Bijlage IV bij de Overeenkomst tot levering van Voorziening E-Publicatie door <leverancier> aan UWV

Beveiligings- en verwerkersovereenkomst (BVO)

<Opdrachtnemersnaam> en UWV

Versie:	4.0
Status:	Definitief
Datum:	14 juli 2020

Structuur van de Beveiligings- en verwerkersovereenkomst

UWV stuurt op veilig gebruik van gegevens en een betrouwbare informatievoorziening, gebaseerd op IB&P wet en regelgeving en UWV Beleidskaders. Wanneer leveranciers een Dienst leveren aan UWV, dienen zij te ervoor te zorgen dat UWV aan Informatiebeveiligings- en privacybeschermingswet en -regeling kan voldoen die op UWV van toepassing zijn. Daarom maken UWV en de leverancier afspraken, om Informatiebeveiliging en privacybescherming te borgen ten aanzien van de te leveren Dienst. Deze afspraken worden vastgelegd in een Beveiligings- en verwerkersovereenkomst (BVO), dat onderdeel is van de Overeenkomst met de leverancier. Voor iedere Overeenkomst – dient de BVO aangepast te worden aan de specifieke omstandigheden die voor de Overeenkomst van toepassing zijn.

De Beveiligings- en verwerkersovereenkomst bestaat uit vier secties. Deze secties zijn de volgende:

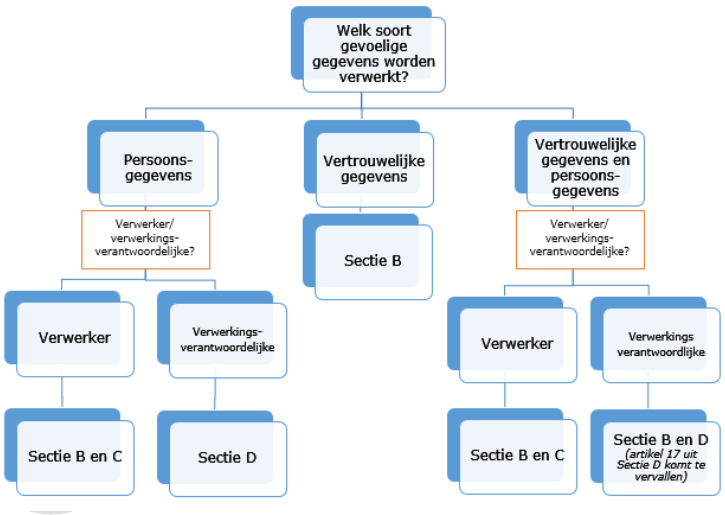
- Sectie A: Algemene bepalingen
- Sectie B: Bepalingen ten aanzien van de Beveiliging
- Sectie C: Bepalingen ten aanzien van de Verwerker
- Sectie D: Bepalingen ten aanzien van de Verwerkingsverantwoordelijke

Sectie A is te allen tijde van toepassing. In hoeverre Sectie B wordt toegepast, is afhankelijk van:

- De aard van de gegevens die verwerkt worden bij het leveren van de Dienst (Persoonsgegevens, Vertrouwelijke gegevens anders dan Persoonsgegevens[1] of beiden)
- En de relatie tussen Leverancier en UWV (Verwerkers of Verwerkingsverantwoordelijke)

Sectie C en D zijn niet van toepassing voor de aanbesteding Voorziening E-Publicatie.

Onderstaande beslisboom kan gevolg worden voor het bepalen welke secties worden toegepast in de BVO:



Sectie B – ofwel de bepalingen ten aanzien van Beveiliging – bestaat uit een Algemene en Bijzondere Bepalingen. Van de Algemene Bepalingen kan worden gesteld dat deze in bijna alle gevallen van toepassing zullen zijn. De Bijzondere Bepalingen zijn specifiek voor het soort Dienst dat wordt afgenomen en is opgedeeld in bepalingen ten aanzien van:

- Beheer (geldt voor Diensten betreffende Software, Servers en Netwerken en Clouddiensten).
- Systemen
- Netwerken en Servers
- Clouddiensten

[1] Vertrouwelijke gegevens omvatten bedrijfsgevoelige gegevens zoals bijvoorbeeld financiële gegevens.

Inhoud

De Partijen:

1. Uitvoeringsinstituut werknemersverzekeringen (UWV), rechtspersoon naar de wet als bedoeld in artikel 2 Wet Structuur uitvoering werk en inkomen, gevestigd te Amsterdam,
   vertegenwoordigd door <….>, <functie>
   hierna te noemen: "Opdrachtgever",

en

2. "*Opdrachtnemersnaam*", gevestigd te "*plaatsnaam*",
   vertegenwoordigd door "*naam 1e vertegenwoordiger*", lid "*bestuursorgaan*",
   en *(voor zover van toepassing)* "*naam 2e vertegenwoordiger*", directeur "*afdelingsnaam*",
   hierna te noemen: "Opdrachtnemer"."

Middels deze BVO nemen Partijen het volgende in overweging

- Partijen hebben een Overeenkomst gesloten voor te leveren Diensten zoals beschreven in <definiëren in>.
- Opdrachtnemer is verwerker/verwerkingsverantwoordelijke (doorhalen wat niet van toepassing is)
- Partijen van deze BVO leggen afspraken vast betreffende de te nemen passende technische en organisatorische maatregelen om de beschikbaarheid, integriteit en vertrouwelijkheid van de gegevens en de bedrijfsvoering van Opdrachtgever te waarborgen.
- De Baseline Informatiebeveiliging Overheid is van toepassing en is op onderdelen nader uitgewerkt in deze BVO.

En komen het volgende overeen:

Sectie A: Algemene bepalingen

Artikel 1 Begripsbepalingen en onderliggende documenten

1. In deze BVO wordt een aantal begrippen met een beginhoofdletter gebruikt. Aan deze begrippen komt de betekenis toe die hieraan is gegeven in bijlage 1.
2. Van de BVO maken de volgende bijlagen deel uit:
    a. Begrippenkader
    b. Register verwerking
    c. Dienstenbeschrijving
    d. Beveiligingskader

Artikel 2 Looptijd

1. Deze BVO treedt in werking op de datum van ondertekening van Overeenkomst door contracterende partijen en loopt gedurende de gehele duur van de Dienst zoals gespecificeerd in de Overeenkomst. Jaarlijks vindt een evaluatie plaats op de actualiteit van deze BVO. Aan de hand van de evaluatie is Opdrachtgever gerechtigd deze BVO aan te passen. Partijen gaan bij een aanpassing van de BVO in overleg over de consequenties die de aangepaste BVO heeft op de Dienst.
2. Opdrachtnemer voert de onder de Overeenkomst overeengekomen Diensten uit conform de in/bij deze BVO vastgelegde afspraken.
3. De nietigheid van enige bepaling van deze BVO tast de geldigheid van de overige bepalingen niet aan.
4. Voorwaarden van deze BVO die naar hun aard bedoeld zijn om voort te duren, blijven naar hun strekking van kracht na beëindiging van de BVO.
5. In geval van strijdigheid tussen bepalingen van de BVO en de Overeenkomst, prevaleert de bepaling van de Overeenkomst, tenzij expliciet anders overeengekomen.
6. Partijen zijn niet gerechtigd zonder voorafgaande schriftelijke toestemming van de andere Partij de rechten en/of plichten voortvloeiende uit deze BVO aan een Derde over te dragen.
7. Aan het einde van de Overeenkomst of wanneer Opdrachtgever dit verzoekt, worden bedrijfsmiddelen van Opdrachtgever die aan Opdrachtnemer, zijn Personeel of Onderaannemers ter beschikking zijn of worden gesteld, geretourneerd.
8. Opdrachtnemer waarborgt dat bij de verwerking en opslag van gegevens, te allen tijde de bij de Opdrachtnemer opgeslagen gegevens kunnen worden overgedragen aan Opdrachtgever zodra deze daarom verzoekt.

Artikel 3 Onderaanneming

1. Indien Opdrachtnemer bij de uitvoering van een Overeenkomst, gebruik wil maken van een Onderaannemer, dan zal hij daartoe slechts bevoegd zijn na verkregen Schriftelijke toestemming van Opdrachtgever. De toestemming zal niet zonder redelijke grond worden geweigerd; Opdrachtgever is echter gerechtigd aan het verlenen van deze toestemming voorwaarden te verbinden dan wel deze in tijd te beperken.
2. Wanneer Opdrachtnemer een Onderaannemer inschakelt om ten behoeve van Opdrachtgever activiteiten te verrichten, legt bij een overeenkomst Opdrachtnemer aan deze Onderaannemer dezelfde verplichtingen inzake Beveiliging en gegevensverwerking op als die welke in deze BVO zijn opgenomen.

Artikel 4 Continuïteit en weerbaarheid van de Bedrijfskritische Processen van Opdrachtgever

Artikel 4.1 Toepasselijkheid van artikel 4

Artikel 4 is van toepassing wanneer Opdrachtnemer Diensten levert in het kader van Bedrijfskritische processen van Opdrachtgever. Opdrachtgever bepaalt wanneer er sprake is van een Bedrijfskritisch Proces.

Artikel 4.2 Het waarborgen van de continuïteit en weerbaarheid van Bedrijfskritische processen van Opdrachtgever

Opdrachtnemer zal de beschikbaarheid, integriteit en vertrouwelijkheid van de voor Bedrijfskritische processen benodigde gegevens waarborgen, opdat de continuïteit en weerbaarheid van de Bedrijfskritische processen niet in gevaar komt. Opdrachtnemer zal dit doen door het implementeren en gebruiken van adequate fraudepreventie en –opsporing voor de applicaties,

servers, endpoints en het netwerk. Dit is inclusief mechanismen om kwetsbaarheden te identificeren en het tijdig doorvoeren van security patches. Opdrachtnemer gebruikt vastgelegde procedures om de Vertrouwelijkheid en de integriteit van de voor Bedrijfskritische processen benodigde gegevens, software en andere bedrijfsmiddelen te waarborgen.

Artikel 4.3 Continuïteitsplan

1. Opdrachtnemer stelt na ondertekening van de Overeenkomst binnen de door Opdrachtgever gestelde termijn, in afstemming met Opdrachtgever een Continuïteitsplan op met betrekking tot de Diensten. In dit Continuïteitsplan worden de procedures zoals bedoeld in artikel 4.2, richtlijnen en maatregelen beschreven die de continuïteit van de Dienst borgen. Opdrachtnemer zorgt in afstemming met Opdrachtgever, dat dit plan actueel is en blijft. Beide partijen zorgen voor bekendheid van dit plan op alle niveaus in hun organisatie.

2. De beschrijving van de procedures zoals omschreven in artikel 4.2, omvat in ieder geval:
   a. Het doel van een procedure;
   b. De aanleiding om een procedure te starten en de frequentie van een uitvoering van een procedure;
   c. Contactmomenten en contactpersonen gedurende de procedure;
   d. Waar de procedure betrekking op heeft;
   e. De wijze waarop toezicht kan worden gehouden op en verantwoording kan worden afgelegd over de wijze waarop een procedure is gevolgd.

Artikel 5 Gebruik faciliteiten van Opdrachtgever op de fysieke locaties van Opdrachtgever

De Opdrachtnemer en zijn Personeel en Onderaannemers mogen de door Opdrachtgever ter beschikking gestelde faciliteiten van de Opdrachtgever uitsluitend gebruiken voor de Dienst aan Opdrachtgever. Zij zijn daarbij gehouden aan de Gedragscode UWV en andere beveiligingsmaatregelen en richtlijnen die gelden op de locatie van Opdrachtgever. Opdrachtgever zal Opdrachtnemer op de hoogte stellen van de Gedragscode en andere beveiligingsmaatregelen en richtlijnen.

Artikel 6 Audits

Artikel 6.1 Documentatie en administratie

1. Opdrachtnemer onderhoudt een volledige en nauwkeurige documentatie en administratie, die betrekking heeft op deze BVO. De documentatie en administratie bevatten voor Opdrachtgever informatie om een redelijke zekerheid te bieden dat Opdrachtnemer voldoet aan het gestelde in de BVO. De Opdrachtnemer bewaart deze documentatie en administratie gedurende de looptijd van de BVO.
2. Opdrachtnemer verstrekt op specifiek verzoek van Opdrachtgever (of haar gemachtigde vertegenwoordigers en waar nodig toezichthouders zoals de Autoriteit Persoonsgegevens) binnen een door Opdrachtgever gestelde redelijke termijn, toegang tot de gevraagde documentatie en administratie.
3. Opdrachtgever of haar gemachtigde vertegenwoordigers en waar nodig toezichthouders (zoals de Autoriteit Persoonsgegevens) kan informatie uit en kopieën van deze documentatie en administratie voor auditdoeleinden gebruiken. Het gebruik van deze gegevens is onderworpen aan de standaard praktijk ten aanzien van audits.

Artikel 6.2 Het uitvoeren van audits

1. Opdrachtgever of haar gemachtigde vertegenwoordigers en waar nodig toezichthouders (zoals de Autoriteit Persoonsgegevens) hebben het recht om op elk moment tijdens kantooruren, met inachtneming van een aankondigingstermijn van één (1) maand, een audit uit te voeren op de naleving van de BVO.
2. Opdrachtnemer verleent de Opdrachtgever en haar gemachtigde vertegenwoordigers en waar nodig toezichthouders (zoals Autoriteit Persoonsgegevens) toegang tot de faciliteiten van de Opdrachtnemer en haar Onderaannemers, documenten en administratie zoals bedoeld in artikel 6.1, lid 1. Opdrachtnemer verstrekt alle in redelijkheid te verlangen informatie en verleend bijstand bij het uitvoeren van de audits.
3. Opdrachtnemer zal de inhoud van Artikel 6.2 opnemen in de overeenkomst(-en) met de Onderaannemer(s) die zijn betrokken bij de levering van deze Dienst.

Artikel 6.3 Corrigerende maatregelen

1. In audits geconstateerde tekortkomingen worden door Opdrachtnemer opgepakt en omgezet tot een plan waarin wordt aangegeven hoe de geconstateerde tekortkomingen op zo kort mogelijke termijn worden verholpen. Dit plan wordt binnen tien (10) kalenderdagen na schriftelijke rapportage over de constatering, ter beoordeling en goedkeuring aan Opdrachtgever aangeboden.
2. Opdrachtnemer draagt voor eigen rekening zorg voor de implementatie van de corrigerende maatregel en documenteert de corrigerende maatregel. Deze documentatie moet de effectiviteit van de maatregel aantonen. Opdrachtnemer moet de geconstateerde tekortkoming onmiddellijk verhelpen, maar in geen geval later dan dertig (30) kalenderdagen na ontvangst van de kennisgeving van deze tekortkoming, tenzij de partijen anders zijn overeengekomen.

Sectie B: Bepalingen ten aanzien van Beveiliging

Deel I: Algemene bepalingen

Artikel 7 Informatiebeveiligingsbeleid en –technologieën

Artikel 7.1 Eisen aan Informatiebeveiliging

1. Opdrachtnemer draagt er, binnen de reikwijdte van zijn Dienst op grond van de Overeenkomst, zorg voor dat Opdrachtgever te allen tijde kan voldoen aan de volgende wetgeving en standaarden voor Informatiebeveiliging:
    a. Algemene Verordening Gegevensbescherming
    b. Wet Digitale Overheid/Wet Structuur Uitvoeringsorganisatie Werk en Inkomen
    c. Baseline Informatiebeveiliging Overheid /ISO 27001:2017/relevante controls ISO 27002:2017
    d. Grip op Secure Software Development/Open Web Application Security Project

2. Indien daarvoor aanleiding bestaat, maakt Opdrachtgever met Opdrachtnemer (nadere) afspraken hoe de standaarden worden geïmplementeerd en wat hierbij de impact is van implementatie.
3. Opdrachtgever en Opdrachtnemer leggen de gemaakte afspraken omtrent Informatiebeveiliging schriftelijk vast in een Beveiligingskader dat als bijlage bij de BVO wordt gevoegd. Opdrachtnemer verwerkt dit Beveiligingskader in zijn Beveiligingsplan. Opdrachtnemer zal het in Beveiligingsplan het Beveiligingskader vertalen naar beleid, procedures en werkinstructies. Opdrachtnemer is verplicht dit Beveiligingsplan actueel te houden.
4. Opdrachtnemer verplicht zich te allen tijde op de hoogte te zijn van de laatste in de markt toegepaste informatiebeveiligingstechnologieën en –technieken. In overleg met Opdrachtgever wordt vastgesteld wat de impact is van implementatie van deze informatiebeveiligingstechnologieën en – technieken. Hierbij is het uitgangspunt marktstandaarden te volgen.
5. Opdrachtnemer voert risicoanalyses uit op realisatietrajecten en onderhoudstrajecten en levert de resultaten van deze risicoanalyses aan Opdrachtgever. Een GEB kan deel uitmaken van een dergelijke risicoanalyse. Onderkende risico's en op basis daarvan door Opdrachtgever geformuleerde aanvullende informatiebeveiligingseisen worden door Opdrachtgever aan Opdrachtnemer schriftelijk kenbaar gemaakt en maken vanaf dat moment deel uit van het in artikel 7.1 lid 3 bedoelde Beveiligingskader.
6. Opdrachtnemer is verplicht uit eigen beweging of op verzoek van de Opdrachtgever bij projecten, nieuwbouw en doorontwikkeling van programmatuur Opdrachtgever te wijzen op risico's, voortvloeiend uit de AVG, die niet of onvoldoende gedekt worden door de door Opdrachtgever opgeleverde (functionele) documentatie of Opdrachtomschrijving.
7. Nadat aanvullende informatiebeveiligingseisen kenbaar zijn gemaakt dienen Opdrachtnemer en Opdrachtgever binnen een overeengekomen termijn de impact te bepalen van aanvullende informatiebeveiligingseisen, op dezelfde wijze zoals beschreven in artikel 7.1 lid 2.
8. In geen geval mag door handelen of nalaten van Opdrachtnemer het niveau van Informatiebeveiliging minder zijn dan:
    a. Het basisniveau van Informatiebeveiliging zoals omschreven in de standaarden van Informatiebeveiliging zoals genoemd in artikel 7.1 lid 1, dan wel de aanvullende afspraken tussen Opdrachtgever en Opdrachtnemer zoals bedoeld in artikel 7.1 lid 2;

    b. Dan wel het laatste -tijdens de uitvoeringsfase- in een onafhankelijke toets vastgestelde feitelijke niveau van Informatiebeveiliging, indien dit hoger is dan het hiervoor in artikel 7.1 lid 1, omschreven basisniveau of artikel 7.1 lid 2 aanvullende afspraken.

Artikel 7.2 Certificering van de Informatiebeveiliging

1. Opdrachtnemer dient, voor de onder de Overeenkomst overeengekomen Diensten, op basis van ISO 27001:2017 (of gelijkwaardig), gecertificeerd te zijn en te blijven of over een aantoonbare gelijkwaardige baseline op het gebied van Informatiebeveiliging te beschikken.
2. Bij uitzondering, en alleen indien dit in of bij de Overeenkomst nadrukkelijk is bepaald, kan Opdrachtnemer bij het ondertekenen van de Overeenkomst niet ISO 27001:2017 (of gelijkwaardig) gecertificeerd zijn, of over een aantoonbare gelijkwaardige baseline op het

gebied van Informatiebeveiliging beschikken, voor de overeengekomen Diensten. Opdrachtnemer dient in dat geval zorg te dragen voor dat hij binnen 60 kalenderdagen (of een door Opdrachtgever en Opdrachtnemer overeengekomen periode) na de ondertekening van de Overeenkomst beschikt over een ISO 27001:2017 (of gelijkwaardig) certificering of over een aantoonbare gelijkwaardige baseline op het gebied van Informatiebeveiliging voor de Diensten die onder deze Overeenkomst vallen.

Artikel 7.3 Beschrijving van de Informatiebeveiliging van een Dienst
Opdrachtnemer is verplicht binnen de door Opdrachtgever gestelde termijn in de Dienstenbeschrijving, de Informatiebeveiliging van een Dienst op hoofdlijnen te beschrijven. Deze beschrijving van de Informatiebeveiliging van een Dienst op hoofdlijnen dient actueel te worden gehouden en omvat alle informatie die Opdrachtgever inzicht biedt in de wijze waarop Opdrachtnemer voldoet aan de vereisten ten aanzien van Informatiebeveiliging van Opdrachtgever. Deze Dienstenbeschrijving wordt opgenomen in bijlage 3.

Artikel 7.4 Informatiebeveiligingsbeleid
Opdrachtnemer zal zich houden aan al het beleid en procedures die door Opdrachtgever schriftelijk bekend zijn gemaakt aan Opdrachtnemer. Opdrachtgever is gerechtigd beleid en procedures te wijzigen. Dit beleid en procedures kunnen, zonder beperking, regels en eisen voor de bescherming van gebouwen, materialen, apparatuur en Personeel omvatten.

Artikel 7.5 Informatiebeveiligingsorganisatie
1. Opdrachtnemer beschikt over een reguliere informatiebeveiligingsorganisatie waarin naast duidelijke participatie van het hoogste management, een beveiligingsfunctionaris is benoemd die verantwoordelijk is voor het opstellen, de implementatie, het onderhoud en de naleving van het beleid betreffende Informatiebeveiliging. Daar waar Opdrachtnemer geen reguliere beveiligingsfunctionaris heeft, vervult een daartoe aangewezen lid van de directie van Opdrachtnemer die functie.
2. De beveiligingsfunctionaris van Opdrachtgever en de beveiligingsfunctionaris van Opdrachtnemer zoals benoemd in de SLA c.q. DAP hebben regulier beveiligingsoverleg. De inhoud van dit beveiligingsoverleg zal mede worden bepaald door:
    a. Het Beveiligingsprogramma, zoals het goedkeuren van (aanpassingen op) per Dienst door Opdrachtgever, na overleg met Opdrachtnemer;
    b. Periodiek de risico's voor Opdrachtgever ten gevolge van specifieke bedreigingen en kwetsbaarheden voor de afgenomen Diensten te identificeren en te beoordelen;
    c. De communicatie over actuele en geactualiseerde versies van beleid en/of richtlijnen;
    d. Het beoordelen of passende risico mitigerende maatregelen zijn getroffen door Opdrachtnemer, ten aanzien van de afgenomen Diensten - inclusief bijbehorende controles, opleidingen en het beheer van middelen;
    e. Het in kaart brengen van de consequenties en de eventueel benodigde aanpassing van de Dienst als gevolg van gewijzigd beleid.
    f. Formele afspraken over de beschikbaarheid en bereikbaarheid van de beveiligingsfunctionarissen en vervanging van deze functionarissen.
    g. Beveiligingsrapportages, zoals ofwel specifiek genoemd in de DAP ofwel in overleg wordt afgesproken.
    h. Het Beveiligingsprogramma te monitoren en te testen om zo de doeltreffendheid ervan te waarborgen.

3. Beide partijen handelen overeenkomstig de in de SLA opgenomen afspraken over de beschikbaarheid, bereikbaarheid en vervanging van deze beveiligingsfunctionarissen.
4. Opdrachtnemer houdt Personeel dat direct of indirect ingeschakeld worden bij de werkzaamheden ten behoeve van Opdrachtgever op de hoogte van beleid en voorschriften op het gebied van Informatiebeveiliging, zodat deze hier naar kunnen handelen en voor afwijkingen verantwoordelijk kunnen worden gesteld.
5. Opdrachtnemer verantwoordt zich stelselmatig door middel van rapportages over de Informatiebeveiliging en de daarover gemaakte afspraken. De frequentie van rapportages

wordt opgenomen het Beveiligingskader. Met het oog op de mogelijke toetsing van deze rapportages geldt:

a. Opdrachtgever en Opdrachtnemer spreken een voor de blijvende kwaliteit van de Informatiebeveiliging relevant stelsel van toetsen af;
b. De beschrijving van het stelsel van toetsen is opgenomen in het Beveiligingskader. Hierbij is ten minste beschreven:
    - Doel en opzet van de toets;
    - Werkwijze en methode van toetsing;
    - Definitie van de metingen en de performance indicatoren over de Informatiebeveiliging;
    - Wijze en frequentie van rapportage over de toetsen.

Artikel 8 Beveiligingsmaatregelen

Artikel 8.1 Classificatie van middelen

1. Opdrachtnemer classificeert alle door hem voor de uitvoering van Dienst ingezette gegevens, software en andere middelen - met inachtneming van de door Opdrachtgever verstrekte classificatie en/of risicoanalyse.
2. Opdrachtnemer zal van alle in artikel 8.1 lid 1 bedoelde gegevens, software en andere middelen registreren wie de eigenaar is.

Artikel 8.2 Identiteits- en toegangsmanagement

1. Opdrachtnemer voorziet het Personeel en Onderaannemers alleen van toegang tot de systemen, software en gegevens wanneer dit nodig is voor de uitvoering van taken en functies, waarvoor zij verantwoordelijk zijn. Door middel van functiescheiding is voorkomen dat een combinatie van toegangsrechten kan leiden tot een ongeautoriseerde cyclus van handelingen, waarmee scheiding van noodzakelijke functiehandelingen wordt doorbroken.
2. Opdrachtnemer verstrekt informatie over diens mechanismen voor het verlenen van elektronische toegang tot de systemen en gegevens van Opdrachtgever. Opdrachtnemer stelt Opdrachtgever op de hoogte van wijzigingen in de mechanismen voor het verlenen van elektronische toegang tot de systemen.
3. Opdrachtnemer voorziet Opdrachtgever periodiek of op verzoek van een geactualiseerde lijst van Personeel die namens de Opdrachtnemer en/of haar dochterondernemingen toegang hebben tot de systemen, software en gegevens, inclusief het niveau van de toegang die zij hebben. Dit lijst geeft inzicht in autorisaties op basis van rollen en functies. Alleen als er zwaarwegende gronden zijn (bijvoorbeeld vermoeden van fraude of misbruik) en aan de eisen van de AVG is voldaan worden op eerste verzoek van Opdrachtgever in dit kader ook persoonsgegevens verstrekt.

Artikel 8.3 Beveiliging van fysieke (mobiele) gegevensdragers

1. Opdrachtnemer draagt ten alle tijden zorg voor de Beveiliging van fysieke (mobiele) gegevensdragers – met als doel het voorkomen van onbevoegde kennisneming en diefstal (door verplaatsing van de fysieke gegevensdragers of het maken van een al dan niet gedeeltelijke kopie van de gegevens op de fysieke gegevensdrager).
2. Onder fysieke (mobiele) gegevensdragers wordt onder meer verstaan:
    a. Papier waarop gegevens staan;
    b. USB-sticks, harde schijf, Cd-roms, laptops, floppy’s en Pc’s.

Artikel 8.4 Ruimten bij Opdrachtnemer

1. Opdrachtnemer is verantwoordelijk voor de technische voorzieningen in de ruimten bij Opdrachtnemer, zoals klimaatbeheersing en stroomvoorziening.
2. Opdrachtnemer is verantwoordelijk voor de fysieke toegangsbeveiliging tot de ruimte bij Opdrachtnemer. Opdrachtnemer laat fysieke toegang tot ruimten waar zich gegevens, software en andere bedrijfsmiddelen - en middelen (o.a. apparatuur) die nodig zijn om de Dienst uit te voeren - bevinden, alleen toe aan personen die hiertoe door Opdrachtnemer geautoriseerd zijn.
3. Opdrachtnemer kan (en zal desgevraagd) de Opdrachtgever inzicht bieden in autorisaties die nodig zijn voor het leveren van een Dienst, die door Opdrachtnemer aan diens Personeel heeft verleend. Dit inzicht wordt verschaft op basis van rollen en functies. Alleen als er zwaarwegende gronden zijn (bijvoorbeeld vermoeden van fraude of misbruik) en aan de eisen

van de AVG is voldaan worden op eerste verzoek van Opdrachtgever in dit kader ook persoonsgegevens verstrekt.

Artikel 8.5 Monitoring en afhandeling van Beveiligingsincidenten

1. Opdrachtnemer neemt maatregelen met betrekking tot de preventie en opsporing van Beveiligingsincidenten. Het gebruik van de systemen en de toegang daartoe wordt vastgelegd op een manier die in overeenstemming is met het risico en zodanig dat oorzaak, veroorzaker en gevolg aantoonbaar zijn. De vastlegging is zodanig voorzien van maatregelen dat de vastlegging blijft bestaan en niet gewijzigd kan worden. De vastlegging dient bewaart te worden voor een termijn die in overeenstemming is met wettelijke eisen – de bewaartermijnen zijn vastgelegd in de SLA.
2. Opdrachtgever en Opdrachtnemer werken samen aan de monitoring van Informatiebeveiligingsrisico's en de afhandeling van Beveiligingsincidenten. De verantwoordelijkheid voor de monitoring van de Informatiebeveiligingsrisico's voor de Dienst, ligt bij Opdrachtnemer. De verantwoordelijkheid voor de monitoring van de Informatiebeveiligingsrisico's binnen de bedrijfsvoering van Opdrachtgever, ligt bij Opdrachtgever. De raakpunten zijn aan beide kanten gedefinieerd en vastgelegd in het Beveiligingskader. De monitorings- en afhandelingsprocedures van Beveiligingsincidenten en de ingestelde regels en escalatiedrempels zijn vastgesteld door Opdrachtgever. De monitorings- en afhandelingsprocedures worden vastgelegd in de DAP
3. Opdrachtnemer zal Beveiligingsincidenten direct melden aan Opdrachtgever conform het in de DAP afgesproken proces. Opdrachtnemer zal de consequenties van een Beveiligingsincident gelijktijdig met de melding of –als gelijktijdig met de melding niet mogelijk is- zo spoedig mogelijk na de melding aan Opdrachtgever inzichtelijk maken. Voor Inbreuken in verband met persoonsgegevens in het geval Opdrachtnemer een Verwerker is, gelden aanvullend hierop hetgeen in artikel 15.6 (Inbreuken in verband met persoonsgegevens [Datalekken]) is opgenomen.
4. Opdrachtnemer zal in geval dat Opdrachtnemer een Beveiligingsincident signaleert, alle redelijkerwijs benodigde maatregelen treffen om (verdere) schending van de vertrouwelijkheid te voorkomen of te beperken.
5. Opdrachtnemer rapporteert periodiek aan Opdrachtgever over gesignaleerde Beveiligingsincidenten en de genomen maatregelen. Opdrachtnemer verstrekt deze rapportage minstens 1 keer per kwartaal, of op verzoek van Opdrachtgever. De rapportage omvat alle informatie die Opdrachtgever redelijkerwijs nodig heeft om te kunnen bepalen welke risico's de incidenten leveren voor de bedrijfsvoering van Opdrachtgever.
6. Opdrachtnemer zal de consequenties en zo mogelijk de oorzaak van het Beveiligingsincident aan Opdrachtgever inzichtelijk maken. Als Opdrachtnemer overeengekomen Diensten vanwege een Beveiligingsincident niet meer of beperkt kan leveren, wordt dit vastgelegd en wordt Opdrachtgever hiervan per direct op de hoogte gesteld via een rapportage. Opdrachtgever beslist na overleg met Opdrachtnemer of de Dienst (tijdelijk) aangepast wordt (niet of beperkt geleverd zal worden), dan wel wanneer deze Dienst volledig hervat dient te worden.

Artikel 9 Personeel

1. Opdrachtnemer draagt ervoor zorg dat zijn Personeel en Onderaannemers voldoen aan de beleidslijnen en procedures van Opdrachtgever.
2. Opdrachtnemer houdt Personeel dat direct of indirect ingeschakeld worden bij de werkzaamheden ten behoeve van Opdrachtgever op de hoogte van beleid en voorschriften op het gebied van Informatiebeveiliging, zodat deze hier naar kunnen handelen en voor afwijkingen verantwoordelijk kunnen worden gesteld.
3. Opdrachtnemer laat Personeel en de door hem ingeschakelde Onderaannemer de verplichting tot geheimhouding bekrachtigen middels een ondertekende verklaring.
4. Opdrachtgever behoudt zich het recht voor om voor bepaald(e) (groepen) Personeel van Opdrachtnemer en de door hem ingeschakelde Onderaannemer, een VOG te kunnen eisen. De kosten van deze VOG komen ten laste van de Opdrachtnemer.
5. Opdrachtnemer toont op verzoek van Opdrachtgever aan dat diens Personeel en door Opdrachtnemer ten behoeve van de Dienst ingeschakelde Onderaannemers verplichtingen uit deze BVO evenals de geheimhoudingsverplichtingen zoals vastgelegd in de Algemene Inkoopvoorwaarden naleven.
6. Indien een partij constateert dat een personeelslid de op hem rustende geheimhoudingsverplichting niet nakomt of niet is nagekomen, en hierdoor de

Informatiebeveiliging van de overeengekomen Dienst in gevaar komt of is gekomen, dient zij de andere partij hiervan terstond op de hoogte te stellen.

7. Als een personeelslid van Opdrachtnemer dit beleid of procedures schendt of negeren, heeft Opdrachtgever het recht om die personeelslid van Opdrachtnemer toegang tot de locaties, gegevens en middelen van Opdrachtgever onmiddellijk te ontzeggen.
8. In onderling overleg wordt bepaald welke maatregelen getroffen zullen worden om de gevolgen van de schending van de geheimhoudingsverplichting te beperken en herhaling van schending te voorkomen.

Artikel 10 Vertrouwelijke gegevens

1. Alle vertrouwelijke gegevens van Opdrachtgever en aan Opdrachtnemer beschikbaar gestelde gegevens, evenals de in het kader van de Overeenkomst door Opdrachtnemer verworven gegevens worden geacht eigendom te zijn van Opdrachtgever. Opdrachtnemer en zijn Personeel en Onderaannemers gebruiken deze gegevens alleen voor zover dit noodzakelijk is voor het leveren van Diensten ter uitvoering van de Overeenkomst.
2. Opdrachtnemer draagt er zorg voor dat alleen Personeel toegang heeft, dat voor de levering van de Diensten aan Opdrachtgever toegang tot vertrouwelijke gegevens nodig heeft. Opdrachtnemer neemt daarom adequate maatregelen ter borging van de geheimhouding en de vertrouwelijkheid door de toegang tot vertrouwelijke gegevens te beperken tot degenen die voor het uitvoeren van de hun toegewezen taken de noodzaak hebben voor toegang tot deze gegevens.
3. Opdrachtnemer meldt, van welke bron dan ook, onmiddellijk alle verzoeken tot het delen of verzoeken tot toegang tot vertrouwelijke gegevens Opdrachtnemer en zijn Personeel en Onderaannemers zijn niet bevoegd vertrouwelijke gegevens aan Derden te verstrekken zonder de voorafgaande schriftelijke toestemming van Opdrachtgever. Een verzoek tot toestemming kan naar eigen inzicht door Opdrachtgever worden geweigerd.
4. Op het moment dat de Overeenkomst afloopt of wordt beëindigd of op een ander tijdstip op schriftelijk verzoek van de Opdrachtgever, worden alle vertrouwelijke gegevens (anders dan Persoonsgegevens) en alle kopieën van deze gegevens die in bezit of beheer zijn bij de Opdrachtnemer of Onderaannemers, in welke vorm dan ook, teruggegeven in een voor de Opdrachtgever verwerkbare vorm, tenzij Opdrachtgever op dat moment verzoekt deze gegevens te vernietigen. In dat geval levert Opdrachtnemer na de uitvoering van de vernietiging aan Opdrachtgever een “Verklaring van vernietiging” van een onafhankelijke Derde.

Artikel 11 Bepalingen ten aanzien van beheer van Software, Netwerken, Servers en Clouddiensten

1. Opdrachtnemer zal de taken, verantwoordelijkheden en bevoegdheden voor de uitvoering van de beheerwerkzaamheden, beschrijven in het Beveiligingskader. Onder deze beheerwerkzaamheden vallen de processen configuratiebeheer, incidentbeheer, probleembeheer, wijzigingsbeheer, releasebeheer, capaciteitsbeheer, beschikbaarheidsbeheer en continuïteitsbeheer.
2. Deze taken betreffen in ieder geval:
   a. Het stelselmatig toetsen van de beheersmaatregelen en het treffen van adequate verbetermaatregelen indien de beheersmaatregelen ontoereikend zijn om het afgesproken beveiligingsniveau te borgen;
   b. Het inrichten, in stand houden en toepassen van een kwaliteitssysteem, teneinde de naleving van de BVO ook na wijzigingen te kunnen garanderen;
   c. Logisch beheren van de software, gegevens en andere middelen;
   d. Op eigen initiatief contact opnemen met Opdrachtgever, indien bevindingen uit een risicoanalyse of de kwaliteitsbeheersing van Opdrachtnemer daartoe aanleiding geven;
   e. Fysiek en/of logisch beheren van de gebruikte componenten;
   f. Beheren van registraties van autorisaties;
   g. Fysiek en/of logisch toekennen en intrekken van autorisaties;
   h. Beheren van apparatuur op afstand;
   i. Beheersen van de personele bezetting;

Artikel 12 Bepalingen ten aanzien van Systemen (Hard- en Software)

Artikel 12.1 Ontwikkeling van systemen conform SSD

Opdrachtnemer voldoet aan de eisen uit Grip op Secure Software Development, ISO 27001:2017 en relevante controls van de ISO 27002:2017 ten aanzien van de software die ingezet wordt. Wanneer specifieke eisen niet van toepassing zijn, geeft Opdrachtgever dit aan bij Opdrachtnemer. Als Opdrachtnemer niet (of deels) aan de eisen voldoet, informeert Opdrachtnemer Opdrachtgever hierover en bepaald Opdrachtgever welke vervolgstappen worden genomen.

Artikel 12.2 Onderhoud en ontwikkeling van systemen

1. Opdrachtnemer borgt dat de door hem beheerde hard- en/of software permanent blijft voldoen aan de eisen op grond van deze BVO:
   a. Opdrachtnemer zal hiertoe stelselmatig en op eigen initiatief marktontwikkelingen en adviezen volgen met betrekking tot noodzakelijke patchniveaus;
   b. Opdrachtnemer heeft een actieve informatieplicht naar Opdrachtgever m.b.t. de kwaliteit van de geleverde hard- en/of software. Hieronder valt ten minste het informeren over nieuwe marktontwikkelingen, het informeren over patches en bedreigingen en het informeren over de compatibiliteit en het uit support raken van de hardware en/of software stack voor zover door Opdrachtgever gebruikt.

2. Om zich te verantwoorden over de getroffen kwaliteit borgende maatregelen biedt Opdrachtnemer door middel van rapportages inzicht in de inrichting van het proces voor ontwikkel- en onderhoudswerkzaamheden. Opdrachtnemer rapporteert bij elke wijziging aan het systeem die een afgesproken SSD-norm raakt over de uitkomsten van de kwaliteitsborging m.b.t. die SSD-norm aan Opdrachtgever conform de rapportagevorm zoals neergelegd in de Overeenkomst.

3. Bij onderhoud van software is Opdrachtnemer gehouden alle – voor het waarborgen van de vertrouwelijkheid, beschikbaarheid en betrouwbaarheid noodzakelijke - patches en fixes die door fabrikanten beschikbaar worden gesteld te installeren, zodanig dat de overeengekomen Dienst aan de Opdrachtgever gewaarborgd is:
   a. Opdrachtnemer volgt de markt en gaat na of nieuwe patches beschikbaar zijn voor de systemen die gebruikt worden voor de aan Opdrachtgever geleverde Diensten;
   b. Opdrachtnemer test de patches en beoordeelt de impact op de Dienst van Opdrachtgever, alvorens de patch aan te brengen en neemt zo nodig contact met Opdrachtgever op volgens de afspraken in de DAP.

Artikel 12.3 Bepalingen ten aanzien van testen en testgegevens

1. Wijzigingen aan systemen binnen de levenscyclus van de ontwikkeling behoren te worden beheerst door het gebruik van formele procedures voor wijzigingsbeheer
2. Nieuwe (of aangepaste) software of configuraties worden vooraf getest in gescheiden omgevingen – de ontwikkelomgeving, de testomgeving en de acceptatieomgeving (OTA). De OTA-omgevingen staan los van de feitelijke productieomgeving.
3. Voor nieuwe informatiesystemen, upgrades en nieuwe versies behoren programma's voor het uitvoeren van acceptatietests en gerelateerde criteria te worden vastgesteld.
4. Er mag niet met Productiedata worden getest. Dit impliceert:
    a. Dat Productiedata door Opdrachtgever zover als mogelijk worden geanonimiseerd voordat ze als testdata worden aangeleverd en als zodanig mogen worden gebruikt;
    b. Leverancier in het tactisch overleg terugkoppelt over het gebruik en de aard van de testdata en eventuele afwijkingen meldt;
    c. Opdrachtgever en Opdrachtnemer bepalen in overleg hoe met de geconstateerde afwijkingen wordt omgegaan.

12.4 Bepalingen specifiek ten aanzien van Internet of Things (IoT): systemen

12.4.1 Bepalingen ten aanzien van Internet of Things: Algemeen

1. Opdrachtnemer is verantwoordelijk voor de veilige werking van IoT-devices
2. Middels een risico-analyse stelt Opdrachtnemer periodiek vast wat de kwetsbaarheden van een IoT device zijn, welke dreigingen bestaan die deze kwetsbaarheden kunnen uitnutten en welke maatregelen Opdrachtnemer treft voor mitigeren van risico's. Opdrachtgever bepaalt welke risico's acceptabel zijn.
3. Opdrachtnemer zal de processen configuratiebeheer, incidentbeheer, probleembeheer, wijzigingsbeheer, releasebeheer, capaciteitsbeheer, beschikbaarheidsbeheer en continuïteitsbeheer, de taken en verantwoordelijkheden voor de uitvoering van de beheerwerkzaamheden beschrijven en op verzoek hierover rapporteren.
4. Opdrachtnemer legt de autorisaties op IoT-devices (op netwerkniveau, applicatieniveau en operating system niveau) vast in een register en houdt dit register actueel.

12.4.2 Bepalingen ten aanzien van Internet of Things: Interfaces

Interfaces dienen kenbaar te zijn bij Opdrachtnemer en periodiek dan wel bij belangrijke wijzigingen te worden getest middels penetratietesten.

12.4.3 Bepalingen ten aanzien van Internet of Things: Operating System

Opdrachtnemer borgt dat de Operating Systems van de door hem beheerde IoT-devices permanent blijven voldoen aan de eisen op grond van deze BVO:

1. Opdrachtnemer zal zich stelselmatig en op eigen initiatief op de hoogte stellen van marktontwikkelingen en adviezen met betrekking tot noodzakelijke patchniveaus, onder meer naar aanleiding van de Open Web Application Security Project. Over deze marktontwikkelingen en adviezen, informeert Opdrachtnemer actief Opdrachtgever. Opdrachtnemer en Opdrachtgever stellen in overleg vast welke marktontwikkelingen en adviezen toegepast moeten worden.;
2. Opdrachtnemer draagt zorg voor het minimaliseren van het aanvalsoppervlak op het Operating System van het IoT-device

Artikel 13 Bepalingen ten aanzien van Servers en Netwerken

Artikel 13.1 Algemeen

1. Opdrachtnemer treft detectiemaatregelen en voert analyses uit om verdachte patronen te kunnen vaststellen en neemt maatregelen die noodzakelijk zijn.
2. Op basis van risico-analyse moeten worden bepaald in hoeverre sessies volledig versleuteld dienen te zijn, zowel in de externe naar interne verbindingen als vice versa (end to end).

Artikel 13.2 Bepalingen specifiek ten aanzien van Internet of Things: servers en netwerken

1. Sessies dienen in principe volledig versleuteld te zijn, op basis van een risico-analyse, zowel in de externe naar interne verbindingen als vice versa (end to end).
2. Bij de toepassing van encryptiesleutels/certificaten op meerdere apparaten van dezelfde compatibiliteit, dienen de encryptiesleutels/certificaten verschillend te zijn.

Artikel 14 Bepalingen ten aanzien van Public Clouddiensten

Artikel 14.1 Algemeen

Opdrachtnemer garandeert een veilige afscherming (van de verwerking) van de gegevens, als (delen van) omgevingen worden ingezet voor gemeenschappelijk gebruik door meerdere partijen of als deze logisch of fysiek met elkaar verbonden zijn, die tenminste voldoet aan de eisen die Opdrachtgever heeft gesteld. Opdrachtgever en Opdrachtnemer bekijken periodiek gedurende de looptijd van de Overeenkomst, welke nieuwe ontwikkelingen er zijn op het gebied van Clouddiensten. Op basis van deze ontwikkelingen bepaalt Opdrachtgever welke aanscherpingen noodzakelijk zijn.

Artikel 14.2 Bepalingen specifiek ten aanzien van Internet of Things: Clouddiensten

1. Opdrachtnemer verstrekt op verzoek van Opdrachtgever informatie over de mechanismen voor het verlenen van elektronische toegang tot de systemen en Vertrouwelijke gegevens van Opdrachtgever.
2. Indien Vertrouwelijke gegevens binnen de systemen worden verwerkt, dienen cryptografische maatregelen te zijn getroffen – conform het Cryptografiebeleid UWV.
3. Vertrouwelijke gegevens van Opdrachtgever mogen alleen gebruikt worden voor doeleinden van Opdrachtnemer met instemming van Opdrachtgever.

Sectie C: Bepalingen ten aanzien van een Verwerker

Artikel 15 Algemene Verordening Gegevensbescherming (AVG) – Verwerkersovereenkomst

Artikel 15.1 Algemeen

1. Dit artikel is alleen van toepassing indien Opdrachtnemer Verwerker is en Opdrachtgever Verwerkingsverantwoordelijke voor de verwerking van Persoonsgegevens in het kader van de uitvoering van de Overeenkomst en geldt in aanvulling op alle andere bepalingen in deze BVO.
2. Opdrachtnemer verwerkt in opdracht van Opdrachtgever Persoonsgegevens in het kader van de uitvoering van de Overeenkomst voor de duur van de Overeenkomst en de daaruit voortvloeiende Diensten. De aard en het doel van de verwerking, het soort Persoonsgegevens en de categorieën van betrokkenen wiens Persoonsgegevens worden verwerkt, als ook de eventuele categorieën van ontvangers, zijn in Bijlage 2 omschreven.
3. Indien deze BVO een verbijzondering van de bepalingen uit de wet- en regelgeving inhoudt, dan ontslaat deze verbijzondering Opdrachtnemer in haar verhouding tot Opdrachtgever niet van de verantwoordelijkheden die uit de toepasselijke wet- en regelgeving voortvloeien.
4. In zijn hoedanigheid van Verwerker van Persoonsgegevens van Opdrachtgever zal Opdrachtnemer Persoonsgegevens van Opdrachtgever verwerken op de wijze die is vermeld in de Overeenkomst en conform overige verwerkingsinstructies van Opdrachtgever.
5. Indien Opdrachtnemer van mening is dat een instructie van Opdrachtgever een inbreuk oplevert op de AVG of andere toepasselijke wet-of regelgeving op het gebied van gegevensbescherming, dan stelt hij Opdrachtgever hiervan onmiddellijk in kennis.
6. Opdrachtnemer zal bijstand verlenen aan Opdrachtgever bij het doen nakomen van verplichtingen die op Opdrachtgever rusten uit hoofde van gegevensbeschermingseffectbeoordelingen in de zin van artikel 35 AVG en voorafgaande raadplegingen in de zin van artikel 36 AVG.
7. Opdrachtnemer stelt Opdrachtgever onverwijld in kennis indien een daartoe bevoegde instantie een juridisch bindend verzoek om verstrekking van de Persoonsgegevens heeft gedaan, tenzij het Opdrachtnemer omwille van gewichtige redenen van algemeen belang niet is toegestaan Opdrachtgever hiervan in kennis te stellen.

Artikel 15.2 Subverwerkers

1. Opdrachtnemer is niet bevoegd om de Persoonsgegevens op enige wijze door een Subverwerker te laten Verwerken, anders dan met de voorafgaande schriftelijke toestemming van Opdrachtgever. Opdrachtgever is gerechtigd aan het verlenen van toestemming nadere voorwaarden te verbinden c.q. deze in tijd te beperken. In Bijlage 3 zijn de Subverwerkers opgenomen die bij het sluiten van de Overeenkomst zijn toegestaan.
2. Opdrachtnemer draagt zorg voor een actueel overzicht van de door hem ingeschakelde Subverwerkers en de werkzaamheden waarvoor elke Subverwerker wordt ingeschakeld, door Bijlage 3 periodiek, minimaal éénmaal per jaar, te vernieuwen en Opdrachtgever een afschrift hiervan te sturen.
3. Opdrachtnemer is verantwoordelijk en aansprakelijk voor door hem ingeschakelde Subverwerkers in de nakoming van diens verplichtingen ten aanzien van de Verwerking van Persoonsgegevens. Opdrachtnemer waarborgt dat de Verwerking van Persoonsgegevens door de Subverwerker voldoet aan de eisen die voortvloeien uit de Overeenkomst en deze BVO en zal aan de Subverwerker in ieder geval de verplichting opleggen om te voldoen aan de hiervoor bedoelde eisen.
4. Indien de Verwerking van Persoonsgegevens door de door Opdrachtnemer ingeschakelde Subverwerker niet voldoet aan de eisen die voortvloeien uit de Overeenkomst en deze BVO, is Opdrachtgever gerechtigd om de verleende toestemming voor de inzet van de Subverwerker in te trekken dan wel de inzet van de Subverwerker te verbieden.

Artikel 15.3 Informatiebeveiliging

1. De Partijen beoordelen de technische en organisatorische maatregelen die in de Overeenkomst en deze BVO worden omschreven als passend in de zin van artikel 32 AVG, om de in het kader van de Overeenkomst verwerkte Persoonsgegevens te beschermen.

2. Opdrachtnemer zal uit eigen beweging Opdrachtgever informeren wanneer naar zijn oordeel de maatregelen ten aanzien van Informatiebeveiliging nog verder aangescherpt kunnen worden.
3. Indien Opdrachtgever aanvullende maatregelen ten aanzien van Informatiebeveiliging verzoekt, zal Opdrachtnemer aan Opdrachtgever per omgaande, uiterlijk binnen één (1) week na het verzoek, een offerte doen toekomen, om deze maatregelen zo snel mogelijk te implementeren.

Artikel 15.4 Doorgifte Persoonsgegevens buiten de Europese Economische Ruimte (EER)

1. Opdrachtnemer zal geen Persoonsgegevens die hij in het kader van de Overeenkomst onder zich heeft, buiten de grenzen van de EER verwerken zonder voorafgaande schriftelijke toestemming van Opdrachtgever.
2. Opdrachtnemer zorgt dat de in lid 1 bedoelde overdracht in overeenstemming is met de toepasselijke wet- of regelgeving op het gebied van gegevensbescherming.

Artikel 15.5 Rechten Betrokkenen

1. Opdrachtnemer stelt Opdrachtgever te allen tijde in staat en verleent bijstand om binnen de wettelijke termijnen te voldoen aan de verplichtingen op grond van de AVG waar het betreft de rechten van Betrokkenen, in de zin van hoofdstuk III AVG.
2. Op verzoek van Opdrachtgever verstrekt Opdrachtnemer, een kopie van alle Persoonsgegevens betreffende een Betrokkene die in zijn bezit of beheer zijn alsmede een kopie van alle documenten en een overzicht van alle systemen waarin deze Persoonsgegevens zijn opgenomen en alle overige Verwerkingen van deze Persoonsgegevens die door Opdrachtnemer worden uitgevoerd, een en ander conform aanwijzingen van Opdrachtgever.
3. Op verzoek van Opdrachtgever zal Opdrachtnemer bepaalde Persoonsgegevens verwijderen, wijzigen of de toegang ertoe beperken, dan wel vastleggen en Opdrachtgever informeren dat aan dergelijke verzoeken geen gevolg wordt gegeven en de redenen hiervan, een en ander conform aanwijzingen van Opdrachtgever. Indien Opdrachtnemer zelf verzoeken om uitoefening van rechten ontvangt van Betrokkenen, zal Opdrachtnemer deze onverwijld aan Opdrachtgever doorsturen.

Artikel 15.6 Inbreuken in verband met persoonsgegevens (Datalekken)

1. Opdrachtnemer meldt een (vermeende) Inbreuk in verband met persoonsgegevens aan Opdrachtgever zo spoedig mogelijk doch in ieder geval binnen 24 uur nadat Opdrachtnemer kennis heeft genomen van de (vermeende) Inbreuk. Opdrachtnemer doet de melding per mail aan het e-mailadres meldplicht-datalekken@uwv.nl. In de melding bedoeld moet in ieder geval de volgende informatie zijn opgenomen:
   a. Naam, statutaire vestiging en KvK-nummer van Opdrachtnemer.
   b. Aanduiding van de overeenkomst(en) tussen Opdrachtnemer en Opdrachtgever op grond waarvan door Opdrachtnemer de Persoonsgegevens worden verwerkt waarop de (vermeende) Inbreuk in verband met persoonsgegevens betrekking heeft. Opdrachtnemer vermeldt daarbij dat hij ten aanzien van die verwerkingen Verwerker is in de zin van de AVG.
   c. Naam en contactgegevens van degene die namens Opdrachtnemer de melding aan Opdrachtgever doet.
   d. Datum en tijdstip waarop de (vermeende) inbreuk zich heeft voorgedaan.
   e. Datum en tijdstip waarop de (vermeende) inbreuk bij Opdrachtnemer bekend wordt.
   f. Een zo concreet en volledig mogelijk overzicht van het de (vermeende) inbreuk, waarbij in ieder geval wordt aangegeven:
      - wat er precies gebeurd is en op welke manier een inbreuk in verband met de Persoonsgegevens heeft plaatsgevonden (bijv. gegevens onbevoegd gelezen, gegevens onbevoegd gekopieerd, gegevens onbevoegd gewijzigd, gegevens onbevoegd verstrekt, gegevens onbevoegd verwijderd of vernietigd, gegevens onbevoegd aangetast zoals het blokkeren van bestanden of versleutelen via malware of diefstal van gegevens);
      - welke Persoonsgegevens betrokken zijn bij de (vermeende) inbreuk;
      - van welke categorieën personen (zoals bijv. klanten van Opdrachtgevers en Personeel van Opdrachtgevers) de Persoonsgegevens betrokken zijn bij het de (vermeende) inbreuk;
        - een inschatting van het aantal personen van wie Persoonsgegevens betrokken zijn bij de (vermeende) inbreuk.

- Welke technische en organisatorische maatregelen zijn getroffen om de nadelige gevolgen (schade) te beperken en om herhaling van de (vermeende) inbreuk te voorkomen.

2. Indien zich na de melding aan Opdrachtgever, als hierboven bedoeld, nieuwe, relevante ontwikkelingen voordoen, waaronder begrepen de maatregelen die Opdrachtnemer treft om aan zijn kant de gevolgen van de (vermeende) inbreuk te beperken en herhaling te voorkomen, dan stelt Opdrachtnemer Opdrachtgever daarvan onverwijld op de hoogte.
3. Opdrachtnemer zal op eigen kosten alle redelijkerwijs benodigde maatregelen treffen om de hiervoor bedoelde ongeautoriseerde verwerkingen en inbreuken en (verdere) schending van de AVG of andere regelgeving betreffende de verwerking van de Persoonsgegevens, te voorkomen, te beperken of achteraf te herstellen. Dit laat onverlet de verplichting van Opdrachtnemer om de eventueel door Opdrachtgever daardoor geleden schade te vergoeden.
4. Opdrachtnemer is verplicht financiële sancties te vergoeden die uit hoofde van AVG en/of de UAVG aan Opdrachtgever worden opgelegd wegens het niet nakomen door Opdrachtnemer van zijn verplichtingen met betrekking tot het verwerken van Persoonsgegevens, indien en voor zover de sanctie toerekenbaar is aan Opdrachtnemer.
5. Opdrachtnemer verleent Opdrachtgever volledige medewerking aan het adequaat informeren van de Betrokkenen in het kader van de meldplicht ten aanzien van Inbreuken in verband met persoonsgegeven in de zin van artikel 34 AVG.
6. Indien en voor zover een tijdelijke aanpassing of stopzetting van de Diensten benodigd is om de gevolgen van een Inbreuk in verband met persoonsgegevens te beperken of te verhelpen, treedt Opdrachtnemer per direct in overleg met Opdrachtgever en beslist Opdrachtgever of en hoe de Diensten gewijzigd worden. .

Artikel 15.7 Voortdurende verplichtingen
Onverminderd het elders in deze BVO bepaalde, dienen na afloop van de Overeenkomst naar keuze van Opdrachtgever:

1. alle Persoonsgegevens, kopieën en bewerkingen daarvan, alsmede alle gegevensdragers, voor zover eigendom van Opdrachtgever, waarop de Persoonsgegevens, kopieën of bewerkingen daarvan zijn of zullen worden vastgelegd, onmiddellijk op eerste verzoek van Opdrachtgever te worden geretourneerd c.q. verstrekt aan Opdrachtgever (of een door Opdrachtgever aan te wijzen Derde), of
2. de data of de drager te worden vernietigd. Opdrachtnemer zal op verzoek van Opdrachtgever een verklaring van een onafhankelijke Derde overleggen waaruit blijkt dat de vernietiging van de data of de drager heeft plaatsgevonden.

Sectie D: Bepalingen ten aanzien van een verwerkingsverantwoordelijke

Artikel 16 Algemene Verordening Gegevensbescherming – bepalingen ten aanzien van de verwerkingsverantwoordelijke

1. Deze sectie is alleen van toepassing indien Opdrachtnemer Verwerkingsverantwoordelijke is voor de verwerking van Persoonsgegevens in het kader van de uitvoering van de Overeenkomst.
2. Opdrachtnemer verwerkt de Persoonsgegevens in overeenstemming met de AVG en eventuele andere van toepassing zijnde wet- en regelgeving met betrekking tot het verwerken van Persoonsgegevens.
3. Opdrachtnemer verwerkt de in het kader van de Overeenkomst ontvangen of verzamelde Persoonsgegevens alleen voor zover dat noodzakelijk is voor de uitvoering van de Diensten op grond van de Overeenkomst.
4. Partijen verstrekken elkaar die informatie en verlenen elkaar die medewerking die nodig is om te voldoen aan de AVG en eventuele andere toepasselijke wet- en regelgeving.
5. Opdrachtnemer heeft passende technische en organisatorische maatregelen, als bedoeld in artikel 32 AVG, getroffen om de Persoonsgegevens te verwerken voor de uitvoering van de Overeenkomst. Opdrachtnemer zal de getroffen maatregelen periodiek evalueren en verscherpen, aanvullen of verbeteren voor zover de eisen of (technologische) ontwikkelingen daartoe aanleiding geven. Opdrachtnemer rapporteert op verzoek, Opdrachtgever over de naleving van de getroffen maatregelen. Opdrachtgever zal zo'n verzoek in principe maximaal éénmaal per jaar doen. Indien daar naar het oordeel van Opdrachtgever gegronde redenen voor zijn, kan Opdrachtgever zo'n verzoek vaker doen. Het rapport wordt opgesteld door een onafhankelijk gecertificeerde externe deskundige die een verklaring afgeeft. Opdrachtgever zal vooraf aangeven of er, en zo ja welke, specifieke eisen aan de gecertificeerde deskundige worden gesteld.
6. Opdrachtnemer zal, onverminderd zijn verplichting tot het melden van Inbreuken in verband met persoonsgegevens aan de Autoriteit persoonsgegevens, Opdrachtgever direct informeren over (vermeende) Inbreuken in verband met persoonsgegevens. Opdrachtnemer zal de consequenties van een Inbreuk in verband met persoonsgegevens gelijktijdig met het informeren van Opdrachtgever over de (vermeende) Inbreuk in verband met persoonsgegevens of, als gelijktijdig met het informeren niet mogelijk is zo spoedig mogelijk na het informeren van Opdrachtgever, inzichtelijk maken. Over de aard en reikwijdte van de te melden Inbreuken in verband met persoonsgegevens zullen Partijen nadere afspraken vastleggen in de DAP. Opdrachtnemer verstrekt op verzoek van Opdrachtgever informatie over de geïdentificeerde Inbreuken in verband met persoonsgegevens en de genomen maatregelen.
7. Opdrachtgever beslist na overleg met Opdrachtnemer of en hoe de Inbreuk in verband met persoonsgegevens leidt tot een (al dan niet tijdelijke) aanpassing of stopzetting van de Dienst op grond van de Overeenkomst en over het moment dat de aanpassing of stopzetting van de Dienst wordt opgeheven.

Artikel 17 Informatiebeveiliging

1 Opdrachtnemer dient, voor de onder de Overeenkomst overeengekomen Diensten, op basis van ISO 27001:2017 (of gelijkwaardig), gecertificeerd te zijn en te blijven of over een aantoonbare gelijkwaardige baseline op het gebied van Informatiebeveiliging te beschikken.

2 Bij uitzondering, en alleen indien dit in of bij de Overeenkomst nadrukkelijk is bepaald, kan Opdrachtnemer bij het ondertekenen van de Overeenkomst niet ISO 27001:2017 (of gelijkwaardig) gecertificeerd zijn, of over een aantoonbare gelijkwaardige baseline op het gebied van Informatiebeveiliging beschikken, voor de overeengekomen Diensten. Opdrachtnemer dient in dat geval zorg te dragen voor dat hij binnen 60 kalenderdagen (of een door Opdrachtgever en Opdrachtnemer overeengekomen periode) na de ondertekening van de Overeenkomst beschikt over een ISO 27001:2017 (of gelijkwaardig) certificering of over een aantoonbare gelijkwaardige baseline op het gebied van Informatiebeveiliging voor de Diensten die onder deze Overeenkomst vallen.

Bijlage 1: Begripsomschrijvingen BVO

AVG	Algemene Verordening Gegevensbescherming
Bedrijfskritische processen	De processen in de bedrijfsvoering van Opdrachtgever die essentieel zijn voor Opdrachtgever om te voldoen aan zijn verplichtingen.
Beschikbaarheid	De toegang voor geautoriseerde gebruikers op de overeengekomen momenten tot gegevens en aanverwante bedrijfsmiddelen zoals informatiesystemen, oftewel het zorgen voor een ongestoorde voortgang van de informatievoorziening.
Betrokkene	Natuurlijk Persoon op wie een Persoonsgegeven betrekking heeft.
Beveiliging	Het geheel van maatregelen dat getroffen is om de Dienst en/of gegevens tegen een ongewenste verstoring of inbreuk te beschermen.
Beveiligingsincident	Gebeurtenis of actie waarbij de beveiliging van hardware, software, informatie, een proces of organisatie mogelijk in gevaar is gebracht of geheel of gedeeltelijk is doorbroken.
Beveiligingskader	De tussen Opdrachtgever en Opdrachtnemer gemaakte afspraken omtrent de eisen waaraan de beveiliging moet voldoen alsmede het stelsel van toetsen
Beveiligingsplan	Een plan waarin de organisatie van Opdrachtnemer wordt beschreven en waarin staat wat er beveiligd moet worden en hoe deze beveiliging plaats dient te vinden.
Beveiligingsprogramma	Een door Opdrachtnemer opgesteld en door Opdrachtgever goed te keuren overzicht van alle beveiligingsinspanningen en –maatregelen, waarmee Opdrachtnemer een nadere invulling geeft aan het Beveiligingskader en het Beveiligingsplan, voor zover inspanningen en maatregelen buiten de normale werkwijze van de partijen vallen. Opdrachtgever zal dit programma prioriteren en in de tijd uitzetten.
BVO	De onderhavige Beveiligings- en Verwerkersovereenkomst.
Clouddienst	Een Dienst die via een al dan niet openbaar elektronisch netwerk toegankelijk is.
Continuïteitsplan	Plan waarin staat wat te doen bij storingen die ernstige gevolgen hebben voor de organisatie
DAP	Dossier Afspraken en Procedures. Een beschrijving van de afspraken over de manier van samenwerking tussen aanbieder en afnemer.
Derde	Ieder, niet zijnde de betrokkene, noch de Verwerkingsverantwoordelijke, noch de Verwerker, noch de personen die onder rechtstreeks gezag van de Verwerkingsverantwoordelijke of de Verwerker gemachtigd zijn om de Persoonsgegevens te verwerken.
Dienst(en)	De door Opdrachtnemer volgens de Overeenkomst te verrichten werkzaamheden of het tot stand te brengen resultaat
Dienstenbeschrijving	Overzicht van de beschrijvingen van de door Opdrachtnemer volgens de Overeenkomst te verrichten werkzaamheden of het tot stand te brengen resultaat.

Doelbinding	Het principe dat iemand (persoon of organisatie) alleen informatie mag vragen, opslaan, gebruiken, delen ten behoeve van welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden.
GEB	Gegevensbeschermingseffectenbeoordeling (ook wel Data Privacy Impact Assessment – DPIA). Onderzoek waarmee een organisatie inzicht krijgt in de privacy risico's.
Inbreuk in verband met persoonsgegevens (Datalek)	Een inbreuk als bedoeld in artikel 4 sub 12 van de AVG. Het betreft 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 ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens. Hierbij moet bijvoorbeeld worden gedacht aan het verlies van gegevensdragers waarop Persoonsgegevens staan, het verzenden van Persoonsgegevens naar een geadresseerde voor wie de Persoonsgegevens niet zijn bedoeld, of een gehackte database met Persoonsgegevens.
Informatiebeveiliging	Alles wat men doet om ervoor te zorgen dat men bij informatie kan komen wanneer men dat wil, dat de informatie klopt en de informatie niet bij anderen terecht komt. Het gaat daarbij vaak om een computersysteem, maar dat hoeft niet. Het gaat om maatregelen, procedures en processen die beveiligingsproblemen voorkomen, opsporen, onderdrukken en oplossen. Ontstaat er wel een probleem met de informatie? Dan zorgt Informatiebeveiliging ervoor dat de gevolgen zoveel mogelijk beperkt worden.
Informatiebeveiligings-risico	Zie risico.
Integriteit	De juistheid, tijdigheid, actualiteit en volledigheid van gegevens en de verwerking daarvan. Een onderdeel van Integriteit betreft de onweerlegbaarheid (non-repudiation). Dit is de mate waarin kan worden aangetoond dat acties of gebeurtenissen hebben plaatsgevonden, zodat deze acties of gebeurtenissen later niet kunnen worden ontkend.
IoT-devices:	Een netwerk van 'slimme' apparaten, sensoren en andere objecten die (vaak verbonden met het internet), gegevens verzamelen over hun omgeving, deze kunnen uitwisselen en op basis daarvan (semi)autonome beslissingen en/of acties nemen die van invloed zijn op hun omgeving.
Onderaannemer	Een Derde partij die door Opdrachtnemer wordt ingeschakeld om (delen van) de Diensten te leveren aan Opdrachtgever.
Opdrachtnemer	De contractspartij bij een Overeenkomst met Opdrachtgever.
Overeenkomst	Iedere rechtsbetrekking tussen Opdrachtgever en Opdrachtnemer met betrekking tot levering van een Prestatie, waarvan deze BVO onderdeel uitmaakt.
Personeel	De door partijen bij de uitvoering van de Overeenkomst in te schakelen personeelsleden en/of hulppersonen.
Persoonsgegeven	Een persoonsgegeven als bedoeld in artikel 4 sub 1 van de AVG. Een persoonsgegeven betreft alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon.

Risico	Een bedreiging of een omstandigheid die de Beschikbaarheid, Vertrouwelijkheid of Integriteit van gegevens of de continuïteit van de levering van de Dienst volgens deze Overeenkomst in gevaar brengt.
Schriftelijk	Onder Schriftelijk wordt in deze BVO verstaan op schrift. Als partijen enig ander communicatiemiddel zoals e-mail, internet of enig ander elektronisch medium gelijk wensen te stellen met Schriftelijk, dient dat uitdrukkelijk in de Overeenkomst te worden bepaald.
SLA	Service Level Agreement. Een beschrijving van de te leveren Dienst(-en) of product(-en) en de bijbehorende prestatie-indicatoren en kwaliteitseisen.
Subverwerker	De natuurlijke persoon of rechtspersoon die ten behoeve van de Verwerker (een deel) van de Persoonsgegevens verwerkt.
Weerbaarheid	De mogelijkheid voor te bereiden en aan te passen aan veranderende risico's en bedreigingen en het weerstaan van alle gevaren en het vermogen van de Diensten tot preventie en bescherming en tot snel herstel van verstoringen door incident- en calamiteitafhandeling en mitigatie.
Vertrouwelijke gegevens	Gegevens die naar hun aard alleen met een gerechtvaardigd doel aan Derden mogen worden verstrekt of ter inzage gegeven. Hieronder worden in ieder geval de volgende gegevens begrepen (bijzondere) persoonsgegevens, financiële gegevens, competitieve strategie gegevens of marketingplannen.
Vertrouwelijkheid	Het classificeren van de toegankelijkheid van gegevens en waarborgen dat deze alleen toegankelijk is voor degenen die hiertoe zijn geautoriseerd, dat wil zeggen vanuit de functie, taken en verantwoordelijkheden hiertoe gerechtigd zijn.
Verwerken	Elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, ver/-bewerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.
Verwerker	Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een Dienst of een ander orgaan die/ dat ten behoeve van de Verwerkingsverantwoordelijke Persoonsgegevens verwerkt.
Verwerkings-verantwoordelijke	De natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van Persoonsgegevens vaststelt.

Bijlage 2: Overzicht Persoonsgegevensverwerkingen

In deze bijlage moet in ieder geval het volgende nader worden gespecificeerd:

De naam van de Verwerking	
Het doel van de Verwerking	
De aard van de Verwerking	
Beschrijving Soort Persoonsgegevens (Categorieën)	
Beschrijving categorieën Betrokkenen	

Bijlage 3: Dienstenbeschrijving

Naam product en/of Dienst	
Soort product en/of Dienst	
Beknopte uitleg en werking product en Dienst	
Doelgroep product en/of dienst	
Gebruik van Onderaannemers/Subverwerkers in levering Dienst? Zo ja, welke?	
Beveiligingsmaatregelen op hoofdlijnen	