

(Bijlage bij Nota naar aanleiding van het Verslag wetsvoorstel 34203)

# Privacy Impact Assessment (PIA)

## Burgerregelingen

Naam afdeling of projectteam:	Strategie en Beleid
Datum:	28 juli 2015
Naam auteur:	Marco Zevenhuizen
Versie:	Versie.2.0

# Analyse

## Documentbeheer

Document naam

Privacy Impact Assessment (PIA) Burgerregelingen

## Inhoudsopgave

1	Inleiding	5
2	Privacy Impact Assessment (PIA)	5

## 1 Inleiding

De uitvoering van een aantal burgerregelingen van het Zorginstituut Nederland (voorheen College van Zorgverzekeringen) wordt aan het CAK overgedragen. Het gaat om een viertal regelingen: wanbetalers, onverzekerden, de administratie voor gemoedsbezwaarden en het uitvoeren van de 'buitenlandtaak': het heffen en innen van bijdragen in verband met het recht op zorg in verdragslanden, het uitvoeren van de daarmee samenhangende administratie en de verrekening van ziektekosten van verzekerden die in een verdragsland zorg hebben genoten.

Dit betekent dat het CAK aanvullend op het huidige takenpakket een aantal taken gaat uitvoeren waarvoor het CAK persoonsgegevens moet gaan verzamelen. Middels een Privacy Impact Assessment (PIA) kunnen de gevolgen van de overheveling van taken op met name op het terrein van privacy en informatiebeveiliging in kaart worden gebracht. Het hier gebruikte PIA-toetsmodel is ontwikkeld voor de Rijksoverheid.

De overheveling van de burgerregelingen zal voor de burger zelf een minimale impact op zijn of haar privacy hebben. De bestaande situatie wijzigt immers niet. De regelingen worden slechts uitgevoerd door een ander bestuursorgaan. De burger mag op geen enkele wijze nadelen of schade ondervinden van de feitelijke overdracht.

Risico's die samenhangen met de overdracht worden zo veel mogelijk ondervangen. Deze risico's kunnen zich voordoen op het gebied van:

- Integriteit: door het afsplitsen van bestanden van het Zorginstituut zouden gegevens zoek of beschadigd kunnen raken;
- Beschikbaarheid: door het overdragen van bestanden kan de beschikbaarheid van gegevens en de continuïteit van de processen in het geding komen;
- Vertrouwelijkheid: bij het overdragen kunnen gegevens beschikbaar komen voor niet bevoegden.

Deze risico's zullen worden ondervangen door risico beperkende maatregelen te treffen tijdens het proces van overgang.

Het CAK voert op dit moment diverse andere regelingen uit. Het CAK waarborgt dat de gegevensbestanden met betrekking tot de burgerregelingen technisch en organisatorisch gescheiden worden gevoerd, zodanig dat koppeling met privacygevoelige informatie uit of met gegevensbestanden m.b.t. de andere regelingen niet mogelijk is.

## 2 Privacy Impact Assessment (PIA)

Het toetsmodel is alleen in pdf beschikbaar, hieronder zijn alle vragen uit het model beantwoord.

### I. Basisinformatie: type persoonsgegevens, type verwerking en noodzaak/gegevensminimalisering

1. Wilt u als verantwoordelijke persoonsgegevens gaan gebruiken voor de verwerking die u voorziet? Zo ja, van welk type?.

*Het CAK is als uitvoerder de verantwoordelijke. Het gaat om persoonsgegevens en om bijzondere persoonsgegevens (gegevens over iemands gezondheid). De burgerregelingen worden 'as is' van het Zorginstituut worden overgenomen, hieruit vloeit voort dat het CAK alleen die persoonsgegevens zal gaan gebruiken die ook al door het Zorginstituut worden gebruikt voor de uitvoering van de regelingen.*

2. Andere specifieke persoonsgegevens? Is het de bedoeling om gegevens over de financiële of economische situatie van betrokkenen, of andere gegevens die kunnen leiden tot stigmatisering of uitsluiting te verwerken?

*Ja. Ten aanzien van alle regelingen worden financiële of inkomensgegevens verwerkt. Om de bijdrage van verdragsgerechtigden te kunnen berekenen hebben wij inkomensgegevens nodig. Om de bijdrage aan de spaarpot van gemoedsbezwaarden te kunnen berekenen zijn inkomensgegevens nodig. Bij invordering van niet betaalde (rest)schulden wordt om de hoogte van een afbetalingsregeling vast te stellen vaak inkomensinformatie en andere informatie gebruikt. Bij de regeling wanbetalers is er sprake van schulden.*

2b. Is het de bedoeling om gegevens over kwetsbare groepen of personen te verwerken?  
Toelichting: hieronder vallen bijvoorbeeld minderjarigen, verstandelijk gehandicapten, mensen die te maken hebben met stalking, klokkenluiders of informanten voor politie.

*Nee.*

2c. Is het de bedoeling gebruikersnamen, wachtwoorden en andere inloggegevens te verwerken?

*Nee.*

2d. Is het de bedoeling om uniek identificerende gegevens, zoals biometrische gegevens, te verwerken?

*Nee.*

2e. Is het de bedoeling om het BSN-nummer, of een ander persoonsgebonden nummer te verwerken?

*Ja, het BSN-nummer. Dit is noodzakelijk voor de identificatie van de betreffende burgers.*

3. Kan van elk van de onder vraag I.1 en vraag I.2 opgevoerde typen persoonsgegevens worden gesteld dat zij beleidsmatig of technisch direct van belang en onontbeerlijk zijn voor het bereiken van de beleidsdoelstelling? Wat zou er precies niet inzichtelijk worden als ervoor wordt gekozen bepaalde gegevens niet te verwerken? Licht per te verwerken persoonsgegeven toe.

*Registratie gemoedsbezwaarden:*

*BSN: identificatie*

*NAW: identificatie*

*Geslacht: identificatie*

*Geboortedatum: identificatie*

*Inkomen: bepalen bijdrage vervangende belasting*

*Medische gegevens: bepalen uitkering vergoeden kosten van zorg*

*Wettelijk vertegenwoordiger: identificatie*

*Verzekerdenadministratie buitenland*

*BSN: identificatie*

*NAW: identificatie*

*Geslacht: identificatie*  
*Geboortedatum: identificatie*  
*Verzekeringsperiode: gebruik regeling*  
*Aard inkomen: bepalen bijdrage*  
*Inschrijvingsnummer zorgverzekeraar: identificatie*  
*Inschrijvingsnummer uitkeringsinstantie*  
*Wettelijk vertegenwoordiger: identificatie*

*Wanbetalers*  
*BSN: identificatie*  
*NAW: identificatie*  
*Geslacht: identificatie*  
*Geboortedatum: identificatie*  
*Polisnummer: identificatie*  
*Medeverzekerden: identificatie/bepaling bestuursrechtelijke premie*  
*Werkgever/uitkeringsinstantie: (bron)inhouding*  
*Financiële situatie: betaalcapaciteit*  
*Wettelijk vertegenwoordiger: identificatie*

*Onverzekerden*  
*BSN: identificatie*  
*NAW: identificatie*  
*Geslacht: identificatie*  
*Geboortedatum: identificatie*  
*Polisnummer: identificatie*  
*Werkgever/uitkeringsinstantie: (bron)inhouding*  
*Wettelijk vertegenwoordiger: identificatie*

4. Kan, als het gaat om gevoelige persoonsgegevens, hetzelfde beleidseffect of technisch resultaat worden bereikt op een van de volgende wijzen: (a) door (gecombineerd) gebruik van normale persoonsgegevens, (b) door gebruik van geanonimiseerde of gepseudonimiseerde gegevens?

*Nee, uitvoering van de regelingen is dan niet mogelijk.*

5. In welk breder wettelijk, beleidsmatig of technisch kader wordt het voorziene beleid/databestand/informatiesysteem ontwikkeld en wat voor soort(en) verwerking(en) van persoonsgegevens gaan hiervan deel uitmaken bij het voorziene traject? Wordt hierbij gebruikt gemaakt van (nieuwe) technologie of informatiesystemen?

*De werkzaamheden vinden plaats in het kader van de Zorgverzekeringswet. De overheveling van de burgerregelingen van het Zorginstituut NL naar het CAK vindt plaats per 1 januari 2016. Voor de overheveling is een plan van aanpak opgesteld waarin een aantal deelprojecten worden onderkend. De informatiesystemen (applicaties) worden as-is overgezet op een door het CAK beschikbaar gestelde infrastructuur. Deze CAK infrastructuur architectuur is niet gelijk aan die bij het Zorginstituut. De beveiliging van deze infrastructuur is vergelijkbaar met de beveiliging van de al aanwezige infrastructuur voor de uitvoering van andere regelingen bij het CAK en geschikt voor het veilig verwerken van de persoonsgegevens.*

## II. Doelbinding, koppeling, kwaliteit en profilering

### Doeleinden/doelbinding en koppeling

1. Hebt u het/de specifieke doel(en) waarvoor u de persoonsgegevens gaat verwerken in detail vastgesteld? Geldt hiervoor één en hetzelfde specifieke doel?

*Voor alle regelingen specifiek en expliciet vastgelegd, iedere regeling heeft evenwel een eigen doel.*

*Gemoedsbezwaarden: artikel 70 Zorgverzekeringswet en artikel 6.4.1 Regeling zorgverzekering; Verzekerdenadministratie Buitenland: Artikel 69 Zvw, EG verordening 1408/71;*

*Wanbetalers: artikel 18a e.v. Zorgverzekeringswet;*

*Onverzekerden: Artikel 9a tot en met 9d Zorgverzekeringswet.*

2. Gaat het bij het project/systeem om gebruik van nieuwe persoonsgegevens voor een bestaand doel, of bestaande doelen binnen al bestaande systemen? (scenario toevoeging nieuwe persoonsgegevens).

*Het gaat om het gebruik van voor het CAK nieuwe persoonsgegevens voor een bestaand doel. Het CAK zal alleen die persoonsgegevens gebruiken die ook al door het Zorginstituut werden gebruikt voor de uitvoering van de regelingen. De informatiesystemen (applicaties) worden as-is overgezet op een door het CAK beschikbaar gestelde infrastructuur.*

3. Gaat het bij het project/systeem om het nastreven van nieuwe/aanvullende doeleinden door bestaande persoonsgegevens, of verzamelingen daarvan, te gebruiken, vergelijken, delen, koppelen of anderszins verder te verwerken? (scenario toevoeging doeleinden). Zo ja, hebben alle personen/instaties/systemen die betrokken zijn bij de verwerking dezelfde doelstelling met de verwerking van de desbetreffende persoonsgegevens of is daarmee spanning mogelijk gelet op hun taak of hun belang? Gelden dezelfde doelen voor het hele proces?

*Nee*

4. Indien u positief hebt geantwoord op vragen II.2 of II.3, hoe wordt een dergelijk voorgenomen gebruik (d.w.z. gebruik van nieuwe persoonsgegevens in bestaande systemen of van bestaande persoonsgegevens voor nieuwe doeleinden) gemeld aan: (a) de functionaris voor de gegevensbescherming, of (b) het Cbp indien er geen FG is?

*De functionaris voor de gegevensbescherming.*

5. Indien u positief geantwoord hebt op vragen II.2 of II.3, welke (nadere) controles op een dergelijk gebruik (d.w.z. gebruik van nieuwe persoonsgegevens in bestaande systemen of van bestaande persoonsgegevens voor nieuwe doeleinden) zijn voorzien?

*De overheveling van de burgerregelingen van het Zorginstituut NL naar het CAK vindt plaats per 1 januari 2016. Vanaf die datum vinden nadere controles plaats aan de hand van de reeds voor andere regelingen bestaande processen en procedures. Het gaat hierbij om het bestaande Informatiebeveiligingsbeleid en al het beleid met betrekking tot privacy. De persoonsgegevens worden bewerkt in van het Zorginstituut overgenomen informatiesystemen (applicaties) op een door het CAK beschikbaar gestelde infrastructuur.*

6. Welke periodieke en incidentele controles zijn voorzien om de juistheid, nauwkeurigheid



en actualiteit van de in het wetsvoorstel op overheids ICT-systeem verwerkte persoonsgegevens na te gaan?

*Het gekozen scenario voor overheveling wordt voorafgaand aan de overheveling onderworpen aan een audit door PwC. Bij het CAK vindt periodiek een EDP-audit op de systemen plaatsvindt. Daarnaast vinden controles plaats op basis van het bestaande Informatiebeveiligingsbeleid en al het beleid met betrekking tot privacy.*

*Alle informatie die het CAK verwerkt, is steeds afkomstig van daarvoor bedoelde bronnen, waaronder de RvIG, Belastingdienst, SVB, UWV, zorgverzekeraars, werkgevers en de burger zelf. In de processen worden steeds de meest actuele gegevens gebruikt.*

7. Zullen de verzamelde/verwerkte persoonsgegevens gebruikt worden om het gedrag, de aanwezigheid of de prestaties van mensen in kaart te brengen en/of te beoordelen en/of te voorspellen?

*Het Centraal Bureau voor de Statistiek (CBS) maakt gebruik van de bestanden van het Zorginstituut om de wanbetalers en onverzekerdenpopulatie in kaart te brengen. Het ligt voor de hand dat het CAK deze uitwisseling voortzet en deze onderdeel maakt van een reeds bestaande convenant dat het CAK en het CBS hebben afgesloten. Er dient nog wel te worden onderzocht of gebruik kan worden gemaakt van geanonimiseerde gegevens. In de wanbetalersregeling zal mogelijk 'positieve profiling' plaatsvinden. Goed betalende wanbetalers worden aangemeld bij hun zorgverzekeraar om te kijken of de zorgverzekeraar niet (alsnog) een regeling met de wanbetaler kan treffen.*

*Verder kan koppeling aan GBA gegevens plaatsvinden om te zien of iemand nog wel ingeschreven is. Als er geen GBA inschrijving is dan moet de zorgverzekeraar de verzekeringssituatie van de wanbetaler onderzoeken en zo nodig afmelden. De aanwezigheid en prestaties van mensen wordt niet in kaart gebracht, wel het betaalgedrag. Zijn de betrokkenen daarvan op de hoogte? Ja  
Zijn de gegevens die hiervoor worden gebruikt, afkomstig uit verschillende (eventueel externe) bronnen.*

*Nee.*

Zijn zij oorspronkelijk voor andere doelen verzameld?

*Nee.*

8. Wordt bij deze analyse/beoordeling/voorspelling gebruik gemaakt van vergelijking van persoonsgegevens die technisch geautomatiseerd is (d.w.z. niet door mensen zelf wordt uitgevoerd)?

*De registratie van de betaling of het uitblijven ervan vindt geautomatiseerd plaats.*

Zo ja, hoe wordt geregeld dat, indien dit geautomatiseerde proces tot een beoordeling of voorspelling over een bepaalde persoon leidt, hierop pas concrete actie wordt ondernomen na tussenkomst en (tweede) controle van (menselijk) personeel?

*Dit zal in het betaalproces geschieden indien dwangmiddelen worden ingezet.*

## III. Betrokken instanties/systemen en verantwoordelijkheid

1. Welke interne en externe instantie(s) en/of systemen is/zijn betrokken bij de voorziene verwerking in elk van de onder 1.5 onderscheiden fasen? Welke verstrekkers zijn er en welke ontvangers? Welke bestanden of deelbestanden en welke infrastructuren?

*De overheveling van de burgerregelingen van het Zorginstituut naar het CAK vindt plaats per 1 januari 2016. Het Zorginstituut is verstrekker en het CAK ontvanger. De informatiesystemen (applicaties) van het Zorginstituut worden as-is overgezet op een door het CAK beschikbaar gestelde infrastructuur.*

2. Is (in ieder stadium) duidelijk wie verantwoordelijk is voor de verwerking van de persoonsgegevens?

*Ja, dat is tot en met 31 december 2015 het Zorginstituut, en direct aansluitend vanaf 1 januari 2016 het CAK.*

Zo ja, is deze persoon of organisatie daarop voldoende voorbereid en geëquipeerd wat betreft de nodige voorzieningen en maatregelen, waaronder middelen, beleid, taakverdeling, procedures en intern toezicht?

*Het CAK is reeds uitvoerder van diverse wettelijke taken en voldoet daarvoor aan de gestelde eisen vanuit de Wbp.*

3. Wie binnen uw organisatie, en elk van de andere betrokken organisaties, krijgen precies toegang tot de persoonsgegevens?

*Er wordt een autorisatieschema ontwikkeld en technisch geïmplementeerd.*

Bestaat de kans dat bij het gebruik ervan de gegevens ter beschikking komen van onbevoegden?

*Door het werken met autorisaties is deze kans geminimaliseerd.*

4. Geldt voor een of meer van de betrokken instanties een beperking van de mogelijkheid om persoonsgegevens te verwerken als gevolg van geheimhoudingsverplichtingen (in verband met functie/wet)?

*Nee.*

5. Zijn alle stappen van de verwerking in de zin van soorten gegevens en uitwisselingen, in kaart gebracht of te brengen, zodanig dat daardoor voor de betrokkenen inzichtelijk is bij wie, waarom en hoe de persoonsgegevens worden verwerkt?

*Alle geautomatiseerde uitwisselingen zijn in kaart gebracht. Handmatige uitwisselingen zijn in de werkinstructies en procedures vastgelegd door het Zorginstituut. Het CAK vormt zich nog een oordeel over de volledigheid hiervan. Dit wordt gemonitord en is onderdeel van de readiness assessment.*

6. Zijn er beleid en procedures voorzien voor het creëren en bijhouden van een verzameling van de persoonsgegevens die u wilt gaan gebruiken?

*Het gaat hierbij om het bestaande Informatiebeveiligingsbeleid en al het beleid met betrekking tot privacy.*

Zo ja, hoe vaak en door wie zal de verwerking worden gecontroleerd?

*Dit is onderdeel van periodieke lijncontroles. Daarnaast heeft de functionaris voor de gegevensbescherming een toezichhoudende rol.*

Omvat de verzameling een verwerking die namens u wordt uitgevoerd (bijvoorbeeld door een onderaannemer)?

*Voor de onverzekerden geldt nu dat VEKTIS en de SVB de bestandskoppeling doen en dat zij bij constatering van verzekeringsplicht maar geen verzekering en terugkoppeling doen aan het Zorginstituut*

*Bij verdragsgerechtigden geldt dat de pensioenfondsen en uitkeringsinstanties in mandaat van het Zorginstituut de broninhouding plegen. Voor de uitvoering van de burgerregelingen maakt het Zorginstituut ook gebruik van de Suwinet inkijkfunctie en de RBVZ inkijkfunctie. Het deurwaardersproces wordt namens het CAK door een derde (deurwaarder) uitgevoerd.*

7. Is er sprake van overdracht van persoonsgegevens naar een (overheids)instantie buiten de EU/EER?

*Ja, verzekeringsinstellingen in verdragslanden*

Heeft dit land een niveau van gegevensbescherming dat als passend is beoordeeld door een besluit van de Europese Commissie of de Minister van Veiligheid en Justitie? Alleen voor zover het landen binnen de EU betreft. Worden daarbij alle of een gedeelte van de persoonsgegevens doorgegeven?

*Ja*

## IV. Beveiliging en bewaring/vernietiging

1. Is het beleid met betrekking tot gegevensbeveiliging binnen uw organisatie op orde?

*Ja, het Informatiebeveiligingsbeleid is recent geactualiseerd en op 20 maart 2015 vastgesteld. Zo ja, wie/welke afdeling(en) is/zijn binnen de organisatie verantwoordelijk voor het opstellen, implementeren en handhaven hiervan?*

*Opstellen: Corporate Control en Strategie & Beleid, de FG.*

*Implementeren: het lijnmanagement.*

*Handhaven: Interne Controle.*

Is dit beleid specifiek gericht op gegevensbescherming en gegevensbeveiliging ?

*Ja.*

2. Indien (een deel van) de verwerking bij een bewerker plaatsvindt, hoe draagt u zorg voor de gegevensbeveiliging, en het toezicht daarop, bij die bewerker?

*Het CAK hanteert bij alle afgesloten overeenkomsten de Algemene Rijksvoorwaarden voor het verstrekken van opdrachten tot het verrichten van diensten 2014 (ARVODI-2014), in deze voorwaarden*

*zijn bepalingen opgenomen met betrekking tot gegevensbescherming en gegevensbeveiliging. Indien deze algemene bepalingen niet afdoende zijn wordt aanvullend een standaardbewerkingsovereenkomst afgesloten.*

3. Welke technische en organisatorische beveiligingsmaatregelen zijn getroffen ter voorkoming van niet-geautoriseerde of onrechtmatige verwerking/misbruik van (a) gegevens die in een geautomatiseerd format staan (bv. wachtwoord-bescherming, versleuteling, encryptie) en (b) gegevens die handmatig zijn opgetekend (bv. sloten op kasten)? Is er een hoger beschermingsniveau om gevoelige persoonsgegevens te beveiligen?

*Het CAK stelt hoge eisen aan het personeel gezien de vertrouwelijkheid van de gegevens waarmee wordt gewerkt. Zo dient elke medewerker een geheimhoudingsverklaring te ondertekenen bij indiensttreding. Daarnaast dient elke medewerker een VOG te overleggen. Om op het netwerk van het CAK te komen is een account met wachtwoordbescherming aanwezig. Daarnaast is per applicatie eveneens een account met wachtwoordbescherming aanwezig. Binnen de applicatie is een autorisatieschema van toepassing. Het CAK werkt zoveel mogelijk digitaal en niet met papier. Indien toch papier noodzakelijk is, wordt gewerkt met afgesloten kasten.*

*Aan klanten wordt alleen informatie verstrekt op basis van de intern van toepassing zijnde privacy matrix. De externe gegevensuitwisseling vindt plaats op basis van versleutelde bestanden..*

4. Welke procedures bestaan er in geval van inbreuken op beveiligingsvoorschriften?

*Het CAK werkt met ITIL Het proces Incidentmanagement van toepassing.*

En voor het detecteren ervan?

*Medewerkers kunnen melding maken van inbreuk op beveiligingsvoorschriften.*

Is er een calamiteitenplan om het gevolg van een onvoorziene gebeurtenis waarbij persoonsgegevens worden blootgesteld aan onrechtmatige verwerking of verlies van persoonsgegevens af te handelen?

*Er is een calamiteitenplan voor incidenten.*

5. Hoe lang worden de persoonsgegevens bewaard? Geldt dezelfde bewaartermijn voor elk van de typen van verzamelde persoonsgegevens? Is het project onderworpen aan enige wettelijke/sectorale eisen met betrekking tot bewaring?

*De bewaartermijnen van persoonsgegevens liggen vast in beleid. Per type van verzamelde persoonsgegevens kan dit wisselen, afhankelijk van het doel van de verzameling. De Wbp is leidend bij de eisen met betrekking tot bewaring.*

6. Op welke beleidsmatige en technische gronden is deze termijn van bewaring vereist?

*Zie 5.*

7. Welke maatregelen zijn voorzien om de persoonsgegevens na afloop van de bewaartermijn te vernietigen? Worden alle persoonsgegevens, inclusief log-gegevens, vernietigd? Is er controle op de vernietiging, en door wie?

*Vernietiging vindt plaats aan de hand van een archiefbeheersregeling en een selectielijst. Alle persoonsgegevens zullen worden vernietigd. Controle vindt geautomatiseerd plaats en kan ook steekproefsgewijs door bijvoorbeeld de functionaris voor de gegevensbescherming worden uitgevoerd.*

## V. Transparantie en rechten van betrokkenen

1. Is het doel van het verwerken van de gegevens bij de betrokkenen bekend of kan het bekend gemaakt worden?

Ja.

Wat is de procedure om betrokkenen indien nodig te informeren over het doel van de verwerking van hun persoonsgegevens?

*In het deelproject Communicatie wordt beschreven hoe de burgers worden geïnformeerd. De betreffende burgers ontvangen een brief waarin staat dat het CAK deze burgerregelingen gaat uitvoeren. Hiermee zijn de burgers geïnformeerd over de verwerking van hun persoonsgegevens. Voor burgers die nieuw in een regeling instromen geldt dat zij altijd schriftelijk over het doel worden geïnformeerd.*

*Betrokkenen kunnen zich altijd tot het CAK richten indien zij (verder) geïnformeerd wensen te worden over het doel van de verwerking van de persoonsgegevens. De procedure staat op de CAK website (<http://www.hetcak.nl/portalserver/portals/cak-portal/pages/x1-cak-privacystatement.html>).*

2. Indien u de persoonsgegevens direct van de betrokkenen verkrijgt, hoe stelt u hen van uw identiteit en het doel van de verwerking op de hoogte vóór het moment van verwerking?

*De grondslag van de gegevensverwerking ligt in de wet en de daarop gebaseerde regelingen en niet in het geven van toestemming door de verzekerde. Wij maken ons in de meeste gevallen bij de burger bekend middels een beschikking, bijvoorbeeld het opleggen van een boete bij een onverzekerde of het opleggen van een 130% bestuurlijke premieplicht bij een wanbetaler. Of bij een verdragsgerechtigde met een beschikking over het opleggen van een bijdrageplicht en de broninhouding. In de beschikking is dan uitgelegd waarom wij de burger aanschrijven. Bij een onverzekerde is dat omdat uit bestandskoppeling is gebleken dat er sprake is van onverzekerde zijn. Bij een wanbetaler is dat, omdat de zorgverzekeraar de wanbetaler bij ons heeft gemeld. Bij gemoedsbezwaarden is dat, omdat men zich als zodanig heeft gemeld (via SVB) en bij verdragsgerechtigden is dat meestal omdat men zich heeft ingeschreven in het verdragsland (middels een E-formulier).*

Vraag 4: Indien u de persoonsgegevens via een andere (overheids)organisatie verkrijgt, hoe zullen de betrokkenen van uw identiteit en het doel van de verwerking op de hoogte worden gesteld op het moment van verwerking?

Zie 1.

4. Indien u toestemming tot verwerking van persoonsgegevens aan de betrokkene vraagt (opt-in), kan de betrokkene deze toestemming dan op een later tijdstip weer intrekken (opt-out)?

*Niet van toepassing*

Bij een weigering toestemming te geven, of bij een dergelijke intrekking, wat is dan de implicatie voor de betrokkene?

*Niet van toepassing*

5. Via welke procedure hebben betrokkenen de mogelijkheid zich tot de verantwoordelijke te wenden met het verzoek hen mede te delen of hun persoonsgegevens worden verwerkt?

*De procedure staat op de CAK website (<http://www.hetcak.nl/portalserver/portals/cak-portal/pages/x1-cak-privacystatement.html>) .*

Hoe worden derden, die mogelijk bedenkingen hebben tegen een dergelijke mededeling, in de gelegenheid gesteld hun zienswijze te geven?

*Via de reguliere klachtenprocedure van het CAK (<http://www.hetcak.nl/portalserver/portals/cak-portal/pages/k1-10-contact>).*

6. Hoe kan een verzoek van een betrokkene tot verbetering, aanvulling, verwijdering of afscherming van persoonsgegevens in behandeling worden genomen?

*De procedure staat op de CAK website (<http://www.hetcak.nl/portalserver/portals/cak-portal/pages/x1-cak-privacystatement.html>) .*