

## **Toelichting bij aanvraagformulier IVC V4.0**

Het Informatieveiligheidscomité bevat twee kamers: de kamer Sociale Zekerheid en Gezondheid en de kamer Federale Overheid.

### **Aanvragen voor de kamer Federale Overheid**

De werking van de kamer federale overheid van het informatieveiligheidscomité wordt geregeld in de (nieuwe) artikelen 35/1 tot 35/5 van de wet van 15 augustus 2012 houdende oprichting en organisatie van een federale dienstenintegrator.

De kamer federale overheid beraadslaagt over de mededelingen van persoonsgegevens door overheidsdiensten en openbare instellingen van de federale overheid aan derden die geen instelling van sociale zekerheid zijn, voor zover de betrokken verwerkingsverantwoordelijken niet tot een akkoord komen of minstens één verwerkingsverantwoordelijke om een beraadslaging verzoekt.

De mededeling van persoonsgegevens door overheidsdiensten en openbare instellingen van de federale overheid aan openbare instellingen van sociale zekerheid en federale overheidsdiensten belast met de toepassing van de sociale zekerheid vereist een beraadslaging van de verenigde kamers van het informatieveiligheidscomité, maar enkel voor zover de betrokken verwerkingsverantwoordelijken niet tot een akkoord komen of minstens één verwerkingsverantwoordelijke om een beraadslaging verzoekt.

De mededeling van persoonsgegevens door overheidsdiensten en openbare instellingen van de federale overheid aan andere instellingen van sociale zekerheid vereist steeds een beraadslaging van de verenigde kamers van het informatieveiligheidscomité.

De mededeling van persoonsgegevens door instanties van de federale overheid (andere dan het Rijksregister) aan andere derden dan de instellingen van sociale zekerheid vereist slechts een beraadslaging van de kamer Federale Overheid, voor zover de verwerkingsverantwoordelijken van de meedelende instantie en de ontvangende instantie er niet in slagen een protocol te sluiten.

Zie <https://bosa.belgium.be/nl/themas/digitale-overheid/samenwerking-en-kennisdeling/informatieveiligheids-comite-ivc>

### **Aanvragen voor de kamer Sociale Zekerheid en Gezondheid**

Wanneer moet een aanvraag aan de kamer SZ&G ingediend worden?

De bevoegdheid van de kamer sociale zekerheid en gezondheid van het informatieveiligheidscomité is opgenomen in de KSZ-wet, art.46:

#### **Voor gezondheidsgegevens**

De kamer sociale zekerheid en gezondheid van het informatieveiligheidscomité is bevoegd voor het verlenen van beraadslagingen voor de mededelingen van persoonsgegevens die de

gezondheid betreffen, voor zover die beraadslagingen worden opgelegd door artikel 42 van de wet van 13 december 2006 houdende diverse bepalingen betreffende gezondheid of door een andere bepaling vastgesteld door of krachtens de wet.

Artikel 42 §2, 3° van de wet van 13 december 2006 bepaalt:

3° het verlenen van een principiële machtiging met betrekking tot elke mededeling van persoonsgegevens die de gezondheid betreffen, behalve in de volgende gevallen:

- indien de mededeling gebeurt tussen beroepsbeoefenaars in de gezondheidszorg die door het beroepsgeheim gebonden zijn en persoonlijk betrokken zijn bij de uitvoering van diagnostische, preventieve of zorgverlenende handelingen ten opzichte van een patiënt;
- indien de mededeling is toegestaan door of krachtens een wet, een decreet of een ordonnantie en na advies van de GBA
- in de gevallen door de Koning bepaald, bij een besluit vastgesteld na overleg in de Ministerraad en na advies van de GBA
- indien gegevens worden meegedeeld tussen instanties van eenzelfde Gemeenschap of Gewest die geen gebruik maken van de basisdiensten van het eHealth-platform, bedoeld in de wet van 21 augustus 2008 houdende oprichting en organisatie van het eHealth-platform en diverse bepalingen.

## **Referenties naar het formulier**

### **1. Algemeen**

#### **1.1. De aanvrager**

De aanvrager is de uiteindelijke verwerker van de gevraagde gegevens. Hij initieert de aanvraag bij het IVC.

De aanvrager zal optreden als verwerkingsverantwoordelijke (AVG Art.4.7) vermits hij het doel en de middelen van de verwerking bepaalt. Indien het doel en de middelen samen met andere partijen bepaald worden, dan zijn deze partijen mede-verwerkingsverantwoordelijke en moeten ze eveneens op het formulier vermeld worden.

De precieze verantwoordelijkheden van elke mede-verwerkingsverantwoordelijke moeten gedocumenteerd worden.

#### **1.2. Type aanvraag**

Indien de aanvrager nog geen machtiging van het IVC bekomen heeft voor de betreffende verwerking, dan betreft het een nieuwe aanvraag.

Indien de verwerking een aanpassing of uitbreiding betreft van een vroegere verwerking waarvoor reeds een beraadslaging bestaat, dan dient de aanvrager deze beraadslaging op te vragen en de nodige aanpassingen in track changes voor te stellen.

### 1.3. Bestaande beraadslagingen

Vermeld hier relevante beraadslagingen die de aanvrager vroeger al gekregen heeft of protocols die afgesloten werden voor gelijkaardige verwerkingen.

### 1.4. Toegang Rijksregister en gebruik van rijksregisternummer

Zowel de toegang tot gegevens in het Rijksregister als het gebruik van het rijksregisternummer zijn onderwerp van een aparte machtiging.

Indien deze toegang en/of gebruik noodzakelijk is voor het realiseren van de beoogde verwerking, dan moet hier de oorsprong van de machtiging vermeld worden.

Indien de verwerking uitsluitend op basis van gepseudonimiseerde gegevens gebeurt, dan moet er niet noodzakelijk dergelijke machtiging zijn. Bvb KSZ koppelt gegevens van verschillende bronnen op basis van het rijksregisternummer, maar de aanvrager ontvangt pseudoniemen. Hier moet de aanvrager zelf geen machtiging hebben om het rijksregister te raadplegen of het rijksregisternummer te gebruiken.

Overeenkomstig de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen, gewijzigd bij wet van 25 november 2018 houdende diverse bepalingen met betrekking tot het Rijksregister en de bevolkingsregisters, wordt de toegang tot de gegevens van het Rijksregister gemachtigd door de minister bevoegd voor Binnenlandse Zaken.

Zie <https://www.ibz.rrn.fgov.be/nl/rijksregister/aanvraag-toegang-tot-het-rijksregister/>

### 1.5. Verwerker

De aanvrager kan voor de uiteindelijke verwerking beroep doen op één of meerdere verwerkers in de zin van AVG art.4.8.

Hierbij is het nog steeds de verwerkingsverantwoordelijke die het doel en de middelen voor de verwerking bepaalt. De verwerker werkt in opdracht en onder toezicht van de verwerkingsverantwoordelijke.

Tussen de verwerkingsverantwoordelijke en de verwerker moet een overeenkomst gesloten worden die conform is met de vereisten van AVG art.28.

De overeenkomst moet de precieze omvang en taken van de verwerker documenteren.

## 2. Verloop van de mededeling van persoonsgegevens

### 2.1. Bijzondere categorieën

Met deze bijzondere categorieën wordt verwezen naar AVG art. 9 en art.10. Voor deze categorieën gelden specifieke vereisten die verwerking mogelijk maken. Het IVC wil nagaan in hoeverre de aanvrager hieraan kan voldoen.

Art.9:

Verwerking van persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid.

Art.10:

Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen.

## 2.2. Personen van wie de persoonsgegevens zullen worden verwerkt

Hier dient uitvoerig gedocumenteerd te worden welke de begrenzingscriteria zijn voor de beoogde verwerking. Welke doelgroepen of categorieën van personen worden in de verwerking opgenomen en volgens welke selectiecriteria.

## 2.3. Betrokken instanties

Hier wordt gedocumenteerd wie de gegevenshouders en wie de ontvangers van gegevens zijn.

## 2.4. Gegevenshouders

Opsomming van alle instanties die als gegevenshouder gegevens zullen aanleveren.

## 2.5. Contactpersonen

Gegevens van de contactpersonen per instantie (gegevenshouders en gegevensontvangers) die op de hoogte zijn van de beoogde gegevensverwerking.

## 2.6. Gegevensstromen

Schematisch overzicht van de gegevensstromen vanaf de gegevenshouders via eventuele Trusted Third Parties (TTP) naar de gegevensontvangers.

Toelichting bij elke vermelde stroom in het schema.

Deze toelichting verduidelijkt de beoogde koppelingen van gegevensstromen en de tussenliggende stappen die de TTP neemt om de identificatie van betrokkenen te pseudonimiseren/anonimiseren.

### 3. Finaliteit

#### 3.1. Algemene doeleinden

Beschrijf de algemene doeleinden van de beoogde verwerking

#### 3.2. Wettelijke grondslag voor de verwerking

'JA' verwijst naar AVG Art.9.2 voor de verwerking van bijzondere categorieën van persoonsgegevens. Deze verwerking is in principe verboden, tenzij aan één of meerdere van de aangegeven voorwaarden is voldaan.

Bij wetenschappelijk onderzoek inzake experimenten op mensen en op reproductief menselijk materiaal is een ethisch advies vereist op basis van een onderzoeksprotocol. 'NEE' verwijst naar AVG Art.6.1 dat de voorwaarden aangeeft voor rechtmatige verwerking.

Opmerking: sommige uitzonderingen van Art.9.2 mappen impliciet op Art.6.1 (toestemming, vitale belangen, algemeen belang). Indien er geen impliciete mapping is moet er voor de verwerking ook steeds een rechtsgrond aanwezig zijn op basis van Art.6.1. Dit laatste geldt ook voor verwerkingen op basis van Art.10.

#### 3.3. Toepasselijke regelgeving

AVG Art.5 bepaalt de beginselen voor verwerking van persoonsgegevens. Deze zijn rechtmatigheid, behoorlijkheid, transparantie, doelbinding, minimale gegevensverwerking, juistheid, opslagbeperking, integriteit en vertrouwelijkheid.

Waar deze beginselen hun oorsprong hebben in regelgeving dient deze regelgeving hier gedetailleerd (artikelniveau) vermeld te worden.

### 4. Latere verwerking

Wanneer gegevens verwerkt worden die oorspronkelijk voor andere doeleinden werden verzameld, dan moet hier per gegevenshouder aangegeven worden welke gegevens voor welke doeleinden verzameld werden.

### 5. Transparantie

AVG Art.13 en Art.14 bepalen de informatie die aan de betrokkenen moet verstrekt worden wanneer de gegevens bij de betrokkenen werden verzameld (art.13) of niet (art.14).

'JA' Hier moet aangegeven worden op welke manier de betrokkenen geïnformeerd worden. Dit kan bvb via Informed Consent Formulier (ICF) waarin de precieze omvang van de verwerking aangegeven is.

'NEEN' Wanneer de gegevens niet bij de betrokkene werden verzameld kan men (gemotiveerd) één van de aangegeven opties aanduiden.

## 6. Soort gegevens

### 6.1. Aard gegevens

AVG Art.89.1 Geeft aan de verwerking moet gebeuren op anonieme gegevens indien de doeleinden daarmee kunnen verwezenlijkt worden. In tweede instantie dient de verwerking te gebeuren op gepseudonimiseerde gegevens indien de doeleinden daarmee kunnen verwezenlijkt worden. Enkel wanneer de doeleinden uitsluitend kunnen gerealiseerd worden op basis van identificeerbare gegevens.

De criteria voor anonimiteit zijn aangegeven in AVG overweging (26).

### 6.2. Gevraagde gegevensset

Waar in 2.6 de schematische gegevensstromen werden verduidelijkt, dient men hier een exhaustieve beschrijving van elke gegevensbron te geven.

Het betreft dus een lijst van informatievelden met hun betekenis, per gegevenshouder, per gegevensset. Hierbij moet aangegeven worden welke velden op welke manier gepseudonimiseerd zijn.

### 6.3. Identificatiegegevens

Alle hier vermelde identificatiegegevens aanduiden die voorkomen in een gegevensset vermeld in 6.2.

### 6.4. Wijzigingen ontvangen

Deze rubriek is van toepassing wanneer de identificatiegegevens uit 6.3 betrokken worden via een dienstenintegrator, bvb KSZ.

In het eerste punt wordt aangegeven indien men toegang nodig heeft tot de historiek van wijzigingen van de identificatiegegevens uit 6.3.

In het tweede punt wordt aangegeven of toekomstige wijzigingen van de identificatiegegevens uit 6.3 automatisch aan de verwerker moeten meegedeeld worden. Dergelijke mededeling gebeurt door de dienstenintegrator en is nuttig voor een gegevensset die op lange termijn bewaard moet worden door de verwerker van de gegevens.

## 7. Proportionaliteit / Minimale gegevensverwerking

### 7.1. Geldigheidsduur van de beraadslaging

De aanvraag kan dienen voor het éénmalig realiseren van bepaalde doelstellingen. In dit geval zal de beraadslaging een tijdelijke geldigheidsduur hebben. Wanneer de doelstellingen op lange termijn moeten gerealiseerd worden en blijven of van repetitieve aard zijn, dan kan de beraadslaging een permanente geldigheidsduur hebben.

In ieder geval moet de gevraagde geldigheidsduur gemotiveerd worden en gestaafd aan de hand van de toepasselijke regelgeving.

### 7.2. Bewaartermijn

AVG Art 5.1.e schrijft opslagbeperking voor.

Hiervoor dient bepaald te worden hoelang de gegevens bewaard zullen blijven

na het realiseren van de éénmalige of tussentijdse doelstellingen. Indien de gegevens voor langere tijd zullen bewaard blijven dient dit gemotiveerd te worden met verwijzing naar de toepasselijke regelgeving.

#### 7.3. Proportionaliteit

In 6.2 werden de gevraagde gegevenssets toegelicht. Hier moet vermeld worden per gegeven of blok van gegevens waarom deze nodig zijn voor het realiseren van de doelstellingen, met verwijzing naar de toepasselijke regelgeving. Ook de toegepaste selectiecriteria en de maatregelen die genomen worden om de her-identificatie van betrokkenen te vermijden worden toegelicht.

#### 7.4. Frequentie

De frequentie voor het opvragen van de gegevens hangt samen met de geldigheidsduur van de beraadslaging (zie 7.1).

#### 7.5. Interne gebruikers

Wie (dienst, functie) zal toegang hebben tot de gevraagde gegevens en waarom. Mogelijk zal de instantie die de gegevens ontvangt ook al gelijkaardige gegevens verwerken op basis van wettelijke of contractuele verplichtingen. In voorkomend geval dient binnen de instantie een aparte entiteit opgericht te worden voor de verwerking van de gevraagde gegevens zodat er een voldoende functiescheiding wordt gecreëerd.

#### 7.6. Externe gebruikers

Indien de gevraagde gegevens ook toegankelijk zijn of meegedeeld worden aan derden, dan moeten deze instanties hier vermeld worden en dienen deze eveneens over een machtiging te beschikken.

### 8. Veiligheidsbeleid

#### 8.1. Functionaris voor gegevensbescherming

Hier dient voor elke instantie, ontvanger van gegevens, de Functionaris voor gegevensbescherming vermeld te worden.

#### 8.2. Vragenlijst

Deze vragenlijst toetst het veiligheidsbeleid af voor elke instantie die gegevens ontvangt. Instanties die tot het netwerk van de sociale zekerheid behoren dienen deze vragenlijst niet in te vullen omdat zij een jaarlijkse evaluatielijst moeten indienen bij de KSZ op basis van de minimale normen.

#### 8.3. DPIA

Raadpleeg op de website van de GBA ook de lijst van verwerkingen (nr. 01/2019 van 16 januari 2019) waarvoor de GBA heeft aangegeven dat er steeds een gegevensbeschermingseffectbeoordeling (DPIA) dient te worden uitgevoerd.

Hierbij moet ook rekening worden gehouden met AVG Art.35.1 en Art.35.3.

#### 8.4. Koppeling van informatiesystemen

Deze rubriek is uitsluitend van toepassing wanneer informatiesystemen met elkaar gekoppeld worden om informatie door te geven naar derden en daarbij het Rijksregisternummer van betrokkenen als identificatiemiddel gebruikt wordt.

#### 8.5. Intermediaire organisatie

Sommige types aanvragers moeten overeenkomstig de Kruispuntbankwet gegevens uitwisselen met tussenkomst van de KSZ. Evenwel kan hiervoor een vrijstelling bekomen worden wanneer KSZ hierbij geen toegevoegde waarde kan bieden. Dit moet hier desgevallend gemotiveerd worden.

Veelal zal een Trusted Third Party (TTP) nodig zijn om identificatiegegevens te pseudonimiseren of te anonimiseren. Een andere TTP kan nodig zijn voor het koppelen van gegevenssets afkomstig van verschillende gegevenshouders, op basis van deze pseudoniemen. Typisch voor verwerkingen op gezondheidsgegevens worden hier respectievelijk eHealth en KSZ als TTP gekozen.

#### 8.6. SCRA

Er werd in de rubrieken 6.2 en 7.3 al rekening gehouden met het verminderen van de kans op her-identificatie van betrokkenen door bijvoorbeeld beperkingen in de selectiecriteria, het gebruik van berekende velden in plaats van microdata, het vermijden van datums of gebruik van relatieve datums, het vermijden van locatiegegevens of combinaties van andere gegevens die her-identificatie zouden mogelijk maken.

Het IVC kan een bijkomende Small Cell Risk Analysis (SCRA) opleggen om verdere stappen te zetten in het onderzoek naar mogelijke her-identificatie.

Hierbij kan eventueel beroep gedaan worden op de SCR-Pool die gecoördineerd wordt door het federale Health Data Agency (HDA), indien daarvoor de nodige capaciteit voorhanden is.

#### 8.7. Vertrouwelijkheidsplicht

Art.9 van de wet van 30 juli 2018 regelt de vertrouwelijkheidsplicht van de betrokken medewerkers die deelnemen aan de beoogde verwerking. Wanneer dit artikel van toepassing is moet de vertrouwelijkheidsplicht hier gestaafd worden.

#### 8.8. Gezondheidsgegevens

Per instantie die gegevens ontvangt dient de verantwoordelijke beroepsbeoefenaar in de gezondheidszorg te worden aangeduid.

### 9. Gebruik van beveiligingsdiensten

Dit betreft beschikbare diensten van het eHealth platform die al dan niet kunnen gebruikt worden in het kader van het realiseren van de te realiseren koppelingen en gegevensaanlevering.