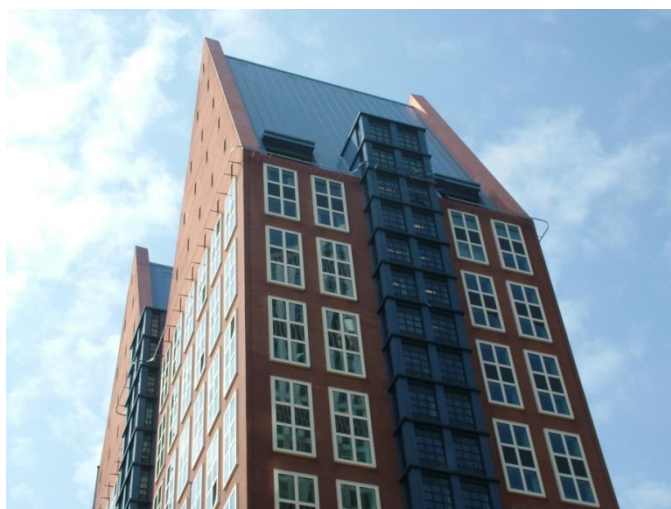


Quickscan Informatiebeveiliging

Bijdragen aan de indiening & beoordeling van
Geneesmiddelenonderzoeken in het kader van
WMO/CTR.



Versie: 1.0

Datum: 08-06-2022

Status: Definitief

1. Contactgegevens

Organisatie Ministerie van Volksgezondheid, Welzijn en Sport (VWS)
Directie Organisatie, Bedrijfsvoering en Personeel
Afdeling Centrale Commissie Mensgebonden Onderzoek (CCMO)
Vestiging adres Parnassusplein 5
Postcode & plaats 2511 VX Den Haag
Telefoonnummer 070-3405555 (keuze 1)
Website <https://www.rijksoverheid.nl/ministeries/ministerie-van-volksgezondheid-welzijn-en-sport>

Workshop

Datum 21-04-2022

Locatie

Straat Parnassusplein 5
Postcode & plaats 2511 VX Den Haag

Deelnemers

Uitvoerder	Functie	Organisatie	E-mail
5.1.2.e	5.1.2.e	CCMO	5.1.2.e@ccmo.nl
		CISO-Kern	5.1.2.e@minvws.nl
Deelnemer	Functie	Organisatie	E-mail
5.1.2.e	5.1.2.e	CCMO	5.1.2.e@ccmo.nl
		CCMO	5.1.2.e@ccmo.nl
		VWS/OBP	5.1.2.e@minvws.nl

Versiebeheer

Versie	Datum	Omschrijving	Auteur	Status
0.1	21-04-2022	Eerste concept	5.1.2.e	concept
0.2	13-5-2022	Naam vaststellen	5.1.2.e	concept
0.3	17-05-2022	Aanvulling concept	5.1.2.e	concept
0.4	20-05-2022	n.a.v. feedback	5.1.2.e	concept
0.5	20-05-2022	n.a.v. 2 ^{de} feedback	5.1.2.e	concept
0.6	25-05-2022	aanvulling	5.1.2.e	concept
0.7	02-06-2022	Feedback CISO-Kern	5.1.2.e	concept
0.8	02-06-2022	afstemming	5.1.2.e	concept
1.0	08-06-2022	Finale versie	5.1.2.e	Definitief
		Marjolein zaaknummer:		
		1030224		

2. Inleiding

Achtergrond

Het doel van de Quickscan-Informatiebeveiliging (QS-IB) is om op een snelle en eenduidige wijze inzicht te krijgen of:

- een proces een Te Beschermen Belang (TBB:2015) is;
- voor het proces de Algemene Verordening Gegevensbescherming (AVG:2018) in voldoende mate is geïmplementeerd en of er een Gegevensbescherming Effecten Beoordeling (GEB; DPIA) wenselijk of noodzakelijk is alsmede het vullen van het verwerkingenregister.
- voor de combinatie van het proces en een informatiesysteem de maatregelen uit de Baseline Informatiebeveiliging Overheid (BIO:2018) voldoende zijn om de informatiebeveiligingsrisico's af te dekken en welk basis beveiligingsniveau (BBN) daarbij van toepassing is.
- het informatiesysteem kritiek, bedrijfskritisch of niet kritiek en niet bedrijfskritisch is, in relatie tot beschouwd proces, ten behoeve van de 'In Control Verklaring' (ICV:2018).
- het betrouwbaarheidsniveau indien het een digitale dienst aan een burger of bedrijf betreft (eIDAS:2018).

Het uitvoeren van een QS-IB kent een aantal onderdelen. Deze onderdelen bestaan uit de stappen die genomen moeten worden om een proces, applicatie of gegevensset te verantwoorden omtrent informatiebeveiliging. Deze stappen zijn:

1. Organiseren bijeenkomst QS-IB
2. Voorbereiden bijeenkomst QS-IB
3. Analyse op aanwezige documentatie.
4. Bijeenkomst:
 - a. Doel Quickscan-Informatiebeveiliging (QS-IB)
 - b. Proces informatie
 - c. Analyse Te Beschermen Belangen (TBB)
 - d. Analyse Algemene Verordening Gegevensbescherming (AVG)
 - e. Analyse Quickscan Baseline Informatiebeveiliging Overheid (BIO)
 - f. Analyse Betrouwbaarheidsniveaus voor digitale dienstverlening (eIDAS)
 - g. Conclusies QS-IB
5. Bijstellen rapportage QS-IB
6. Afstemmen rapportage QS-IB
7. Vaststellen rapportage QS-IB
8. Vastleggen rapportage QS-IB

Scope

Proces

Deze QS-IB beperkt zich tot het proces: 'Bijdragen aan de indiening & beoordeling van Geneesmiddelenonderzoeken in het kader van WMO/CTR' van de CCMO van het Ministerie van VWS.

Vanuit het EU-indieningsplatform CTIS (EMA) wordt middels een API de gegevens(data en bestanden) voor de beoordeling van de Nederlandse onderzoeksprotocollen meermaals per dag automatisch ingelezen in een MSTeams omgeving (NCP, National Collaboration Platform). Indien een nieuwe indiening dan wordt de indiening gevalideerd door een medewerker van de CCMO. Afhankelijk van de voorgestelde of verplichte danwel beschikbare ToetsingsCommissie (TC) [*buiten scope*] wordt de indiening toegewezen aan de TC (METC of CCMO). Medewerkers van de desbetreffende TC krijgen

een melding dat er een nieuwe indiening klaarstaat. In het systeem kan men de beoordelingen benaderen die men toegewezen heeft gekregen. In het systeem wordt een notificatie aangemaakt voor de financiële afdeling van de CCMO om een factuur voor de beoordeling op te stellen. In het systeem kan communicatie plaatsvinden tussen de CCMO en de METC's.

De werkzaamheden die een TC moet uitvoeren vinden buiten het NCP plaats. (*Dus buiten scope van deze QS-IB&P*). Vragen aan de indiener, beoordelingsrapport beschikbaar stellen aan de indiener vindt plaats in CTIS. Uitkomsten en antwoorden worden via de API weer ingelezen het NCP. Na de initiële indiening worden de nieuwe gegevens (waaronder amendementen etc.) direct doorgezet naar de TC die de beoordeling doet.

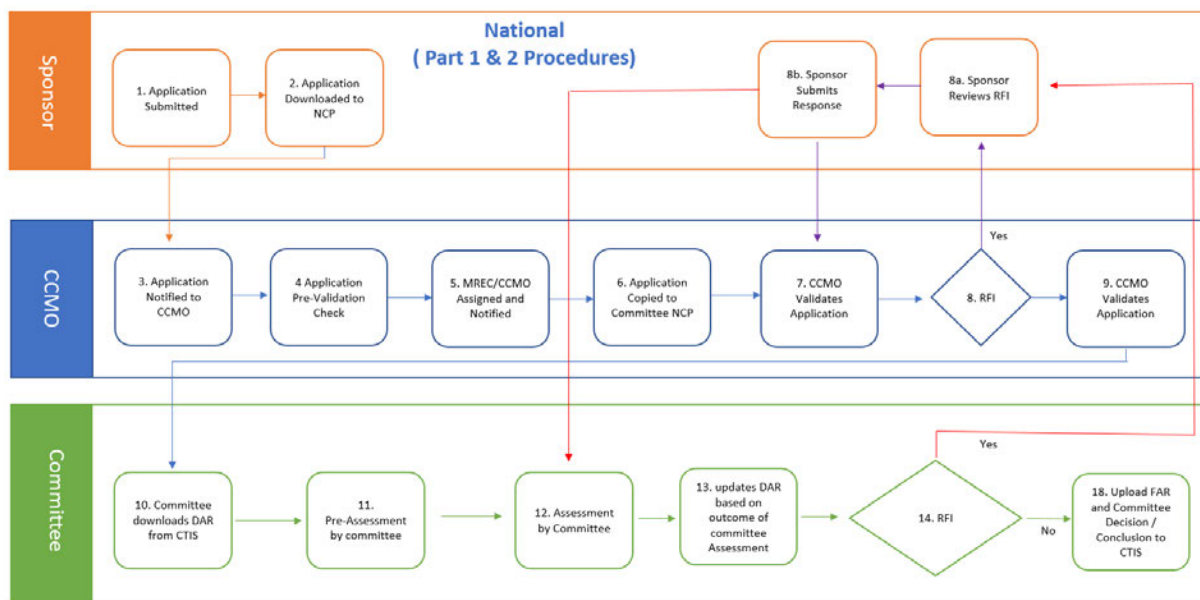
De onderzoeksvoorstellen bevatten bedrijfsgevoelige informatie over geneesmiddelen of medisch hulpmiddelen (DepV). Indien sprake is van niet onder CTR ingediende onderzoeksprotocollen (*dus buiten scope!*): veiligheidsmeldingen (SAE's, SUSAR's) met gepseudonimiseerde persoonsgegevens. Onder de CTR dienen deze ingediend te worden middels Eudravigilance. (*dus buiten scope!*)

De toetsingscommissie beoordeelt onderzoeksvoorstellen in specifieke onderzoeksgebieden zoals in de wet vastgelegd. Betreft de wetten: Wet medisch-wetenschappelijk onderzoek met mensen (WMO) & Embryowet.

Informatiesysteem

Deze QS-IB beperkt zich tot het geautomatiseerde informatiesysteem National Collaboration Platform [NCP] rond het beschouwde proces. Bijdragen aan de indiening & beoordeling van Geneesmiddelenonderzoeken in het kader van WMO/CTR.

Betreft NCP, kantoorautomatisering en Marjolein (registratie en archivering besluiten CCMO) en Viadesk (delen stukken t.b.v. besluitvorming CCMO).



Figuur 1 Proces diagram CCMO

Buiten scope

Niet-geautomatiseerde informatiesystemen die het proces 'Bijdragen aan de indiening & beoordeling van Geneesmiddelenonderzoeken in het kader van WMO/CTR ' ondersteunen vallen buiten de scope van de QS-IB en zullen apart moeten worden geanalyseerd. CTIS, het voor de CTR verplicht gestelde indieningsplatform in de EU en EudraCT zijn buiten scope. CTIS (archivering alle bescheiden ingediende onderzoeksprotocollen en besluiten).

Indien NIET onder CTR meegenomen wordt betreft het ook ToetsingOnline (samen met Viadesk, kantoorautomatisering, EudraCT (indieners delen stukken) en Marjolein (archief alle ingediende stukken en besluitvorming)

Informatiesystemen die geen directe relatie aan het beschouwde informatiesysteem National Collaboration Platform [NCP] hebben vallen ook buiten de scope van de QS-IB en zullen apart moeten worden geanalyseerd. Dit zijn informatiesystemen zonder welke het beschouwde informatiesysteem niet naar behoren werkt.

3. Samenvatting

Hieronder de samengevatte uitkomsten van de QS-IB voor het proces: Bijdragen aan de indiening & beoordeling van Geneesmiddelenonderzoeken in het kader van WMO/CTR

Resultaten QS-IB proces 1 - Bijdragen aan de indiening & beoordeling van Geneesmiddelenonderzoeken in het kader van WMO/CTR

Naam proces	Bijdragen aan de indiening & beoordeling van Geneesmiddelenonderzoeken in het kader van WMO/CTR
TBB proces-classificatie	4
TBB gegevens-classificatie	Departementaal VERTROUWELIJK (Dep.V.)
AVG gegevens-classificatie	gewone persoonsgegevens
AVG Implementatie	onvoldoende
GEB uitvoeren	Niet noodzakelijk
BIO proces-classificatie	Strategisch
eIDAS-betrouwbaarheids-niveau	n.v.t.

Naam van het informatiesysteem	National Collaboration Platform [NCP]
BIO informatiesysteem-classificatie	Belangrijk
BIO BBN-niveau	BBN 2
ICV-classificatie	<u>niet</u> Kritiek en <u>niet</u> Bedrijfskritisch

Naam van het informatiesysteem	Marjolein
BIO informatiesysteem-classificatie	Belangrijk
BIO BBN-niveau	BBN 2
ICV-classificatie	<u>niet</u> Kritiek en <u>niet</u> Bedrijfskritisch

Naam van het informatiesysteem	ViaDesk
BIO informatiesysteem-classificatie	Nuttig
BIO BBN-niveau	BBN 2
ICV-classificatie	<u>niet</u> Kritiek en <u>niet</u> Bedrijfskritisch

Detailbeschrijving proces Bijdragen aan de indiening & beoordeling van Geneesmiddelenonderzoeken in het kader van WMO/CTR

Naam proces	Bijdragen aan de indiening & beoordeling van Geneesmiddelenonderzoeken in het kader van WMO/CTR
Korte procesbeschrijving	Vanuit het EU-indieningsplatform CTIS (EMA) wordt middels een API de gegevens(data en bestanden) voor de beoordeling van de Nederlandse onderzoeksprotocollen meermaals per dag automatisch ingelezen in een MStTeams omgeving (NCP, National Collaboration Platform). Indien een nieuwe indiening dan wordt de indiening gevalideerd door een medewerker van de CCMO. Afhankelijk van de voorgestelde of verplichte danwel beschikbare ToetsingsCommissie (TC) [<i>buiten scope</i>] wordt de indiening toegewezen aan de TC (METC of CCMO). Medewerkers van de desbetreffende TC krijgen een melding dat er een nieuwe indiening klaarstaat. In het systeem kan men de beoordelingen benaderen die men toegewezen heeft gekregen. In het systeem wordt een notificatie aangemaakt voor de financiële afdeling van de CCMO om een factuur voor de beoordeling op te stellen. In het systeem kan communicatie plaatsvinden tussen de CCMO en de METC's. De werkzaamheden die een TC moet uitvoeren vinden buiten het NCP plaats. Vragen aan de indiener, beoordelingsrapport beschikbaar stellen aan de indiener vindt plaats in CTIS. Uitkomst en antwoorden worden via de API weer ingelezen in het NCP. Na de initiële indiening worden de nieuwe gegevens (waaronder amendementen etc.) direct doorgezet naar de TC die de beoordeling doet. De toetsingscommissie beoordeelt onderzoeksvorstellen in specifieke onderzoeksgebieden zoals in de wet vastgelegd. Betreft de wetten: Wet medisch-wetenschappelijk onderzoek met mensen (WMO) & Embryowet.
Proceseigenaar	Algemeen secretaris/directeur CCMO
Gegevenseigenaar	Algemeen secretaris/directeur CCMO
De klant van het proces	Indieners geneesmiddelenonderzoek
De output van het proces is:	Goedgekeurd/afgekeurd geneesmiddelenonderzoek
Koppelvlakken met andere processen zijn:	Ntb
De gebruikte informatiesystemen zijn:	National Collaboration Platform [NCP] Marjolein ViaDesk
De beveiligingsincidenten van het afgelopen jaar zijn:	ntb

Detailbeschrijving informatiesysteem: National Collaboration Platform [NCP]

Naam van het informatiesysteem	National Collaboration Platform [NCP]
Informatiesysteemeigenaar	Algemeen secretaris/directeur CCMO
De gebruikers van het informatiesysteem zijn:	intern Aantal: circa 200 (incl. de METC's)
De output van het informatiesysteem is:	Gedeelde bestanden
Koppelvlakken met andere informatiesystemen zijn:	ViaDesk Marjolein
Processen die gebruik maken van het informatiesysteem zijn:	Bijdragen aan de indiening & beoordeling van Geneesmiddelenonderzoeken in het kader van WMO/CTR.

Detailbeschrijving informatiesysteem: ViaDesk

Naam van het informatiesysteem	ViaDesk
Informatiesysteemeigenaar	Algemeen secretaris/directeur CCMO
De gebruikers van het informatiesysteem zijn:	intern Aantal: circa 50 (medewerkers CCMO & leden CCMO)
De output van het informatiesysteem is:	Gedeelde bestanden
Koppelvlakken met andere informatiesystemen zijn:	NCP Marjolein
Processen die gebruik maken van het informatiesysteem zijn:	Bijdragen aan de indiening & beoordeling van Geneesmiddelenonderzoeken in het kader van WMO/CTR.

Detailbeschrijving informatiesysteem: Marjolein (beperkt tot CCMO gebruikers)

Naam van het informatiesysteem	Marjolein vwb CCMO gebruikers
Informatiesysteemeigenaar	Algemeen secretaris/directeur CCMO
De gebruikers van het informatiesysteem zijn:	intern Aantal: circa 30 (medewerkers CCMO)
De output van het informatiesysteem is:	Gedeelde bestanden
Koppelvlakken met andere informatiesystemen zijn:	NCP ViaDesk
Processen die gebruik maken van het informatiesysteem zijn:	Bijdragen aan de indiening & beoordeling van Geneesmiddelenonderzoeken in het kader van WMO/CTR.

4. Inhoud

1. Contactgegevens	2
2. Inleiding	3
3. Samenvatting.....	6
4. Inhoud	9
5. Analyse Te Beschermen Belangen (TBB)	10
6. Analyse Algemene Verordening Gegevensbescherming (AVG)	14
B. Beginselen voor verwerking (hoofdstuk II AVG)	14
V. Verwerkingsverantwoordelijke en Verwerker (hoofdstuk IV AVG)	18
R. Rechten van de betrokkene (hoofdstuk III AVG).....	22
E. Extra vragen t.b.v. AVG register	23
7. Quicksan BIO.....	25
8. Analyse Betrouwbaarheidsniveaus voor digitale dienstverlening	28
Bijlage 1: TBB Categorieën (Vraag 5 TBB).....	30
Bijlage 2: TBB Classificatie (Vraag 5 TBB)	31
Bijlage 3: AVG Toelichting (Vraag B1 t/m E7 AVG).....	33
Bijlage 4: AVG Logische gegevensverwerkingsgroepen (Vraag B4 AVG)	42
Bijlage 5: BIO Proces-classificatie (Vraag 1 BIO).....	43
Bijlage 6: BIO Informatiesysteem-classificatie (Vraag 1 BIO)	45
Bijlage 7: BIO Beschikbaarheid-classificatie (Vraag 2 BIO)	46
Bijlage 8: BIO Integriteit-classificatie (Vraag 2 BIO)	47
Bijlage 9: BIO Vertrouwelijkheid-classificatie (Vraag 2 BIO)	48
Bijlage 10: BIO Basisbeschermingsniveau (BBN) (Vraag 10 BIO).....	49
Bijlage 11: ICV Toelichting	52
Bijlage 12: eIDAS Toelichting.....	53

5. Analyse Te Beschermen Belangen (TBB)

Doelstelling TBB

Onder Te Beschermen Belangen (TBB) wordt verstaan: informatie, informatiesystemen, materieel, goederen, (bewinds)personen en objecten die beveiligd moeten worden om de werking van de Rijksoverheid zoveel mogelijk ongestoord doorgang te laten vinden.

Kennisname of aantasting hiervan door vreemde mogendheden of derden kan de Nationale Veiligheid, het algemeen (economisch/politiek) belang en/of de integriteit van de Rijksoverheid aantasten. Bij het bepalen van de TBB staan de primaire processen centraal.

Bij de TBB analyse betreft het informatie(gegevens)set, informatiesystemen die beveiligd moeten worden om de bedrijfsvoering en andere gewichtige belangen en processen van de Rijksoverheid ongestoord doorgang te laten vinden. De overige categorieën zijnde: materieel, (bewinds)personen of objecten worden buiten beschouwing gelaten. Dit omdat de QS-IB zich richt op informatie-beveiliging. Aan elk proces moet een niveau worden toegekend, gerelateerd aan de impact die ontstaat als gevolg van een incident: in oplopende zwaarte van 4 naar 1 of n.v.t.

De Quickscan TBB (QS-TBB) bepaalt aan de hand van een aantal vragen (zie toelichting Bijlage 1) het TBB-niveau van het betreffende proces.

Resultaten QS-TBB

Proces: **Bijdragen aan de indiening & beoordeling van Geneesmiddelenonderzoeken in het kader van WMO/CTR**

1	Kan falen van één of meer beveiligingsmaatregelen leiden tot langdurige (imago)schade van VWS of de Rijksdienst?	<u>Politieke schade</u>	
		n.v.t.: Geen politieke schade	
		4:	Politieke schade voor bewindspersoon
		3:	Aftreden bewindspersoon
		2:	Aftreden kabinet
		1:	Parlementaire crisis
		<u>Imago schade</u>	
		n.v.t.:	Geen imago schade
		4:	Verlies van publiek respect
		3:	Publieke verontwaardiging
		2:	Verlies aan vertrouwen
		1:	Structureel verlies aan vertrouwen
		<u>Diplomatieke schade</u>	
		n.v.t.:	Geen diplomatieke schade
		4:	Te herstellen door ambtelijke opschaling
		3:	Te herstellen door politieke opschaling
		2:	Externe bemiddeling noodzakelijk
		1:	Lange termijn schade t.o.v. bondgenoten, oorlog
		<u>Financiële schade voor de staat</u>	
		n.v.t.:	<= 50 mln.
		4:	> 50 mln.
		3:	> 500 mln.

		2: > 5 mld. 1: > 50 mld. <u>Financiële schade door misbruik bedrijfsinformatie</u> n.v.t.: < = 1 mln. 4: > 1 mln. 3: > 5 mln. 2: > 500 mln. 1: > 5 mld.
	Score	[n.v.t.] [4] [3] [2] [1]
	Toelichting	Het falen heeft mogelijk grote financiële gevolgen doordat lekken IMPD met geneesmiddelen duidelijke impact heeft. B.v. inbreuk op intellectueel eigendom van patenten kunnen claims opleveren die substantieel zijn. Ook imago schade kan ontstaan door falen van maatregelen met verlies van respect door indieners en/of farmacie-organisaties en/of academische instellingen.

2	Kan falen van één of meer beveiligingsmaatregelen leiden tot maatschappelijke ontwrichting, ernstig letsel aan of de dood van één of meerdere personen?	<u>Letselschade aan personen of groepen van personen</u> n.v.t.: Geen letselschade 4: Individuele gewonde 3: Individuele dode, ernstig gewond 2: Meerdere doden, zeer ernstig gewond 1: Groepen doden
	Score	[n.v.t.] [4] [3] [2] [1]
	Toelichting	Bij de directe uitvoering van de processen zal er geen letselschade kunnen plaatsvinden.

3	Is de dienstverlening aan burgers of bedrijven in belangrijke mate afhankelijk van het proces?	<u>Schade aan vitale processen van de samenleving</u> n.v.t.: Geen invloed 4: Verlies van zekerheid van continuïteit 3: Tijdelijk verlies van continuïteit 2: Langdurig verlies van continuïteit 1: Blijvende uitval van processen <u>Financiële schade voor de economie</u> n.v.t.: <= 50 mln. 4: > 50 mln. 3: > 500 mln. 2: > 5 mld. 1: > 50 mld.
	Score	[n.v.t.] [4] [3] [2] [1]

	Toelichting	Dienstverlening van burgers of bedrijven is niet uitsluitend afhankelijk van deze processen.
--	--------------------	--

4	Zijn belangrijke processen binnen mede-overheden afhankelijk van het proces?	<u>Schade voor vitale processen medeoverheden</u> n.v.t.: Geen invloed 4: Verlies van zekerheid van continuïteit 3: Tijdelijk verlies van continuïteit 2: Langdurig verlies van continuïteit 1: Blijvende uitval van processen
	Score	[n.v.t.] [4] [3] [2] [1]
	Toelichting	Mede-overheden worden niet geraakt door deze processen.

5	Wat is de exclusiviteitswaarde van de informatie die binnen het proces wordt verwerkt?	<u>VIR-BI informatie-rubricering</u> n.v.t.: Geen <i>bijzondere informatie</i> 4: Departementaal VERTROUWELIJK (Dep.V.) 3: Staatsgeheim CONFIDENTIEEL (Stg.C) 2: Staatsgeheim GEHEIM (Stg.G) 1: Staatsgeheim ZEER GEHEIM (Stg.ZG) <u>EU informatie-rubricering</u> n.v.t.: EU unclassified 4: EU restricted 3: EU confidential 2: EU secret 1: EU top secret <u>NATO informatie-rubricering</u> n.v.t.: NATO unclassified 4: NATO restricted 3: NATO confidential 2: NATO secret 1: NATO top secret
	Score	[n.v.t.] [4] [3] [2] [1]
	Toelichting	De onderzoeksvoorstellen zijn concurrentie gevoelig en er kunnen grote commerciële en financiële belangen mee gemoeid zijn. Bovendien zijn geneesmiddelenonderzoeken niet alleen nationaal maar ook Europees gericht. Vandaar de classificatie Dep.V.

Conclusie QS-TBB

Bepaal hoogste niveau van vraag 1-5	Classificatie (Bijlage 2)
[n.v.t.] [4] [3] [2] [1]	[n.v.t.] [laag] [midden] [hoog] [zeer hoog]

6. Analyse Algemene Verordening Gegevensbescherming (AVG)

Doelstelling

De AVG is de wet die voorschrijft hoe organisaties om moeten gaan met persoonsgegevens in de breedste zin. De invulling hiervan bedraagt voornamelijk: inzichtelijk hebben welke persoonsgegevens worden verwerkt, het bijhouden van een register, risico's afwegen en maatregelen invoeren. Dit ter bescherming van de persoonsgegevens en de rechten van de betrokkenen.

Voor meer informatie over de AVG zie:

<https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/handleidingalgemeneverordeninggegevensbescherming.pdf>

en

<http://www.privacy-regulation.eu/nl/index.htm>

De Quickscan AVG (QS-AVG) bepaalt aan de hand van een aantal vragen (zie toelichting Bijlage 3) of voor het proces de AVG in voldoende mate is geïmplementeerd en of er een Gegevensbescherming Effecten Beoordeling (GEB) wenselijke of noodzakelijk is alsmede het vullen van het verwerkingen-register.

Resultaten QS-AVG

Proces: **Bijdragen aan de indiening & beoordeling van Geneesmiddelenonderzoeken in het kader van WMO/CTR**

Lijst ondersteunende informatiesystemen: **National Collaboration Platform [NCP]
Marjolein & ViaDesk**
Geef aan indien er sprake is van (semi-)geautomatiseerde besluitvorming, profilering of big data-verwerkingen in de informatiesystemen.

Resultaten horizontale AVG analyse voor het proces: Bijdragen aan de indiening & beoordeling van Geneesmiddelenonderzoeken in het kader van WMO/CTR

B. Beginselen voor verwerking (hoofdstuk II AVG)

Vraag		Toelichting	
B1	Is er al eerder een QS PIA uitgevoerd?	Indien Ja: Datum en vindplaats van de documenten aangeven	[Ja]/[Nee]
Datum		Vindplaats	
<u>29-01-2019</u>		<u>CCMO/Bedrijfsvoering/Integriteit &</u>	
<u>11-07-2019</u>		<u>informatiebeveiliging/Informatiebeveiliging/Audits/2019</u>	

Vraag		Toelichting	
B2	Worden er persoonsgegevens verwerkt?	Persoonsgegevens zijn alle gegevens aan de hand waarvan een natuurlijk persoon kan worden geïdentificeerd. Dit kunnen persoonsgegevens zijn van: medewerkers, gebruikers, bezoekers, consumenten, klanten, leveranciers, patiënten, zakelijke contacten etc.. Indien Ja: soort betrokkene aangeven	[Ja]/[Nee]
Betrokkene			
Indieners onderzoek voorstel			
Onderzoekers onderzoek voorstel			
Sponsors onderzoek voorstel			

! Indien vraag B2 met Ja is beantwoord ga door met QS AVG.

Vraag		Toelichting	
B3	Welke persoonsgegevens worden er verwerkt?	Geef per betrokkene aan wat voor soort persoonsgegevens worden verwerkt. Soorten persoonsgegevens zijn o.a.: - NAW-gegevens - persoon identificerende nummer(s) - gebruikersnamen/inloggegevens - identiteitsgegevens - financiële gegevens - bijzondere gegevens (ras, politiek, religie, vakbond, genetisch, biometrisch, gezondheid, seksueel gedrag) - strafrechtelijke gegevens Geef ook aan welk type persoonsgegeven het is. Typen zijn gewoon, bijzonder, strafrechtelijk en wettelijk identificerend.	
Betrokkene		Soort gegevens	Type persoonsgegeven
Indieners onderzoek voorstel		Naam, email, soms telefoonnummer	Gewone persoonsgegevens
Onderzoekers onderzoek voorstel		Naam, email, soms telefoonnummer	Gewone persoonsgegevens
Sponsors onderzoek voorstel		Naam, email, soms telefoonnummer	Gewone persoonsgegevens

Vraag		Toelichting	
B4	Vallen de persoonsgegevens onder de AVG?	Uitzonderingen AVG: - Wet inlichtingen en veiligheidsdiensten - Kieswet - Basisregistratie personen - Persoonlijke (voor de werknemer) archieven (e-mail, p-schijf etc..) Geef per verwerking betrokkene – soort gegevens aan Ja/Nee. Bij Nee geef een toelichting waarom de verwerking niet onder de AVG valt.	
Betrokkene	Soort gegevens	Vallen onder AVG	Toelichting uitzondering
Indieners onderzoek voorstel	Naam, email, soms telefoonnummer	[Ja]/[Nee]	
Onderzoekers onderzoek voorstel	Naam, email, soms telefoonnummer	[Ja]/[Nee]	
Sponsors onderzoek voorstel	Naam, email, soms telefoonnummer	[Ja]/[Nee]	

I Indien bij één of meer verwerkingen vraag B4 met Ja is beantwoord ga door met QS AVG voor deze verwerkingen.

Voor het bepalen van logische gegevensverwerkingsgroepen (GVG) zie Bijlage 4 'AVG Logische gegevensverwerkingsgroepen'.

Logische gegevensverwerkingsgroepen

Gegevens-verwerkingsgroep	Betrokkene	Soort gegevens	Toelichting verwerking
IND01	Indieners onderzoek voorstel	Naam, email, soms telefoonnummer	Logische gegevens verwerkingsgroep
OND01	Onderzoekers onderzoek voorstel	Naam, email, soms telefoonnummer	Logische gegevens verwerkingsgroep
SPR01	Sponsors onderzoek voorstel	Naam, email, soms telefoonnummer	Logische gegevens verwerkingsgroep

Vraag		Toelichting
B5	Bevatten de persoonsgegevens bijzondere persoonsgegevens?	Geef per gegevensverwerkingsgroep aan of deze bijzondere persoonsgegevens bevatten. Bij Ja: Toelichting welke bijzondere persoonsgegevens (meerdere mogelijk) worden verwerkt en beoordeel of één van de wettelijke uitzonderingen op het verwerkingsverbod van toepassing zijn.
Gegevensverwerkingsgroep		Bijzondere persoonsgegevens
IND01		[Ja]/[Nee]
OND01		[Ja]/[Nee]
SPR01		[Ja]/[Nee]

Vraag		Toelichting
B6	Is de verwerking opgenomen in een register?	Geef per gegevensverwerkingsgroep aan Ja/Nee. Bij Ja: toelichting register invullen (o.a. naamregister, vindplaats documenten etc..)
Gegevensverwerkingsgroep		In register
IND01		[Ja]/[Nee]
OND01		[Ja]/[Nee]
SPR01		[Ja]/[Nee]

Vraag		Toelichting
B7	Zijn de doelen van de verwerking vastgesteld?	Geef per gegevensverwerkingsgroep aan Ja/Nee. Bij Ja: bij toelichting de doeleinden invullen. Indien de persoonsgegevens voor een ander doel worden verwerkt dan oorspronkelijk verzameld, beoordeel of deze verdere verwerking verenigbaar is met het doel waarvoor de persoonsgegevens oorspronkelijk zijn verzameld.
Gegevensverwerkingsgroep		Doelen
IND01		[Ja]/[Nee]
OND01		[Ja]/[Nee]
SPR01		[Ja]/[Nee]

Vraag		Toelichting
B8	Zijn de grondslagen van de verwerking vastgesteld?	Geef per gegevensverwerkingsgroep aan Ja/Nee. Bij Ja: geef een <u>uitgebreide</u> toelichting bij de grondslagen (zie Bijlage 3 voor een nadere uitleg).
Gegevensverwerkingsgroep		Toelichting grondslagen
IND01		[Ja]/[Nee] Gerechtvaardigd belang. Onderdeel van de normale bedrijfsvoering.
OND01		[Ja]/[Nee] Gerechtvaardigd belang. Onderdeel van de normale bedrijfsvoering.
SPR01		[Ja]/[Nee] Gerechtvaardigd belang. Onderdeel van de normale bedrijfsvoering.

Vraag		Toelichting
B9	Is er wet- en regelgeving en/of beleid dat gevolgen heeft voor de verwerkingen?	Benoem de wet- en regelgeving, met uitzondering van de AVG en de Richtlijn, en het beleid met mogelijke gevolgen voor de gegevensverwerkingen (zie Bijlage 3 voor een nadere uitleg).
Gegevensverwerkingsgroep		Toelichting juridische en beleidsmatige kaders
IND01		[Ja]/[Nee] WMO & Embryowet
OND01		[Ja]/[Nee] WMO & Embryowet
SPR01		[Ja]/[Nee] WMO & Embryowet

Vraag		Toelichting
B10	Zijn de bewaartermijnen van de verwerking vastgesteld?	Geef per gegevensverwerkingsgroep aan Ja/Nee. Bij Ja: toelichting bewaartermijn invullen (o.a. welke bewaartermijn van toepassing is, vindplaats documenten, etc..)
Gegevensverwerkingsgroep		Toelichting bewaartermijn
IND01		[Ja]/[Nee] Archiefwet; Selectielijst CCMO maximaal 30 jaar na afronding onderzoek.
OND01		[Ja]/[Nee] Archiefwet; Selectielijst CCMO maximaal 30 jaar na afronding onderzoek.
SPR01		[Ja]/[Nee] Archiefwet; Selectielijst CCMO maximaal 30 jaar na afronding onderzoek.

V. Verwerkingsverantwoordelijke en Verwerker (hoofdstuk IV AVG)

Vraag		Toelichting
V1	Wie is de verwerkingsverantwoordelijke?	Geef per gegevensverwerkingsgroep aan Functieaanduiding/organisatieonderdeel.
Gegevensverwerkingsgroep		Organisatie
IND01		Algemeen secretaris/directeur CCMO Ministerie van VWS

OND01	Algemeen secretaris/directeur CCMO	Ministerie van VWS
SPR01	Algemeen secretaris/directeur CCMO	Ministerie van VWS

Vraag		Toelichting	
V2	Welke verwerkers zijn er?	Geef per gegevensverwerkingsgroep aan verwerkers/ organisatie.	
Gegevensverwerkingsgroep		Verwerker	Organisatie
IND01; OND01; SPR01		Marjolein; Directie OBP	Ministerie van VWS
IND01; OND01; SPR01		ViaDesk: CCMO	Ministerie van VWS
IND01; OND01; SPR01		NCP: Azure; Microsoft	Microsoft NL

! Indien voor één of meer van de verwerkingen er verwerkers zijn geef dan een antwoord op de vraag V3 en V4. Anders ga door naar vraag V5.

Vraag		Toelichting		
V3	Zijn er met alle verwerkers verwerkerovereenkomsten/ verwerkerafspraken gesloten?	Geef per gegevensverwerkingsgroep - verwerker – organisatie aan Ja/Nee		
Gegevensverwerkingsgroep		Verwerker	Organisatie	Overeenkomst/ afpraak
IND01; OND01; SPR01		Marjolein; Directie OBP	Ministerie van VWS	Ja
IND01; OND01; SPR01		ViaDesk: CCMO	Ministerie van VWS	Ja
IND01; OND01; SPR01		NCP: Azure; Microsoft	Microsoft NL	Nog op te stellen

Vraag		Toelichting		
V4	Is de verwerking aangesloten op het proces 'Melden Datalekken'?	Geef per gegevensverwerkingsgroep - verwerker aan Ja/Nee.		
Gegevensverwerkingsgroep		Verwerker	Aangesloten	Toelichting aansluiting
IND01; OND01; SPR01		Marjolein; Directie OBP	Ja	
IND01; OND01; SPR01		ViaDesk: CCMO	Ja	
IND01; OND01; SPR01		NCP: Azure; Microsoft	Nee	Nog te bepalen

Vraag		Toelichting
V5	Zijn bij de ontwikkeling van de verwerking principes van Privacy by Design toegepast?	Geef per gegevensverwerkingsgroep aan Ja/Nee.

Gegevensverwerkingsgroep	Privacy by Design	Toelichting Privacy by Design
IND01	[Ja]/[Nee]	Er is b.v. vanaf het begin rekening mee gehouden dat gegevens gescheiden toegankelijk zijn op basis van logische toegangsbeveiliging. Er zal een risico inventarisatie worden gedaan voordat een oplossing wordt aangeschaft.
OND01	[Ja]/[Nee]	Er is b.v. vanaf het begin rekening mee gehouden dat gegevens gescheiden toegankelijk zijn op basis van logische toegangsbeveiliging. Er zal een risico inventarisatie worden gedaan voordat een oplossing wordt aangeschaft.
SPR01	[Ja]/[Nee]	Er is b.v. vanaf het begin rekening mee gehouden dat gegevens gescheiden toegankelijk zijn op basis van logische toegangsbeveiliging. Er zal een risico inventarisatie worden gedaan voordat een oplossing wordt aangeschaft.

Vraag		Toelichting
V6	Is een GEB noodzakelijk?	Geef per gegevensverwerkingsgroep aan Ja/Nee. Geef in de toelichting aan waarom GEB van toepassing is. Een verwerking die aard, omvang, doeleinden, context en complexiteit waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van betrokken. Bijvoorbeeld grootschalige monitoring, profilering, verwerking van bijzondere persoonsgegevens en/of gegevens m.b.t. strafbare feiten. Zie Bijlage 3 voor de criteria van de Europese toezichthouder en de Autoriteit persoonsgegevens.
Gegevensverwerkingsgroep		GEB nodig Toelichting noodzaak
IND01		[Ja]/[Nee]
OND01		[Ja]/[Nee]
SPR01		[Ja]/[Nee]

! Indien GEB noodzakelijk is voor één of meer van de verwerkingen geef een antwoord op de vraag
! V7. Anders ga door naar vraag V8.

Vraag		Toelichting
V7	Is een GEB uitgevoerd?	Geef per gegevensverwerkingsgroep aan Ja/Nee

		Bij Ja: toelichting GEB invullen (o.a. vindplaats documenten, etc.)
Gegevensverwerkingsgroep	GEB	Toelichting uitvoering GEB
IND01	[Ja]/[Nee]	
OND01	[Ja]/[Nee]	
SPR01	[Ja]/[Nee]	

Vraag	Toelichting	
V8 Worden de gegevens door gegeven aan andere verwerkings-verantwoordelijken?	Geef per gegevensverwerkingsgroep aan Ja/Nee. Bij Ja: aan wie (organisatie)	
Gegevensverwerkingsgroep	Doorgifte	Organisatie
IND01	[Ja]/[Nee]	EMA
OND01	[Ja]/[Nee]	EMA
SPR01	[Ja]/[Nee]	EMA

Indien voor één of meer van de verwerkingen de gegevens worden doorgegeven aan andere verwerkingsverantwoordelijke geef een antwoord op de vragen V9, V10 en V11. Anders ga door naar vraag R1.

Vraag	Toelichting		
V9 Zijn er afspraken en garanties vastgelegd m.b.t. het doorgeven van gegevens aan andere verwerkings-verantwoordelijke?	Geef per gegevensverwerkingsgroep - organisatie aan Ja/Nee Bij Ja: Toelichting m.b.t. de afspraken (o.a. vindplaats documenten)		
Gegevensverwerkingsgroep	Organisatie	Afspraken	Toelichting afspraken
IND01	EMA	[Ja]/[Nee]	Op nationaal niveau samenwerkings-overeenkomst
OND01	EMA	[Ja]/[Nee]	Op nationaal niveau samenwerkings-overeenkomst
SPR01	EMA	[Ja]/[Nee]	Op nationaal niveau samenwerkings-overeenkomst

Vraag	Toelichting	
V10 Waar worden de persoons-gegevens verwerkt?	Geef per gegevensverwerkingsgroep aan in welk land ze worden verwerkt en door welke actor.	
Gegevensverwerkingsgroep	Actor	Land
IND01	EMA	NL
OND01	EMA	NL
SPR01	EMA	NL

--	--	--

Vraag		Toelichting
V11	Worden de gegevens door gegeven aan andere verwerkingsverantwoordelijken buiten de EU?	Geef per gegevensverwerkingsgroep aan Ja/Nee/N.v.t.. Bij Ja: welk land
Gegevensverwerkingsgroep		Buiten EU
IND01		[Ja]/[Nee]
OND01		[Ja]/[Nee]
SPR01		[Ja]/[Nee]

R. Rechten van de betrokkene (hoofdstuk III AVG)

Vraag		Toelichting
R1	Is er een informatieplicht naar betrokkene van toepassing?	Geef per gegevensverwerkingsgroep aan Ja/Nee. Voor gegevens die je direct bij een betrokkene verzamelt verstrek je bij het verzamelen al informatie over grondslag, doel verwerking, bewaartermijn, verantwoordelijkheden etc.. etc.. Voor gegevens die worden aangeleverd door een andere verwerkingsverantwoordelijke, wordt de betrokkene actief geïnformeerd. Als gegevens verder worden doorgeleverd, moet ook hiertoe informatie worden verstrekt. AVG Artikel 14.5 b-d geeft de uitzonderingen m.b.t. de informatieplicht aan. Bij Ja: Beschrijving hoe betrokkene wordt geïnformeerd
Gegevensverwerkingsgroep		Info.plicht
IND01		[Ja]/[Nee]
OND01		[Ja]/[Nee]
SPR01		[Ja]/[Nee]

Vraag		Toelichting
R2	Is er een proces ingericht en in werking t.b.v. het recht op inzage, correctie, vernietiging, bezwaar?	Geef per gegevensverwerkingsgroep aan Ja/Nee. Bij Ja: Toelichting op proces (wat wel/wat niet)
Gegevensverwerkingsgroep		Proces rechten
IND01		[Ja]/[Nee]
OND01		[Ja]/[Nee]
SPR01		[Ja]/[Nee]

Vraag		Toelichting
R3	Worden er besluiten geautomatiseerd genomen die rechtgevolgen kunnen hebben voor betrokkene?	Geef per gegevensverwerkingsgroep aan Ja/Nee. Bij Ja: Geef aan of het gedocumenteerd is
Gegevensverwerkingsgroep		Geautomatiseerd besluit
IND01		[Ja]/[Nee]
OND01		[Ja]/[Nee]
SPR01		[Ja]/[Nee]

E. Extra vragen t.b.v. AVG register

Vraag		Toelichting
E1	Wie levert de persoonsgegevens aan?	Geef per gegevensverwerkingsgroep aan wat de bron is. Indien het niet de betrokkene zelf is geef een toelichting
Gegevensverwerkingsgroep		Bron
IND01		betrokkene
OND01		betrokkene
SPR01		betrokkene

Vraag		Toelichting
E2	Is de aanlevering van de persoonsgegevens verplicht?	Geef per gegevensverwerkingsgroep aan of deze verplicht aangeleverd moet worden. Bij Ja: Toelichting over de verplichte aanlevering
Gegevensverwerkingsgroep		Verplichte aanlevering
IND01		[Ja]/[Nee]
OND01		[Ja]/[Nee]
SPR01		[Ja]/[Nee]

--	--	--

Vraag		Toelichting
E3	Zijn de persoonsgegevens gepseudonimiseerd?	Geef per gegevensverwerkingsgroep aan of deze gepseudonimiseerd zijn. Bij Ja: Toelichting m.b.t. de pseudonisering
Gegevensverwerkingsgroep		Pseudonisering
IND01		[Ja]/[Nee]
OND01		[Ja]/[Nee]
SPR01		[Ja]/[Nee]

Vraag		Toelichting
E4	Zijn de persoonsgegevens geëncrypt?	Geef per gegevensverwerkingsgroep aan of deze geëncrypt zijn. Bij Ja: Toelichting m.b.t. de encryptie (meerdere mogelijk)
Gegevensverwerkingsgroep		Encryptie
IND01		[Ja]/[Nee]
		[Ja, de persoonsgegevens worden versleuteld tijdens verzending] [Ja, de gegevensopslag is versleuteld]
OND01		[Ja]/[Nee]
SPR01		[Ja]/[Nee]

Vraag		Toelichting
E5	Worden de persoonsgegevens via elektronische weg verzonden?	Geef per gegevensverwerkingsgroep aan of deze via elektronische weg worden verzonden. Bij Ja: Toelichting m.b.t. de verzending (meerdere mogelijk)
Gegevensverwerkingsgroep		Via elektronische weg verzonden
IND01		[Ja]/[Nee]
		[Ja, via een eigen netwerk] [Ja, via een publiek netwerk; dan standaard versleuteling van persoonsgegevens.]
OND01		[Ja]/[Nee]
		[Ja, via een eigen netwerk] [Ja, via een publiek netwerk; dan standaard versleuteling van persoonsgegevens.]
SPR01		[Ja]/[Nee]
		[Ja, via een eigen netwerk] [Ja, via een publiek netwerk; dan standaard versleuteling van persoonsgegevens.]

7. Quickscan BIO

Doelstelling Quickscan BIO (QS-BIO)

De BIO beschrijft de normen waaraan elk informatiesysteem binnen de Rijksoverheid minimaal moet voldoen.

Voor de combinatie van het proces en een informatiesysteem moet achterhaald worden of de maatregelen uit de Baseline Informatiebeveiliging Overheid (BIO:2018) voldoende zijn om de informatiebeveiligings-risico's af te dekken en welk basis beveiligingsniveau (BBN 1, BBN2, BBN3 of boven BBN3) daarbij van toepassing is.

Tevens kan door middel van de QS-BIO worden bepaald of een informatiesysteem kritiek, bedrijfskritisch of niet kritiek en niet bedrijfskritisch is ten behoeve van de 'In Control Verklaring' (ICV).

Daartoe worden zowel het proces als de informatiesystemen geanalyseerd volgens de richtlijnen in de Bijlagen 5, 6, 7, 8, 9, 10 en 11.

Resultaten QS-BIO

Proces: **Bijdragen aan de indiening & beoordeling van Geneesmiddelenonderzoeken in het kader van WMO/CTR**

Informatiesystemen: **National Collaboration Platform [NCP], Marjolein en ViaDesk.**

1 - Classificatie

Classificatie van het proces	[Kritisch strategisch] [Strategisch] [Bijdragend] [Ondersteunend]
Argumentatie van de gekozen classificatie van het proces	Bijdragen aan geneesmiddelenonderzoek door CCMO heeft, naast een wettelijke taak, ook een directe relatie met de doelstellingen van het ministerie van VWS. Vandaar de classificatie strategisch.
Classificatie van het informatiesysteem	[Vitaal] [Belangrijk] [Nuttig]
Argumentatie van de gekozen classificatie van het informatiesysteem	Het gebruik van het NCP door circa 200 gebruikers is substantieel en het heeft een grote bijdrage aan de efficiency en effectiviteit van de werkzaamheden van de CCMO en de METC's. Vandaar de keuze van classificatie voor belangrijk.

2 - Betrouwbaarheidseisen

Beschikbaarheid	[Laag] [Midden] [Hoger dan midden]
Argumentatie van de gekozen beschikbaarheid	Het systeem kan niet langer dan een week werkdag niet beschikbaar zijn, omdat anders de termijnen in het proces niet gerealiseerd kunnen worden en bij het overschrijven van Europese wettelijke termijnen wordt een onderzoek automatisch positief beoordeeld. Dit kan implicaties hebben voor de proefpersonen en voor de positie van klinisch onderzoek in Nederland (zowel academisch als industrieel) . Dit kan ook mogelijke klachten in het publieke domein tot gevolg hebben. En dit heeft weer imago schade tot gevolg van CCMO/VWS. Er is op dit moment nog geen SLA afgesloten. Het NCP is een tussenapplicatie tussen het verplichte Europese CTR indieningsportal CTIS voor de werkzaamheden van de CCMO en de werkzaamheden, waaronder samenwerking met, van de METC's. Op het moment dat een indiening in CTIS heeft plaatsgevonden gaat er ene notificatie naar het NCP zodat de noodzakelijke acties als validatie en het proces om tot een beoordeling door een toetsingscommissie (CCMO of METC) uitgevoerd kunnen worden. Vertraging beperkt de tijd die resulteert in gedegen en juiste beoordeling van het onderzoek. De werkzaamheden van de CCMO zullen plaatsvinden op werkdagen terwijl de indieningen in CTIS 24/7 ingediend kunnen worden.

Integriteit	[Laag] [Midden] [Hoger dan midden]
Argumentatie van de gekozen integriteit	De keuze van Dep.V. voor de gegevens op basis van concurrentiegevoeligheid maakt het nodig om de juistheid en volledigheid extra te waarborgen. Ook de mogelijke grote commerciële/financiële waarde van voorstellen voor geneesmiddelenonderzoeken en de extra grote vertrouwelijkheid van IMPD's zijn van belang voor de keuze van midden classificatie.

Vertrouwelijkheid	[Laag] [Midden] [Hoog]
Argumentatie van de gekozen vertrouwelijkheid	De vertrouwelijkheid van de gegevens in de informatiesystemen is cruciaal voor dit proces. Als die niet gewaarborgd wordt dan leidt dit tot verlies van respect van

	onderzoekers, academische instellingen en farmaceutische bedrijven en publiek respect, en mogelijke klachten vanuit de samenleving en andere stakeholders. Ook door de commerciële/financiële belangen die spelen in dit proces maken de vertrouwelijkheid van minimaal midden noodzakelijk.
--	--

BBN-niveau	[BBN 1] [BBN 1+] [BBN 2] [BBN 2+] [BBN 3] [BBN 3+]
Toelichting gekozen BBN-niveau	Door de keuze van midden, midden & midden is het BBN-niveau overeenkomstig de toelichtingen BBN 2.

Resultaten ICV-classificatie

Proces: **Bijdragen aan de indiening & beoordeling van Geneesmiddelenonderzoeken in het kader van WMO/CTR**

Informatiesysteem: **National Collaboration Platform [NCP]**

ICV:2018 Informatiesysteemclassificatie conform TBB

TBB proces-classificatie	QS-BIO Informatiesysteem-classificatie
[n.v.t.] [4] [3] [2] [1]	[Vitaal] [Belangrijk] [Nuttig]

ICV:2018 Informatiesysteemclassificatie conform QS-BIO

Proces-classificatie	Informatiesysteem-classificatie	Beschikbaarheid	Integriteit	Vertrouwelijkheid
[Kritisch strategisch] [Strategisch] [Bijdragend] [Ondersteunend]	[Vitaal] [Belangrijk] [Nuttig]	[L] [M] [>M]	[L] [M] [>M]	[L] [M] [H]

Het informatiesysteem National Collaboration Platform [NCP] is:

[Kritiek]/ [Bedrijfskritisch]/ **[niet Kritiek en niet Bedrijfskritisch]** in relatie tot het proces en conform de definities van ICV:2018 (zie Bijlage 11).

8. Analyse Betrouwbaarheidsniveaus voor digitale dienstverlening

Het doel van de risicoanalyse eIDAS is om het betrouwbaarheidsniveau van een digitale dienst vast te stellen (zie <https://www.forumstandaardisatie.nl/thema/handreiking-betrouwbaarheidsniveaus>). De analyse van de risico's in de elektronische dienst bepaalt de gewenste betrouwbaarheid van (met name) authenticatie en dat bepaalt de sterkte van het gebruikte middel.

Vraag	
Betreft het een digitale dienst aan een burger of bedrijven?	[Ja]/[Nee]
Toelichting	Het is een intern VWS/CCMO proces gebruikmakend van de samenwerking op Europees niveau via EMA.

Indien bovenstaande vraag met Ja is beantwoord ga door met vraag 1.1.

Indien bovenstaande vraag met Nee is beantwoord is een risicoanalyse eIDAS niet nodig.

1. Persoonsgegevens

Vraag	
1.1	Wat is het risico van een persoonsgegevens-verwerking?
	Zie bijlage 12 voor een nadere toelichting.
eIDAS-betrouwbaarheids-niveau	
[Geen] [Laag] [Substantieel] [Hoog]	
Toelichting	

Vraag	
1.2	Wordt het BSN verwerkt door de digitale dienst?
	Zie bijlage 12 voor een nadere toelichting.
eIDAS-betrouwbaarheids-niveau	
[Geen] [Laag] [Substantieel] [Hoog]	
Toelichting	

2. Rechtsgevolg

Vraag	
2.1	Heeft het gebruik van de dienst rechtsgevolgen?
	Zie bijlage 12 voor een nadere toelichting.
eIDAS-betrouwbaarheids-niveau	
[Geen] [Laag] [Substantieel] [Hoog]	
Toelichting	

3. Gegevenswijzigingen basisregistraties

Vraag	
3.1	Worden er gegevens in de basisregistraties gewijzigd?
	Zie bijlage 12 voor een nadere toelichting.
eIDAS-betrouwbaarheids-niveau	
[Geen] [Laag] [Substantieel] [Hoog]	

Toelichting	
-------------	--

4. Economisch belang

Vraag		
4.1	Wat is het economisch belang van de dienst?	Zie bijlage 12 voor een nadere toelichting.
	eIDAS-betrouwbaarheids-niveau	[Geen] [Laag] [Substantieel] [Hoog]
	Toelichting	

5. Publiek belang

Vraag		
5.1	Wat is (potentieel) van toepassing betreft publicitaire onrust?	Zie bijlage 12 voor een nadere toelichting.
	eIDAS-betrouwbaarheids-niveau	[Geen] [Laag] [Substantieel] [Hoog]
	Toelichting	

Vraag		
5.2	Wat is (potentieel) van toepassing betreft maatschappelijke ontwrichting?	Zie bijlage 12 voor een nadere toelichting.
	eIDAS-betrouwbaarheids-niveau	[Geen] [Laag] [Substantieel] [Hoog]
	Toelichting	

6. Correctiefactoren

Vraag		
6.1	Zijn er risicoverhogende factoren van toepassing?	Zie bijlage 12 voor een nadere toelichting.
		[Ja] [Nee]
	Toelichting	

Vraag		
6.2	Zijn er risicoverlagende factoren van toepassing?	Zie bijlage 12 voor een nadere toelichting.
		[Ja] [Nee]
	Toelichting	

Resultaten eIDAS-analyse

Het hoogste van bovenstaande inschattingen is bepalend voor het te hanteren betrouwbaarheids-niveau (inclusief toepassing van correctiefactoren).

Vraag		
	Betreft het een digitale dienst aan een burger of bedrijven?	[Ja]/[Nee]
	eIDAS-betrouwbaarheids-niveau	[n.v.t.] [Geen] [Laag] [Substantieel] [Hoog]

Bijlage 1: TBB Categorieën (Vraag 5 TBB)

ZEER HOOG	Zeer ernstige schade voor de Staat, zeer nadelige invloed Er zijn geen alternatieven of adequate tegenmaatregelen op korte of middellange termijn beschikbaar	Van zeer ernstige schade is sprake indien kennisneming of aantasting door niet- gerechtigden kan leiden tot een dusdanig nadelig effect op de bedrijfsvoering en/of andere gewichtige belangen van de Rijksoverheid dat tenietdoen van dat effect niet of eerst na zeer grote investeringen in tijd, arbeid en kapitaal mogelijk is.
HOOG	Ernstige schade voor de Staat, nadelige invloed Er zijn beperkte alternatieven of beperkte adequate tegenmaatregelen op korte of middellange termijn beschikbaar.	Van ernstige schade is sprake indien kennisneming of aantasting door niet-gerechtigden kan leiden tot een dusdanig nadelig effect op de bedrijfsvoering en/of andere gewichtige belangen van de Rijksoverheid dat tenietdoen van dat effect slechts na grote investeringen in tijd, arbeid en kapitaal mogelijk is.
MIDDEN	Schade voor de Staat, beperkt nadelige invloed Er zijn alternatieven of adequate tegenmaatregelen op korte of middellange termijn beschikbaar	Van schade is sprake indien kennisneming of aantasting door niet-gerechtigden kan leiden tot een dusdanig nadelig effect op de bedrijfsvoering en/of andere gewichtige belangen van de Rijksoverheid dat tenietdoen van dat effect na beperkte investeringen in tijd, arbeid en kapitaal mogelijk is.
LAAG	Beperkte schade voor één departement, beperkte invloed Er zijn alternatieven of adequate tegenmaatregelen op korte of middellange termijn beschikbaar	Van beperkte schade is sprake indien kennisneming of aantasting door niet-gerechtigden kan leiden tot een beperkt nadelig effect op de bedrijfsvoering en/of andere belangen van de Rijksoverheid.

Bijlage 2: TBB Classificatie (Vraag 5 TBB)

Categorie	Belang	Schade
TBB 1 Impact: ZEER HOOG	Beschikbaarheid, integriteit: Zeer ernstige schade voor de Staat, zeer nadelige invloed Er zijn geen alternatieven of adequate tegenmaatregelen op korte of middellange termijn beschikbaar. Schade is onacceptabel. Vertrouwelijkheid: Stg. ZEER GEHEIM en (inter)nationale equivalente - Rubriceringen Bij verwerking van gerubriceerde informatie die krachtens een internationaal verdrag of een internationale overeenkomst is verkregen kunnen andere beveiligingseisen gelden dan voor het nationaal equivalent voldoende worden geacht.	Van zeer ernstige schade is sprake indien kennisname door niet-gerechtigden, aantasting, verlies kan leiden tot een dusdanig nadelig effect op het functioneren van de Rijksoverheid dat tenietdoen van dat effect niet of eerst na zeer grote investeringen in tijd, arbeid en kapitaal mogelijk is. Indien kennisname door niet-geautoriseerden zeer ernstige schade kan toebrengen aan een van de vitale belangen van de Staat en/of zijn bondgenoten.
TBB 2 Impact: HOOG	Beschikbaarheid, integriteit: Ernstige schade voor de Staat, nadelige invloed. Er zijn beperkte alternatieven of beperkte adequate tegenmaatregelen op korte of middellange termijn beschikbaar. Schade is in beginsel niet acceptabel. Vertrouwelijkheid: Stg. GEHEIM en (inter)nationale equivalente rubriceringen Bij verwerking van gerubriceerde informatie die krachtens een internationaal verdrag of een internationale overeenkomst is verkregen kunnen andere beveiligingseisen gelden dan voor het nationaal equivalent voldoende worden geacht.	Van ernstige schade is sprake indien kennisneming door niet-gerechtigden, aantasting, verlies kan leiden tot een dusdanig nadelig effect op het functioneren van de Rijksoverheid dat tenietdoen van dat effect slechts na grote investeringen in tijd, arbeid en kapitaal mogelijk is. Indien kennisname door niet-geautoriseerden ernstige schade kan toebrengen aan een van de vitale belangen van de Staat en/of zijn bondgenoten.
TBB 3 Impact:	Beschikbaarheid, integriteit: Schade voor de Staat, beperkt nadelige invloed.	Van schade is sprake indien kennisneming door niet-gerechtigden, aantasting, verlies kan leiden tot een dusdanig nadelig effect op het

MIDDEN	Er zijn alternatieven of adequate tegenmaatregelen op korte of middellange termijn beschikbaar. Schade moet zoveel mogelijk worden voorkomen. Vertrouwelijkheid: Stg. CONFIDENTIEEL en (inter)nationale equivalente rubriceringen Bij verwerking van gerubriceerde informatie die krachtens een internationaal verdrag of een internationale overeenkomst is verkregen kunnen andere beveiligingseisen gelden dan voor het nationaal equivalent voldoende worden geacht.	functioneren van de Rijksoverheid dat tenietdoen van dat effect na beperkte investeringen in tijd, arbeid en kapitaal mogelijk is. Indien kennisname door niet-geautoriseerden schade kan toebrengen aan één van de vitale belangen van de Staat en/of zijn bondgenoten.
TBB 4 Impact: LAAG	Beschikbaarheid, integriteit: Beperkte schade voor één departement, beperkte invloed. Er zijn alternatieven of adequate tegenmaatregelen op korte of middellange termijn beschikbaar. Schade is ongewenst Vertrouwelijkheid: Departementaal VERTROUWELIJK en (inter)nationale equivalente rubriceringen: Bij verwerking van gerubriceerde informatie die krachtens een internationaal verdrag of een internationale overeenkomst is verkregen kunnen andere beveiligingseisen gelden dan voor het nationaal equivalent voldoende worden geacht. Ongerubriceerd met merking: Door middel van een merking (bijv. Medisch Geheim, Personeelsvertrouwelijk, Commercieel Vertrouwelijk) kan een specifieke beperking van de kring van gerechtigden worden gegeven dan wel een specifieke behandeling van de informatie.	Van beperkte schade is sprake indien kennisneming door niet-gerechtigden, aantasting, verlies kan leiden tot een beperkt nadelig effect op het functioneren van de Rijksoverheid. Indien kennisname door niet-geautoriseerden schade kan toebrengen aan de belangen van één of meerdere ministeries.

Bijlage 3: AVG Toelichting (Vraag B1 t/m E7 AVG)

Toelichting vraag B2: Worden er persoonsgegevens verwerkt?

Persoonsgegevens zijn alle gegevens aan de hand waarvan een natuurlijk persoon kan worden geïdentificeerd.

Dit kunnen persoonsgegevens zijn van:

medewerkers, gebruikers, bezoekers, consumenten, klanten, leveranciers, patiënten, zakelijke contacten etc..

Toelichting vraag B3: Welke persoonsgegevens worden er verwerkt?

Soorten persoonsgegevens zijn o.a.:

- NAW-gegevens
- persoon identificerende nummer(s)
- gebruikersnamen/inloggegevens
- identiteitsgegevens
- financiële gegevens
- bijzondere gegevens (ras, politiek, religie, vakbond, genetisch, biometrisch, gezondheid, seksueel gedrag)
- strafrechtelijke gegevens

Toelichting vraag B4: Vallen de persoonsgegevens onder de AVG?

Uitzonderingen AVG:

- Wet inlichtingen en veiligheidsdiensten
- Kieswet
- Basisregistratie personen
- Persoonlijke (voor de werknemer) archieven (e-mail, p-schijf etc..)

Zie artikel 2 lid 2 van de AVG: <http://www.privacy-regulation.eu/nl/artikel-2-materieel-toepassingsgebied-EU-AVG.htm>

Geef per verwerking:

betrokkene – soort gegevens aan Ja/Nee.

Bij Nee geef een toelichting onder welke uitzondering ze vallen en waarom ze daar onder vallen.

Toelichting vraag B7: Zijn de grondslagen van de verwerking vastgesteld?

In de AVG staan de volgende 6 grondslagen voor het verwerken van persoonsgegevens:

1. U heeft toestemming van de persoon om wie het gaat.
2. Het is noodzakelijk om gegevens te verwerken om een overeenkomst uit te voeren.
3. Het is noodzakelijk om gegevens te verwerken omdat u dit wettelijk verplicht bent.
4. Het is noodzakelijk om gegevens te verwerken om vitale belangen te beschermen.
5. Het is noodzakelijk om gegevens te verwerken om een taak van algemeen belang of openbaar gezag uit te oefenen.

6. Het is noodzakelijk om gegevens te verwerken om uw gerechtvaardigde belang te behartigen.

Voor verdere uitleg wanneer welke grondslag gebruikt mag en kan worden: [Mag u persoonsgegevens verwerken? | Autoriteit Persoonsgegevens](#)

Zie ook: Model gegevensbeschermingseffectbeoordeling Rijksdienst (PIA)
<https://www.rijksoverheid.nl/documenten/rapporten/2017/09/29/model-gegevensbeschermingseffectbeoordeling-rijksdienst-pia> Onderdeel 11 : Rechtsgronden.

Toelichting vraag B8: Is er wet- en regelgeving en/of beleid dat gevolgen heeft voor de verwerkingen?

Naast of in de plaats van de AVG en de Richtlijn kan (sectorale) regelgeving de mogelijkheden voor gegevensverwerkingen creëren, conditioneren of beperken.

Voorbeelden van dergelijke wetten zijn:

Wet algemene bepalingen Burgerservicenummer, Wet gebruik Burgerservicenummer in de zorg, Wet basisregistratie personen, Algemene wet inzake rijksbelastingen, Archiefwet, Telecommunicatiewet, Kadasterwet, Handelsregisterwet 2007, Kieswet, Wet bijzondere maatregelen grootstedelijke problematiek, Wet op de geneeskundige behandelingsovereenkomst, Omgevingswet, Jeugdwet, Wet maatschappelijke ondersteuning 2015 en Participatiewet.

Deze lijst is niet uitputtend.

Er kan ook departementaal of rijksbreed beleid zijn dat de mogelijkheden voor de voorgenomen gegevensverwerkingen conditioneert of beperkt. Bijvoorbeeld ten aanzien van de opslag en beveiliging van persoonsgegevens.

Toelichting vraag V2: Welke belangen heeft de verwerkings-verantwoordelijke?

Bij de beoordeling van de rechtmatigheid van de gegevensverwerkingen kunnen tevens de belangen (lees: de waarde of de voordelen) die met de gegevensverwerkingen gemoeid zijn een rol spelen. Het kan hierbij zowel gaan om de private belangen van de verwerkingsverantwoordelijke, betrokkene en derden als het algemeen belang.

Het gaat hier dus niet om de (mogelijk) negatieve gevolgen voor de betrokkenen. Denk hierbij bijvoorbeeld aan: bedrijfsbelangen, financiële belangen en commerciële belangen, het handhaven van juridische vorderingen, toezicht op medewerkers ten behoeve van de veiligheid of managementdoeleinden, (nationale of openbare) veiligheid, zoals de preventie van fraude, misbruik en netwerkbeveiliging, en gezondheid.

Het belang dat gemoeid is met de gegevensverwerkingen werkt door in de toets van de noodzaak

Toelichting vraag V9: Is een GEB noodzakelijk?

Geef in de toelichting aan waarom GEB van toepassing is.

Criteria Europese toezichthouder

<https://www.autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia#wat-zijn-de-criteria-van-de-europese-privacytoezichthouders-6668>

De Europese privacytoezichthouders hebben 9 criteria opgesteld om te beoordelen of uw voorgenomen verwerking van persoonsgegevens een hoog privacyrisico oplevert voor de betrokken personen. Als vuistregel kunt u hanteren dat u een DPIA moet uitvoeren als uw verwerking aan 2 of meer van de onderstaande 9 criteria voldoet.

1. Beoordelen van mensen op basis van persoonskenmerken

Het gaat hierbij onder meer om profiling en het maken van prognoses, met name op basis van kenmerken als iemands beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren of interesses, betrouwbaarheid of gedrag, locatie of verplaatsingen.

Voorbeelden hiervan zijn een bank die de kredietwaardigheid van klanten bepaalt (creditscoring), een bedrijf dat DNA-testen aan consumenten levert om gezondheidsrisico's te testen en een bedrijf dat bezoekers van zijn website volgt en op basis daarvan profielen van deze mensen opstelt.

2. Geautomatiseerde beslissingen

Het gaat hierbij om beslissingen die voor de betrokkene rechtsgevolgen of vergelijkbare wezenlijke gevolgen hebben. Zo'n gegevensverwerking kan er bijvoorbeeld toe leiden dat mensen worden uitgesloten of gediscrimineerd. Gegevensverwerkingen met geringe of geen gevolgen voor mensen vallen niet onder dit criterium.

Voor meer informatie, zie de guidelines over geautomatiseerde besluitvorming en profilering van de Europese privacytoezichthouders.

3. Stelselmatige en grootschalige monitoring

Het gaat hierbij om monitoring van openbaar toegankelijke ruimten, bijvoorbeeld met cameratoezicht. Hierbij kunnen persoonsgegevens worden verzameld zonder dat betrokkenen weten wie hun gegevens verzamelt en wat daar vervolgens mee gebeurt. Bovendien kan het onmogelijk zijn voor mensen om zich in openbare ruimten aan deze gegevensverwerking te onttrekken.

4. Gevoelige gegevens

Het gaat hierbij om bijzondere categorieën van persoonsgegevens (zie artikel 9 van de AVG), zoals informatie over iemands politieke voorkeuren. Ook strafrechtelijke gegevens vallen hieronder. Tot slot gaat het hier ook om gegevens die over het algemeen als privacygevoelig worden beschouwd, zoals gegevens over elektronische communicatie, locatiegegevens en financiële gegevens.

Artikel 9 lid 1: 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 zijn verboden.

5. Grootschalige gegevensverwerkingen

De AVG geeft geen definitie van 'grootschalige gegevensverwerkingen'. De Europese privacytoezichthouders adviseren om met de volgende criteria te bepalen of hiervan sprake is:

- de hoeveelheid mensen van wie gegevens worden verwerkt;
- de hoeveelheid gegevens en/of de verscheidenheid aan gegevens die worden verwerkt;
- de tijdsduur van de gegevensverwerking;
- de geografische reikwijdte van de gegevensverwerking.

Zie ook: wat ziet de AVG als een grootschalige verwerking van persoonsgegevens?

6. Gekoppelde databases

Het gaat hierbij om gegevensverzamelingen die aan elkaar gekoppeld of met elkaar gecombineerd zijn. Bijvoorbeeld databases die voortkomen uit twee of meer verschillende gegevensverwerkingen met verschillende doelen en/of uitgevoerd door verschillende verantwoordelijken, op een manier die betrokkenen niet redelijkerwijs kunnen verwachten.

7. Gegevens over kwetsbare personen

Bij het verwerken van dit type gegevens kan een DPIA nodig zijn omdat er sprake is van een ongelijke machtsverhouding tussen de betrokkene en de verantwoordelijke. Dit heeft als gevolg dat betrokkenen niet in vrijheid toestemming kunnen geven of weigeren voor het verwerken van hun gegevens. Het kan hierbij om bijvoorbeeld werknemers, kinderen en patiënten gaan.

8. Gebruik van nieuwe technologieën

De AVG is er duidelijk over dat een DPIA nodig kan zijn bij het gebruik van een nieuwe technologie. De reden hiervoor is dat dit gebruik gepaard kan gaan met nieuwe manieren om gegevens te verzamelen en gebruiken, met mogelijk grote privacyrisico's.

De persoonlijke en maatschappelijke gevolgen van het gebruik van een nieuwe technologie kunnen zelfs nog onbekend zijn. Een DPIA helpt de verantwoordelijke dan om de risico's te begrijpen en te verhelpen.

Sommige 'Internet of Things'-toepassingen bijvoorbeeld kunnen een grote impact hebben op het dagelijks leven en de privacy van mensen, waardoor hierbij een DPIA nodig is.

9. Blokkering van een recht, dienst of contract

Het gaat hierbij om gegevensverwerkingen die tot gevolg hebben dat betrokkenen:

- een recht niet kunnen uitoefenen of;
- een dienst niet kunnen gebruiken of;
- een contract niet kunnen afsluiten.

Bijvoorbeeld een bank die persoonsgegevens verwerkt om te bepalen of zij een lening aan iemand willen verstrekken.

Verantwoordingsplicht

Let op: deze 9 criteria zijn een handreiking om in te schatten of u een DPIA moet uitvoeren. Ook als u aan slechts één of geen van deze criteria voldoet, moet u goed kunnen onderbouwen waarom u ervoor kiest om geen DPIA uit te voeren. Dit maakt onderdeel uit van de verantwoordingsplicht.

Criteria Autoriteit persoonsgegevens

<https://www.autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia#voor-welke-soorten-verwerkingen-is-het-uitvoeren-van-een-dpia-verplicht-6667>

AP-lijst van verwerkingen waarvoor een DPIA verplicht is:

1. Heimelijk onderzoek

Grootschalige verwerkingen en/of stelselmatige monitoring van persoonsgegevens waarbij informatie wordt verzameld met onderzoek, zonder de betrokkene daarvan vooraf op de hoogte te stellen.

Bijvoorbeeld heimelijk onderzoek door particuliere recherchebureaus, onderzoek voor fraudebestrijding en onderzoek op internet voor bijvoorbeeld online handhaving van auteursrechten. Een DPIA is ook verplicht bij heimelijk cameratoezicht door werkgevers om diefstal of fraude door werknemers te bestrijden. Hierbij moet soms ook een DPIA worden uitgevoerd vanwege de ongelijkwaardige machtsverhouding tussen werknemer en werkgever.

2. Zwarte lijsten

Verwerkingen waarbij persoonsgegevens over strafrechtelijke veroordelingen en strafbare feiten, gegevens over onrechtmatig of hinderlijk gedrag of gegevens over slecht betalingsgedrag door organisaties of particulieren worden verwerkt en gedeeld met derden.

Bijvoorbeeld zwarte lijsten of waarschuwingslijsten, zoals verzekeraars, horecabedrijven, winkelbedrijven en telecomproviders die gebruiken. En ook zwarte lijsten die gaan over onrechtmatig gedrag van werknemers, bijvoorbeeld in de zorg of door uitzendbureaus.

3. Fraudebestrijding

Grootschalige verwerkingen en/of stelselmatige monitoring van (bijzondere) persoonsgegevens voor fraudebestrijding. Bijvoorbeeld fraudebestrijding door sociale diensten of door fraudeafdelingen van verzekeraars.

4. Creditscores

Grootschalige verwerkingen en/of stelselmatige monitoring van persoonsgegevens die leiden tot of gebruik maken van inschattingen van de kredietwaardigheid van natuurlijke personen, bijvoorbeeld tot uitdrukking gebracht in een creditscore.

5. Financiële situatie

Grootschalige verwerkingen en/of stelselmatige monitoring van financiële gegevens waaruit de inkomens- of vermogenspositie of het bestedingspatroon van mensen valt af te leiden. Bijvoorbeeld overzichten van bankoverschrijvingen, overzichten van de saldi van iemands bankrekeningen of overzichten van mobiele- of pinbetalingen.

6. Genetische persoonsgegevens

Grootschalige verwerkingen en/of stelselmatige monitoring van genetische persoonsgegevens. Bijvoorbeeld DNA-analyses om persoonlijke kenmerken in kaart te brengen, bio-databanken.

7. Gezondheidsgegevens

Grootschalige verwerkingen van gegevens over gezondheid (bijvoorbeeld door instellingen of voorzieningen voor gezondheidszorg of maatschappelijke dienstverlening, arbodiensten, reïntegratiebedrijven, (speciaal)onderwijsinstellingen, verzekeraars en onderzoeksinstituten), waaronder ook grootschalige elektronische uitwisseling van gegevens over gezondheid. Let op: individuele artsen en individuele zorgprofessionals zijn op grond van overweging 91 van de AVG uitgezonderd van de verplichting een DPIA uit te voeren.

8. Samenwerkingsverbanden

Het delen van persoonsgegevens in of door samenwerkingsverbanden waarin gemeenten of andere overheden met andere publieke of private partijen bijzondere persoonsgegevens of persoonsgegevens van gevoelige aard met elkaar uitwisselen, zoals gegevens over gezondheid, verslaving, armoede, problematische schulden, werkloosheid, sociale problematiek, strafrechtelijke gegevens, betrokkenheid van jeugdzorg of maatschappelijk werk. Bijvoorbeeld in wijkteams, veiligheidshuizen of informatieknooppunten.

9. Cameratoezicht

Grootschalige verwerkingen en/of stelselmatige monitoring van openbaar toegankelijke ruimten met camera's, webcams of drones.

10. Flexibel cameratoezicht

Grootschalig en/of systematisch gebruik van flexibel cameratoezicht. Bijvoorbeeld camera's op kleding of helm van brandweer- of ambulancepersoneel, dashcams gebruikt door hulpdiensten.

11. Controle werknemers

Grootschalige verwerkingen en/of stelselmatige monitoring van persoonsgegevens om activiteiten van werknemers te monitoren. Bijvoorbeeld controle van e-mail en internetgebruik, GPS-systemen in (vracht)auto's van werknemers of cameratoezicht voor diefstal- en fraudebestrijding.

12. Locatiegegevens

Grootschalige verwerkingen en/of stelselmatige monitoring van locatiegegevens van of herleidbaar tot natuurlijke personen. Bijvoorbeeld door (scan)auto's, navigatiesystemen, telefoons, of verwerking van locatiegegevens van reizigers in het openbaar vervoer.

13. Communicatiegegevens

Grootschalige verwerkingen en/of stelselmatige monitoring van communicatiegegevens inclusief metadata herleidbaar tot natuurlijke personen, tenzij en voor zover dit noodzakelijk is ter bescherming van de integriteit en de veiligheid van het netwerk en de dienst van de betrokken aanbieder of het randapparaat van de eindgebruiker.

14. Internet of things

Grootschalige verwerkingen en/of stelselmatige monitoring van persoonsgegevens die worden gegenereerd door apparaten die verbonden zijn met internet en die via internet of anderszins gegevens kunnen versturen of uitwisselen. Bijvoorbeeld 'internet of things'- toepassingen, zoals slimme televisies, slimme huishoudelijke apparaten, connected toys, smart cities, slimme energiemeters, medische hulpmiddelen, etc..

15. Profilerings

Systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen gebaseerd op geautomatiseerde verwerking (profilering). Bijvoorbeeld beoordeling van beroepsprestaties, prestaties van leerlingen, economische situatie, gezondheid, persoonlijke voorkeuren of interesses, betrouwbaarheid of gedrag.

16. Observatie en beïnvloeding van gedrag

Grootschalige verwerkingen van persoonsgegevens waarbij op systematische wijze via geautomatiseerde verwerking gedrag van natuurlijke personen wordt geobserveerd of beïnvloed, dan wel gegevens die daarover worden verzameld en/of vastgelegd, inclusief gegevens die voor het doel online behavioural advertising worden verzameld.

17. Biometrische gegevens

Grootschalige verwerkingen en/of stelselmatige monitoring van biometrische gegevens met als doel een natuurlijk persoon te identificeren.

Toelichting vraag R1: Is er een informatieplicht naar betrokkene van toepassing?

AVG Artikel 14.5 b-d geeft de uitzonderingen m.b.t. de informatieplicht aan:

- a) de betrokkene reeds over de informatie beschikt;
- b) het verstrekken van die informatie onmogelijk blijkt of onevenredig veel inspanning zou vergen, in het bijzonder bij verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden;
- c) het verkrijgen of verstrekken van de gegevens uitdrukkelijk is voorgeschreven bij Unie- of lidstatelijk recht dat op de verwerkingsverantwoordelijke van toepassing is en dat recht voorziet in passende maatregelen om de gerechtvaardigde belangen van de betrokkene te beschermen;
- d) de persoonsgegevens vertrouwelijk moeten blijven uit hoofde van een beroepsgeheim in het kader van Unierecht of lidstatelijk recht, waaronder een statutaire geheimhoudingsplicht.

<http://www.privacy-regulation.eu/nl/artikel-14-te-verstrekken-informatie-wanneer-de-persoonsgegevens-niet-van-de-betrokkene-zijn-verkregen-EU-AVG.htm>

Toelichting vraag E6: Bevatten de persoonsgegevens bijzondere persoonsgegevens?

Geef aan welke van de onderstaande bijzondere gegevens onderdeel zijn van de verwerking.

- Persoonsgegevens waaruit ras of etnische afkomst blijkt
- Persoonsgegevens waaruit politieke opvattingen blijken
- Persoonsgegevens waaruit religieuze of levensbeschouwelijke overtuigingen blijken
- Persoonsgegevens waaruit het lidmaatschap van een vakbond blijkt
- Genetische gegevens
- Biometrische gegevens met het oog op de unieke identificatie van een persoon
- Gegevens over gezondheid
- Gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid
- Gegevens betreffende strafrechtelijke veroordelingen en strafbare feiten

Toelichting vraag E7: Is de gegevensverwerking de meest privacy vriendelijke verwerking?

De privacyregelgeving geef als beginsel dat de gegevensverwerking wordt beperkt tot wat noodzakelijk is voor de verwerkingsdoeleinden. Dit beginsel van minimale gegevensverwerking/ dataminimalisatie komt verder tot uitdrukking door het gebruik van het woord 'noodzakelijk' in artikel 6 AVG en artikel 8 Richtlijn.

De AVG en Richtlijn eisen hiermee dat de gegevensverwerking noodzakelijk is voor het verwezenlijken van de doeleinden. De gegevensverwerking moet daarbij voorts de toets aan de beginselen van proportionaliteit en subsidiariteit kunnen doorstaan.

Proportionaliteit betekent dat moet worden beoordeeld of de indringendheid van de voorgenomen

gegevensverwerking in een redelijke verhouding staat tot het doel. Bij proportionaliteit wordt gewogen of de realisatie van de verwerkingsdoeleinden zodanig gewicht heeft dat de gegevensverwerkingen, gelet op de mate waarin deze de privacy beperken, deze rechtvaardigen (zijn de beperkingen van het grondrecht en het doel dat met de verwerking wordt beoogd met elkaar in balans?). Daarbij zal onder meer moeten worden gekeken of de voorgenomen gegevensverwerking effectief is om het beoogde doel te bereiken en of de aangevoerde redenen relevant en toereikend zijn om het beoogde doel te bereiken.

Daarbij kunnen empirische onderzoeksresultaten helpen.

Bij subsidiariteit wordt bekeken of de verwerkingsdoeleinden met minder ingrijpende middelen kunnen worden bereikt. Bijvoorbeeld:

- kan bij het gebruik van bijzondere of strafrechtelijke persoonsgegevens hetzelfde resultaat behaald worden met gebruikmaking van een combinatie van gewone persoonsgegevens?
- kan het verwerken van de persoonsgegevens in een beperktere vorm of met minder verwerkingen?

Zo kan in bepaalde gevallen met foto's hetzelfde doel worden bereikt (bijvoorbeeld: identificatie) als met het verwerken van filmbeelden. Het subsidiariteitsbeginsel houdt bijvoorbeeld ook in dat als persoonsgegevens openbaar gemaakt gaan worden, niet automatisch alle persoonsgegevens openbaar worden gemaakt, maar een selectie wordt gemaakt op grond van gerechtvaardigde criteria.

Bijlage 4: AVG Logische gegevensverwerkingsgroepen (Vraag B4 AVG)

Bepaal per betrokkene en gegevenscombinatie een logische gegevensverwerkingsgroep (LGVG).
Aan een logische gegevensverwerkingsgroep wordt een unieke codering toegekend.

Bijvoorbeeld:

- **Betrokkene:** Medewerkers,
- **Soortgegevens:** naam, adres, privé e-mail, gebruikersnaam
- **Gegevensverwerkingsgroep:** MDW01

- **Betrokkene:** Leveranciers
- **Soortgegevens:** naam contactpersoon, adres, werk e-mail, werktelefoonnummer
- **Gegevensverwerkingsgroep:** LEV01

Vervolgens verwijst de code MDW01 naar de soort gegevens van de betrokkene.

Gegevens-verwerkingsgroep	Betrokkene	Soort gegevens
MDW01	Medewerkers	naam, adres en privé e-mail, gebruikersnamen
LEV01	Leveranciers	naam contactpersoon, adres, werk e-mail, werk telefoonnummer

Bijlage 5: BIO Proces-classificatie (Vraag 1 BIO)

Voor het realiseren van de doelstellingen van de organisatie moeten de bedrijfsprocessen goed functioneren. Ieder proces wordt geclassificeerd naar de mate van belang. In onderstaande tabel worden de classificaties weergegeven.

Classificatie: Kritisch strategisch

Taak: Kerntaak

In relatie tot de doelstellingen van het ministerie /kerndepartement of uitvoeringsorganisatie speelt het bedrijfsproces een primaire rol. Het hoort bij de primaire taken waarop het ministerie/kerndepartement of uitvoeringsorganisatie direct kan worden aangesproken. Het ministerie/kerndepartement of uitvoeringsorganisatie ontleent haar bestaansrecht aan het uitvoeren van deze taken.

- Het betreft een maatschappelijk vitaal proces. Deze vitale belangen zijn als volgt gedefinieerd:
 - a. territoriale veiligheid: het ongestoord functioneren van Nederland als onafhankelijke staat, en in het bijzonder de territoriale integriteit van het grondgebied en de internationale positie;
 - b. fysieke veiligheid: het ongestoord functioneren van de mens in Nederland en zijn omgeving;
 - c. economische veiligheid: het ongestoord functioneren van Nederland als een effectieve en efficiënte economie;
 - d. ecologische veiligheid: het beschikken over voldoende zelf herstellend vermogen van de leefomgeving bij aantasting;
 - e. sociale en politieke stabiliteit: het ongestoorde voortbestaan van een maatschappelijk klimaat waarin groepen mensen goed met elkaar kunnen samenleven binnen de kaders van de democratische rechtstaat en gedeelde kernwaarden.
- De instelling krijgt 80% of meer van de inkomsten uit dit proces, c.q. het budget van de organisatie wordt voor meer dan 80% uitgeput door dit proces.
- Als de activiteit langer dan één week stilvalt of niet goed verloopt, heeft dit ernstige gevolgen voor het voortbestaan van de organisatie, c.q. het brengt het ministerie/kerndepartement of uitvoeringsorganisatie in een hachelijke positie.

Classificatie: Strategisch

Taak: Afgeleide kerntaak

Het proces heeft een directe relatie naar het uitvoeren van de doelstellingen van het ministerie/kerndepartement of uitvoeringsorganisatie. Het is het primaire proces van de directie, agentschap, raad, etc..

- Aan het proces kan een ontwikkelpotentieel worden toegekend. Met andere woorden, het wordt in de toekomst belangrijker in verband met mogelijke veranderingen in de strategische doelstellingen van het ministerie/kerndepartement of uitvoeringsorganisatie.
- Een aanzienlijk deel van de omzet (50% - 80%) wordt gegenereerd met dit proces of een aanzienlijk deel (50% - 80%) van het te besteden budget komt ten goede aan dit proces.
- Het proces heeft te maken met de uitvoering van wettelijke taken (het betreft hier primaire processen met wettelijk/ contractueel vastgelegde termijnen).

Classificatie: Bijdragend

Taak: Subtaak

Er is slechts sprake van een indirecte relatie met de hoofdactiviteiten van het ministerie/kerndepartement of uitvoeringsorganisatie. Het ontbreken van het "bijdragende proces" heeft echter wel effectiviteits- en efficiencyverliezen binnen het primaire proces tot gevolg.

Classificatie: Ondersteunend

Taak: Voorwaardenscheppend

De activiteiten waaraan de typering “handig om te hebben” kan worden toegekend.

Deze activiteiten hebben geen directe relatie naar het voortbrengen van de producten/diensten waaraan de instelling haar bestaansrecht ontleent. In de meeste gevallen is hier sprake van een ondersteunende rol naar de lijn. De activiteiten vormen een waardevol support van het primaire proces.

Bijlage 6: BIO Informatiesysteem-classificatie (Vraag 1 BIO)

Om het proces goed te kunnen laten functioneren wordt gebruik gemaakt van een aantal ondersteunende informatiesystemen. In onderstaande tabel is een overzicht gegeven van mogelijke classificaties van het informatiesysteem. De classificaties geven een waarde aan die men hecht aan het informatiesysteem ter ondersteuning van het proces.

Typering	Waardering
Vitaal (V)	• Het uitvoeren van de bedrijfsprocessen of het tot stand brengen van producten/diensten is (nagenoeg) onmogelijk zonder de inzet van het informatiesysteem. • Inzet van het informatiesysteem is essentieel voor een goede uitvoering van het bedrijfsproces.
Belangrijk (B)	• Het informatiesysteem levert een belangrijke bijdrage aan de activiteiten binnen het proces en/of de levering van producten/diensten. • Slechts met grote, onevenredige inspanning is voortzetting van het proces mogelijk. • Inzet van het informatiesysteem heeft een positief effect op de doeltreffendheid en doelmatigheid van de organisatie. • Het informatiesysteem wordt door veel (interne/ externe) medewerkers / burgers gebruikt.
Nuttig (N)	• Het informatiesysteem geeft support bij de activiteiten binnen het bedrijfsproces en is 'handig om te hebben'.

Bijlage 7: BIO Beschikbaarheid-classificatie (Vraag 2 BIO)

Beschikbaarheid betreft het waarborgen, dat vanuit hun functie geautoriseerde gebruikers op de juiste momenten tijdig toegang hebben tot informatie en aanverwante bedrijfsmiddelen (informatiesystemen) (uit: Voorschrift Informatiebeveiliging Rijksdienst 2007).

Laag	Het informatiesysteem mag incidenteel uitvallen voor maximaal twee weken (ook in piekperiodes) en heeft nauwelijks of geen gevolgen voor burgers/gebruikers. Uitval kan leiden tot beperkte schade, bijvoorbeeld: - financiële gevolgen; op te vangen binnen de vastgestelde ruimte binnen de - begroting van het ministerie of uitvoeringsorganisatie; leidt nog niet uit het niet - krijgen van een accountants verklaring; of - beperkt verlies van management control; of - irritatie en ongemak bij burgers geventileerd in de media; of - interne negatieve publiciteit (imagoschade). Deze gevolgen worden als volgt gekwantificeerd: - Kantoorautomatisering en dienstspecifieke systemen hebben tijdens openingstijden - een beschikbaarheid van minimaal 98% op maandbasis ook in piekperiodes; - maximaal dataverlies 28 uur; - maximale hersteltijd in geval van incidenten is binnen 40 werkuren (5 werkdagen van 8 uur) in 85% van de gevallen.
Midden	Het informatiesysteem mag beperkt korte tijd uitvallen voor maximaal één week (ook in piekperiodes) en heeft voelbare gevolgen voor burgers/gebruikers. Uitval kan leiden tot beperkte schade, bijvoorbeeld: - politieke schade aan een bewindspersoon: bewindspersoon moet voor - verantwoording naar de Tweede Kamer, bijvoorbeeld n.a.v. Kamervragen; of - diplomatieke schade te herstellen door ambtelijke opschaling; of - financiële gevolgen: niet meer op te vangen binnen de vastgestelde ruimte binnen - de begroting van het ministerie of uitvoeringsorganisatie; geen - accountantsverklaring afgegeven; of - belangrijk verlies van management control; of - verlies van publiek respect; klachten van burgers; of - Rijksbrede negatieve publiciteit (imagoschade) of significant verlies van motivatie van medewerkers. De beschikbaarheid wordt als volgt gekwantificeerd: - Kantoorautomatisering en dienstspecifieke systemen hebben tijdens openingstijden - een beschikbaarheid van minimaal 98% op maandbasis ook in piekperiodes; - maximaal dataverlies 24 uur; - maximale hersteltijd in geval van incidenten is binnen 16 werkuren (2 dagen van 8 uur).
Hoger dan midden	Ernstigere schade dan het bij "Midden" beschreven schadescenario. De beschikbaarheids eis overstijgt het standaard niveau dat een dienstenleverancier op dit moment kan leveren. In overleg met een dienstenleverancier moeten specifiek voor de situatie benodigde maatregelen worden afgesproken.

Bijlage 8: BIO Integriteit-classificatie (Vraag 2 BIO)

Integriteit betreft het waarborgen van de juistheid en volledigheid van informatie en de verwerking ervan. De juistheid en volledigheid van de informatie is een directe verantwoordelijkheid van de eigenaar van het systeem en de hem ondersteunende managers en medewerkers (uit: Voorschrift Informatiebeveiliging Rijksdienst 2007).

Laag	Er zijn geen bijzondere maatregelen noodzakelijk om de juistheid, tijdigheid en volledigheid (VIR definitie) te waarborgen. Het verlies van integriteit kan leiden tot beperkte schade, bijvoorbeeld: - financiële gevolgen; op te vangen binnen de vastgestelde ruimte binnen de begroting van het ministerie of uitvoeringsorganisatie; leidt nog niet uit het niet krijgen van een accountants verklaring; of - beperkt verlies van management control; of - irritatie en ongemak bij burgers geventileerd in de media; of - interne negatieve publiciteit (imagoschade).
Midden	Er zijn passende maatregelen noodzakelijk om de juistheid, tijdigheid en volledigheid (VIR definitie) te waarborgen. Het verlies van integriteit kan leiden tot forse schade, bijvoorbeeld: - politieke schade aan een bewindspersoon: bewindspersoon moet voorverantwoording naar de Tweede Kamer, bijvoorbeeld n.a.v. Kamervragen; of - diplomatieke schade te herstellen door ambtelijke opschaling; of - financiële gevolgen: niet meer op te vangen binnen de vastgestelde ruimte binnen de begroting van het ministerie of uitvoeringsorganisatie; geen accountants-verklaring afgegeven; of - belangrijk verlies van management control; of - verlies van publiek respect; klachten van burgers; of - Rijksbrede negatieve publiciteit (imagoschade) of significant verlies van motivatie van medewerkers.
Hoger dan midden	Ernstigere schade dan het bij "Midden" beschreven schadescenario. De integriteitseis overstijgt het standaard niveau dat een dienstenleverancier op dit moment kan leveren. In overleg met een dienstenleverancier moeten specifiek voor de situatie benodigde maatregelen worden afgesproken.

Bijlage 9: BIO Vertrouwelijkheid-classificatie (Vraag 2 BIO)

Vertrouwelijkheid betreft het waarborgen dat informatie alleen toegankelijk is voor degenen, die hiertoe zijn geautoriseerd. Het gaat hier onder andere om het beveiligen van de toegang tot de gebouwen, de informatiesystemen en de ICT-infrastructuur tegen onbevoegden (hackers en andere indringers) en malafide software (virussen, trojan horses). En het gaat ook om maatregelen om te voorkomen dat de eigen medewerkers toegang krijgen tot informatie die niet voor hen is bedoeld (uit: Voorschrift Informatiebeveiliging Rijksdienst 2007).

Laag	Kennisname van informatie door ongeautoriseerden (buitenstaanders) is niet gewenst, maar leidt niet tot schade van enige omvang. Het gaat hier om ongerubriceerde informatie. Het openbaar worden van deze informatie kan leiden tot: - financiële gevolgen: op te vangen binnen de begroting van het ministerie of uitvoeringsorganisatie; of - irritatie en ongemak bij burgers geventileerd in de media; of - interne negatieve publiciteit (imagoschade).
Midden	Bescherming van gegevens en andere te beschermen belangen in de processen van de Rijksdienst, waar o.a. vertrouwelijkheid aan de orde is, omdat het om gevoelige informatie gaat. Het openbaar worden van de gegevens, kan leiden tot: - politieke schade aan een bewindspersoon: bewindspersoon moet voor verantwoording naar de Tweede Kamer, bijvoorbeeld n.a.v. Kamervragen; of - diplomatieke schade te herstellen door ambtelijke opschaling; of - financiële gevolgen: niet meer op te vangen binnen de begroting van het ministerie of uitvoeringsorganisatie; geen accountantsverklaring afgegeven; of - verlies van publiek respect; klachten van burgers of significant verlies van motivatie van medewerkers; of - bindende aanwijzing van de AP in verband met schending van de privacy; of - directe imagoschade, bijvoorbeeld door negatieve publiciteit.
Hoog	- Verlies van informatie heeft een grote impact, waarvan niet uit te leggen is als deze niet gerubriceerd is en beschermd wordt op het niveau van BBN3; - informatie wordt door derden geleverd met een rubricering (niet zijnde BBN2); of - aansluiting op een infrastructuur vereist (bijvoorbeeld om al op de infrastructuur aanwezige gerubriceerde informatie niet in gevaar te brengen) BBN3 om informatie te kunnen verwerken op deze infrastructuur; of - weerstand tegen statelijke actoren is noodzakelijk.

Bijlage 10: BIO Basisbeschermingsniveau (BBN) (Vraag 10 BIO)

Om risicomanagement hanteerbaar en efficiënt te houden, kiest de BIO voor een diepgang van de uitwerking van het risicomanagement die proportioneel is aan de te beschermen belangen in combinatie met relevante dreigingen. Daarom onderscheidt de BIO drie basisbeveiligingsniveaus (BBN). Voor BBN1 ligt de nadruk op 'wat mag minimaal verwacht worden?'. Voor BBN2 ligt de nadruk op de bescherming van de meest voorkomende categorieën informatie volgens het principe 'valt de maatregel onder goed huisvaderschap; toont deze beveiliging de betrouwbare overheid?'. BBN3 is van toepassing op gerubriceerde informatie (Departementaal Vertrouwelijk of vergelijkbaar) waarbij weerstand tegen statelijke actoren of vergelijkbare dreigingen nodig is.

Bepalen BBN-niveau van het beschouwde informatiesysteem

Het BBN-niveau is standaard: **BBN2**

Stap 1: Bepaal Informatiesysteem gegevens-classificatie

Bepaal de Informatiesysteem gegevens-classificatie aan de hand van geanalyseerde TBB-gegevens-classificatie.

Informatiesysteem gegevens-classificatie:	[Geen bijzondere informatie]
	[Departementaal VERTROUWELIJK (Dep.V.)]
	[Staatsgeheim CONFIDENTIEEL (Stg.C)]
	[Staatsgeheim GEHEIM (Stg.G)]
	[Staatsgeheim ZEER GEHEIM (Stg.ZG)]

Indien Informatiesysteem gegevens-classificatie hoger is dan Dep.V. dan is het BBN-niveau: **BBN3+**

Als BBN-niveau 'BBN3+' is ga door met stap 5

Stap 2: Bepaal dreigingsprofiel

Weerstand zwaarder dan voor Statelijke actoren/Criminele organisaties nodig: [Ja]/[Nee]

Indien Ja en gegevens-classificatie is Dep.V. dan is het BBN-niveau: **BBN3+**

Weerstand tegen Statelijke actoren/Criminele organisaties nodig: [Ja]/[Nee]

Indien Ja en gegevens-classificatie is Dep.V. dan is het BBN-niveau: **BBN3**

Als BBN-niveau 'BBN3+' of 'BBN3' is ga door met stap 5.

Stap 3: Is BBN2 voldoende?

Meestal is BBN2 van toepassing op een specifiek informatiesysteem. Het kan echter zijn dat BBN2 niet voldoende is.

- A - Wordt de informatie geleverd door derden en vereist deze derden voor de beveiliging van de betreffende gegevens BBN3: [Ja]/[Nee]
- B - Is BBN3 vereist om informatie te kunnen verwerken op de infrastructuur (bijvoorbeeld om al op de infrastructuur aanwezige gerubriceerde informatie niet in gevaar te brengen): [Ja]/[Nee]

Indien één of meer van de vragen met Ja is beantwoord dan is het BBN-niveau: **BBN3**

Indien BBN-niveau 'BBN3' is ga door met stap 5.

Stap 4: Is BBN2 te zwaar?

Kan het ongewenst of onbedoeld openbaren van informatie leiden tot:

- A - politieke schade aan een bewindspersoon: bewindspersoon moet voor verantwoording naar de Tweede Kamer, bijvoorbeeld n.a.v. Kamervragen: [Ja]/[Nee]
- B - diplomatieke schade te herstellen door ambtelijke opschaling: [Ja]/[Nee]
- C - financiële gevolgen: niet meer op te vangen binnen de begroting van het ministerie of uitvoeringsorganisatie; geen accountantsverklaring afgegeven: [Ja]/[Nee]
- D - verlies van publiek respect; klachten van burgers of significant verlies van motivatie van medewerkers: [Ja]/[Nee]
- E - bindende aanwijzing van de AP in verband met schending van de privacy: [Ja]/[Nee]
- F - directe imagoschade, bijvoorbeeld door negatieve publiciteit: [Ja]/[Nee]

Indien alles met Nee is beantwoord is het BBN-niveau: **BBN1.**

Indien één of meer vragen met Ja is beantwoord is het BBN-niveau: **BBN2.**

Stap 5: Bepaal passendheid gekozen BBN-niveau?

- A - bepaal beschikbaarheid-classificatie van het informatiesysteem: [Laag]
[Midden]
[Hoger dan midden]
- B - bepaal integriteit-classificatie van het informatiesysteem: [Laag]
[Midden]
[Hoger dan midden]
- C - bepaal vertrouwelijkheid-classificatie van het informatiesysteem: [Laag]
[Midden]
[Hoog]

De basisbeveiligingsniveaus zijn uitgewerkt langs de lijnen beschikbaarheid, integriteit en vertrouwelijkheid. De BBN-toets helpt bij het kiezen van het best passende niveau. De beschikbaarheidsniveaus zijn gebaseerd op de geldende beschikbaarheidsniveaus die door de grote interne dienstenleveranciers worden gehanteerd. De vertrouwelijkheidsniveaus zijn in lijn gebracht met de schadescenario's die gelden voor de Te Beschermen Belangen.

De onderverdeling is als volgt:

	Beschikbaarheid	Integriteit	Vertrouwelijkheid
BBN1	Laag	Laag	Laag
BBN1+	>Laag	Laag	Laag
BBN1+	Laag	>laag	Laag
BBN2	Laag	Laag	Midden
BBN2	Midden	Midden	Midden
BBN2+	>Midden	Midden	Midden
BBN2+	Midden	>Midden	Midden
BBN2+	>Midden	>Midden	Midden
BBN2+	Laag/Midden/Hoog	Laag/Midden/Hoog	Hoog m.b.t. Persoonsvertrouwelijk
BBN3	Laag/Midden	Laag/Midden	Hoog
BBN3+	>Midden	Midden	Hoog
BBN3+	Midden	>Midden	Hoog
BBN3+	>Midden	>Midden	Hoog

Indien het BBN-niveau dat in stap 1-4 is vastgesteld lager is dan bovenstaande onderverdeling neem dan het BBN-niveau uit de bovenstaande onderverdeling.

Conclusie: BBN niveau is: [BBN1]/[BBN1+]/ [BBN2]/[BBN2+]/[BBN3]/ [BBN3+]

Bijlage 11: ICV Toelichting

Kritiek systeem

Een informatiesysteem is kritiek als bij falen de uitvoering van een kerntaak niet langer kan worden gegarandeerd of een te beschermen belang van de organisatie niet langer kan worden beschermd.

Om een systeem als kritiek systeem aan te merken kunnen twee veelgebruikte methodieken binnen de Rijksdienst worden gebruikt. Dit zijn de Quickscan BIO of de Leidraad Te Beschermen Belangen:

Kritiek systeem conform 'Quickscan BIO':

- het proces wordt aangemerkt als kritisch strategisch (kerntaak) *en*
- het informatiesysteem is vitaal voor dit proces *en*
- één of meer betrouwbaarheidseisen (B, I, V) scoren zeer hoog.

Kritiek systeem conform 'Leidraad Te Beschermen Belangen':

- het proces valt in TBB categorie 1 *en*
- het informatiesysteem is vitaal voor dit proces.

Een Ministerie kan besluiten om ook verantwoording af te leggen over de bedrijfskritische systemen of anderszins een ruimere scope te kiezen, zoals aangegeven bij de reikwijdte.

Bedrijfskritisch systeem

Om een systeem als bedrijfskritisch aan te merken kunnen twee veelgebruikte methodieken binnen de Rijksdienst worden gebruikt. Dit zijn de Quickscan BIO of de Leidraad Te Beschermen Belangen:

Bedrijfskritisch systeem conform 'Quickscan BIO':

- het proces wordt aangemerkt als strategisch (afgeleide kerntaak) *en*
- het informatiesysteem is vitaal voor dit proces *en*
- één of meer betrouwbaarheidseisen (B, I, V) scoren hoog.

Bedrijfskritisch systeem conform 'Leidraad Te Beschermen Belangen':

- het proces valt in TBB categorie 2 *en*
- het informatiesysteem is vitaal voor dit proces.

Bijlage 12: eIDAS Toelichting

Vraag 1.1

Wat is de aard van de persoonsgegevens die gebruikt worden?

eIDAS-betrouwbaarheids-niveau	Toelichting
Geen	Er worden geen persoonsgegevens verwerkt of het gaat om openbare persoonsgegevens waarvan het algemeen aanvaard is dat deze geen risico opleveren voor de betrokkene. Denk bijvoorbeeld aan gegevens uit telefoonboeken, brochures en websites.
Laag	Er is sprake van een beperkt aantal (niet-bijzondere) persoonsgegevens en er is sprake van één type vastlegging, bijvoorbeeld één lidmaatschap, arbeidsrelatie of klantrelatie.
Substantieel	Er worden bijzondere persoonsgegevens gebruikt (zoals genoemd in artikel 16 van de Wbp) of financieel-economische gegevens van de betrokkene.
Hoog	Er worden gegevens van opsporingsdiensten gebruikt, gegevens uit DNA-databanken, gegevens waar een bijzondere, wettelijk bepaalde, geheimhoudingsplicht op rust en gegevens die onder het beroepsgeheim vallen (zoals medische gegevens) in de zin van artikel 9, vierde lid, van de Wbp.

Vraag 1.2

Wordt het BSN verwerkt door uw digitale dienst?

eIDAS-betrouwbaarheids-niveau	Toelichting
Geen	Het BSN wordt niet verwerkt.
Laag	Het BSN wordt uitsluitend opgegeven door de gebruiker.
Substantieel	Het BSN wordt in samenhang met aanvullende persoonsgegevens verwerkt.
Hoog	

Vraag 2.1

Wat is de aard van de verwerking?

Het gebruik van de dienst kan rechtsgevolgen hebben.

Als er bij de dienst slechts sprake is van feitelijk handelen, is dit veelal niet het geval. Denk aan het verstrekken van inlichtingen. In dat geval is uw dienst niet op rechtsgevolg gericht.

Daarnaast is het mogelijk dat de dienst gericht is op feitelijk handelen, zoals het registreren van afvalcontainers op naam en adres. Maar dit kan vervolgens tot rechtsgevolg leiden: de gegevens gebruikt u mogelijk voor handhaving. In dat geval spreken we over indirect rechtsgevolg.

Tot slot kan de dienst zijn grondslag vinden in wetgeving en leiden tot rechtshandelingen. Denk bijvoorbeeld aan een besluit dat vatbaar is voor bezwaar en beroep. Er is dan sprake van rechtsgevolg.

eIDAS-betrouwbaarheids-niveau	Toelichting
Geen	Geen rechtsgevolgen
Laag	Indirecte rechtsgevolgen
Substantieel	Er zijn rechtsgevolgen
Hoog	

Vraag 3.1

Worden er gegevens in de basisregistraties gewijzigd?

Gegevens in een basisregistratie vormen een bijzondere categorie. Als deze gegevens worden verwerkt, kunnen de gevolgen groot zijn. Deze gegevens worden immers aan een grote groep afnemers verstrekt.

Onder basisregistratiegegevens vallen authentieke gegevens. Elke opname of mutatie daarvan moet met de grootste zekerheid en zorgvuldigheid gebeuren, want afnemers moeten deze authentieke gegevens zonder nadere controle overnemen en kunnen vertrouwen (het zogenoemde verplicht gebruik).

Over het algemeen past bij deze categorie het betrouwbaarheidsniveau hoog. Maar er is een uitzondering. Worden er gegevens verwerkt die bestemd zijn voor opname in een basisregistratie maar vindt daarop nog een aanvullende controle plaats door de instantie die verantwoordelijk is voor de basisregistratie? Dan geldt in bepaalde gevallen voor deze gegevensverwerking niveau substantieel. Dit is bijvoorbeeld voor veel processen van de Burgerlijke Stand het geval.

eIDAS-betrouwbaarheids-niveau	Toelichting
Geen	Er worden geen gegevens gewijzigd.
Laag	
Substantieel	Er worden authentieke of niet-authentieke gegevens opgegeven of wijzigingen hierop worden opgegeven om opgenomen te worden in basisregistraties. Op deze opgegeven mutaties vindt nog controle plaats.
Hoog	Er worden authentieke gegevens gecreëerd, gewijzigd of functioneel beëindigd in basisregistraties of er worden andere gegevens direct opgenomen of gewijzigd in basisregistraties, zonder verdere controle.

Vraag 4.1

Wat is het economisch belang van de dienst?

Is er sprake van economisch belang bij de dienst? Of kan er economische schade ontstaan bij een foutieve identificatie, identiteitsfraude of verkeerde verwerking van gegevens? Denk bijvoorbeeld aan financiële schade door misbruik of fraude, verlies van geld of economische positie, aansprakelijkheidsstelling, onbevoegden die toegang krijgen tot concurrentiegevoelige informatie (potentiële 'lost order') of koersgevoelige informatie die uitlekt.

Steeds zijn hierbij twee niveaus te beschouwen:

- De economische schade zoals die geleden wordt bij de individuele burger of het individuele bedrijf dat een elektronische dienst van een overheidsorganisatie afneemt. Op het individuele niveau dient u uit te gaan van de potentiële schade voor de bepaling van het gewenste niveau.
- De economische schade die op systeemniveau geleden wordt, dat wil zeggen de burgers of bedrijven gezamenlijk of de overheid in zijn totaal. Hierbij kan van ervaringscijfers worden uitgegaan.

Het hoogste van beide inschattingen is bepalend voor het te hanteren betrouwbaarheidsniveau.

Er kan ook aansluiting worden gezocht bij de TBB-analyse vraag 3.

eIDAS-betrouwbaarheids-niveau	Toelichting
Geen	Belang is nihil
Laag	Belang is gering
Substantieel	Belang is gemiddeld
Hoog	Belang is groot

Vraag 5.1

Wat is (potentieel) van toepassing betreft publicitaire onrust?

eIDAS-betrouwbaarheids-niveau	Toelichting
Geen	Er is geen sprake van publicitaire onrust.
Laag	Er is sprake van klachten, er verschijnen berichten in de media.
Substantieel	Er is bijvoorbeeld een interventie van de Nationale Ombudsman en er zijn Kamervragen.
Hoog	De politiek verantwoordelijke komt in de problemen.

Vraag 5.2

Wat is (potentieel) van toepassing betreft maatschappelijke ontwrichting?

eIDAS-betrouwbaarheids-niveau	Toelichting
Geen	Er is geen sprake van maatschappelijke onrust.
Laag	Er zijn verstoringen die door één organisatie kunnen worden opgelost.
Substantieel	Er zijn verstoringen die vragen om een gecoördineerd optreden van meerdere organisaties (vaak publiek en privaat).
Hoog	Er is sprake van een noodtoestand. Er zijn bijvoorbeeld verstoringen die noodmaatregelen vereisen buiten de normale juridische en financiële kaders.

Vraag 6.1

Zijn er risicoverhogende factoren van toepassing?

Risicoverhogende factoren hangen samen met de aard en context van uw dienst. Denk bijvoorbeeld aan politieke of bestuurlijke gevoeligheid of imago. Als risico verhogende factoren van toepassing zijn, is verhoging van het betrouwbaarheidsniveau waarschijnlijk nodig. We raden u aan een volledige risicoanalyse uit te voeren.

Er zijn vier factoren voor een volledige risicoanalyse:

- Aan de dienst zit een groot politiek, bestuurlijk of imago-risico vast;
- Het risico is moeilijk bepalen, omdat de directe gevolgen van een incident beperkt zijn. Tegelijkertijd is de potentiële vervolgschade groot;
- De dienst loopt grote kans op grootschalig misbruik door georganiseerde criminaliteit. Dit doet zich vooral voor bij de combinatie van massale processen, beperkte controlemogelijkheden en als (grootschalig) misbruik veel gewin oplevert;
- De dienst is een aantrekkelijk doelwit voor terreurorganisaties of buitenlandse inlichtingendiensten.

De aard van de verwerking leidt tot extra risico's, die ertoe leiden om een hoger betrouwbaarheidsniveau te vereisen.

- Verwerkt uw dienst een groot aantal gegevens per individu (meerdere vastleggingen, meerdere doelen), zodat verlies en onrechtmatige verwerking tot een bovenmatige inbreuk op de persoonlijke levenssfeer leidt? Het uitlekken van een compleet medisch dossier leidt over het algemeen bijvoorbeeld tot een grotere inbreuk dan het uitlekken van een herhaalrecept.
- Doel of doelen waarvoor de persoonsgegevens worden verwerkt. Naarmate de beslissingen die op basis van de verwerkte persoonsgegevens worden genomen ingrijpender zijn, is ook de impact van verlies of onrechtmatige verwerking groter.
- De mate waarin de gegevens bruikbaar zijn voor misbruik. Denk vooral aan de mogelijkheid van identiteitsfraude.

Vraag 6.2

Zijn er risicoverlagende factoren van toepassing?

Risicoverlagende factoren komen vooral voor als er extra processtappen zijn, waarin het risico verminderd wordt. Op basis hiervan kunt u voldoende reden hebben om een lager betrouwbaarheidsniveau te kiezen dan het classificatiemodel aangeeft.

Er zijn vijf risicoverlagende factoren:

- In het vervolgproces moet de belanghebbende zich fysiek melden en legitimeren (met een wettelijk identiteitsdocument en BSN). Op die manier weet u zeker dat hij daadwerkelijk uw dienst in kwestie wil afnemen met de gegevens die hij heeft aangeleverd.
- Er is een terugkoppeling van wijzigingen in gegevens of van (voorgenomen) besluiten via een ander kanaal dan het kanaal van uw dienst. NB Een ander kanaal kan daarin ook een ander elektronisch kanaal betreffen. Een transactie (of de uitkomst daarvan) op een overheidswebsite bevestigen via de Berichtenbox kwalificeert in dat geval dus. Uiteraard moet het andere kanaal van bereikbaarheidsgegevens gebruikmaken, die los staan van de transactie in kwestie. Een

transactie op een overheidswebsite bevestigen via een e-mail terugkoppelen, waarvan het e-mailadres in die transactie wordt opgegeven, kwalificeert nadrukkelijk niet.

- In het vervolgproces komen gegevens of documenten voor die, los van uw dienst, bewijzen dat de gebruiker echt betrokken is bij uw dienst en er toestemming voor heeft gegeven.
- Er is sprake van voortdurende en actieve monitoring van uw dienst. Daarmee voorkomt u dat uw dienst in korte tijd heel vaak benaderd wordt door dezelfde gebruiker. Ook ziet u daarmee verdachte gebruikspatronen die op fraude duiden. Houdt u risico- of handhavingsprofielen bij, dan werkt dat ook risicoverlagend.
- Is het economisch belang bepalend voor het betrouwbaarheidsniveau van uw dienst? En is er sprake van een financiële dienst? Dan werkt verificatie van de rekeninggegevens voor betalingen risicoverlagend.