

Instructie:

- Voor zover teksten '<OPTIONEEL>' zijn is dat aangegeven in de tekst.
- Bij teksten waar 'OF' tussen de bepalingen in staat, dient een keuze tussen de verschillende opties gemaakt te worden. De overige optie(s) verwijderen uit de overeenkomst.
- Deze Verwerkersovereenkomst vormt een onlosmakelijk geheel met een op de ARVODI-2025 gebaseerde Overeenkomst en kan derhalve alleen in combinatie daarmee worden gesloten. Bepalingen over geheimhouding, aansprakelijkheid e.d. die in de Overeenkomst zijn vastgelegd, hoeven derhalve niet nog eens afzonderlijk in de Verwerkersovereenkomst te worden opgenomen. Zie voor meer informatie de Toelichting bij het gebruik van het Model Verwerkersovereenkomst ARVODI (te vinden op Rijksportaal).

N.B. Bij gebruik van de overeenkomst, deze instructie verwijderen.

Datumversie: maart 2025

Verwerkersovereenkomst ARVODI-2025

Contractnummer: [...].

De ondergetekenden:

1. De Staat der Nederlanden, waarvan de zetel is gevestigd te Den Haag, hierbij vertegenwoordigd door **de Minister van/voor/ Staatssecretaris van Onderwijs, Cultuur en Wetenschap,** namens deze, **[functie en naam ondertekenaar]** hierna te noemen: OCW of Verwerkingsverantwoordelijke,

en

2. **[volledige naam en rechtsvorm Opdrachtnemer]**, (statutair) gevestigd te [...], hierbij vertegenwoordigd door **[naam ondertekenaar]** hierna te noemen: Opdrachtnemer,

hierna gezamenlijk te noemen: Partijen;

OVERWEGENDE DAT:

- Partijen hebben op **[datum]** de Overeenkomst **[titel]** met betrekking tot **[korte omschrijving van de Overeenkomst]** gesloten;
- voor zover Opdrachtnemer Persoonsgegevens Verwerkt in het kader van de Overeenkomst, Opdrachtnemer als verwerker kwalificeert en OCW als Verwerkingsverantwoordelijke voor de Verwerking van Persoonsgegevens krachtens artikel 4, onderdeel 7 en onderdeel 8, van de Verordening;
- Partijen in deze Verwerkersovereenkomst, zoals bedoeld in artikel 28, derde lid, van de Verordening, hun afspraken over de Verwerking van Persoonsgegevens door Opdrachtnemer wensen vast te leggen.

KOMEN OVEREEN:

Instructie Artikel 1

- Met 'Overeenkomst' (artikel 1.6) wordt de hoofdovereenkomst bedoeld, waarin NWO, OCW en Opdrachtnemer hun afspraken hebben vastgelegd over de reikwijdte en uitvoer van de Opdracht.

Artikel 1. Begrippen

In deze Verwerkersovereenkomst wordt een aantal begrippen met een beginhoofdletter gebruikt. Aan deze begrippen komt de betekenis toe die hieraan wordt gegeven in de ARVODI-2025 of de Verordening, met dien verstande dat een aantal begrippen op de Verwerkersovereenkomst zijn toegespitst. Aldus en in aanvulling daarop wordt onder de volgende begrippen, ongeacht of ze in meervoud of enkelvoud, of als werkwoord of zelfstandig naamwoord worden gebruikt, in deze Verwerkersovereenkomst verstaan:

- 1.1 ARVODI-2025: Algemene Rijksvoorwaarden voor het verstrekken van opdrachten tot het uitvoeren van Diensten 2025.
- 1.2 Betrokkene: degene op wie een Persoonsgegevens betrekking heeft.
- 1.3 EER: Europese Economische Ruimte, zijnde alle EU-landen plus Liechtenstein, Noorwegen en IJsland.
- 1.4 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.
- 1.5 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. Overheidsinstanties die mogelijk Persoonsgegevens ontvangen in het kader van een bijzonder onderzoek overeenkomstig het Unierecht of het lidstatelijke recht gelden echter niet als Ontvangers; de Verwerking van die gegevens door die overheidsinstanties strookt met de gegevensbeschermingsregels die op het betreffende verwerkingsdoel van toepassing zijn.
- 1.5 Opdrachtgever: De Nederlandse Organisatie voor Wetenschappelijk Onderzoek, ten behoeve van haar onderdeel het Nationaal Kennisinstituut Onderwijs, statutair gevestigd aan de Laan van Nieuw Oost-Indië 300, 2593 CE te Den Haag, Kamer van Koophandel nummer 27367015
- 1.6 Overeenkomst: de overeenkomst tussen Opdrachtgever, Opdrachtnemer en OCW, inzake [titel] van [datum], met kenmerk [kenmerk].
- 1.7 Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon, die Opdrachtnemer in het kader van de Overeenkomst ten behoeve van OCW Verwerkt.
- 1.8 Toeziethoudende autoriteit: een door een lidstaat ingevolge artikel 51 van de Verordening ingestelde onafhankelijke overheidsinstantie.
- 1.9 Verordening: Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van de Richtlijn 95/46/EG (algemene verordening gegevensbescherming).
- 1.10 Verwerker: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de Verwerkingsverantwoordelijke Persoonsgegevens Verwerkt.
- 1.11 Verwerkersovereenkomst: deze overeenkomst inclusief overwegingen en bijbehorende bijlagen.

- 1.12 Verwerking: een bewerking of een geheel van bewerkingen in het kader van de Overeenkomst met betrekking tot Persoonsgegevens, of een geheel van Persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.
- 1.13 Verwerkingsverantwoordelijke: de Minister van/voor/Staatssecretaris van Onderwijs, Cultuur en Wetenschap.

Artikel 2. Voorwerp van deze Verwerkersovereenkomst

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

Artikel 3. Inwerkingtreding en duur

- 3.1 Deze Verwerkersovereenkomst treedt in werking op het moment waarop deze door Partijen is ondertekend.
- 3.2 Deze Verwerkersovereenkomst eindigt nadat Opdrachtnemer alle Persoonsgegevens heeft gewist, terugbezorgd en bestaande kopieën heeft verwijderd met inachtneming van artikel 10 van deze Verwerkersovereenkomst.
- 3.3 Deze Verwerkersovereenkomst is niet tussentijds opzegbaar.

Artikel 4. Omvang verwerkingsbevoegdheid Opdrachtnemer

- 4.1 Opdrachtnemer Verwerkt de Persoonsgegevens uitsluitend in opdracht en op basis van schriftelijke instructies van OCW, tenzij een op Opdrachtnemer van toepassing zijnde wettelijk voorschrift hem tot Verwerking verplicht. In dat geval stelt Opdrachtnemer OCW voorafgaand aan de Verwerking in kennis van dat wettelijk voorschrift, tenzij dat wettelijk voorschrift deze kennisgeving om gewichtige redenen van algemeen belang verbiedt.
- 4.2 Opdrachtnemer heeft geen zeggenschap over het doel van en de middelen voor de Verwerking als bedoeld in de Verordening.

Artikel 5. Beveiliging van de Verwerking

- 5.1 Onverminderd artikel 2.3 van deze Verwerkersovereenkomst treft Opdrachtnemer de technische en organisatorische beveiligingsmaatregelen zoals beschreven in Bijlage 2.
- 5.2 Partijen erkennen dat het waarborgen van een passend beveiligingsniveau voortdurend kan dwingen tot het treffen van aanvullende beveiligingsmaatregelen. Opdrachtnemer waarborgt een op het risico afgestemd beveiligingsniveau.
- 5.3 Opdrachtnemer geeft op verzoek van Opdrachtgever en OCW inzicht in de getroffen beveiligingsmaatregelen.
- 5.4 Voor zover OCW daarom uitdrukkelijk schriftelijk verzoekt, treft Opdrachtnemer aanvullende maatregelen met het oog op de beveiliging van de Persoonsgegevens.

- 5.5 Opdrachtnemer Verwerkt Persoonsgegevens niet buiten de EER, tenzij hij daarvoor uitdrukkelijk schriftelijk toestemming, zo nodig voorzien van nadere voorwaarden, heeft verkregen van OCW en behoudens afwijkende wettelijke verplichtingen.
- 5.6 Opdrachtnemer informeert OCW zonder onredelijke vertraging zodra hij kennis heeft genomen van onrechtmatige Verwerkingen van Persoonsgegevens of tekortschieten (in de naleving van) technische en organisatorische beveiligingsmaatregelen zoals bedoeld in het eerste en tweede lid.
- 5.7 Opdrachtnemer verleent OCW bijstand bij het doen nakomen van de verplichtingen uit hoofde van de artikelen 32 tot en met 36 van de Verordening.

Artikel 6. Geheimhouding door Personeel van Opdrachtnemer

- 6.1 De Persoonsgegevens hebben een vertrouwelijk karakter als bedoeld in artikel 11.1 van de ARVODI-2025.
- 6.2 Opdrachtnemer waarborgt dat zijn Personeel zich ertoe heeft verbonden vertrouwelijkheid in acht te nemen als bedoeld in artikel 11.2 van de ARVODI-2025.

Artikel 7. Subverwerker

Wanneer Opdrachtnemer, met inachtneming van het bepaalde in artikel 6 van de ARVODI-2025, een andere Verwerker inschakelt om namens OCW verwerkingsactiviteiten te verrichten, worden aan deze andere Verwerker bij een overeenkomst dezelfde verplichtingen inzake gegevensbescherming opgelegd als die welke in deze Verwerkersovereenkomst zijn opgenomen.

Artikel 8. Bijstand vanwege rechten van Betrokkene

- 8.1 Voor zover mogelijk en rekening houdend met de aard van de Verwerking door middel van passende technische en organisatorische maatregelen, verleent Opdrachtnemer OCW bijstand bij het vervullen van diens plicht om verzoeken om uitoefening van de in hoofdstuk III van de Verordening vastgelegde rechten van de Betrokkene te beantwoorden.
- 8.2 Partijen dragen elk de door henzelf in verband met de in het eerste lid te maken kosten.
- 8.3 Opdrachtnemer stuurt een verzoek vanuit een Betrokkene zo spoedig mogelijk aan OCW.

Artikel 9. Inbreuk in verband met Persoonsgegevens

- 9.1 Opdrachtnemer informeert OCW zonder onredelijke vertraging, zodra hij kennis heeft genomen van een Inbreuk in verband met Persoonsgegevens, overeenkomstig de afspraken zoals vastgelegd in Bijlage 3.
- 9.2 Opdrachtnemer informeert OCW ook na een melding op grond van het eerste lid over ontwikkelingen betreffende de Inbreuk in verband met Persoonsgegevens.
- 9.3 Partijen dragen elk de door henzelf te maken kosten gerelateerd aan de Inbreuk in verband met Persoonsgegevens.

Artikel 10. Terugbezorgen of wissen Persoonsgegevens

- 10.1 Na afloop van de Overeenkomst, of zoveel eerder als overeengekomen, draagt Opdrachtnemer er zorg voor dat hij, naar gelang de keuze van OCW, alle Persoonsgegevens wist of terugbezorgt aan OCW en bestaande kopieën verwijdt, tenzij opslag van de Persoonsgegevens op basis van een wettelijk voorschrift verplicht is. **<OPTIONEEL>** In geval van wissen en/of verwijderen van kopieën door Opdrachtnemer informeert hij OCW zodra hij dit heeft gedaan.
- 10.2 Partijen kunnen voor afzonderlijke of categorieën Persoonsgegevens bewaartermijnen overeenkomen. Na afloop van de overeengekomen bewaartermijn draagt Opdrachtnemer

zorg voor het wissen of terugbezorgen en het verwijderen van kopieën van de betreffende Persoonsgegevens, tenzij opslag van deze Persoonsgegevens op basis van een wettelijk voorschrift verplicht is.

- 10.3 **<OPTIONEEL>** Opdrachtnemer [wist of bezorgt terug] de Persoonsgegevens binnen [aantal] [dagen/weken] na afloop van de Overeenkomst, of zoveel eerder als overeengekomen, bij gebreke waarvan Opdrachtnemer een boete verschuldigd is van €[...] per dag, met een maximum van €[...]. Betaling van de boete laat de verplichtingen uit artikel 10 en de gehoudenheid van Opdrachtnemer om de schade die het gevolg is van de schending te vergoeden onverlet.
- 10.4 **<OPTIONEEL>** Persoonsgegevens worden in de door OCW aangegeven vorm en op de door OCW aangegeven wijze terugbezorgd.

OF

- 10.4 **<OPTIONEEL>** De Persoonsgegevens worden als volgt terugbezorgd: [bestandsformaat] [wijze van terugbezorging inclusief vermelding beveiligingsmaatregelen] [adres].

Artikel 11. Informatieverplichting en audit

- 11.1 Opdrachtnemer stelt alle informatie ter beschikking die nodig is om aan te tonen dat de verplichtingen uit deze Verwerkersovereenkomst zijn en worden nagekomen.
- 11.2 OCW kan een audit van de onder deze Verwerkersovereenkomst vallende verwerkingsactiviteiten (laten) uitvoeren als concrete omstandigheden daartoe aanleiding geven. Opdrachtnemer verleent alle medewerking aan audits, waaronder begrepen audits bij Personeel van Opdrachtnemer, tenzij dit redelijkerwijs niet van hem kan worden verwacht.
- 11.3 Opdrachtnemer stelt OCW onmiddellijk in kennis indien naar zijn mening een instructie van OCW in het kader van artikel 11 eerste en/of tweede lid van deze Verwerkersovereenkomst, inbreuk oplevert met een wettelijk voorschrift inzake gegevensbescherming.
- 11.4 Partijen dragen zelf de kosten die zij maken in verband met de in dit artikel bedoelde informatieverstrekking en audits, waaronder begrepen de kosten van door hen ingeschakelde derden.
- 11.5 OCW is te allen tijde bevoegd om naar aanleiding van de op grond van dit artikel verkregen informatie nadere maatregelen voor te stellen. Opdrachtnemer is gehouden aan die maatregelen in redelijkheid uitvoering te geven.

Den Haag, [datum]

[Plaats], [datum]

DE MINISTER VAN/
/ STAATSSECRETARIS VAN ONDERWIJS,
CULTUUR EN WETENSCHAP

namens deze,
[ondertekenaar]

[naam ondertekenaar]

[naam ondertekenaar]

CONCEPT

Bijlage 1. De Verwerking van Persoonsgegevens

Instructie:

Voor de inhoud van deze bijlage kan onder meer gebruik worden gemaakt van de registratie die de Verwerkingsverantwoordelijke op grond van artikel 30 van de Verordening dient aan te houden.

N.B. bij gebruik van de bijlage, deze en de instructieteksten in grijs verwijderen.

Algemene instructie Bijlage 1

- Bijlage 1 is een nadere uitwerking van Artikel 2 van de Verwerkersovereenkomst, en is een verplichte bijlage.
- Bijlage 1 bepaalt welke Persoonsgegevens Opdrachtnemer mag verwerken en wat Opdrachtnemer er mee mag doen. Deze bijlage dient dus zo correct en volledig mogelijk te worden ingevuld, waar nodig in overleg met Opdrachtnemer.
- Op grond van de AVG heeft OCW de plicht tot **dataminimalisatie**. Dit betekent dat Opdrachtnemer absoluut niet meer Persoonsgegevens mag verwerken en niet meer met de Persoonsgegevens mag doen dan **strikt noodzakelijk** is voor het uitvoeren van de Opdracht.

Instructie De aard en het doel van de Verwerking

- Hier moet zo specifiek en concreet mogelijk worden toegelicht op welke wijze Opdrachtnemer de Persoonsgegevens zal gaan verwerken. Onder 'verwerken' wordt verstaan elke handeling die met de Persoonsgegevens wordt uitgevoerd. Het gaat hier dus niet om een omschrijving van de Opdracht zelf, maar om wat voor acties Opdrachtnemer precies gaat uitvoeren met de Persoonsgegevens.
- Veel voorkomende voorbeelden van verwerkingshandelingen zijn: verzamelen, vastleggen, opslaan, wijzigen, opvragen, raadplegen, verstrekken, wissen, pseudonimiseren/anonimiseren etc.
- Vervolgens moet worden toegelicht ten behoeve van welk(e) doel(en) Opdrachtnemer de persoonsgegevensverwerkingen uitvoert. Hieruit moet blijken waarom de beschreven verwerkingshandelingen **noodzakelijk** zijn om het/de beoogde doel(en) te bereiken.

De aard en het doel van de Verwerking

[...]

Instructie De rechtsgrondslag voor de Verwerking

- OCW heeft een juridische basis nodig om de beoogde persoonsgegevensverwerkingen uit te mogen voeren (of Opdrachtnemer daar opdracht toe te geven). Dit is de rechtsgrondslag. Zonder rechtsgrondslag is het OCW noch Opdrachtnemer toegestaan om de Persoonsgegevens ten behoeve van het beoogde doel te verwerken.
- De AVG kent een limitatieve lijst van zes rechtsgrondslagen:
 1. De verwerking is noodzakelijk om de publieke taak van OCW te kunnen uitvoeren.
 2. De verwerking is noodzakelijk om te voldoen aan een wettelijke plicht die op OCW rust.
 3. OCW heeft toestemming van de Betrokkenen om hun persoonsgegevens ten behoeve van het hiervoor beschreven doel te verwerken.
 4. De verwerking is noodzakelijk om een overeenkomst met de Betrokkene (dus niet met Opdrachtnemer!) te kunnen uitvoeren
 5. OCW heeft een gerechtvaardigd belang dat de verwerking nodig maakt en dat zwaarder weegt dan de privacy van de Betrokkenen
 6. De verwerking is noodzakelijk ter bescherming van iemands levensbelang.
- Kies welke van de bovenstaande rechtsgrondslagen in dit geval van toepassing is/zijn en leg uit waarom. OCW zal zich **veelal enkel op rechtsgrondslag 1, 2 of 3 kunnen** beroepen.

De rechtsgrondslag voor de Verwerking

[...]

Instructie Categorieën Betrokkenen en Persoonsgegevens

- In onderstaand veld dient in de linkerkolom een volledige opsomming te worden gegeven van welke personen Opdrachtnemer gegevens zal gaan verwerken (de 'Betrokkenen'). Geef vervolgens per categorie Betrokkene in de rechterkolom een opsomming van de Persoonsgegevens die Opdrachtnemer van die Betrokkenen gaat verwerken.
- Bedenk per persoonsgegeven goed of kan worden beargumenteerd dat verwerking van dit persoonsgegeven strikt noodzakelijk is voor het uitvoeren van de Opdracht. Zo niet, dan is verwerking van dit persoonsgegeven enkel toegestaan met expliciete toestemming van de Betrokkene.
- Een 'persoonsgegeven' is dat iets zegt over een identificeerbare natuurlijke persoon, zoals NAW-gegevens, contactgegevens, geboortedatum, loopbaaninformatie, BSN-nummer, IBAN, kopie paspoort etc. Ook op zichzelf anonieme gegevens die in combinatie met bijvoorbeeld NAW-gegevens iets zeggen over een natuurlijke personen moeten worden aangemerkt als persoonsgegevens.
- De verwerking van 'bijzondere persoonsgegevens' (gegevens over ras of etnische afkomst, politieke, religieuze of levensbeschouwelijke opvattingen, genetische en biometrische gegevens, gegevens over gezondheid, seksuele gerichtheid en gegevens van strafrechtelijke aard) is in beginsel verboden. Indien wordt beoogd dit soort gegevens te gaan verwerken, neem dan contact op met JZ via Topdesk (optie 'privacy vraag' onder tegel 'Privacy & security').

Categorieën Betrokkenen	Categorieën Persoonsgegevens
1. [...]	[...]
2. [...]	[...]
3. [...]	[...]

Instructie Subverwerkers

- Subverwerkers zijn alle externe partijen die Opdrachtnemer inschakelt om (een deel van) de persoonsgegevensverwerkingen uit te voeren. Zo zal bijvoorbeeld ook een cloudleverancier van Opdrachtnemer in onderstaand overzicht moeten worden vermeld als subverwerker, indien bovengenoemde persoonsgegevens op diens servers worden opgeslagen.
- In onderstaand veld dient een keuze te worden gemaakt tussen drie opties. OCW kan kiezen tussen de mogelijkheid om Opdrachtnemer **algemene toestemming** te geven voor het inschakelen van subverwerkers of om alleen **specifieke toestemming** te geven voor het gebruik van de daaronder opgesomde subverwerkers. In beide gevallen moet in onderstaand veld een volledige opsomming worden gegeven van alle subverwerkers die Opdrachtnemer inschakelt. Bij specifieke toestemming heeft Opdrachtnemer eerst expliciete schriftelijke toestemming nodig van OCW om de ingeschakelde subverwerkers te kunnen wijzigen. In geval van algemene toestemming hoeft Opdrachtnemer enkel NWO over een wijziging van subverwerkers te informeren. OCW kan er ook voor kiezen om Opdrachtnemer geen toestemming te geven voor het inschakelen van subverwerkers.
- Toestemming voor het inschakelen van een subverwerker gevestigd buiten de Europese Economische Ruimte is uitsluitend toegestaan na afstemming met privacy@minocw.nl. Er wordt geadviseerd om in dat geval eerst met Opdrachtnemer alternatieven binnen de EER te verkennen.

Subverwerkers

OCW verleent Opdrachtnemer **geen toestemming/algemene toestemming/specifieke toestemming** voor het inschakelen van subverwerkers.

Naam subverwerker	Persoonsgegevens die worden verwerkt	Verwerkings-handelingen	Land van verwerking	Vestigingsland subverwerker

Instructie Ontvangers

- In onderstaand veld moet worden ingevuld met welke derde (externe) partijen ('ontvangers') het Opdrachtnemer is toegestaan persoonsgegevens te delen. Dit kan Opdrachtnemer namelijk in beginsel alleen doen met expliciete

toestemming van OCW. OCW kan die toestemming alleen geven als er voor de doorgifte een rechtsgrondslag is.

- Toestemming voor het verstrekken van persoonsgegevens aan ontvangers gevestigd buiten de Europese Economische Ruimte is uitsluitend toegestaan na afstemming met privacy@minocw.nl.
- De passage “aan de volgende partijen” moet worden verwijderd indien wordt gekozen voor de optie ‘geen toestemming’.
- Onder ‘doorgiftemechanisme’ dient te worden gespecificeerd op welke wijze de doorgifte plaatsvindt. De doorgifte is alleen toegestaan indien de doorgifte met voldoende beveiligingsmaatregelen is omkleed.

Ontvangers

OCW verleent Opdrachtnemer **geen toestemming/specifieke toestemming** voor doorgifte van Persoonsgegevens **aan de volgende partijen**:

Naam ontvangende partij	Persoonsgegevens die worden verstrekt	Doeleinden van de doorgifte	Doorgifte-mechanisme	Vestigingsland ontvanger

Bijlage 2. Passende technische en organisatorische maatregelen

In deze bijlage moeten de normen en maatregelen die Opdrachtnemer in het kader van de beveiliging van de Verwerking moet hanteren respectievelijk treffen worden gespecificeerd. Hiervoor kan worden verwezen naar documenten waarin normen en maatregelen zijn vastgelegd, zoals in voorkomend geval het programma van eisen of de offerteaanvraag.

Algemene instructie Bijlage 2

- Bijlage 2 is een nadere uitwerking van Artikel 5 van de Verwerkersovereenkomst, en is een verplichte bijlage.
- Bijlage 2 dient in afstemming met Opdrachtnemer te worden ingevuld. In deze bijlage moeten de normen en maatregelen worden gespecificeerd die Opdrachtnemer hanteert ter beveiliging van de Verwerking. OCW mag alleen Opdrachtnemers inschakelen die een beveiligingsniveau (kunnen) garanderen dat passend is voor de beoogde persoonsgegevensverwerkingen.
- De Opdrachtnemer dient te verklaren volgens welke norm diens beveiligingsmaatregelen zijn ingericht. Vink aan welke situatie voor Opdrachtnemer van toepassing is. Daarnaast dient de Opdrachtnemer de beveiligingsmaatregelen nader toe te lichten. Uit de certificering/periodieke externe controles/audits of uit de eigen controles/beschrijvingen blijkt of kan worden afgeleid dat de beveiliging passend is bij de verwerking(en) genoemd in Bijlage 1.
- Er kan worden verwezen naar documenten waarin normen en maatregelen zijn vastgelegd, zoals bijvoorbeeld het programma van eisen of de offerteaanvraag. Verwijzingen naar weblinks (bijvoorbeeld naar de website van de Opdrachtnemer) dienen te worden vermeden, omdat deze aan verandering onderhevig zijn.

Opdrachtnemer dient bij onderdeel I, II en III aan te geven hoe de technische en organisatorische maatregelen zijn ingericht.

I. Verklaring passende technische en organisatorische maatregelen

☐ Opdrachtnemer werkt volgens een algemeen erkende norm voor informatiebeveiliging en is volgens deze norm <<wel / niet >> gecertificeerd, te weten:

[vermeld normenstelsel, zoals bijvoorbeeld NEN7510, NEN/ISO 27001, PCI/DSS]

Datum laatste certificering:

☐ Opdrachtnemer werkt volgens een algemeen erkende overheidsnorm zoals de BIO, of vergelijkbaar, [vermeld normenstelsel]

☐ Opdrachtnemer werkt volgens een algemeen andere norm, te weten:

[vermeld normenstelsel]

II. Toereikendheid van de technische en organisatorische maatregelen

De door Opdrachtnemer genomen technische en organisatorische maatregelen

De toereikendheid van de informatiebeveiliging blijkt uit het volgende:

- ☐ Opdrachtnemer verstrekt een actueel en geldig certificaat en verklaring van toepasselijkheid (VVT);
- ☐ Rapportages van periodieke externe controles zoals audits, pentesten of TPM's (bijv. ISAE3xxx SOC type II);
- ☐ Een assurance rapport (TPM) van een auditor die is aangesloten bij NOREA;
- ☐ Eigen controles of eigen mededelingen over de beveiligingsmaatregelen zoals hieronder beschreven:

LET OP: Uit de certificering/periodieke externe controles/audits of uit de eigen controles/beschrijvingen blijkt of kan worden afgeleid dat de beveiliging passend is bij de verwerking(en) genoemd in Bijlage 1.

III. Verklaring Aansluiting bij goedgekeurde gedragscode

☐ Opdrachtnemer is aangesloten bij een door een toezichthoudende autoriteit goedgekeurde gedragscode, te weten:

[vermeld sector, gedragscode, datum goedkeuring toezichthoudende autoriteit en naam toezichthoudende autoriteit]

☐ Opdrachtnemer is niet aangesloten bij een door een toezichthoudende autoriteit goedgekeurde gedragscode.

LET OP: Substantiële wijzigingen in het bovenstaande en achteruitgang van de voorwaarden geeft Opdrachtnemer op korte termijn aan OCW door.

IV. Beschrijving van de beveiligingsmaatregelen

Hoofdonderwerpen	Toelichting op concrete maatregelen (aan de hand van onderstaande suggesties)
Informatiebeveiligingsbeleid (fysiek en digitaal)	Actueel en vastgesteld IB-beleid Goedkeuringsniveau Het IB-beleid is van toepassing op de volledige organisatie dan wel specifiek dit domein Back-up -beleid en business continuïteits-beleid?
Toegangsbeveiliging	Toegangsminimalisatie Toegangsbeheer Toegangscontrole & bewijsvoering
Personele aspecten	Bewustwordingsbeleid. Integriteitsbeleid Rollen en verantwoordelijkheden Screening VOG Geheimhouding Training informatiebeveiliging
Privacy enhancing technologies	Cryptologie /cryptografiebeleid pseudonimisering anonimisering
Veilige apparatuur en verantwoord databeheer	Hardening Disposal
Life cycle management	Terugbezorgen / wissen / verwijderen van bestaande (kopieën van) persoonsgegevens Back-ups Beveiliging in elke fase van de verwerking (verzending, opslag, etc.)
Risico & Beveiligingsincident management	Verantwoordelijkheden en procedures Rapportages Opvolging incidenten
Rapportages & toezicht	Logging en monitoring Interne controle/ in control-verklaring Of externe audits Periodieke overleggen tussen OCW en Opdrachtnemer waarbij naleving van de privacy & informatiebeveiligingsafspraken en eventuele incidenten standaard op de agenda staat.

Bijlage 3: Afspraken betreffende Inbreuken in verband met Persoonsgegevens (waaronder datalekken)

Algemene instructie Bijlage 3

- Bijlage 3 is een nadere uitwerking van Artikel 9.1 van de Verwerkersovereenkomst, en is een verplichte bijlage.
- Bijlage 3 schrijft voor hoe Opdrachtnemer OCW informeert over Inbreuken in verband met Persoonsgegevens (ook wel datalekken), en welke informatie Opdrachtnemer OCW ten minste moet verstrekken.

Procedure

Opdrachtnemer stelt OCW zonder onredelijke vertraging en uiterlijk binnen 24 uur na kennisneming over (een redelijk vermoeden van) een Inbreuk in verband met Persoonsgegevens. Opdrachtnemer informeert OCW via de contactpersoon en de contactgegevens van OCW zoals vermeld met meldpuntdatalekken@minocw.nl in de cc. Opdrachtnemer vermeld daarbij voor zover mogelijk de onderstaande informatie. Opdrachtnemer garandeert dat de verstrekte informatie volledig, correct en accuraat is.

Zie verder: Zie pdf, bijlage "Bijlage 3 bij VWOK -Procesbeschrijving Melden afhandelen en oplossen datalek".

Informatie die ten minste door Opdrachtnemer moet worden verstrekt

Datum en tijdstip van de constatering van de (vermoedelijke) Inbreuk in verband met Persoonsgegevens
Aard van de Inbreuk in verband met Persoonsgegevens
De soort, categorieën en het aantal Persoonsgegevens en Betrokkene
Waarschijnlijke gevolgen van de Inbreuk in verband met Persoonsgegevens
Maatregelen die Opdrachtnemer heeft voorgesteld of genomen om de Inbreuk in verband met Persoonsgegevens aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan