**

Wet Basisregistratie Personen.

* 1. **Datalek** (in de AVG aangeduid als als ‘inbreuk in verband met persoonsgegevens’)**:**

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. **Dienstverleningsovereenkomst:**

De tussen verwerkingsverantwoordelijke en verwerker gesloten overeenkomst <omschrijving contract, nummer, datum, etc.>, uit hoofde waarvan verwerker in opdracht van verwerkingsverantwoordelijke persoonsgegevens verwerkt; dit is de onderliggende hoofdovereenkomst

* 1. **Functionaris:**

De functionaris voor de gegevensbescherming (FG) als bedoeld in artikel 62 van de Wbp c.q. artikel 37-39 AVG.

* 1. **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 Bijlage 1.

* 1. **Verwerkersovereenkomst:**

De onderhavige verwerkersovereenkomst, inclusief de Bijlagen.

* 1. **Toezichthouder**:

de Autoriteit Persoonsgegevens (AP) is het zelfstandig bestuursorgaan dat in Nederland bij wet als toezichthoudende autoriteit is belast met toezicht houden op de naleving van wet- en regelgeving met betrekking tot de bescherming van persoonsgegevens, waaronder de AVG.

* 1. **Uitvoeringswet:**

Uitvoeringswet Algemene verordening gegevensbescherming.

* 1. **Wbp:**

Wet bescherming persoonsgegevens.

**Ingangsdatum en duur**

**Artikel 2**

2.1 Deze verwerkersovereenkomst gaat in op het moment van ondertekening en duurt voort zolang de Dienstverleningsovereenkomst, inclusief eventuele verlengingen daarvan, tussen de verwerker en de verwerkingsverantwoordelijke voortduurt.

2.2 Deze verwerkersovereenkomst eindigt van rechtswege bij de beëindiging van de Dienstverleningsovereenkomst. De beëindiging van deze verwerkersovereenkomst zal partijen niet ontslaan van hun verplichtingen die voortvloeien uit deze verwerkersovereenkomst die naar hun aard worden geacht ook na beëindiging voort te duren, waaronder doch niet uitsluitend geheimhouding en verplichtingen met betrekking tot dataportabiliteit en vernietiging van Persoonsgegevens.

**Onderwerp van deze verwerkersovereenkomst**

**Artikel 3**

* 1. De verwerker verwerkt de door of via verwerkingsverantwoordelijke ter beschikking gestelde persoonsgegevens uitsluitend in opdracht van de verwerkings-verantwoordelijke in het kader van de Dienstverleningsovereenkomst. De door de verwerker uit te voeren werkzaamheden waar deze verwerkersovereenkomst betrekking op heeft, worden nader omschreven in Bijlage 2. Verwerker zal de persoonsgegevens niet voor enig ander doel verwerken dan ter uitvoering van zijn werkzaamheden in het kader van de Dienstverleningsovereenkomst, behoudens afwijkende wettelijke verplichtingen.
  2. De verwerker verbindt zich om in het kader van de in lid 1 van dit artikel bedoelde werkzaamheden de door verwerkingsverantwoordelijke ter beschikking gestelde of anderszins door verwerker in het kader van de werkzaamheden verkregen persoonsgegevens op behoorlijke en zorgvuldige wijze te verwerken.
  3. De verwerkingsverantwoordelijke is ten aanzien van de in diens opdracht uit te voeren verwerkingen van persoonsgegevens de (verwerkings)verantwoordelijke in de zin van artikel 1 onder d. Wbp c.q. artikel 4, zevende lid, AVG. Verwerker is verwerker in de zin van artikel 1 onder e. Wbp c.q. artikel 4, achtste lid, AVG. De verwerkingsverantwoordelijke heeft en houdt zelfstandige zeggenschap over het doel en de middelen van de verwerking van de persoonsgegevens.

**Verplichtingen verwerker**

**Artikel 4**

* 1. De verwerker verwerkt de persoonsgegevens uitsluitend in opdracht en ten behoeve van verwerkingsverantwoordelijke en in overeenstemming met diens schriftelijke instructies.
  2. De verwerker heeft geen zeggenschap over de onder deze verwerkersovereenkomst ter beschikking gestelde of anderszins verstrekte persoonsgegevens. Zo neemt hij geen beslissingen over ontvangst en gebruik van de gegevens, de doeleinden van de verwerking, de verstrekking aan derden en de (duur van de) opslag van de persoonsgegevens.
  3. De verwerker zal bij de verwerking van persoonsgegevens in het kader van de in artikel 3 genoemde werkzaamheden steeds handelen in overeenstemming met de toepasselijke wet- en regelgeving betreffende de bescherming van persoonsgegevens. Hieronder worden in ieder geval doch niet uitsluitend verstaan: tot 25 mei 2018 de Wbp en met ingang van 25 mei 2018 de AVG en de Uitvoeringswet en, indien de verwerking van persoonsgegevens door verwerker valt onder de reikwijdte van de BRP, de BRP en aanverwante regelgeving.
  4. De verwerker zal alle redelijke instructies van verwerkingsverantwoordelijke opvolgen, behoudens afwijkende wettelijke voorschriften. In geval van een afwijkend wettelijk voorschrift stelt verwerker verwerkingsverantwoordelijke voorafgaand aan de verwerking van de persoonsgegevens in kennis van dat wettelijke voorschrift, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt.
  5. De verwerker zal te allen tijde op eerste verzoek van verwerkingsverantwoordelijke onmiddellijk alle van verwerkingsverantwoordelijke afkomstige persoonsgegevens met betrekking tot deze verwerkersovereenkomst ter beschikking stellen in een door verwerkingsverantwoordelijke in redelijkheid gewenst format.
  6. De verwerker stelt verwerkingsverantwoordelijke te allen tijde in staat om binnen de wettelijke termijnen te voldoen aan de verplichtingen op grond van de Wbp en de AVG, meer in het bijzonder de rechten van betrokkenen, zoals, maar niet beperkt tot, een verzoek om inzage, rectificatie, verwijdering, rectificatie of wissing, verwerkingsbeperking of overdraagbaarheid van persoonsgegevens en het uitvoeren van een gehonoreerd aangetekend bezwaar.
  7. De verwerker verbindt zich ertoe verwerkingsverantwoordelijke bij te staan in de analyse van de vraag of een gegevensbeschermingseffectbeoordeling (DPIA) noodzakelijk is voor de verwerking van de persoonsgegevens door de verwerker. Dit impliceert bijvoorbeeld dat indien de verwerking door de verwerker het gebruik van nieuwe technologieën vereist, of indien de verwerker het plausibel acht dat de gebruikte technologie als “nieuw” kan worden gekwalificeerd, de verwerker voor de start van de verwerking van de persoonsgegevens de verwerkingsverantwoordelijke hiervan op de hoogte brengt.
  8. Wanneer de verwerkingsverantwoordelijke een gegevensbeschermings-effectbeoordeling nodig acht, verbindt de verwerker zich ertoe de verwerkings-verantwoordelijke bij te staan bij de uitvoering van de gegevensbeschermings-effectbeoordeling. De verwerker verstrekt de verwerkingsverantwoordelijke in zulk geval ten minste de informatie opgenomen in Bijlage 6, en start de verwerking pas na de (evaluatie van de) gegevensbeschermingsbeoordeling en de schriftelijke instructies hiertoe van de verwerkingsverantwoordelijke.
  9. Op verzoek van verwerkingsverantwoordelijke verstrekt verwerker een accountantsverklaring aan verwerkingsverantwoordelijke waaruit blijkt dat verwerker werkt in overeenstemming met de in artikel 4.3 bedoelde toepasselijke wet- en regelgeving ten aanzien van de bescherming van persoonsgegevens.
  10. Indien, naar zijn mening, een verzoek of instructie van de verwerkingsverantwoordelijke een inbreuk oplevert van de AVG of andere toepasselijke wet- en regelgeving, zal verwerker verwerkingsverantwoordelijke hiervan onmiddellijk in kennis stellen.

**Geheimhoudingsplicht**

**Artikel 5**

* 1. Medewerkers in dienst van, dan wel anderszins werkzaam ten behoeve van verwerker, evenals verwerker zelf, zijn verplicht tot geheimhouding met betrekking tot de persoonsgegevens waarvan zij kennis kunnen nemen, behoudens voor zover een bij, of krachtens de wet gegeven voorschrift tot verstrekking verplicht of zijn taak daartoe noodzaakt. De medewerkers van verwerker tekenen hiertoe een geheimhoudingsverklaring.
  2. De verwerker verschaft enkel toegang tot de persoonsgegevens aan zijn medewerkers voor zover dit nodig is voor het verwezenlijken van de in Bijlage 1 beschreven werkzaamheden.
  3. Indien de verwerker op grond van een wettelijk voorschrift gegevens dient te verstrekken, zal verwerker de grondslag van het verzoek en de identiteit van de verzoeker verifiëren en verwerker zal verwerkingsverantwoordelijke onmiddellijk, voorafgaand aan de verstrekking, ter zake informeren, tenzij wettelijke bepalingen dit verbieden.

**Meldplicht Datalekken en beveiligingsincidenten**

**Artikel 6**

6.1 De verwerker zal de verwerkingsverantwoordelijke zo spoedig mogelijk – doch uiterlijk binnen 24 uur na de eerste ontdekking – informeren over alle (vermoedelijke) Datalekken alsmede andere (beveiligings)incidenten die op grond van wetgeving moeten worden gemeld aan de toezichthouder of betrokkene, onverminderd de verplichting de gevolgen van Datalekken en incidenten zo snel mogelijk ongedaan te maken dan wel te beperken, al dan niet onder verbeurte van een boete in geval van niet-nakoming, conform artikel 10.2 van deze Verwerkersovereenkomst. Verwerker zal voorts, op het eerste verzoek van de verwerkingsverantwoordelijke, alle inlichtingen verschaffen die de verwerkingsverantwoordelijke noodzakelijk acht om het Datalek of het incident te kunnen beoordelen. Daarbij verschaft verwerker in ieder geval de informatie aan de verwerkingsverantwoordelijke zoals omschreven in Bijlage 3.

6.2 De verwerker beschikt over een gedegen plan van aanpak betreffende de omgang met en afhandeling van Datalekken en zal de verwerkingsverantwoordelijke, op diens verzoek, inzage verschaffen in het plan. Verwerker stelt de verwerkings-verantwoordelijke op de hoogte van materiële wijzigingen in het plan van aanpak.

6.3 De verwerker zal het doen van meldingen aan de toezichthouder(s) overlaten aan de verwerkingsverantwoordelijke.

6.4 De verwerker zal alle noodzakelijke medewerking verlenen aan het zo nodig, op de kortst mogelijke termijn, verschaffen van aanvullende informatie aan de toezichthouder(s) (zoals de AP) en/of betrokkene(n). Daarbij verschaft verwerker in ieder geval de informatie, zoals beschreven in Bijlage 3, aan de verwerkingsverantwoordelijke.

6.5 De verwerker houdt een gedetailleerd logboek bij van alle (vermoedens van) Datalekken, evenals de maatregelen die in vervolg op Datalekken zijn genomen waarin minimaal de informatie zoals bedoeld in Bijlage 3 is opgenomen, en geeft daar op eerste verzoek van de verwerkingsverantwoordelijke inzage in.

**Beveiligingsmaatregelen en controle**

**Artikel 7**

* 1. Rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen neemt de verwerker alle passende technische en organisatorische maatregelen om de persoonsgegevens welke worden verwerkt ten dienste van de verwerkingsverantwoordelijke te beveiligen en beveiligd te houden tegen verlies of tegen enige vorm van onrechtmatige verwerking. De wijze van beveiliging en de in dat kader door verwerker te treffen maatregelen worden nader omschreven in Bijlagen 1 en 4.
  2. De verwerkingsverantwoordelijke is te allen tijde gerechtigd de verwerking van persoonsgegevens, en in het bijzonder de door de verwerker in acht te nemen beveiligingsmaatregelen, te (doen) controleren. De verwerker is verplicht de verwerkingsverantwoordelijke, of de onder geheimhouding controlerende instantie in opdracht van verwerkingsverantwoordelijke toe te laten en verplicht medewerking te verlenen, zodat de controle (audit) daadwerkelijk uitgevoerd kan worden.
  3. De verwerkingsverantwoordelijke zal de audit slechts (laten) uitvoeren na een voorafgaande schriftelijke melding aan de verwerker.
  4. De verwerker verbindt zich om binnen een door verwerkingsverantwoordelijke te bepalen termijn verwerkingsverantwoordelijke, of de door verwerkingsverantwoordelijke ingeschakelde derde, te voorzien van de verlangde informatie. Hierdoor kan de verwerkingsverantwoordelijke, of de door de verwerkingsverantwoordelijke ingeschakelde derde, zich een oordeel vormen over de naleving door verwerker van deze verwerkersovereenkomst. De verwerkingsverantwoordelijke, of de door de verwerkingsverantwoordelijke ingeschakelde derde, is gehouden alle informatie betreffende deze controles vertrouwelijk te behandelen.
  5. Verwerker staat er voor in de door verwerkingsverantwoordelijke of de door Verwerkingsverantwoordelijke ingeschakelde derde aangegeven aanbevelingen ter verbetering binnen de daartoe door Verwerkingsverantwoordelijke te bepalen termijn uit te voeren.

7.6. De verwerker rapporteert jaarlijks schriftelijk over de opzet en werking van het stelsel van maatregelen en procedures, gericht op naleving van deze verwerkersovereenkomst.

7.7. Naast rapportages door de verwerker te leveren, en controles door de verwerkingsverantwoordelijke of controlerende instantie in opdracht van de verwerkingsverantwoordelijke, kunnen beide partijen ook overeenkomen gebruik te maken van een Third Party Memorandum (TPM) opgesteld door een onafhankelijke externe deskundige (bijvoorbeeld de IBD).

* 1. De redelijke kosten van de controle worden gedragen door de partij die de kosten maakt, tenzij uit de controle blijkt dat de verwerker enig punt uit deze Verwerkersovereenkomst niet heeft nageleefd. In dat geval worden de kosten van de controle gedragen door de verwerker.

**Inschakeling derden en plaats van verwerking**

**Artikel 8**

8.1 De verwerker is slechts gerechtigd de uitvoering van de werkzaamheden geheel of ten dele uit te besteden aan derden na voorafgaande schriftelijke toestemming van de verwerkingsverantwoordelijke. Indien de verwerkingsverantwoordelijke toestemming heeft gegeven, draagt de verwerker ervoor zorg dat de betreffende derde tenminste dezelfde verplichtingen op zich neemt als opgenomen voor de verwerker in deze verwerkersovereenkomst. De verwerker ziet toe op de naleving van het hier gestelde door de ingeschakelde derde.

8.2 De verwerkingsverantwoordelijke kan aan zijn schriftelijke toestemming voorwaarden verbinden, die door de verwerker aan de derde moeten worden opgelegd.

8.3 De verwerker blijft in de verhouding tussen partijen altijd aanspreekpunt en volledig verantwoordelijk en aansprakelijk voor de naleving van de bepalingen uit deze verwerkersovereenkomst, inclusief de naleving van de eventuele nadere voorwaarden als bedoeld in het voorgaande lid. De verwerker garandeert dat de door hem ingeschakelde derden schriftelijk minimaal dezelfde plichten op zich nemen als tussen de verwerkingsverantwoordelijke en de verwerker zijn overeengekomen en zal de verwerkingsverantwoordelijke, op diens verzoek, inzage verschaffen in de overeenkomsten met deze derden waarin deze plichten zijn opgenomen.

8.4 De verwerker mag de persoonsgegevens uitsluitend verwerken in Nederland. Doorgifte naar andere landen is uitsluitend toegestaan na voorafgaande schriftelijke toestemming van de verwerkingsverantwoordelijke en met inachtneming van de toepasselijke wet- en regelgeving.

8.5 De verwerker houdt een actueel register bij van de door hem ingeschakelde derden en onderaannemers waarin de identiteit, vestigingsplaats en een beschrijving van de werkzaamheden van de derden of onderaannemers zijn opgenomen, alsmede eventuele door de verwerkingsverantwoordelijke gestelde aanvullende voorwaarden. Dit register zal als Bijlage 5 aan deze verwerkersovereenkomst worden toegevoegd en zal door de verwerker actueel worden gehouden.

**Wijziging en gevolgen beëindiging verwerkersovereenkomst**

**Artikel 9**

9.1 De verwerkings-verantwoordelijke 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, of een wijziging in de dienstverlening van verwerker daartoe aanleiding geven. Wijziging van deze verwerkersovereenkomst kan slechts schriftelijk plaatsvinden middels een door beide partijen geaccordeerd voorstel.

9.2 Zodra de verwerkersovereenkomst is beëindigd, zal verwerker (i) alle of een door verwerkingsverantwoordelijke bepaald gedeelte van de door verwerker in het kader van deze verwerkersovereenkomst verwerkte persoonsgegevens aan verwerkingsverantwoordelijke ter beschikking te stellen in een door verantwoordelijk in redelijkheid gewenst format en op een nader overeen te komen wijze én (ii) nadat de terbeschikkingstelling van persoonsgegevens als bedoeld in (i) is geslaagd, de persoonsgegevens die hij van verwerkingsverantwoordelijke heeft ontvangen op alle locaties vernietigen, in welke vorm dan ook en toont dit aan, tenzij partijen iets anders overeenkomen. Deze werkzaamheden worden binnen een nader overeen te komen termijn uitgevoerd en hiervan wordt een verslag opgemaakt door verwerker.

9.3 De verwerker zal te allen tijde de in het vorige lid beschreven dataportabiliteit waarborgen zodanig dat er geen sprake is van verlies van functionaliteit of (delen van) de gegevens.

9.4 Verwerker zal alle derden die betrokken zijn bij de verwerking van de -persoonsgegevens op de hoogte stellen van een beëindiging van de verwerkersovereenkomst en zal waarborgen dat alle derden de persoonsgegevens (laten) vernietigen.

9.5 De verwerker informeert ogenblikkelijk de verwerkingsverantwoordelijke indien zijn faillissement dan wel surséance van betaling dreigt, zodat de verwerkings-verantwoordelijke tijdig kan beslissen de persoonsgegevens terug te vorderen alvorens faillissement wordt uitgesproken.

9.6 Onverlet diens rechten tot opzegging en/of ontbinding voortvloeiend uit de Dienstverleningsovereenkomst is verwerkingsverantwoordelijke, zonder dat dit tot enige verplichting van verwerkingsverantwoordelijke tot schadevergoeding leidt, tevens gerechtigd deze verwerkersovereenkomst en de Dienstverleningsovereenkomst per direct te ontbinden indien verwerker te kennen geeft of anderszins vast komt te staan dat hij niet (langer) kan voldoen aan de betrouwbaarheidseisen die op grond van ontwikkelingen in de wet en/of de rechtspraak aan de verwerking van de persoonsgegevens worden gesteld.

**Aansprakelijkheid**

**Artikel 10**

10.1 Verwerker is jegens verwerkingsverantwoordelijke aansprakelijk voor alle schade of nadeel voortvloeiende uit het door verwerker en/of door verwerker ingeschakelde derden niet-nakomen van verplichtingen voortvloeiende uit deze Verwerkersovereenkomst en/of het door verwerker en/of door verwerker ingeschakelde derden in strijd handelen met de toepasselijke wet- en regelgeving met betrekking tot bescherming van persoonsgegevens. Verwerker is tevens aansprakelijk voor alle schade of nadeel voortvloeiende uit de door zijn werkzaamheden en/of door de werkzaamheden van de door verwerker ingeschakelde derden ontstane inbreuken op de persoonlijke levenssfeer van betrokkenen.

10.2 Indien verwerker toerekenbaar tekortschiet in de nakoming van verplichtingen onder deze Verwerkersovereenkomst, is hij aan verwerkingsverantwoordelijke , zonder dat hiervoor een aanmaning of een voorafgaande verklaring nodig is, een boete verschuldigd van € 50.000,-- per overtreding. Deze boete is niet vatbaar voor verrekening en opschorting en laat de rechten van verwerkingsverantwoordelijke op nakoming, ontbinding en schadevergoeding onverlet.

10.3 Verwerker vrijwaart verwerkingsverantwoordelijke voor alle schade of nadeel (waaronder mede begrepen doch niet uitsluitend aan verwerkingsverantwoordelijke opgelegde boetes van Toezichthouders en kosten van rechtsbijstand) voor zover ontstaan als gevolg van de werkzaamheden van verwerker en/of door de werkzaamheden van de door verwerker ingeschakelde derden..

**Escalatie**

**Artikel 11**

11.1 Als de verwerker (een) in deze Verwerkersovereenkomst genoemde verplichting(en) niet (tijdig) nakomt, worden <naam en positie hoofd van uw organisatie> bij verwerkingsverantwoordelijke en de directie van verwerker onmiddellijk op de hoogte gesteld.

11.2 De directie van verwerker draagt tijdig c.q. onverwijld een oplossing aan en draagt zorg voor de spoedige implementatie van deze oplossing of maatregel.

11.3 Mocht de oplossing of maatregel als genoemd in het tweede lid niet binnen een periode van één maand, afhankelijk van de urgentie (bijvoorbeeld: productieverstoring, dreigende financiële of reputatieschade), leiden tot het voldoen aan de verplichtingen zoals neergelegd in deze Verwerkersovereenkomst, dan worden <naam en positie hoofd van uw organisatie> bij verwerkings-verantwoordelijke en de eigenaar/directeur bij verwerker op de hoogte gesteld.

11.4 De escalatieregeling in dit artikel laat de rechten van verwerkingsverantwoordelijke uit hoofde van de wet, de Dienstverleningsovereenkomst en deze Verwerkersovereenkomst, waaronder mede begrepen het recht om aanspraak te maken op schadevergoeding, nakoming, ontbinding en het opeisen van de uit hoofde van artikel 10.2 verbeurde boetes, onverlet.

**Rangorde**

**Artikel 12**

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

**Toepasselijk recht en geschillen**

**Artikel 13**

13.1 Op deze Verwerkersovereenkomst en op alle geschillen die daaruit voortvloeien of daarmee samenhangen, is Nederlands recht van toepassing.

13.2 Alle geschillen die voortvloeien uit deze Verwerkersovereenkomst, worden uitsluitend beslecht door de rechtbank <te noemen rechtbank voor uw regio>.

**Citeertitel**

**Artikel 14**

Deze Verwerkersovereenkomst kan worden aangehaald als <verwerkersovereenkomst behorend bij <naam hoofdovereenkomst>>.

\*\*\*

[ondertekeningspagina volgt]

Aldus in tweevoud opgesteld en getekend op < datum >

namens de verwerkingsverantwoordelijke:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

de heer/mevrouw <naam en positie hoofd van uw organisatie>.

namens de verwerker:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

<naam directeur> in zijn/haar functie van <functie en bedrijfsnaam>.

**Overzicht Bijlagen:**

Bijlage 1: Beschrijving beveiliging ter uitwerking van artikel 1.8 en 7.

Bijlage 2: Omschrijving werkzaamheden, doeleinden verwerking en categorieën te verwerken persoonsgegevens, ter uitwerking van artikel 3, lid 1.

Bijlage 3: Inlichtingen om incidenten te beoordelen ter uitwerking van art. 6, lid 1 en 5.

Bijlage 4: Toelichting: Maatregelen op basis van de BIG ten aanzien van een verwerker.

Bijlage 5: Omschrijving werkzaamheden ter uitwerking van artikel 8 lid 5.

Bijlage 6: Overzicht van door verwerker aan te leveren informatie ten behoeve van een DPIA.

**Bijlage 1: Beschrijving beveiliging ter uitwerking van artikel 1.8 en 7.**

1. Normenstelsel (kies a of b)
2. De informatiebeveiliging vindt plaats volgens algemeen erkende normen, namelijk (vermeld normenstelsel, zoals bijvoorbeeld NEN7510, NEN/ISO 27001, PCI/DSS)
3. De informatiebeveiliging vindt plaats volgens een algemeen erkende overheidsnorm zoals de BIG of de BIR of vergelijkbaar.
4. De toereikendheid van de informatiebeveiliging blijkt uit:
5. Certificering;
6. Periodieke externe controles zoals audits of TPM’s (bijv. ISAE3xxx SOC type II);
7. Een Assurance rapport met conclusie over de bevindingen van de auditor;
8. Eigen controles of eigen mededelingen.
9. Uit de certificering of periodieke externe controles of uit de audits of uit de eigen controles blijkt of kan afgeleid worden dat de beveiliging voldoet aan of gelijkwaardig is met de toelichting (Bijlage 4) en de daarin omschreven elementen.

LET OP: gemotiveerd afwijken is toegestaan!

**Bijlage 2: Omschrijving werkzaamheden, doeleinden verwerking en categorieën te verwerken persoonsgegevens, ter uitwerking van artikel 3, lid 1.**

1. **Omschrijving werkzaamheden van de verwerker (de verleende diensten en de bijbehorende verwerking. Indien de werkzaamheden van de verwerker afdoende zijn beschreven in een SLA of DVO, mag dit document ook als bijlage dienen).**

Hier een overzicht opnemen met werkzaamheden die veel voorkomen zoals:

* Hosting bestaande uit activiteiten de volgende activiteiten:…
* Back-ups maken en restoren bestaande uit activiteiten de volgende activiteiten:…
* Applicatiebeheer bestaande uit de volgende activiteiten:…
* Technisch beheer bestaande uit de volgende activiteiten:…
* Database beheer bestaande uit de volgende activiteiten:…
* Helpdesk bestaande uit de volgende activiteiten:…
* Communicatievoorziening (zoals berichtenverkeer) bestaande uit activiteiten de volgende activiteiten:…
* Archiefbeheer bestaande uit activiteiten de volgende activiteiten:…
* Vernietiging van gegevensdragers bestaande uit activiteiten de volgende activiteiten:…
* Printing, scanning, kopiëren (lease van Multifunctionals)
* Inhoudelijke werkzaamheden die namens de gemeente worden uitgevoerd zoals:
* Uitgifte parkeervergunningen
* Voeren salarisadministratie
* Bijvoorbeeld: uitvoeren bepaalde gemeentelijke taken uit de BRP, Jeugdwet, WMO, Participatiewet, etc.

Indien de werkzaamheden in de hoofdovereenkomst specifiek omschreven zijn, kan dit overzicht achterwege blijven in dat geval kan worden volstaan met een verwijzing naar de hoofdovereenkomst. De achtergrond van de beschrijving is dat je voldoende duidelijk maakt wat er beveiligd moet worden. Het is de bedoeling dat de zinnen afgemaakt worden met specifieke omschrijvingen!

1. **Omschrijving van de werkzaamheden van de derden (subverwerkers) als deze er zijn, als bedoeld in artikel 8.**

Hieronder aangeven welke werkzaamheden door de betreffende door de verwerker ingehuurde derde(n) worden uitgevoerd.

Voorbeelden van veel voorkomende werkzaamheden zijn:

* Hosting bestaande uit de volgende activiteiten:…
* Back-ups maken en restoren
* Applicatiebeheer bestaande uit de volgende activiteiten:…
* Technisch beheer bestaande uit de volgende activiteiten:…
* Database beheer bestaande uit de volgende activiteiten:…
* Helpdesk bestaande uit de volgende activiteiten:…
* Communicatievoorziening (zoals berichtenverkeer)
* Onderhoud aan multifunctionals
* Overige werkzaamheden, te weten…

Toelichting: De achtergrond van de beschrijving is dat er voldoende duidelijk gemaakt wordt wat er beveiligd moet worden. Ook hier geldt dat de zinnen afgemaakt worden met specifieke omschrijvingen!

1. **Categorieën personen en soorten persoonsgegevens.**

Algemene omschrijving van de categorieën personen waar de gegevens die verwerkt worden betrekking op hebben zoals: personeelsleden, burgers, ingeschrevenen, vergunning aanvragers, voorziening aanvragers (cliënten): ….. Het is de bedoeling dat de zin afgemaakt worden met specifieke omschrijvingen!

Is er bij de verwerkte gegevens sprake van gegevens van gevoelige aard als bedoeld in de

richtsnoeren beveiliging persoonsgegevens (2013) alsmede de beleidsregels meldplicht datalekken (2015), beide van de Autoriteit Persoonsgegevens:

* Bijzondere persoonsgegevens zoals bedoeld in artikel 16 Wbp resp. artikel 9 AVG. Het gaat hierbij om persoonsgegevens over iemands ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond, alsmede genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid .
* Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen als bedoeld in artikel 10 AVG
* Het burgerservicenummer (BSN) of andere nationale identificatienummers.
* 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 biometrische gegevens, kopieën van identiteitsbewijzen en om het BSN.

Ja/nee + beschrijving van betreffende categorieën gevoelige persoonsgegevens die worden verwerkt

Is er sprake van de verwerking van gegevens over kwetsbare groepen zoals:

* minderjarigen;
* mensen die te maken hebben met stalking;
* die in een blijf-van-mijn-lijfhuis verblijven.
* mensen met een verstandelijke handicap.

Ja/nee + toelichting

**Bijlage 3: Inlichtingen om incidenten (waaronder Datalekken) te beoordelen, ter uitwerking van art. 6, lid 1 en 5.**

De verwerker zal alle inlichtingen verschaffen die de verwerkingsverantwoordelijke noodzakelijk acht om het incident te kunnen beoordelen. Daarbij verschaft verwerker in ieder geval de volgende informatie aan de verwerkingsverantwoordelijke:

* wat de (vermeende) oorzaak is van de inbreuk;
* wat het (vooralsnog bekende en/of te verwachten) gevolg is;
* wat de (voorgestelde) oplossing is;
* contactgegevens voor de opvolging van de melding;
* aantal personen waarvan gegevens betrokken zijn bij de inbreuk (indien geen exact aantal bekend is: het minimale en maximale aantal personen waarvan gegevens betrokken zijn bij de inbreuk);
* een omschrijving van de groep personen van wie gegevens betrokken zijn bij de inbreuk;
* het soort of de soorten persoonsgegevens die betrokken zijn bij de inbreuk;
* de datum waarop de inbreuk heeft plaatsgevonden (indien geen exacte datum bekend is: de periode waarbinnen de inbreuk heeft plaatsgevonden);
* de datum en het tijdstip waarop de inbreuk bekend is geworden bij verwerker of bij een door hem ingeschakelde derde of onderaannemer;
* of de gegevens versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk zijn gemaakt voor onbevoegden;
* wat de reeds ondernomen maatregelen zijn om de inbreuk te beëindigen en om de gevolgen van de inbreuk te beperken.

**Bijlage 4:** **Toelichting: Maatregelen op basis van de BIG ten aanzien van een verwerker art. 7.1.**

| **BIG Nummer** | **titel** | **Maatregel verwerker** | **SaaS** | **PaaS** | **IaaS** | **Applicatie beheer** | **Technisch/ database beheer** | **Helpdesk** | **Berichten verkeer** | **Archief beheer** | **Vernietiging van gegevensdragers** | **Lease MFP** | **Inhoudelijk proces** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 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: • 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. |  |  |  |  |  |  |  |  |  |  |  |
| 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 | Een logregel bevat minimaal: • 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 | De volgende gebeurtenissen worden in ieder geval opgenomen in de logging: • 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 logestanden | Logbestanden worden zodanig beschermd dat deze niet aangepast of gemanipuleerd kunnen worden. |  |  |  |  |  |  |  |  |  |  |  |
| 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 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 inconsistentievan 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) |  |  |  |  |  |  |  |  |  |  |  |
| 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. |  |  |  |  |  |  |  |  |  |  |  |

Bijlage 5: Omschrijving werkzaamheden ter uitwerking van artikel 8 lid 5.

Verwerker maakt bij de uitvoering van de verwerkersovereenkomst gebruik van de derden/onderaannemers die in deze bijlage zijn vermeld. De verwerker zal deze bijlage conform artikel 8 van deze verwerkersovereenkomst bijwerken indien er wijzigingen plaatsvinden in de ingeschakelde derden/onderaannemers en deze lijst onverwijld ter beschikking stellen aan de verwerkingsverantwoordelijke.

|  |  |
| --- | --- |
| [PARTIJ 1] | |
| Vestigingsplaats: |  |
| Inschrijvingsnummer handelsregister: |  |
| Beschrijving van de werkzaamheden: |  |
| Voorwaarden van de verwerkingsverantwoordelijke gesteld aan toestemming: |  |

|  |  |
| --- | --- |
| [PARTIJ 2] | |
| Vestigingsplaats: |  |
| Inschrijvingsnummer handelsregister: |  |
| Beschrijving van de werkzaamheden: |  |
| Voorwaarden van de verwerkingsverantwoordelijke gesteld aan toestemming: |  |

**Bijlage 6: Gegevenschermingseffectbeoordeling**

Indien naar mening van verwerkingsverantwoordelijke een gegevenschermings-effectbeoordeling moet worden doorgevoerd verstrekt de verwerker zo snel mogelijk de volgende informatie aan de verwerkingsverantwoordelijke:

(i) Een systematische beschrijving van de beoogde verwerkingen;

(ii) Een beoordeling van de noodzaak en evenredigheid van de verwerkingen met betrekking tot de doeleinden opgenomen in de Dienstverleningsovereenkomst;

(iii) Een beoordeling van de risico’s voor de rechten en vrijheden van de betrokkene(n);

(iv) De beoogde maatregelen om de risico’s aan te pakken, waaronder waarborgen, veiligheidsmaatregelen en mechanismen om de bescherming van persoonsgegevens te garanderen en om aan te tonen dat voldaan is aan de AVG. Hierbij wordt rekening gehouden met de rechten en gerechtvaardigde belangen van de betrokkene(n) en andere personen in kwestie.