Beveiligingsovereenkomst ICT

tussen Centrum Indicatiestelling Zorg (CIZ) en < naam opdrachtnemer >

CIZ
Princenhof Park 3
3972 NG Driebergen
Postbus 232
3970 AE Driebergen
KvK Utrecht 30159219

T 088 - 789 67 00
F 088 - 789 67 01
E info@ciz.nl
www.ciz.nl

DOCUMENT VERSIE 1.0
22 APRIL 2015
STATUS DEFINITIEF

Deze pagina is opzettelijk leeg gelaten

Inhoudsopgave

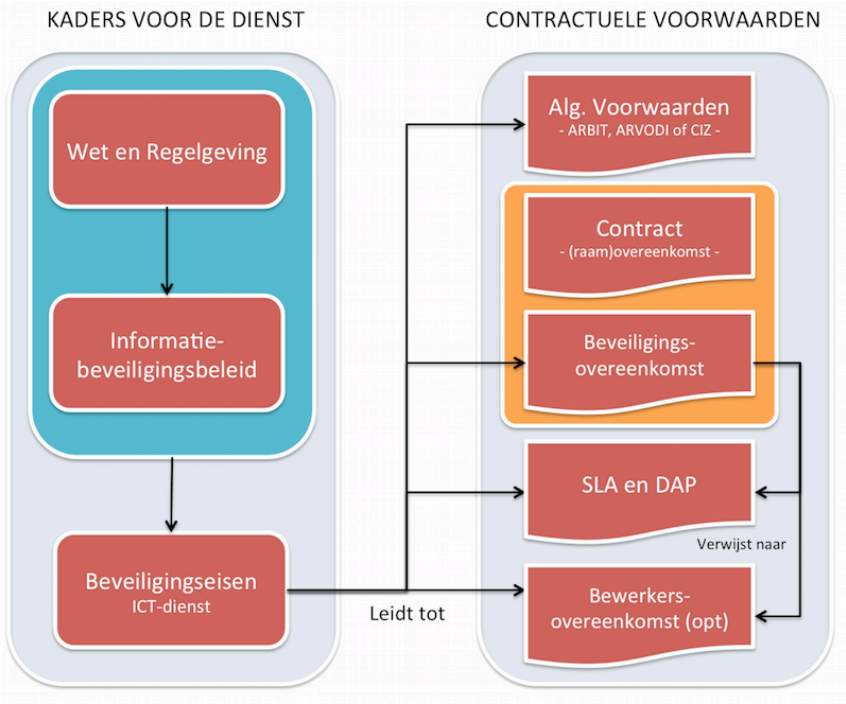
1 *Context*

1.1 Samenhang

De beveiligingsovereenkomst ICT maakt onderdeel uit van een stelsel van contractuele voorwaarden die door CIZ worden gehanteerd bij aanbesteding van ICT diensten. Ze sluit aan op de Algemene Voorwaarden. Hierin zijn condities opgenomen die onafhankelijk zijn van een specifieke dienst.

Afspraken in de overeenkomst kunnen worden uitgewerkt en geconcretiseerd in een Service Level Agreement (SLA) en Dossier Afspraken & Procedures (DAP). Als verwerking van vertrouwelijke gegevens plaatsvindt, dan wordt eveneens een bewerkersovereenkomst overeen gekomen tussen CIZ en de opdrachtnemer.

Dit levert voor de beveiligingsvereisten de volgende verhouding tussen de documenten op.



1.2 Reikwijdte

Deze beveiligingsovereenkomst geeft invulling aan het informatiebeveiligings-beleid van CIZ, waarbij het beleid en daarmee de contractering moet voldoen aan de normenkaders Baseline Informatiebeveiliging Rijksdienst (BIR), Wet Bescherming Persoonsgegevens (WBP) en DigiD.

Dit document helpt CIZ de vereiste verantwoordelijkheden in te vullen, daar waar het de beveiliging van ICT-diensten betreft die zijn uitbesteed.

Naast generieke beveiligingseisen, die van toepassing zijn op alle ICT-diensten, zijn ook specifieke eisen opgenomen die slechts gelden voor één of enkele vormen van diensten. Bijlage 2 toont welke eisen van toepassing zijn voor de diverse diensten.

2 *Beveiligingseisen*

2.1 Algemeen

2.1.1 Bewerkersovereenkomst

Indien Opdrachtnemer systemen beheert waarin persoonsgegevens verwerkt worden, dan zal een bewerkersovereenkomst worden afgesloten. Opdrachtgever stelt hiervoor een concept document op.

2.2 Beleid

2.2.1 Beheersing van de risico's

2.2.1.1 Security Management

Opdrachtnemer hanteert een security management proces voor het waarborgen van de beveiliging van de aangeboden dienst. Het proces is ISO/IEC 27001:2013 gecertificeerd of de werking ervan kan op een gelijkwaardig wijze worden aangetoond, niet later dan negen (9) maanden na de ondertekening van deze overeenkomst.

2.2.1.2 Beveiligingsprogramma

Aan de hand van een actuele risicoanalyse van de aangeboden dienst stelt Opdrachtnemer een beveiligingsprogramma vast en voert deze uit. Het programma wordt periodiek, maar minimaal iedere zes (6) maanden, aan Opdrachtgever voorgelegd en door hem geaccordeerd. Het programma stelt Opdrachtgever in staat om :

1. Periodiek de risico's in de afgenomen dienst te identificeren en beoordelen.
2. Passende risicobeperkende maatregelen te nemen in de eigen organisatie.
3. Het beveiligingsniveau van de dienst te beoordelen en toetsen op doeltreffendheid.

Toelichting 2.2.1.2 : Het beveiligingsprogramma heeft tot doel maatregelen te evalueren en aan te passen in het licht van ingeschatte risico's. Inzicht en er naar handelen door beide partijen heeft tot doel risico's daadwerkelijk af te wenden.

2.3 Maatregelen

2.3.1 Fysieke ruimten

2.3.1.1 Technische voorzieningen

Opdrachtnemer is verantwoordelijk voor alle technische voorzieningen in ruimten waar apparatuur voor de verwerking van gegevens van Opdrachtgever staan opgesteld.

2.3.1.2 Fysieke beveiliging

Opdrachtnemer verzorgt de fysieke beveiliging ter voorkoming van misbruik van de elektronische gegevens van Opdrachtgever. Opdrachtnemer laat fysieke toegang tot beveiligde ruimten alleen toe aan personen die hiertoe zijn geautoriseerd. Dit geldt ook voor de off-site locaties en gedurende fysiek transport.

Toelichting 2.3.1.2 : Onder beveiligde ruimten worden, behalve computer- en beveiligde opslagruimten, ook locaties verstaan van waaruit (remote) beheerwerkzaamheden worden uitgevoerd op de informatiesystemen.

2.3.1.3 Gewenste toegang

Voorafgaand aan de ingang van de overeenkomst is door Opdrachtgever en Opdrachtnemer bepaald en vastgelegd welke fysieke toegang Opdrachtnemer moet hebben tot beveiligde ruimten om de overeengekomen opdracht uit te voeren en welke noodzakelijke beveiligingsmaatregelen hiervoor nodig zijn.

Toelichting 2.3.1.3 : De afspraken hierover worden vastgelegd in de DAP.

2.3.1.4 Verplaatsingen

Opdrachtnemer zal geen apparatuur, programmatuur en vertrouwelijke gegevens van Opdrachtgever uit beveiligde ruimten verwijderen zonder toestemming van Opdrachtgever. Verplaatsingen zullen worden behandeld overeenkomstig standaard afspraken of aangemeld en gecoördineerd via het wijzigingsbeheerproces.

2.3.1.5 Inzicht in de verleende toegang

Opdrachtnemer kan de Opdrachtgever inzicht bieden in de verleende autorisaties voor toegang tot beveiligde ruimten. Dit inzicht wordt verschaft op basis van rollen en functies. Alleen als er zwaarwegende gronden zijn en aan de eisen van de WBP is voldaan - bijvoorbeeld bij vermoeden van fraude of misbruik - worden op eerste verzoek van Opdrachtgever in dit kader ook persoonsgegevens verstrekt.

2.3.2 Inrichtingseisen

2.3.2.1 Inzet van gedeelde omgevingen

Opdrachtnemer draagt zorg voor een veilige afscherming van gegevens van Opdrachtgever als omgevingen worden ingezet voor gemeenschappelijk gebruik door meerdere partijen of als deze logisch of fysiek met elkaar verbonden zijn. Opdrachtnemer en Opdrachtgever bepalen in overleg welk niveau van afscherming voor de ICT- en netwerkvoorzieningen afdoende is. Pas nadat is bepaald dat de afscherming van de gegevens afdoende is gewaarborgd kan de dienst geleverd worden.

2.3.2.2 Basisbeveiligingsniveau

Opdrachtgever hanteert voor de beveiliging van zijn gegevens de volgende normenkaders als basisbeveiligingsniveau (baseline).

1. Baseline Informatiebeveiliging Rijksdienst - Tactisch Normenkader (BIR TNK) : 2012;
2. CBP Richtsnoeren Beveiliging van Persoonsgegevens : 2013.
3. Norm ICT-beveiligingsassessments DigiD : 2012

Opdrachtnemer verbindt zich om bij de uitvoering van de dienst te borgen dat aan de eisen van deze normenkaders wordt voldaan, voor zover van toepassing op de geleverde dienst. Niet later dan zestig (60) dagen na ondertekening van de overeenkomst hebben Opdrachtnemer en Opdrachtgever overeenstemming bereikt over :

1. De (deel)verzameling van eisen die van toepassing zijn op de geleverde diensten;
2. De controls die Opdrachtgever binnen zijn dienstverlening heeft ingericht om aan deze eisen tegemoet te komen.

Toelichting 2.3.2.2 : De normenkaders bevatten beveiligingseisen waar Opdrachtgever aan heeft te voldoen vanuit zijn eigen bedrijfsvoering. Door uitbesteding van IT activiteiten aan Opdrachtnemer komen (delen) van deze eisen in scope bij Opdrachtnemer binnen de diensten die hij aan Opdrachtgever levert. Deze dienen verder op operationeel niveau te zijn afgestemd tussen Opdrachtgever en Opdrachtnemer en geformaliseerd en actueel gehouden in de DAP.

2.3.2.3 Hanteren aanvullende eisen

Opdrachtgever hanteert een aantal aanvullende beveiligingseisen, die worden gehanteerd indien er sprake is van verwerking van zeer vertrouwelijke gegevens overeenkomstig categorie WBP risicoklasse 3 of CIZ gegevens rubricering 'geheim'. Opdrachtnemer verbindt zich om bij de uitvoering van de dienst te borgen dat, daar waar noodzakelijk en aangegeven door Opdrachtgever, aan deze eisen wordt voldaan.

Toelichting 2.3.2.3 : Deze eisen dienen op operationeel niveau afgestemd te zijn tussen Opdrachtnemer en Opdrachtgever en geformaliseerd en actueel gehouden in de DAP.

2.3.2.4 Wijzigingen in de dienst

Wijziging in de dienst worden vooraf door Opdrachtgever beoordeeld op afwijkingen t.o.v. het beveiligingsniveau (2.3.2.2 & 2.3.2.3) en eventuele risico's voor de bedrijfsvoering van Opdrachtgever. Risico's worden door de Opdrachtnemer omgezet in mitigerende maatregelen, waarbij afspraken zijn gemaakt tussen Opdrachtgever en Opdrachtnemer over de termijn van de invoering.

Toelichting 2.3.2.4 : De afwijkingen en de impact daarvan worden behandeld in overleg tussen Opdrachtnemer en Opdrachtgever en vastgelegd in de DAP. In de praktijk vindt dat overleg plaats tussen de Security Officers van Opdrachtnemer en Opdrachtgever.

2.3.2.5 Mitigatie van kwetsbaarheden

Opdrachtnemer zal de beveiliging van de dienst waarborgen door het toepassen van adequate kwetsbaarheden management processen en –technieken.

Toelichting 2.3.2.5 : Voor identificatie en mitigatie van kwetsbaarheden zijn enkele voorbeelden van security best practices beschikbaar zoals security patching, hardening en penetratietesting. Opdrachtnemer is zelf verantwoordelijk voor een juiste selectie van methoden en technieken binnen zijn dienst.

2.3.3 Logische toegangsbeveiliging

2.3.3.1 Toegang beperkt tot een minimum

Opdrachtnemer voorziet het personeel, inhuur en derde partijen alleen met een minimum niveau van toegang nodig om de taken en functies, waarvoor zij verantwoordelijk zijn, uit te voeren. Door middel van functiescheiding is voorkomen dat een combinatie van toegangsrechten kan leiden tot een ongeautoriseerde cyclus van handelingen.

2.3.3.2 Individuele toerekenbaarheid

Het inlogbeleid en de inrichting van de authenticatieomgeving van Opdrachtnemer, biedt voldoende zekerheden voor individuele toerekenbaarheid. Activiteiten zijn herleidbaar naar natuurlijke personen of identificeerbare, geautoriseerde processen.

2.3.3.3 Authenticatie

Toegang tot gegevens van Opdrachtgever vindt alleen plaats na passende authenticatie. Opdrachtnemer past technieken en middelen toe voor het vaststellen van de unieke identiteit van personen en systemen die toegang vereisen om taken en functies uit te voeren. De sterkte van deze middelen is afgestemd op het risicoprofiel van de gebruikersgroep of de koppelingen.

Toelichting 2.3.3.3 : Het toegangsbeleid heeft tot doel alleen geautoriseerde personen en processen (systeemkoppelingen) toegang te verstrekken tot de gegevens. De identificatiemethode houdt rekening met de locatie van waaruit toegang wordt gevraagd, de vertrouwensrelatie en de classificatie van de gegevens waartoe toegang wordt verstrekt. Afspraken worden vastgelegd in de DAP.

2.3.3.4 Toegang voor beheerders

Voorafgaand aan de start van de overeenkomst is door Opdrachtgever en Opdrachtnemer bepaald en vastgelegd welke logische toegang Opdrachtnemer heeft tot gegevens van Opdrachtgever bij het uitvoeren van de overeengekomen opdracht en welke beveiligingsmaatregelen zijn getroffen om onbevoegd gebruik van deze gegevens te voorkomen.

Toelichting 2.3.3.4 : Opdrachtnemer heeft vanaf zijn beheerverantwoordelijkheid verregaande (technische) mogelijkheden om vertrouwelijke gegevens van CIZ te benaderen. Dit is een risico dat moet onderzocht, gekwalificeerd en desgewenst afgedekt met maatregelen. Afspraken hierover worden vastgelegd in de DAP.

2.3.3.5 Centrale registratie

Opdrachtnemer hanteert een centrale administratie waarin de autorisaties zijn vastgelegd (of te herleiden) die zijn uitgegeven voor toegang tot de gegevens van Opdrachtgever. De administratie wordt actueel gehouden en biedt op ieder moment een volledig en betrouwbaar beeld van de verstrekte bevoegdheden aan medewerkers van Opdrachtgever, -Opdrachtnemer en geautomatiseerde processen. Opdrachtnemer hanteert een geformaliseerd proces voor wijzigingen op deze administratie (verlenen, aanpassen, intrekken) en controleert periodiek de actualiteit ervan.

Toelichting 2.3.3.5 : De frequentie waarmee de actualiteit van autorisaties wordt gecontroleerd hangt samen met het risicoprofiel. Autorisaties verstrekt aan medewerkers, zoals systeem-, database- en netwerkbeheerders en medewerkers die toegang hebben tot WBP risicoklasse 3 gegevens, zullen zeer regelmatig gecontroleerd moeten worden. Opdrachtgever en Opdrachtnemer brengen samen de risicoprofielen en groepen in kaart en leggen afspraken over controles vast in de DAP.

2.3.3.6 Inzicht in de toegang

Opdrachtnemer voorziet Opdrachtgever van een actuele lijst van alle personen en processen die toegang hebben tot applicaties en gegevens, inclusief de verstrekte bevoegdheden. De Opdrachtnemer verstrekt deze lijst minstens iedere drie (3) maanden of op verzoek van de Opdrachtgever.

Toelichting 2.3.3.6 : Het rapportageformaat wordt vastgelegd in de DAP.

2.3.4 Monitoring en incidentafhandeling

2.3.4.1 Preventie en opsporing

Opdrachtnemer neemt maatregelen met betrekking tot signalering en registratie van oneigenlijk gebruik van gegevens. Het gebruik van de gegevens 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 registratie is zodanig voorzien van maatregelen dat deze blijft bestaan en niet gewijzigd kan worden.

Toelichting 2.3.4.1 : De bewaartermijnen van de registraties zijn in overeenstemming met wettelijke eisen en vastgelegd in de SLA.

2.3.4.2 **Melden van beveiligingsincidenten**

Opdrachtnemer en Opdrachtgever komen overeen dat in geval Opdrachtnemer (pogingen tot) inbreuken op de beveiligingsmaatregelen van vertrouwelijke gegevens w.o. Persoonsgegevens signaleert, Opdrachtnemer de Opdrachtgever hierover onmiddellijk zal inlichten en alle redelijkerwijs benodigde maatregelen zal treffen om (verdere) schending te voorkomen of te beperken.

Toelichting 2.3.4.2 : Dit artikel helpt Opdrachtnemer bij de beoordeling wanneer hij wel of niet een melding moet maken. Ook leest u hier hoe u een melding doet. Dit artikel is tevens bedoeld als aanvulling op de Wet meldplicht datalekken. In de SLA en DAP is een overzicht opgenomen van potentiële beveiligingsincidenten, prioriteiten en escalatiepaden waarop Opdrachtgever bewaking wil zien incl. rapportage.

2.3.4.3 **Dashboard op risico's**

Om actueel inzicht te hebben in de geïdentificeerde incidenten biedt de Opdrachtnemer een dashboard of rapportage. Het omvat alle informatie die Opdrachtgever redelijkerwijs nodig heeft om te kunnen bepalen welke risico's incidenten leveren voor de bedrijfsvoering van Opdrachtgever. Eventuele aanvullende informatie welke wenselijk wordt geacht door de Opdrachtgever dient aangeleverd te worden.

2.3.4.4 **Periodiek rapportage**

Opdrachtnemer rapporteert Opdrachtgever over de geïdentificeerde incidenten en de genomen maatregelen. Opdrachtnemer verstrekt deze rapportage conform de afspraken in de SLA 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.

Toelichting 2.3.4.4 : De frequentie is afhankelijk van het belang dat Opdrachtgever ziet in het tijdig beschikbaar krijgen van de rapportage.

2.3.4.5 **Rapportage na een incident of calamiteit**

Als Opdrachtnemer overeengekomen dienst vanwege beveiligingsincidenten of –calamiteiten niet meer of beperkt kan leveren, wordt Opdrachtgever hiervan per direct op de hoogte gesteld. Opdrachtnemer zal de consequenties en zo mogelijk de oorzaak van het beveiligingsincident of de beveiligingscalamiteit aan Opdrachtgever inzichtelijk maken, waarna partijen in overleg beslissen of de dienstverlening aangepast zal blijven dan wel volledig hervat dient te worden.

2.4 Vertrouwelijkheid

2.4.1 Non-disclosure van informatie van de Opdrachtgever

2.4.1.1 Doelbinding

Alle vertrouwelijke gegevens van Opdrachtgever wordt geacht eigendom te zijn van Opdrachtgever. Opdrachtnemer en zijn (ingehuurd) personeel en Onderaannemers gebruiken deze gegevens alleen voor het doel waarvoor Opdrachtgever deze informatie heeft verstrekt.

2.4.1.2 Passende toegang

Opdrachtnemer draagt er zorg voor dat alleen diens personeel en Onderaannemers, die voor de levering van de dienst aan Opdrachtgever toegang tot vertrouwelijke gegevens nodig hebben, deze toegang heeft. Opdrachtnemer neemt daarom adequate maatregelen ter borging van de geheimhouding en de vertrouwelijkheid door de toegang tot deze gegevens te beperken tot degenen die voor het uitvoeren van de hun toegewezen taken de noodzaak hebben voor toegang tot deze informatie.

Toelichting 2.4.1.2 : Omdat vertrouwelijke gegevens beschermd moeten zijn tegen onbedoelde openbaarmaking, wordt geen toegang gegeven aan degenen die vanuit hun toegewezen taken niet de noodzaak hebben om toegang te hebben tot deze informatie.

2.4.1.3 Gedragslijnen en procedures

Opdrachtnemer implementeert en onderhoudt passende gedragslijnen en procedures om de vertrouwelijkheid van de informatie op basis van Paragraaf 2.5.1.1 te waarborgen.

Toelichting 2.4.1.3 : In geval van ongeoorloofde openbaarmaking, verlies of vernietiging van vertrouwelijke gegevens, moet de ontvangende partij onmiddellijk de onthullende partij hiervan op de hoogte brengen en alle redelijke maatregelen nemen om eventuele schade of verdere openbaarmaking, verlies of vernietiging van dergelijke vertrouwelijke gegevens te voorkomen.

2.4.1.4 Ketenbinding

Opdrachtnemer staat in voor de nakoming van de in deze overeenkomst vastgelegde verplichtingen, ook door zijn Onderaannemers. Hij legt deze dezelfde geheimhoudingsverplichting op als hij jegens Opdrachtgever heeft en bekrachtigt deze met een ondertekende verklaring.

2.4.1.5 Verstrekking aan Derden

Opdrachtnemer 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.

Toelichting 2.4.1.5 : De verstrekking aan Derden betreft ook wettelijk opgelegde verplichtingen tot openbaar maken zoals de meldplicht Datalekken. Vertrouwelijke gegevens mogen alleen openbaar worden gemaakt aan een ontvangende partij op basis van een vooraf verstrekt schriftelijk advies van de juridisch adviseur van Opdrachtgever. Aan dit advies tot het openbaar maken, met daarin

vastgelegd de ontvangende partij, ligt altijd een wettelijke verplichting of een opdracht van een rechtbank of een overheidsinstantie ten grondslag.

2.4.1.6 Locatie van gegevens

Opdrachtnemer zal kenbaar maken op welke locatie(s) gegevens van Opdrachtgever worden verwerkt en welke overheden en jurisdicties aanspraak kunnen maken op deze gegevens. Opdrachtgever kan aan Opdrachtnemer verzoeken deze verwerking te verplaatsen naar een locatie binnen de Europese Unie (EU). Hiervoor zal een gemotiveerde onderbouwing worden verstrekt.

2.4.1.7 Verzoeken tot openbaarmaking

Opdrachtnemer meldt onmiddellijk alle verzoeken tot het delen van of verzoeken tot toegang tot vertrouwelijke gegevens, voor zover de verzoeken niet afkomstig zijn van personen die op basis van hun taak of functie rechtmatig inzage mogen hebben in deze informatie.

2.4.1.8 Rol van de Opdrachtgever

De Opdrachtgever voorkomt met dezelfde zorg het openbaar maken van vertrouwelijke informatie van de Opdrachtnemer als dat door hem wordt gevraagd.

2.4.2 Afhandelen van het bezit van informatie

2.4.2.1 Teruggave van informatie

Op het moment dat de overeenkomst afloopt of op een ander tijdstip op schriftelijk verzoek van de Opdrachtgever wordt beëindigd, wordt alle informatie en alle kopieën van deze informatie, die in bezit of beheer zijn bij de Opdrachtnemer of Onderaannemers, teruggegeven in een voor de Opdrachtgever verwerkbare vorm, tenzij Opdrachtgever op dat moment verzoekt deze informatie te vernietigen. In dat geval levert Opdrachtnemer na de uitvoering van de vernietiging aan Opdrachtgever een "Verklaring van vernietiging".

2.4.2.2 Uit roulatie nemen bedrijfsmiddelen

Op het moment dat bedrijfsmiddelen met gegevens of software van Opdrachtgever uit roulatie worden genomen, wordt alle informatie en software door Opdrachtnemer vernietigd.

2.4.2.3 Vastlegging uit roulatie genomen bedrijfsmiddelen

Voor de bedrijfsmiddelen die uit roulatie worden genomen legt Opdrachtnemer ten behoeve van Opdrachtgever vast hoe en op welk moment de overdracht, teruggave of vernietiging van gegevens, software en andere bedrijfsmiddelen plaats zal vinden. Hiertoe kan Opdrachtnemer te allen tijde volledig inzicht bieden in:

1. De bedrijfsmiddelen die ter beschikking zijn gesteld;
2. De bedrijfsmiddelen die uit roulatie zijn genomen;
3. De gehanteerde wijze van vernietiging en/of afgifte van gegevens, software en andere bedrijfsmiddelen.

Toelichting 2.4.2.3 : Van bedrijfsmiddelen die uit roulatie worden genomen moet met zekerheid kunnen worden vastgesteld dat de gegevens of software van Opdrachtgever niet toegankelijk is en wordt voor onbevoegden. Bedrijfsmiddelen worden uit roulatie genomen na bijvoorbeeld een defect of het einde van het gebruik.

2.5 Continuïteit

2.5.1 Stelsel van essentiële diensten

2.5.1.1 Inzicht in het stelsel

Voorafgaand aan de ingang van de overeenkomst heeft Opdrachtgever de continuïteitseisen (MTU/MTG) opgesteld voor de belangrijkste processen. Opdrachtnemer beschrijft aan de hand hiervan de essentiële diensten zodanig dat Opdrachtgever een goede inschatting kan maken of de aangeboden dienstverlening gaat voldoen aan de gestelde eisen.

2.5.1.2 Inzicht in de weerbaarheid en continuïteit

Voorafgaand aan de ingang van de overeenkomst beschrijft Opdrachtnemer de belangrijkste maatregelen die zijn getroffen om de continuïteit en de weerbaarheid van de essentiële diensten te garanderen.

2.5.2 Versterken van de essentiële diensten

2.5.2.1 Vergroten van de weerbaarheid en continuïteit

Opdrachtnemer identificeert en analyseert de kansen en mogelijkheden om de weerbaarheid en continuïteit van de essentiële diensten te verbeteren, inclusief de mogelijke gevolgen ervan voor de dienstverlening aan Opdrachtgever.

2.5.2.2 Vaststelling van de baseline

Binnen dertig (30) dagen na ingang van de overeenkomst heeft Opdrachtnemer de als minimum te hanteren baseline voor de continuïteit en de weerbaarheid van de dienst vastgesteld en ter goedkeuring aangeboden aan Opdrachtgever.

2.5.2.3 Evaluatie van de weerbaarheid

Binnen zestig (60) dagen na ingang van de overeenkomst toont Opdrachtnemer in een risico analyse de effectiviteit van de beveiligingsmaatregelen aan en hebben Opdrachtnemer en Opdrachtgever deze analyse geëvalueerd.

2.5.3 Continueren van de essentiële diensten

2.5.3.1 Continuïteitsplanning

Binnen zes (6) maanden na ingang van de overeenkomst heeft Opdrachtnemer continuïteitsplannen voor de essentiële diensten opgesteld. De plannen worden op initiatief van Opdrachtnemer periodiek getest en gecontroleerd op de resultaten.

2.5.4 Voorkomen discontinuïteit

2.5.4.1 Escrow-regeling

Partijen verbinden zich een Escrow-regeling, overeenkomst de vereisten in ARBIT 2014 artikel 47, te treffen ten aanzien van de geleverde dienst, teneinde de continuïteit van de dienstverlening te garanderen in de situatie dat Opdrachtnemer niet kan voldoen aan alle vereisten in de overeenkomst. De regeling geldt voor de duur van de overeenkomst en de periode daarna die nodig is om de continuïteit van de dienstverlening van Opdrachtgever te borgen.

Toelichting 2.6.4.1 : Binnen een Escrow-regeling zijn afspraken vastgelegd over de support, documentatie en het beschikbaar hebben van een actuele versie van de software. Als sprake is van informatie van de Opdrachtgever op de systemen van de Opdrachtnemer, worden in de esrowregeling afspraken vastgelegd over het beschikbaar hebben van een actuele versie van de informatie van de Opdrachtgever, inclusief metagegevens. Als sprake is een geleverde dienst, waarvan de beschikbaarheid van de levering van dedDienst aan de Opdrachtgever een voor de bedrijfsvoering van de Opdrachtgever essentiële dienst bevat, worden in de ecrowregeling afspraken vastgelegd over de tijdige uitwijk, inclusief het tijdig beschikbaar hebben van een actuele versie van de informatie.

2.6 Audits

2.6.1 Documentatie en administratie

2.6.1.1 Bijhouden

Opdrachtnemer onderhoudt een volledige en nauwkeurige documentatie en administratie die betrekking heeft op deze beveiligingsovereenkomst, met inbegrip van elektronische kopieën van al deze documenten en administratie.

2.6.1.2 Inhoud

De documentatie en administratie bevatten voor Opdrachtgever voldoende betrouwbare informatie om een redelijke zekerheid te bieden dat Opdrachtnemer voldoet aan het gestelde in de beveiligingsovereenkomst.

2.6.1.3 Toegang

Opdrachtgever heeft het recht om tijdens kantooruren op deze documenten en administratie of een deel daarvan een audit uit te voeren. Opdrachtnemer verstrekt op specifiek verzoek van Opdrachtgever binnen maximaal vijf werkdagen in elektronische vorm toegang tot de gevraagde documentatie en administratie.

2.6.1.4 Verwerking

Opdrachtgever kan informatie en kopieën van deze documenten en administratie voor auditdoeleinden verwerken. Het gebruik van deze gegevens is onderworpen aan de standaard praktijk ten aanzien van audits.

2.6.1.5 Bewaartermijn

De Opdrachtnemer bewaart de documenten en administratie die betrekking hebben op het uitvoeren van de Dienst tot minimaal : Zeven (7) jaar na de laatste betaling aan de Opdrachtnemer, vijf (5) jaar na de definitieve afronding van alle audits of na sluiting van een geschil met betrekking tot deze overeenkomst of een langere periode, als vereist door de toepasselijke Europese of nationale wet- en regelgeving.

Toelichting 2.6.1.5 : De termijnen zijn afhankelijk van het belang dat Opdrachtgever ziet voor het beschikbaar hebben van de documenten en administratie. De termijnen worden bepaald door de partij die namens Opdrachtgever de audits uitvoert.

2.6.2 Het uitvoeren van audits

2.6.2.1 Recht op audits

Opdrachtgever of haar gemachtigde vertegenwoordigers hebben het recht om op elk moment, met inachtneming van een aankondigingstermijn van één (1) maand na het indienen van een schriftelijke verzoek, een audit uit te voeren op de beveiligingsmaatregelen. Een volledige audit zal niet vaker dan één (1) keer per contractjaar plaatsvinden, tenzij bevindingen uit deze audit aanleiding geven tot één of meerdere heraudits. Opdrachtgever behoud zich dan het recht voor om heraudits uit te voeren tot de bevindingen zijn opgelost. De kosten van de audit zijn voor Opdrachtgever.

2.6.2.2 Deelaudits

Opdrachtgever of haar gemachtigde vertegenwoordigers hebben het recht om op elk moment, met inachtneming van een aankondigingstermijn van één (1) maand na het indienen van een schriftelijke verzoek, een audit uit te voeren op delen van de beveiligingsmaatregelen. De kosten van de audit zijn voor Opdrachtgever.

Toelichting 2.6.2.2 : Deelaudits betreffen beperkte audits op delen van de security omgeving. Denk hierbij aan audits op toegangsbeveiliging, autorisatiebeheer, beveiligingsorganisatie, monitoring, etc.

2.6.2.3 Het verlenen van toegang

Opdrachtnemer verleent de Opdrachtgever of haar gemachtigde vertegenwoordigers toegang tot de faciliteiten van de Opdrachtnemer en haar onderaannemers, documenten en administratie, alle feiten met betrekking tot de prestaties van de dienst en andere bescheiden van Opdrachtnemer, voor zover zij betrekking hebben op deze beveiligingsovereenkomst.

2.6.2.4 Het verlenen van bijstand

Opdrachtnemer zal Opdrachtgever of haar gemachtigde vertegenwoordigers alle informatie verstrekken en bijstand verlenen bij het uitvoeren van de audits. Dit geldt zolang dit niet de levering van de dienst nadelig beïnvloedt.

2.6.2.5 Onderaannemers

Opdrachtnemer zal de inhoud van Paragraaf 2.6.2 opnemen in de overeenkomst(en) met de Onderaannemer(s) die zijn betrokken bij de levering van deze dienst.

2.6.3 Corrigerende maatregelen

2.6.3.1 Correctief plan

In audits geconstateerde tekortkomingen worden door Opdrachtnemer opgepakt en omgezet in een plan. Dit plan wordt binnen tien (10) kalenderdagen na schriftelijke rapportage over de constatering ter beoordeling en goedkeuring aan Opdrachtgever aangeboden.

2.6.3.2 **Implementatie corrigerende maatregel**

Opdrachtnemer draagt voor eigen rekening zorg voor de implementatie van de corrigerende maatregel en documenteert de corrigerende maatregel. Deze documentatie moet aan Opdrachtgever de effectiviteit van de maatregel aantonen. Opdrachtnemer moet de geconstateerde tekortkoming verhelpen, in geen geval later dan dertig (30) dagen na ontvangst van de kennisgeving van deze tekortkoming, tenzij de partijen anders zijn overeengekomen.

3 *Ondertekening*

Als onderdeel van de hoofdovereenkomst wensen partijen door middel van deze beveiligingsovereenkomst afspraken overeen te komen betreffende de beveiliging en privacyaspecten van de onder de dienstverlening vallende informatieverwerking en verdere verbetering van deze aspecten in de toekomst.

Met de ondertekening gaan beide partijen, Opdrachtgever en Opdrachtnemer, akkoord met de afspraken in deze beveiligingsovereenkomst ICT.

3.1 Slotbepaling en handtekeningen

Namens CIZ	Namens de [bedrijfsnaam]
Barend Bol	[naam]
Chief Information Officer	Directeur
dd. _____	dd. _____
Nederland	Nederland
.....	.....

Bijlage 1. Definities en afkortingen

Belangrijkste Onderaannemers: Die Onderaannemers die voor Opdrachtnemer essentieel zijn om te kunnen voldoen aan de in de overeenkomst en SLA gestelde eisen ten aanzien van beschikbaarheid, integriteit en vertrouwelijkheid.

Beschikbaarheid: De toegang voor geautoriseerde gebruikers op de overeengekomen momenten tot gegevens en aanverwante bedrijfsmid-delen zoals informatiesystemen, oftewel het zorgen voor een ongestoorde voortgang van de informatievoorziening.

Betrokkene: Degene op wie een gegeven betrekking heeft.

Bewerker: Degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen.

Controle: De mogelijkheid om met een voldoende mate van zekerheid te kunnen vaststellen of wordt voldaan aan de eisen zoals gesteld in deze overeenkomst en zoals die zijn vastgelegd in wet- en regelgeving.

Coördineren: Het besluitvormingsproces, waarbij de betrokken partijen de gemeenschappelijke doelen bereiken.

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, de bewerker, of enig persoon die onder rechtstreeks gezag van de verantwoordelijke of de bewerker gemachtigd is om persoonsgegevens te verwerken.

Dienst: De door Opdrachtnemer op basis van de Overeenkomst ten behoeve van Opdrachtgever te verrichten werkzaamheden.

Doelbinding: Het principe dat iemand (persoon of organisatie) alleen informatie mag verwerken ten behoeve van welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden.

Essentiële Diensten: De diensten, systemen en bedrijfsmiddelen, fysiek of virtueel, die essentieel zijn om te kunnen voldoen aan de in de overeenkomst en SLA gestelde eisen ten aanzien van beschikbaarheid, integriteit en vertrouwelijkheid.

Integriteit: De juistheid, tijdigheid, actualiteit en volledigheid van informatie 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.

Kritische momenten: Die momenten in de bedrijfsvoering van Opdrachtgever, waarbij de beschikbaarheid van de dienst essentieel is voor Opdrachtgever om te voldoen aan zijn verplichtingen.

MTG : Maximaal Toegestane gegevensverlies. Dit is de maximaal geaccepteerde hoeveelheid data die verloren gaat als gevolg van een calamiteit.

MTU : Maximaal Toegestane Uitvalduur. Dit is de maximaal geaccepteerde tijdsduur dat een proces niet beschikbaar is.

Onderaannemer: Een derde partij die door Opdrachtnemer wordt ingeschakeld om (delen van) de Dienst te leveren aan Opdrachtgever.

Persoonsgegeven: Elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.

Risico: Een bedreiging of een omstandigheid die de continuïteit van de levering van de dienst volgens deze overeenkomst in gevaar brengt.

Samenwerking: Het proces van samenwerken tussen twee of meerdere partijen om gemeenschappelijke doelen te bereiken.

SLA (Service Level Agreement): Een beschrijving van de te leveren dienst(-en) of product(-en) en de bijbehorende prestatie-indicatoren en kwaliteitseisen.
Verantwoordelijke: De natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.

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 persoonsgegevens en financiële informatie.

Vertrouwelijkheid: Het classificeren van de toegankelijkheid van informatie 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.

Verwerking van persoonsgegevens: Elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikking-stelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.

Weerbaarheid: Het vermogen van de dienst om zich aan te passen aan veranderende risico’s en bedreigingen en snel te herstellen van verstoringen door incident- en calamiteitafhandeling.

Bijlage 2. Matrix

Onderstaande matrix toont een overzicht van de eisen, op hoofdlijnen uitgesplitst naar vier groepen van ICT diensten. De argumenten die ten grondslag liggen aan de getoonde groepen zijn het type dienstverlening – deze moet aantoonbaar onderscheidenlijk zijn - en de mate waarin CIZ zijn beveiligingsmaatregelen kan opleggen aan de Opdrachtnemer.

De ICT markt is volop in ontwikkeling en er zijn varianten op de benoemde diensten te bedenken die niet volledig passen in de getoonde groepen. Indien hierdoor een eis niet van toepassing is kan deze worden uitgesloten van de overeenkomst. De motivatie hiervoor dient te worden onderbouwd, gedocumenteerd en geaccordeerd door de CISO en CIO.

Beveiligingseisen	Applicatieontwikkeling	IaaS / PaaS	SaaS	Inhuur personeel
2.1 Algemeen				
2.1.1 Bewerkersovereenkomst	X	X	X	
2.2 Beleid				
2.2.1 Beheersing van de risico's	X	X	X	
2.3 Beveiligingsmaatregelen				
2.3.1 Fysieke ruimten		X		
2.3.2 Inrichtingseisen	X	X	X	
2.3.3 Logische toegangsbeveiliging		X	X	
2.3.4 Monitoring en incidentafhandeling	X	X	X	
2.4 Vertrouwelijkheid				
2.4.1 Non-disclosure van informatie van de Opdrachtgever	X	X	X	X
2.4.2 Afhandelen van het bezit van informatie	X	X	X	X

Beveiligingseisen (vervolg)	Applicatieontwikkeling	IaaS / PaaS	SaaS	Inhuur personeel
2.5 Continuïteit				
2.5.1 Stelsel van Essentiële Diensten		X	X	
2.5.2 Versterken van de Essentiële Diensten		X	X	
2.5.3 Continueren van de Essentiële Diensten		X	X	
2.5.4 Voorkomen discontinuïteit in de beschikbaarheid	X			
2.6 Audits				
2.6.1 Documentatie en administratie	X	X	X	
2.6.2 Het uitvoeren van audits	X	X	X	
2.6.3 Corrigerende maatregelen	X	X	X	