



Logius
Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties

Opdrachtovereenkomst onderzoek beveiliging standaardisatie uitwisseling Fraudesignalen

Opdrachtgever: Zorgverzekeraars Nederland

Opdrachtnemer: Logius

Versie 1.03

Status: voorstel

Datum: 18-08-2015

Colofon

Titel Opdrachtovereenkomst onderzoek beveiliging
standaardisatie uitwisseling Fraudesignalen

Versienummer 1.03

**Opdrachtgever
namens de TIZ**
 Verzekeringen en Uitvoering
E: @zn.nl
T:

Contactpersonen
E: @zn.nl
T:

E: @zn.nl
T:

Afdeling Verzekeringen en Uitvoering
Zorgverzekeraars Nederland
Postbus 520
3700 AM Zeist

**Contactpersoon
Opdrachtnemer**
Afdeling Handel & Transport
Logius
Postbus 96810
2509 JE Den Haag
E: @logius.nl
T:

**Verplichtingennummer
Opdrachtgever** <Indien van toepassing hier opnemen>

**Projectcode
Opdrachtnemer** <Logius nummer voor de administratie>

1 Versiebeheer

Datum	Versie	Auteur	Opmerkingen
24-7-2015	0.9		Collegiaal review en concern controller verwerkt, profielen toegevoegd
31-7-2015	1.0		Opmerkingen verwerkt
3-8-2015	1.02		Achternamen gecorrigeerd van
18-8-2015	1.03		Opmerkingen verwerkt.

2 Inhoudsopgave

Colofon	2
1 Versiebeheer	3
2 Inhoudsopgave	4
3 Opdrachtomschrijving	5
3.1 Inleiding	5
3.2 Uw vraag	6
3.3 Logius als partner	6
4 Plan van Aanpak	8
4.1 Aanpak opdrachtuitvoering	8
4.1.1 Fase 1: Opstartfase	8
4.1.2 Fase 2: Onderzoek	9
4.1.3 Fase 3: Rapportage	9
4.2 Planning	10
4.3 Samenwerking tijdens uitvoering opdracht	11
4.4 Ureninzet	11
4.5 Geheimhouding	11
4.6 Risico's	11
5 Algemene bepalingen	12
5.1 Rollen en verantwoordelijkheden	12
5.2 Diensten van derden	12
5.3 Wijzigen opdracht	12
5.4 Tussentijdse beëindiging van de Opdrachtovereenkomst	12
6 Financiën	13
6.1 Geldigheidsduur	13
6.2 Kosten	13
6.3 Facturatie	13
6.4 Kostenafwijkingen	13
7 Ondertekening	14
BIJLAGE 1 : Profielschets Logius medewerkers	15

3 Opdrachtoomschrijving

3.1 Inleiding

Zorgverzekeraars voeren in het kader van het beheersen van de zorgkosten onder meer onderzoeken uit naar signalen van mogelijke fraude. Deze onderzoeken administreren zij in hun eigen systemen en zij wisselen een deel van deze signalen uit met andere zorgverzekeraars en een aantal (overheids)ketenpartners.

Om de samenwerking tussen de partners te regelen, is het convenant verbetering bestrijding zorgfraude opgesteld, dat de oprichting van de Taskforce Integriteit Zorgsector (TIZ) regelt. De TIZ heeft op 6 juli 2015 besloten gezamenlijk een standaard voor informatie-uitwisseling te ontwikkelen.

In 2014 heeft Zorgverzekeraars Nederland (ZN) een onderzoek laten uitvoeren naar de mogelijkheden om de uitwisseling van fraudesignalen te standaardiseren en daarmee verder te laten automatiseren. Uitkomst van dit onderzoek is dat er zowel technisch als inhoudelijk goede mogelijkheden zijn hiervoor, maar dat de beveiliging van gegevens hierbij nog een belangrijk punt van aandacht is. Bij het uitwisselen van informatie over mogelijke fraudegevallen speelt immers de beveiliging/afscherming van die gegevens een belangrijke rol. In het onderzoek naar de mogelijkheid van de standaardisatie is reeds een aantal beveiligingsrequirements benoemd:

1. Ver- en ontsleutelen (B1)
Dit zijn functies om het bericht gedurende het transport onleesbaar te maken en na transport weer terug leesbaar. Dit zijn geautomatiseerde stappen. De gebruiker hoeft hier niets voor te doen.
2. Toegangsbeveiliging (B2)
Borgen dat het uitwisselproces alleen voor bevoegde medewerkers toegankelijk is. Wat partijen daar precies onder verstaan, is afhankelijk van het benodigde beveiligingsniveau. Het is in ieder geval helder dat toegang op basis van uitsluitend gebruikersnaam-wachtwoord onvoldoende is;
3. Gegevens autorisatie (B3)
Het is belangrijk dat elke partij die gegevens te zien krijgt die nodig zijn voor de interne fraudeprocessen. Echter niet alle partijen mogen alle informatie ontvangen. De verzendfunctie moet 'weten' welke partij welke gegevens mag zien.
4. Audit/trail (B4)
De audit/trail bevat voldoende gegevens om achteraf te kunnen herleiden welke essentiële handelingen wanneer door wie of vanuit welk systeem met welk resultaat zijn uitgevoerd. Tot essentiële handelingen worden in ieder geval gerekend: opvoeren en afvoeren posten, statusveranderingen met wettelijke, financiële of voor de voortgang van het proces, de zaak of de klant beslissende gevolgen.;
5. Verantwoordelijkheidsoverdracht (B5)
Wanneer een bericht wordt ontvangen, wordt geautomatiseerd een ontvangstbevestiging verstuurd. Zodra de ontvangstbevestiging is verzonden, wordt de verantwoordelijkheid voor de data overgedragen aan de ontvangende partij.

Deze opdrachtovereenkomst betreft een vervolgonderzoek naar de beveiliging van de gegevens voor het gestandaardiseerd uitwisselen van fraudesignalen.

3.2 Uw vraag

De behoefte van de convenantpartners is erop gericht om een aanvullend onderzoek uit te voeren naar het benodigde en gewenste beveiligingsniveau van de uitwisseling tussen diverse ketenpartners en bijhorende nadere uitwerking van de beveiligingsmaatregelen, inclusief een doorvertaling te geven naar de technische facilitering hiervan.

De te leveren resultaten van deze opdracht zijn:

- Een uitwerking van het beveiligingsniveau, i.e. een beschrijving van de door alle betrokken partijen gevalideerde betrouwbaarheidsaspecten behorende bij het proces van uitwisseling van fraudesignalen en het (te selecteren) standaardsysteem hierbij.
- Op basis van een gezamenlijke risicoanalyse (met een door opdrachtnemer voorgestelde gangbare methodiek) kan aan de hand van bedreigingen en kwetsbaarheden worden vastgesteld welke beveiligingsmaatregelen genomen dienen te worden.
- De vertaling van de vastgestelde beveiligingsmaatregelen naar een uitgewerkte set van eisen welke opgenomen kan worden bij het totale programma van eisen voor het laten realiseren van de genoemde standaard.

Buiten scope van deze opdracht zijn:

- marktverkenning naar passende oplossingen
- bepaling van een berichtenstandaard
- implementatie van requirements

Uitgangspunt bij deze opdracht.

- Omdat de gegevensuitwisseling plaatsvindt tussen diverse partijen (zowel privaat als publiek) is het van belang om een gezamenlijk referentiekader te creëren ten aanzien van informatiebeveiliging en de bescherming van persoonsgegevens. Binnen de Rijksoverheid leveren het Voorschrift Informatiebeveiliging Rijksdienst 2007, de Baseline Informatiebeveiliging Rijksdienst 2012 en het Voorschrift Informatiebeveiliging Rijksdienst – Bijzondere Informatie 2013 de basis voor risicoanalyses en het opstellen van beveiligingsmaatregelen. Voor alle partijen gelden de wettelijke verplichtingen vanuit de Wet bescherming persoonsgegevens (Wbp). De opdrachtnemer begeleidt het proces om te komen tot een gedeeld en gevalideerd beeld van betrouwbaarheidsaspecten en risicomanagement.

3.3 Logius als partner

Wij danken Zorgverzekeraars Nederland als opdrachtgever vanuit de TIZ voor deze aanvraag en willen deze opdracht graag naar volle tevredenheid uitvoeren.

Logius heeft als missie om eenvoudig, snel, groen en betrouwbaar zaken te regelen tussen bedrijven, burgers en (semi)overheden met als doel een betere dienstverlening, kostenbesparing en administratieve lastenverlichting. Als agentschap van ministerie van BZK vervult Logius hierin een centrale en leidende rol met oog voor de samenhang in de infrastructuur van enerzijds de overheid en anderzijds het bedrijfsleven.

Veilige gegevensuitwisseling

Logius heeft veel ervaring met informatiebeveiliging op het gebied van gegevensuitwisseling tussen ketenpartners. In opdracht van diverse overheden verzorgt Logius met Digipoort de massale gestandaardiseerde gegevensuitwisseling tussen bedrijven en overheden op gebieden zoals verantwoording (Standard Business Reporting), Douane formaliteiten, ziekte- en herstelmeldingen UWV en inkoop- en facturatiegegevens. De ontvangende overheden gebruiken deze gegevens voor hun primaire proces en daarom dient voor het imago van de overheid de gegevensuitwisseling snel, betrouwbaar en veilig plaats te vinden.

Standaarden

Logius heeft veel ervaring met het definiëren en onderhouden van berichten standaarden. Het Forum Standaardisatie beheert de lijst met verplichte open standaarden die gelden voor de gehele publieke sector. Het Centrum voor Standaarden binnen Logius beheert alle open standaarden die zijn opgenomen op de open standaarden lijst van het Forum Standaardisatie.

Fraude

Naast Digipoort beheert Logius vele andere voorzieningen, waaronder DigiD. Het fraudeteam van Logius werkt nauw samen met andere overheden om fraude te bestrijden.

4 Plan van Aanpak

4.1 Aanpak opdrachtuitvoering

De opdracht zal projectmatig worden uitgevoerd volgens de Logius PRINCE2 projectmanagement methodiek en kent de volgende faseringen:

Fase 1: Opstartfase
Fase 2: Onderzoek
Fase 3: Rapportage

Elke fase kent een aantal activiteiten die vanuit Logius worden ingevuld met de volgende rollen:

- Projectleider
- Informatiebeveiliging specialist
- Business consultant

In bijlage 1 vindt u een profielschets van de beoogde medewerkers die de opdracht voor u kunnen uitvoeren.

Hieronder wordt per fase kort toegelicht welke activiteiten worden uitgevoerd en welke producten en/of resultaten worden bereikt.

4.1.1 Fase 1: Opstartfase

Tijdens deze eerste fase wordt een nadere studie uitgevoerd van de beschikbare documentatie in dit dossier. De opdrachtgever stelt de benodigde documentatie beschikbaar. Verder zal met de opdrachtgever de definitieve planning van het onderzoek worden vastgesteld en zullen de organisaties voor de interviews in samenwerking met de opdrachtgever worden geselecteerd en benaderd.

De volgende activiteiten worden hierbij uitgevoerd:

- Documentenstudie
- Interviewgesprekken plannen betrokkenen uitnodigen (totaal maximaal 3 interviews)
- Workshop (maximaal 1) plannen en betrokkenen uitnodigen
- Moment bepalen voor het presenteren van de resultaten in TIZ overleg

Producten fase 1:

- Stakeholderoverzicht
- Ingeplande interviewgesprekken
- Ingeplande workshop
- Ingepland presentatie moment in het TIZ overleg

Benodigde resources fase 1:

- Business consultant Logius
- Informatiebeveiliging specialist Logius
- Projectleider Logius
- Secretariaat ZN

- Beleidsadviseur ZN

4.1.2 *Fase 2: Onderzoek*

Tijdens deze fase wordt een aantal interviewgesprekken en een workshop gehouden. Daarbij is het van groot belang dat de geïnterviewden en workshopdeelnemers voldoende kennis hebben van de onderwerpen en mandaat hebben om beslissingen te mogen nemen namens de partij die zij vertegenwoordigen. Op basis van de verkregen informatie wordt een risicoanalyse uitgevoerd op basis van een afhankelijkheden en kwetsbaarheden (A&K) analyse. Daarbij wordt enerzijds het beveiligingsniveau uitgewerkt en mogelijke bedreigingen en kwetsbaarheden in kaart gebracht en anderzijds worden de te nemen maatregelen beschreven zodat de risico's naar een acceptabel niveau kunnen worden gebracht.

De volgende activiteiten worden hierbij uitgevoerd:

- Interview(s)
 - Voor het verkrijgen van een verdiepingslag van de benodigde informatie, zal een interviewgesprek plaatsvinden met de beleidsadviseurs van ZN die zich met dit onderwerp bezighouden en de informatiebeveiliging specialist en business consultant van Logius.
 - Twee aanvullende interviews met vertegenwoordigers van een zorgverzekeraar en ketenpartners. Van de interviews wordt verslag gemaakt en ter goedkeuring voorgelegd aan de geïnterviewde.
- Risicoanalyse workshop
 - Uitwerking van het beveiligingsniveau
 - Bepalen van bedreigingen en kwetsbaarheden
 - Te nemen maatregelen

Producten fase 2:

- Interviewverslagen
- Workshopverslag
- Risicoanalyse

Benodigde resources fase 2:

- Beleidadviseur(s) ZN
- Secretariaat ZN
- Informatie eigenaar zorgverzekeraar
- Informatie eigenaar ketenpartner
- Per zorgverzekeraar en ketenpartner een informatiemanager of IB specialist met voldoende kennis van zaken en mandaat om beslissingen te mogen nemen.
- Projectleider Logius
- Business consultant Logius
- Informatiebeveiliging specialist Logius

4.1.3 *Fase 3: Rapportage*

In de rapportage fase worden de interview- en workshopresultaten geconsolideerd, geanalyseerd en opgenomen in een bondig eindrapport. In het rapport worden de resultaten van het onderzoek opgenomen zoals

in paragraaf 3.2 staat beschreven. In maximaal twee iteraties wordt het rapport met de opdrachtgever definitief gemaakt, waarbij de opdrachtgever gedurende de iteratieslagen het rapport voorlegt aan de TIZ.

In een korte presentatie (ong. 10 min) in een regulier overleg van de TIZ worden de resultaten op hoofdlijnen gepresenteerd.

Producten fase 3:

- Eindrapport
- Presentatie eindrapport in het TIZ overleg

Benodigde resources fase 3:

- Deelnemers TIZ overleg
- Beleidadviseur(s) ZN
- Projectleider Logius
- Business consultant Logius
- Informatiebeveiliging specialist Logius

4.2

Planning

In onderstaande tabel is de planning per fase en benodigde activiteiten weergegeven. In de planning is uitgegaan van een startdatum van het onderzoek in week 37.

ACTIVITEIT	PLAN BEGIN	PLAN												
		36	37	38	39	40	41	42	43	44	45	46	47	48
Fase 1: Opstartfase														
Inlezen	37													
Stakeholderanalyse	37													
Interviews plannen	37													
Workshop plannen	37													
Presentatie TIZ overleg plannen	37													
Fase 2: Onderzoek														
Interview met ZN + verslag	38													
Interview met zorgverzekeraar(s) + verslag	39													
Interview met ketenpartner(s) + verslag	40													
Workshop + verslag	41													
Resultaat A&K analyse	42													
Fase 3: Rapportage														
Resultaten interviews/workshop consolideren	43													
Opstellen eindrapport	44													
Toelichting eindrapport aan opdrachtgever	45													
Opstellen Powerpoint presentatie	46													
Resultaten presenteren in TIZ overleg	46													

Tabel 1: Planning onderzoek

4.3 Samenwerking tijdens uitvoering opdracht

Gedurende de uitvoering van de opdracht is de projectleider van Logius Single point of contact voor de opdrachtgever. Met de opdrachtgever wordt wekelijks (telefonisch) overleg gevoerd over de uitvoering van de opdracht. Tweewekelijks wordt een korte voortgangsrapportage gemaakt.

4.4 Ureninzet

In onderstaande tabel wordt per fase het aantal uren weergegeven die nodig is voor de uitvoering van de activiteiten.

Fase	Uren
Fase 1: Opstartfase	48
Fase 2: Onderzoek	50
Fase 3: Rapportage	62
Totaal aantal uren	160

Tabel 2: Ureninzet

4.5 Geheimhouding

Alle Logius medewerkers zijn gehouden aan geheimhouding middels een geheimhoudingsverklaring of de algemene geheimhoudingsplicht voor ambtenaren geregeld in de Ambtenarenwet art. 125a, lid 3. In overleg met de opdrachtgever(s) wordt besloten op welke wijze bij Logius documenten worden gearhiveerd. De opdrachtgever(s) is/zijn eigenaar van de documentatie voor zover men redelijkerwijs moet verwachten dat de betreffende stukken van historische waarde zijn of voor zover zij gaan over beleidsmatige, juridische of financiële aangelegenheden. De opdrachtnemer streeft ernaar de documentatie zo veel mogelijk in digitale vorm te vervaardigen en te archiveren.

4.6 Risico's

Om de opdracht binnen de afgegeven planning te kunnen uitvoeren is het van groot belang dat alle geïnterviewden en workshopdeelnemers beschikbaar zijn conform afspraak, voldoende kennis van zaken hebben van de onderwerpen en van hun organisatie het mandaat hebben gekregen om beslissingen te mogen nemen.

5 Algemene bepalingen

5.1 Rollen en verantwoordelijkheden

Logius is een agentschap (baten-lastendienst) en daarmee gebonden aan de bepalingen die zijn vastgelegd door de minister van Financiën in de Regeling Agentschappen. Bij elke opdracht die Logius uitvoert zijn de bepalingen van deze Regeling van kracht en worden de daarin beschreven rollen en verantwoordelijkheden door Logius, Opdrachtgever en Eigenaar in acht genomen.

Opdrachtnemer voor deze opdracht is Logius, onderdeel van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK). De Directeur-Generaal Organisatie en Bedrijfsvoering Rijk (DGOBR) is de eigenaar van Logius. De opdrachtgever voor deze opdracht is Zorgverzekeraars Nederland (ZN) namens de TIZ.

5.2 Diensten van derden

Logius is als opdrachtnemer bevoegd om bij de uitvoering van de afspraken die voortvloeien uit deze Opdrachtovereenkomst gebruik te maken van de diensten van derden. Dit heeft geen invloed op de verantwoordelijkheid van Logius voor de uitvoering van de afspraken.

5.3 Wijzigen opdracht

Een tussentijdse verandering kan ertoe leiden dat gemaakte afspraken in deze Opdrachtovereenkomst moeten worden bijgesteld. Bij kleine wijzigingen zal er een addendum op deze Opdrachtovereenkomst geformuleerd worden. Dit kan ook pragmatisch middels een wederzijdse bevestiging per e-mail.

Bij grote of ingrijpende wijzigingen kan ervoor worden gekozen een nieuwe versie van deze Opdrachtovereenkomst overeen te komen, waarbij de voorgaande versie van deze Opdrachtovereenkomst komt te vervallen. Gewijzigde of nieuwe opdrachtovereenkomsten worden opnieuw ondertekend door zowel Opdrachtgever als Logius.

5.4 Tussentijdse beëindiging van de Opdrachtovereenkomst

Opdrachtgever zal na tussentijdse beëindiging van deze Opdrachtovereenkomst de reeds gemaakte kosten aan Logius vergoeden.

6 Financiën

6.1 Geldigheidsduur

Deze Opdrachtovereenkomst is geldig vanaf de datum van ondertekening door beide partijen tot dechargeverlening van de Opdrachtgever aan Opdrachtnemer.

6.2 Kosten

In onderstaande tabel zijn per fase de kosten weergegeven. Logius hanteert daarbij een plafondprijs zodat het totaalbedrag in principe niet hoger uitkomt dan wat in deze opdrachtovereenkomst is opgenomen.

Fase	Totaal
Fase 1: Opstartfase	€ 6.858
Fase 2: Onderzoek	€ 7.342
Fase 3: Rapportage	€ 9.380
Totaalbedrag	€ 23.580

Tabel 3: Kostenoverzicht

Het totaalbedrag wat met de opdracht gemoeid is komt op **€ 23.580,-**

Genoemde bedragen zijn inclusief reis- en verblijfskosten binnen Nederland en exclusief reis- en verblijfskosten buiten Nederland.

6.3 Facturatie

Na afronding van de opdracht vindt de facturatie plaats op basis van de werkelijke kosten. Zowel Logius als agentschap van ministerie van BZK en ZN als vereniging zijn vrijgesteld van BTW afdracht. Genoemde bedragen worden niet verhoogd met toeslagen.

6.4 Kostenafwijkingen

Alleen de door Logius werkelijk gemaakte kosten worden in rekening gebracht. Mogelijke afwijking van de geraamde kosten worden door Logius tijdig, en voorzien van onderbouwing, gemeld aan Opdrachtgever. In overleg met de Opdrachtgever worden deze afwijkingen geaccepteerd, en bij een overschrijding bekostigd door de Opdrachtgever, of worden door Logius en Opdrachtgever maatregelen genomen. Facturen moeten binnen 30 dagen na de factuurdatum zijn betaald door Opdrachtgever.

7 Ondertekening

Deze Opdrachtovereenkomst is besproken, akkoord bevonden en overeengekomen tussen Zorgverzekeraars Nederland en Logius:

Datum:

Datum:

Logius

Zorgverzekeraars Nederland

.....

.....



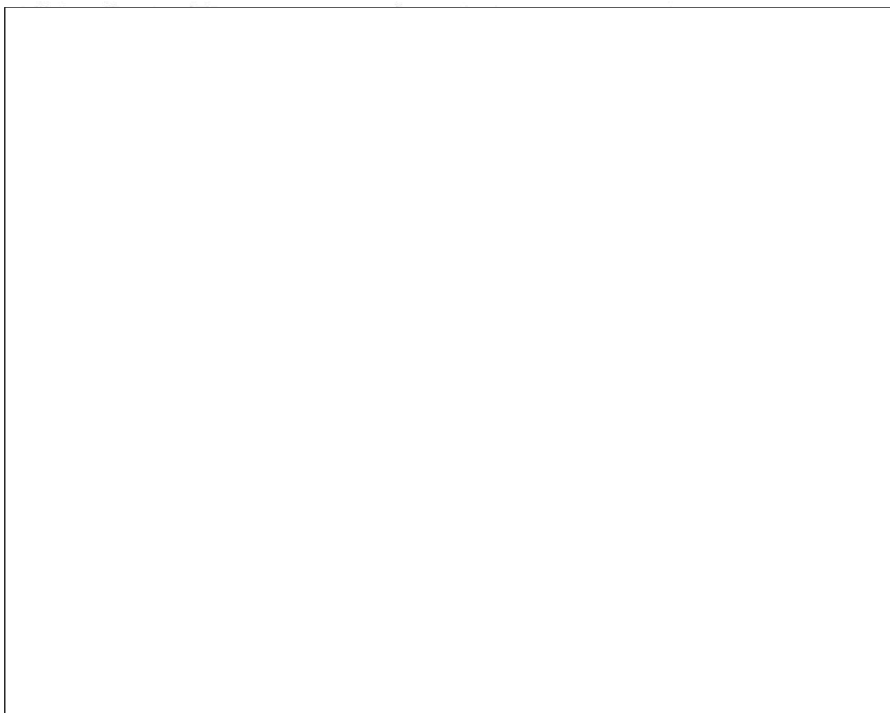
Handel & Transport

[Naam ondertekenaar
Opdrachtgever]
[Functie ondertekenaar
Opdrachtgever]

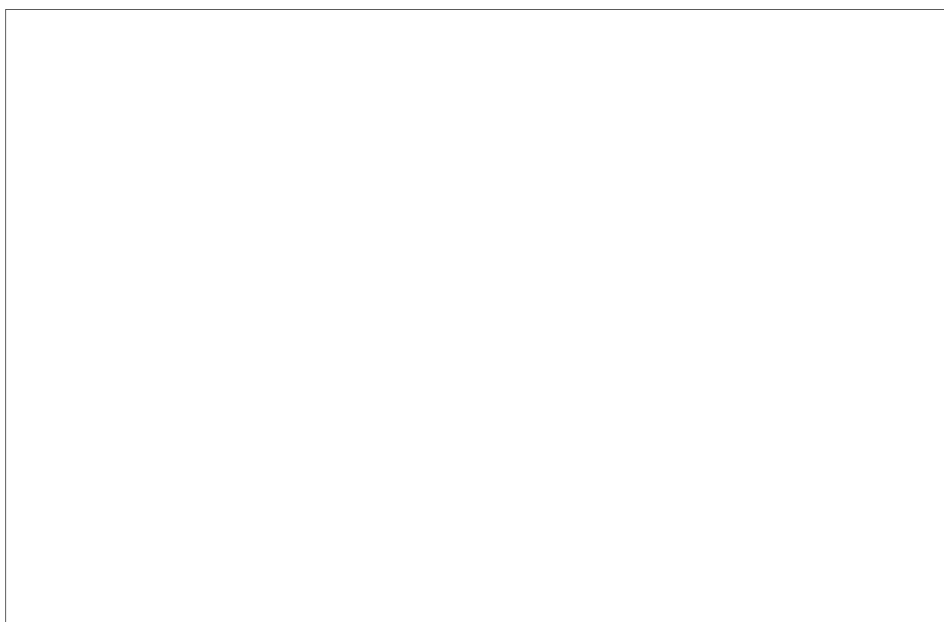
BIJLAGE 1 : Profielschets Logius medewerkers

Onderstaande een korte profielschets van de beoogde medewerkers die de opdracht gaan uitvoeren na akkoord van de opdrachtgever.

Projectleider:



Informatiebeveiliging specialist:



Business consultant: