|  |
| --- |
| AANVRAAG TOT HET VERLENEN VAN EEN BERAADSLAGINGDOOR HET INFORMATIEVEILIGHEIDSCOMITÉ |

|  |
| --- |
| **1. Algemeen** |
| 1. Informatie over de aanvrager: benaming, volledig adres en contactinlichtingen (eventueel te vermelden per aanvrager, indien er meerdere aanvragers zijn)

……………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………… |
| 1. Type aanvraag
	* Nieuwe beraadslaging
	* Wijziging van een bestaande beraadslaging

De aanvraag heeft betrekking op de wijziging van de beraadslaging nr. …/… (*referentienummer*) van … (*datum*). De aanvrager kan een WORD-versie van de meest recente versie van deze beraadslaging verkrijgen bij het secretariaat van het informatieveiligheidscomité (ivc@mail.fgov.be). Hij voert zelf in de meest recente versie van deze beraadslaging de door hem gewenste wijzigingen door (met het systeem van *track changes*) en verschaft daarover een omstandige toelichting (dit document moet dan niet verder worden ingevuld).……………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………… |
| 1. Beschikt de aanvrager reeds over beraadslagingen of protocollen met betrekking tot de verwerking van persoonsgegevens?

Specificaties:……………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………… |

|  |
| --- |
| 1. Heeft de aanvrager voor het realiseren van het doeleinde van de verwerking reeds toegang tot het Rijksregister (overeenkomstig een wet, een koninklijk besluit, een beraadslaging van het sectoraal comité van het Rijksregister of een beslissing van de minister van Binnenlandse Zaken)?

Specificaties:………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………Mag de aanvrager voor het realiseren van het doeleinde van de verwerking reeds het rijksregisternummer gebruiken (overeenkomstig een wet, een koninklijk besluit, een beraadslaging van het sectoraal comité van het Rijksregister of een beslissing van de minister van Binnenlandse Zaken)?Specificaties:……………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………… |
| 1. Wordt er een beroep gedaan op een verwerker (de aanvrager zal de persoonsgegevens niet of niet volledig zelf verwerken)?
* Ja

Specificaties………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………Concrete taken die de verwerker zal vervullen in het kader van deze aanvraag:………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………* Nee
 |

|  |
| --- |
| **2. Verloop van de mededeling van persoonsgegevens** |
| 1. Betreft het bijzondere categorieën persoonsgegevens?
	* Neen, er worden geen bijzondere categorieën persoonsgegevens verwerkt
	* Ja, er worden (ook) bijzondere categorieën persoonsgegevens verwerkt
		1. persoonsgegevens over de gezondheid
		2. persoonsgegevens over strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen
		3. andere:

………………………………………………………………………………….......………………………………………………………………………………….......……………………………………………………………………………………… |
| 1. Personen van wie de persoonsgegevens zullen worden verwerkt:
* Hoedanigheid van de personen[[1]](#footnote-1) + motivering van de selectiecriteria[[2]](#footnote-2)

………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………* Aantal + motivering waarom dit aantal noodzakelijk is

………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………* Selectieprocedure

……………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………… |

|  |  |  |
| --- | --- | --- |
| 1. Betrokken instanties (organisatie die de persoonsgegevens meedeelt/organisatie die de persoonsgegevens ontvangt)

|  |  |
| --- | --- |
| Gegevens zijn afkomstig van * Betrokkenen zelf
* KSZ/openbare instelling van sociale zekerheid uit het primair netwerk van de sociale zekerheid
* Andere (niet-openbare) instelling van sociale zekerheid
* Overheidsdiensten en openbare instellingen van de federale overheid niet uit de sociale sector
* Andere

Specificaties……………………………………….……………………………………….………………………………………. | Ontvanger* Betrokkenen zelf
* KSZ/openbare instelling van sociale zekerheid uit het primair netwerk van de sociale zekerheid
* Andere (niet-openbare) instelling van sociale zekerheid
* Overheidsdiensten en openbare instellingen van de federale overheid niet uit de sociale sector
* Andere

Specificaties…………………………………….....……………………………………….………………………………………. |

 |
| 1. Gegevens van de instanties waaraan persoonsgegevens worden gevraagd:

……………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………… |
| 1. Gegevens van de contactpersonen per instantie, met telefoonnummer en mailadres

……………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………… |
| 1. Schematisch overzicht van de gegevensstromen + toelichting

……………………………………………………………………………………………………….……………………………………………………………………………………………………….………………………………………………………………………………………………………. |

|  |
| --- |
| **3. Finaliteit** |
| 1. Algemene doeleinden

……………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………… |
| 1. Wettelijke grondslag voor gegevensverwerking (met verwijzing naar precies artikel AVG)
2. Betreft het persoonsgegevens die betrekking hebben op de volgende eigenschappen van het individu: ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, het lidmaatschap van een vakbond, gegevens over gezondheid, of gegevens over iemands seksueel gedrag of seksuele gerichtheid
* JA:
	+ - * toestemming van de betrokkene
			* verplichtingen van arbeidsrecht, socialezekerheidsrecht of sociale beschermingsrecht
			* ter bescherming van vitale belangen van een betrokkene of een persoon die niet in staat is om zijn toestemming te geven
			* de verwerking wordt verricht door een stichting, een vereniging of een andere instantie zonder winstoogmerk die op politiek, levensbeschouwelijk, godsdienstig of vakbondsgebied werkzaam is
			* de verwerking heeft betrekking op persoonsgegevens die kennelijk door de betrokkene openbaar zijn gemaakt
			* in verband met een rechtsvordering of in het kader van de rechtsbevoegdheid van het gerecht
			* redenen van algemeen belang
			* doeleinden van preventieve of arbeidsgeneeskunde
			* redenen van algemeen belang op het gebied van de volksgezondheid
			* wetenschappelijk of historisch onderzoek of statistische doeleinden
				+ Advies noodzakelijk van een ethisch comité?
* Ja -> bijvoegen op het ogenblik van de indiening van de aanvraag
* Nee
	+ - NEE:
			* toestemming van de betrokkene
			* ter uitvoering van een overeenkomst 🡪 (bijvoegen)
			* ter uitvoering van wettelijke verplichtingen[[3]](#footnote-3)
			* ter bescherming van vitale belangen
			* ter vervulling van een taak van algemeen belang of het openbaar gezag
			* ter behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is.
 |
| 1. Toepasselijke regelgeving

De verwijzing naar de regelgeving (tot op het niveau van de toepasselijke artikelen) moet het informatieveiligheidscomité in staat stellen om de naleving van de beginselen van *doelbinding* en *minimale gegevensverwerking* te beoordelen.……………………………………………………………………………………………………….……………………………………………………………………………………………………….……………………………………………………………………………………………………….De regelgeving moet in elk geval definitief zijn[[4]](#footnote-4). De beraadslaging treedt in beginsel pas in werking op hetzelfde ogenblik als de regelgeving. Pas dan kunnen er op basis van de beraadslaging persoonsgegevens worden verwerkt.Slechts uitzonderlijk (!) kan de aanvrager het informatieveiligheidscomité verzoeken om reeds vóór de inwerkingtreding van de rechtsgrond reële persoonsgegevens te mogen verwerken voor testdoeleinden.Als de testen uitgevoerd kunnen worden met fictieve of gescramblede gegevens moet voor die werkwijze gekozen worden. Enkel indien dit niet mogelijk blijkt, kan er met reële persoonsgegevens worden getest, onder de volgende voorwaarden:* + het gaat om persoonsgegevens van een beperkte populatie;
	+ ze worden enkel gebruikt voor testdoeleinden, niet om rechten toe te kennen;
	+ ze worden verwijderd na de testen;
	+ de verwerking van de persoonsgegevens voor testdoeleinden wordt gelogd.

De aanvrager licht in voorkomend geval omstandig toe waarom de testen niet met fictieve of gescramblede gegevens uitgevoerd kunnen worden en op welke wijze hij voldoet aan de vier voormelde voorwaarden.……………………………………………………………………………………………………….……………………………………………………………………………………………………….………………………………………………………………………………………………………. |

|  |
| --- |
|  **4. Latere verwerking (gebruik van gegevens die oorspronkelijk ingezameld werden voor andere doeleinden)** |
| * Ja

Beschrijving van het oorspronkelijk gebruik van de persoonsgegevens door de instantie die de gegevens zal bezorgen:………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………* Neen
 |

|  |
| --- |
| **5.Transparantie** |
| 1. Informatieverstrekking aan betrokkenen (met aanduiding van de artikelen 13 of 14 AVG)?
* Ja, hoe? Stuk bijvoegen

………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………* Neen, motivering:
	+ de betrokkene beschikt reeds over de informatie
	+ bij onrechtstreekse inzameling: het verkrijgen of verstrekken van de gegevens uitdrukkelijk is voorgeschreven bij lidstatelijk recht:

……………………………………………………………………………………….……………………………………………………………………………………….……………………………………………………………………………………….* + het verstrekken van die informatie blijkt onmogelijk of vergt onevenredig veel inspanning (te motiveren)

motivering……………………………………………………………………………………….……………………………………………………………………………………….………………………………………………………………………………………. |

|  |
| --- |
| 1. **Soort gegevens**
 |
| 1. Aard gegevens:
* niet-gepseudonimiseerde – worden personen bij naam of INSZ (rijksregisternummer of kruispuntbanknummer) genoemd?

Wie kan de personen identificeren? ……………………………………………………* gepseudonimiseerde – worden de gegevens die betrekking hebben op de identiteit van de persoon, zoals naam, INSZ (rijksregisternummer of kruispuntbanknummer), adres verwijderd?
	1. Is het noodzakelijk het verband tussen de gepseudonimiseerde dataset en de identiteit van de personen te behouden?
* Ja

Wie houdt dit verband bij?………………………………………………………………………………….Motivering ………………………………………………………………………………….………………………………………………………………………………….………………………………………………………………………………….* Nee
* anonieme gegevens (geen persoonsgegevens in de enge zin van het woord)
 |
| 1. Gevraagde gegevensset, te vermelden per gegevensbron (exhaustief – in begrijpelijke bewoordingen – voor zover de gegevens worden beschreven in regelgeving, dienen die specifieke bewoordingen uit de regelgeving te worden gehanteerd mét verwijzing naar de betreffende artikels van de regelgeving – de lijst van gevraagde gegevens kan eventueel als bijlage worden toegevoegd)

De aanvrager dient de geïmplementeerde pseudonimiseringsmaatregelen te beschrijven (bijvoorbeeld mededeling van relatieve datums)……………………………………………………………………………………………….……………………………………………………………………………………………………………….……………………………………………………………………………………………………….………………………………………………………………………………………………………. |
| 1. Identificatiepersoonsgegevens (INSZ, Rijksregister, Kruispuntbankregisters, wachtregister,…)
* gebruik van het INSZ (identificatienummer van de sociale zekerheid: rijksregisternummer of kruispuntbanknummer)
* toegang tot of mededeling van gegevens van het Rijksregister
* toegang tot of mededeling van gegevens van de Kruispuntbankregisters
* toegang tot of mededeling van gegevens van het Wachtregister
* toegang tot of mededeling van gegevens van het register van identiteitskaarten
* toegang tot of mededeling van gegevens van het register van vreemdelingenkaarten
* niet van toepassing
 |
| 1. Wat voormelde identificatiepersoonsgegevens betreft:
* Toegang tot de wijzigingen die in het verleden aan de gevraagde gegevens werden verschaft (historiek):
	1. Beoogde gegevens

………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………* 1. Periode van de historiek

………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………* 1. Rechtvaardiging

………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………* Automatische ontvangst van toekomstige wijzigingen aan de gegevens waar toegang toe wordt gevraagd:
1. Beoogde gegevens

………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………1. Rechtvaardiging

………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………1. Op welke dienstenintegrator doet u hiervoor een beroep?

……………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………… |

|  |
| --- |
| **7. Proportionaliteit / Minimale gegevensverwerking** |
| 1. Geldigheidsduur van de beraadslaging + motivering[[5]](#footnote-5)

……………………………………………………………………………………………………….……………………………………………………………………………………………………….………………………………………………………………………………………………………..……………………………………………………………………………………………………….. |
| 1. Bewaartermijn + motivering[[6]](#footnote-6)

……………………………………………………………..………………………………………………………………………………………………..………………………………………………………………………………………………………………………………………………………….………………………………………………………………………………………………………. |
| 1. Verantwoording van de proportionaliteit per categorie van gegeven en per gegevensbron[[7]](#footnote-7)

……………………………………………………………….……………………………………………………………………………………………………………………………………………….……………………………………………………………………………………………………………………………………………………………………………………………………………… |
| 1. Frequentie van de gegevensopvraging + motivering
* éénmalig
* periodiek (met regelmatige tussenpozen). Periodes voor raadpleging:
	+ jaarlijks
	+ semestrieel
	+ trimestrieel
	+ maandelijks
	+ wekelijks
	+ dagelijks
	+ andere
* permanent
 |
| 1. Interne gebruikers op niveau van de aanvrager en eventuele invoering van een functiescheiding binnen de aanvragende instantie.

Vermeld per categorie van interne gebruikers steeds de dienst, de functie en de reden van toegang. Deze gegevens moeten vermeld worden voor alle categorieën van interne gebruikers die toegang hebben tot de gevraagde gegevens door onderstaande rubriek in te vullen, bij meerdere interne gebruikers dient u een bijlage toe te voegen met de gevraagde gegevens per extra categorie interne gebruikers.1. Dienst

………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………1. Functie

………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………1. Reden

……………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………… |
| 1. Hebben derden toegang tot de gevraagde gegevens?
* Neen
* Ja, vul onderstaande vragen in.
1. Worden de gegevens aan meerdere derden meegedeeld?
* Neen
* Ja
1. Naam van de instantie

…………………………………………………………………………………………………………………………………………………………………………………………………………1. Reden van mededeling

…………………………………………………………………………………………………………………………………………………………………………………………………………1. Beschikt de instantie zelf over een beraadslaging?
* Neen
* Ja → bijvoegen
 |

|  |
| --- |
| **8. Veiligheidsbeleid** |
| 1. Functionaris voor gegevensbescherming

Naam: ………………………………………………………………………………………….Organisatie: ……………………………………………..……………………………………. |
| 1. Vragenlijst met gesloten vragen (niet in te vullen door organisaties die tot het netwerk van de sociale zekerheid behoren)
 |

|  |  |  |  |
| --- | --- | --- | --- |
| ***Evaluatieformulier*** | ***ja*** | ***nee*** | ***commentaar of verwijzing naar bijgevoegde documenten*** |
| 1. Beschikt u over een functionaris voor gegevensbescherming? Zo ja, gelieve de hierboven vermelde rubriek in te vullen? |  |  |  |
| 2. Hebt u de risico’s en beveiligingsbehoeften die eigen zijn aan uw organisatie en die de verwerking van persoonsgegevens betreffen geëvalueerd? |  |  |  |
| 3. Beschikt u over een geschreven versie van uw beveiligingsbeleid en is uw beleid t.a.v. de bescherming van persoonsgegevens daarin geïntegreerd? Zo ja, dient een kopie als bijlage bij de aanvraag te worden gevoegd. |  |  |  |
| 4. Hebt u de diverse dragers van uw organisatie geïdentificeerd waarbij persoonsgegevens betrokken zijn? |  |  |  |
| 5. Zijn de interne en externe personeelsleden die bij de verwerking van persoonsgegevens betrokken zijn, goed op de hoogte van de vertrouwelijkheids- en beveiligingsplichten ten aanzien van deze gegevens die zowel voortvloeien uit de verschillende wettelijke vereisten als uit het beveiligingsplan? |  |  |  |
| 6. Hebt u beheersmaatregelen genomen ter verhindering van de niet-gemachtigde of onnodige fysieke toegang tot dragers die persoonsgegevens bevatten? |  |  |  |
| 7. Hebt u maatregelen genomen ter verhindering van elke fysieke schade die de persoonsgegevens in gevaar zouden kunnen brengen? |  |  |  |
| 8. Hebt u beheersmaatregelen genomen ter bescherming van de verschillende netwerken waarmee de apparatuur die de persoonsgegevens verwerkt, is verbonden? |  |  |  |
| 9. Beschikt u over een actuele lijst van de verschillende bevoegde personen die toegang hebben tot de persoonsgegevens en van hun respectievelijk toegangsniveau (creatie, raadpleging, wijziging, vernietiging)? |  |  |  |
| 10. Hebt u op uw informatiesystemen een mechanisme voor toegangsmachtiging geïnstalleerd zodat de persoonsgegevens en de verwerkingen die er betrekking op hebben enkel toegankelijk zijn voor de personen en toepassingen die hiertoe uitdrukkelijk gemachtigd zijn? |  |  |  |
| 11. Is uw informatiesysteem zodanig ontworpen dat de identiteit permanent geregistreerd wordt van diegenen die toegang hebben gehad tot de persoonsgegevens ? |  |  |  |
| 12. Hebt u erin voorzien dat de geldigheid en de doeltreffendheid in de tijd van de ingestelde organisatorische en technische maatregelen gecontroleerd worden ter garantie van de beveiliging van de persoonsgegevens? |  |  |  |
| 13. Hebt u voorzien in urgentieprocedures en rapporteringsprocedures bij beveiligingsincidenten waarbij persoonsgegevens betrokken zijn? |  |  |  |
| 14. Beschikt u over een bijgewerkte documentatie betreffende de verschillende genomen beheersmaatregelen ter bescherming van persoonsgegevens en de verschillende verwerkingen die er betrekking op hebben? |  |  |  |

|  |
| --- |
| 1. Voor zover van toepassing, werd er een specifieke gegevensbeschermingseffectbeoordeling in uitvoering van artikel 23 van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens uitgevoerd?
* Ja
* Nee, beoogde datum van de uitvoering van de specifieke gegevensbeschermingseffectbeoordeling:

………………………………………………………………………………………………….…………………………………………………………………………………………………. |
| 1. Wordt het gebruik van het rijksregisternummer evenals de geautomatiseerde doorgifte van persoonsgegevens aan derden beoogd door informatiesystemen met elkaar te verbinden en hierbij het rijksregisternummer van de betrokkene als sleutel gebruikt?
* Nee
* Ja
	1. Reden van informatieverstrekking:

………………………………………………………………………………………………………………………………………………………………………………………………* 1. Ontvanger

………………………………………………………………………………………………………………………………………………………………………………………………* 1. Beschikt de ontvanger over een machtiging om het rijksregisternummer te gebruiken?
		1. Ja, referentie: …………………………………...............................................
		2. Nee
	2. Werd de gegevensstroom (verstrekking van gegevens andere dan het rijksregisternummer) gedekt door één of meerdere voorafgaande beraadslagingen door het Informatieveiligheidscomité, één van de voormalige Sectorale comités of de Vlaamse Toezichtcommissie?
		1. Ja, referentie: …………………………………………………………………….
		2. Nee
 |
| 1. Intermediaire organisatie
* Ja
	1. Welke organisatie
		+ eHealth-platform
		+ KSZ
		+ Federale Dienstenintegrator
		+ ……………………………………………………………………………………...…………………………………………………………………………………...…

Bewijs akkoord (in bijlage)* 1. TTP (*trusted third party*)
		+ Koppeling
		+ Pseudonimisering
		+ Anonimisering
	2. Andere
* Nee

Indien de aanvrager van oordeel is dat de door de regelgeving opgelegde tussenkomst van de KSZ geen meerwaarde biedt, kan hij het informatieveiligheidscomité verzoeken om een vrijstelling van de tussenkomst van de KSZ te verlenen. Hij verschaft daartoe een omstandige uitleg.……………………………………………………………………………………………………….……………………………………………………………………………………………………….……………………………………………………………………………………………………….……………………………………………………………………………………………………….In geval van tussenkomst van het eHealth-platform als TTP, dient de aanvrager contact op te nemen met de TTP-dienst van eHealth om na te gaan of de gegevensmededeling technisch haalbaar is. De aanvrager deelt een kopie van dit akkoord mee. |
| 1. SCRA voorzien (*small cell risk* analyse)?
* Ja
	1. Welke organisatie ……………………………………………………………………….

Bewijs akkoord (in bijlage)* Nee (motivering waarom niet)
 |
| 1. Zijn alle medewerkers gehouden aan een vertrouwelijkheidsplicht?
* Ja, geregeld op grond van:
	1. Wettelijke verplichting:

Titel en artikel van de wettelijke bepaling: ……………………………………………* 1. Statutaire verplichting (statuut bijvoegen):
	2. Contractuele verplichting (contract bijvoegen):
* Nee
 |
| 1. Indien gegevens die de gezondheid betreffen worden verwerkt, dient een: verantwoordelijke beroepsbeoefenaar in de gezondheidszorg te worden voorzien.

Naam: ………………………………………………………………………………………………………Functie: ………………………………………………………………………………………………………Organisatie ……………………………………………………………………………………………………… |

|  |
| --- |
| **9. Gebruik beveiligingsdiensten** |
| * Ja
* Beveiligde elektronische brievenbus
* eHealth-certificaten
* Pseudonimisering, anonimisering & trusted third party
* ConsultRR
* Coördinatie van elektronische deelprocessen
* Elektronische datering (timestamping)
* Beheer van loggings
* Geïntegreerd gebruikers- en toegangsbeheer
* Verwijzingsrepertorium
* Portaalsite
* Systeem voor end-to-end vercijfering
* Nee

Loggings bevatten een aanduiding van welke persoon op welk moment voor welk doeleinde welke gegevens heeft verwerkt (“*wie-wanneer-waarom-wat*”) en maken het mogelijk om de ketting van bewerkingen volledig te reconstrueren. De aanvrager licht hierna toe welke rol elke tussenkomende partij op dat vlak te vervullen heeft en hoe globaal kan worden nagegaan wat er in elke fase met de gegevens van een persoon is gebeurd.………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………Met de inschrijving van een persoon in een verwijzingsrepertorium deelt een organisatie mee dat zij over die persoon een bepaald type dossier bijhoudt. Gegevens kunnen immers enkel worden uitgewisseld indien zowel de meedelende instantie als de ontvangende instantie de betrokkene in de gepaste context kennen. De aanvrager licht hierna toe met welke hoedanigheidscodes de betrokkenen zijn opgenomen in welke verwijzingsrepertoria[[8]](#footnote-8).……………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………… |

|  |
| --- |
| **10. Principe van de eenmalige inzameling en opslag van persoonsgegevens** |
| Als persoonsgegevens reeds opgevraagd zijn door en beschikbaar zijn bij een authentieke bron, dan mogen ze geen tweede keer worden ingezameld bij de betrokken personen maar moeten ze bij die authentieke bron worden bekomen.Er mag geen sprake zijn van een overtollige meervoudige opslag van persoonsgegevens voor dezelfde doeleinden. De aanvrager mag de persoonsgegevens die hij opvraagt bij de authentieke bron zelf niet structureel opslaan.De aanvrager licht toe hoe hij met de gevraagde verwerking van persoonsgegevens het principe van de eenmalige inzameling en opslag van persoonsgegevens eerbiedigt of licht toe om welke redenen dat niet het geval is.……………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………… |

|  |
| --- |
| **11. Overzicht van stukken** |

1. De aanvrager deelt aan het informatieveiligheidscomité mee over welke specifieke groep(en) van personen hij gegevens wil verwerken. Dat kan door een duidelijke omschrijving of door een exhaustieve opsomming van categorieën. [↑](#footnote-ref-1)
2. Indien het gaat om een aanvraag van een deelentiteit licht de aanvrager in voorkomend geval toe waarom hij voor het realiseren van het doeleinde van de verwerking ook gegevens van personen van andere deelentiteiten nodig heeft. [↑](#footnote-ref-2)
3. Indien de aanvraag uitgaat van een openbare organisatie (ongeacht het bevoegdheidsniveau) moet in beginsel worden verwezen naar deze rechtsgrond. De toepasselijke regelgeving moet dan uitdrukkelijk in de aanvraag vermeld worden, tot op het niveau van de artikelen (zie verder). [↑](#footnote-ref-3)
4. De noodzakelijke finale ondertekening door de bevoegde instanties volstaat daartoe. De publicatie van de regelgeving in het Belgisch Staatsblad is niet vereist. Is de regelgeving (nog) niet in het Belgisch Staatsblad gepubliceerd, dan voegt de aanvrager de tekst ervan bij zijn aanvraag. [↑](#footnote-ref-4)
5. De aanvrager licht toe gedurende welke periode de gegevens noodzakelijk zijn om de doeleinden van de verwerking te realiseren. Hij biedt een duidelijke argumentering, met een verwijzing naar de toepasselijke regelgeving. [↑](#footnote-ref-5)
6. De aanvrager licht toe gedurende welke periode de gegevens na de ontvangst ervan zullen worden bewaard. Hij vermeldt die periode uitdrukkelijk (met het aantal maanden/jaren na de ontvangst van de gegevens) en motiveert ze concreet, met een verwijzing naar de toepasselijke regelgeving). [↑](#footnote-ref-6)
7. De aanvrager licht per gegeven of minstens per logisch samenhangend blok van gegevens toe waarom hij het nodig heeft voor het realiseren van de doeleinden van de verwerking, met een verwijzing naar de toepasselijke regelgeving (tot op het niveau van het artikel). [↑](#footnote-ref-7)
8. Dit is in het bijzonder van belang indien gegevens uit het netwerk van de sociale zekerheid worden meegedeeld aan een organisatie van een deelentiteit. De vraag is dan immers of de link naar de ontvangende organisatie wordt bijgehouden in het verwijzingsrepertorium van de KSZ of in het verwijzingsrepertorium van de bevoegde instantie van de deelentiteit. [↑](#footnote-ref-8)