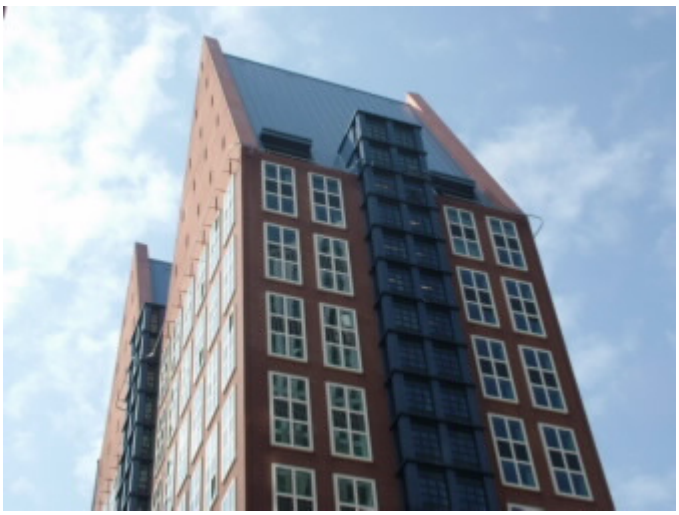
QuickScan Informatiebeveiliging en Privacy

Primaire CCMO kernprocessen met ondersteuning door o.a. ‘National Collaboration Platform’ en overige informatiesystemen.



Versie: 1.0

Datum: 04-06-2024
Status: Definitieve concept ter vaststelling

1. Contactgegevens

Organisatie	Ministerie van Volksgezondheid, Welzijn en Sport (VWS)
Directie	Centrale Commissie Mensgebonden Onderzoek (CCMO)
Afdeling	Nvt
Vestiging adres	Bezuidenhoutseweg 30
Postcode & plaats	2594 AV Den Haag
Telefoonnummer	Nvt
Website	https://www.ccmo.nl/

Workshop

Datum	05-02-2024

Locatie

Straat	Bezuidenhoutseweg 30
Postcode & plaats	2594 AV Den Haag

Deelnemers

Uitvoerder	Functie	Organisatie	E-mail
5.1.2.e	5.1.2.e	Min. VWS, Directie OBP	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
5.1.2.e	5.1.2.e	CCMO	5.1.2.e @ccmo.nl
5.1.2.e	5.1.2.e	CCMO	5.1.2.e @ccmo.nl

Versiebeheer

Versie	Datum	Omschrijving	Auteur	Status
0.1	26-02-2024	Eerste versie o.b.v. Workshop	5.1.2.e	Concept
0.2	06-03-2024	Review en nabespreking 5.1.2.e)	5.1.2.e	Concept
0.3		Feedback 5.1.2.e	5.1.2.e	Concept
0.4	11.03.2024	Samenvoegen comm 5.1.2.e en gestuurd naar 5.1.2.e	5.1.2.e	Concept
0.5	13.03.2024	Missende edits verwerkt in document, naar 5.1.2.e gestuurd	5.1.2.e	Concept
0.6	04.04.2024	Uitstaande comments doorgenomen en waar mogelijk opgelost (5.1.2.e)	5.1.2.e	Concept
0.7	06.05.2024	Final review , na review 5.1.2.e 5.1.2.e	5.1.2.e	Concept
0.8	16.05.2024	Gezamenlijk afgerond (5.1.2.e)	5.1.2.e	Pre-Finaal
0.9	23-05.2024	eIDAS toelichting	5.1.2.e	Pre-Finaal
1.0	04-06-2024	Definitief concept klaar ter vaststelling	5.1.2.e	Finaal

LET OP! INVULLEN VOOR VASTSTELING IN MARJOLEIN! (wijzig ook de status en het versienummer)

Vaststelling

Naam	Functie	Datum	Zaaknummer	Behandelaar

		aanbieden	**Marjolein**	
5.1.2.e	Algemeen Secretaris / Directeur	04-06-2024	1067193	5.1.2.e

2. Managementsamenvatting

Doel van een QuickScan Informatiebeveiliging

Een QuickScan Informatiebeveiliging (QS-IB) heeft als doel, snel vast te stellen of hierbij aan wettelijke eisen op het vlak van informatiebeveiliging en privacy wordt voldaan. Er vindt daarbij toetsing plaats op vier aspecten, nl.:

1. **TBB**: proces **t**e **b**eschermen **b**elang; het betreft een analyse van informatie en systemen die beveiligd moeten worden om de bedrijfsvoering en andere belangen en processen van de Rijksoverheid ongestoord doorgang te laten vinden. Aan elk proces moet een niveau worden toegekend, gerelateerd aan de impact die ontstaat als gevolg van een incident;

2. **AVG**: proces **A**lgemene **V**erordening **G**egevensbescherming (AVG: 2018); is voor het proces de AVG in voldoende mate geïmplementeerd. Is er een verwerkersovereenkomst opgesteld of als er al een is dan moet deze worden getoetst, zijn de verwerkingen opgenomen in het AVG verwerkingsregister en is een Gegevensbescherming Effecten Beoordeling wenselijk of noodzakelijk.

3. **BIO** – **B**aseline **I**nformatiebeveiliging **O**verheid (BIO: 2019): combinatie van proces en informatiesysteem; zijn de vereiste maatregelen voldoende geïmplementeerd, wat is het bedrijfskritisch gehalte van het informatiesysteem in relatie tot het proces en wat is het BBN-niveau. Deze informatie wordt gebruikt in de ICV (In Control Verklaring).

4. **eiDAS** (Electronic Identities And Trust Services): het betrouwbaarheidsniveau indien het een digitale dienst aan een burger of een bedrijf betreft (eiDAS: 2018)

Resultaten QS-IB inclusief duiding van de getallen

1. **TBB**: het classificatieniveau laag is van toepassing; er is een laag risico op financiële impact.

2. **AVG**: Voor het voldoen aan de AVG is het nodig dat de verwerkingen zijn opgenomen in het verwerkingsregister, dat gecontroleerd wordt dat er verwerkersovereenkomsten zijn opgesteld met de verwerkers en een DPIA is uitgevoerd.

3. **BIO**: het proces is geclassificeerd als Strategisch en het systeem als Belangrijk, met BBN-niveau BBN 2+. Het niveau van BBN 2+ is op basis van de classificatie Hoog op vertrouwelijkheid. Dit betekent dat er extra nadruk moet worden gelegd op voldoen aan de normen en maatregelen uit de BIO om de vertrouwelijkheid te borgen. Er kan ook gekozen worden een verdiepende risicoanalyse uit te voeren of de BIO voldoende zorg draagt dat de vertrouwelijkheid van de informatie is gewaarborgd.

4. **eiDAS**: Het Research Portaal levert een digitale dienst aan aanvragers voor de wettelijke toetsing van medisch-wetenschappelijk onderzoek met mensen met

betrouwbaarheidsniveau substantieel. Hiermee moet de authenticatiemethodiek van het Research Portaal aan het niveau substantieel voldoen.

Vervolgactiviteiten naar aanleiding van de QS-IB

1. **Algemeen**
    1. Het definitieve concept moet voorgelegd worden aan de directeur ter vaststelling en goedkeuring.
    2. Idealiter worden de resultaten in het ISMS opgeslagen. Indien er geen ISMS is, dient de QuickScan opgeslagen te worden op een manier zodat deze minstens elke drie jaar wordt herzien, maar idealiter elk jaar.

2. **TBB**
    1. De resultaten van TBB opnemen in het TBB-register.

3. **AVG**
    1. De eerder uitgevoerde DPIA is niet bruikbaar voor dit proces met deze informatiesystemen omdat deze is verouderd en de informatiesystemen niet meer hetzelfde zijn. Een nieuwe DPIA moet daarom uitgevoerd worden, hiervoor kan de oude DPIA wel als inspiratie worden gebruikt. Voor het uitvoeren van de DPIA kan het IB&P Office van het kerndepartement voor advies worden gevraagd of een externe partij kan hiervoor worden ingeschakeld;
    2. Zorg ervoor dat er verwerkingsovereenkomsten zijn met de verwerkers.

4. **BIO**
    1. Toetsen of vastgesteld BBN-niveau voor de BIO in voldoende mate is geïmplementeerd (bv. door uitvoeren van een fit-gap analyse BIO voor proces en/of informatiesysteem).
    2. Besluiten of de BIO voldoende veiligheid garandeert voor de vertrouwelijkheid van de informatie.

5. **eIDAS**
    1. Het Research Portaal is technisch nog niet geschikt om authenticatie met de huidige toegelaten inlogmiddelen voor burgers en bedrijven met betrouwbaarheidsniveau substantieel, te weten DIGID, eHerkenning en eIDAS, te ondersteunen. Aanvragers zullen in het Research Portaal worden verplicht om in te loggen met behulp van multifactor authenticatie, wat valt onder het betrouwbaarheidsniveau laag. De CCMO heeft hier in het verleden bewust voor gekozen om de drempel voor indieningen via het Research Portaal door academische onderzoekers laag te houden. Voorafgaand aan de mogelijke aansluiting van de CCMO op het nieuwe Stelsel Toegang zullen we nagaan of de gekozen uitzonderingsgrond voor authenticatie in het Research Portaal stand kan houden of dat de CCMO alsnog organisatorische en technische maatregelen moeten nemen om aan te sluiten op het Stelsel Toegang en de erkende inlogmiddelen.

3. 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) wenselijke 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 gegevens set 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: 'Primaire CCMO kernprocessen met ondersteuning door o.a. 'National Collaboration Platform' en overige informatiesystemen' van de CCMO.

Informatiesysteem

Deze QS-IB beperkt zich tot de volgende geautomatiseerde informatiesystem:

- 'NCP' (**N**ational **C**ollaboration **P**latform) gebaseerd op MS Teams rond de processen van CCMO.
- 'OMON' (Overzicht van medisch-wetenschappelijk onderzoek in Nederland) – www.onderzoekmetmensen.nl
- 'CTIS' (**C**linical **T**rial **I**nformation **S**ystem)
- Research Portaal

Opmerking: het LTR (Landelijk Trial Register) is begin maart hernoemd naar OMON (Overzicht Medisch-wetenschappelijk Onderzoek in Nederland)

Buiten scope

Niet-geautomatiseerde informatiesystemen die het proces 'Primaire CCMO kernprocessen met ondersteuning door o.a. 'National Collaboration Platform' en 'overige informatiesystemen' ondersteunen vallen buiten de scope van de QS-IB en zullen apart moeten worden geanalyseerd.

Informatiesystemen die geen directe relatie aan de beschouwde informatiesystemen 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.

4. Resultaten per onderdeel

Hieronder de samengevatte resultaten van de QS-IB voor het proces: Primaire CCMO kernprocessen met ondersteuning door o.a. 'National Collaboration Platform' en overige informatiesystemen

Resultaten QS-IB proces 1 - Primaire CCMO kernprocessen met ondersteuning door o.a. 'National Collaboration Platform' en overige informatiesystemen

Naam proces	**Primaire CCMO kernprocessen met ondersteuning door o.a. 'National Collaboration Platform' en overige informatiesystemen**
TBB proces-classificatie	4
TBB gegevens-classificatie	Departementaal VERTROUWELIJK (Dep.V.)
AVG gegevens-classificatie	Bijzondere persoonsgegevens
AVG Implementatie	Voldoende, de DPIA moet geüpdate worden bij voorkeur voor of kort na de go live van het Research Portaal
DPIA uitvoeren	Noodzakelijk
BIO proces-classificatie	Strategisch
eIDAS-betrouwbaarheids-niveau	n.v.t.

Detailbeschrijving proces Primaire CCMO kernprocessen met ondersteuning door o.a. 'National Collaboration Platform' en overige informatiesystemen

Naam proces	Primaire CCMO kernprocessen met ondersteuning door o.a. 'National Collaboration Platform' en overige informatiesystemen
Korte procesbeschrijving	Het is een QuickScan over alle primaire processen van CCMO en bijbehorende informatiesystemen.
Proceseigenaar	Directeur CCMO
Gegevenseigenaar	Directeur CCMO
De klant van het proces	CCMO METC's CCMO collega's Indieners onderzoeken OMON: De burger (bv. Burgerpatiënten, wetenschappers, etc.)
De output van het proces is:	Indieners: Een besluit op de aanvraag METC's: Besluiten registreren De burger: Inzien van informatie Farmacovigilantie van Klinisch onderzoek
Koppelvlakken met andere processen zijn:	Marjolein (archivering) ICTR (WHO studiedatabase) CTIS (aanvraagdossiers en procedureinformatie) alleen van CTIS naar NCP niet vice versa
De gebruikte informatiesystemen zijn:	NCP (gebouwd in Teams) OMON Research portaal CTIS
De beveiligingsincidenten van het afgelopen jaar zijn:	Geen

Detailbeschrijving informatiesysteem: NCP – National Collaboration Platform

Naam van het informatiesysteem	NCP
Informatiesysteemeigenaar	Directeur CCMO
De gebruikers van het informatiesysteem zijn:	Intern: ca. 50 Extern: ca. 100
De output van het informatiesysteem is:	
Koppelvlakken met andere informatiesystemen zijn:	CTIS Research portaal OMON
Processen die gebruik maken van het informatiesysteem zijn:	Primaire CCMO kernprocessen met ondersteuning door o.a. 'National Collaboration Platform' en overige informatiesystemen

Detailbeschrijving informatiesysteem: OMON

Naam van het informatiesysteem	OMON
Informatiesysteemeigenaar	Directeur CCMO
De gebruikers van het informatiesysteem zijn:	Intern: 5 Extern: Iedereen (publiek)
De output van het informatiesysteem is:	
Koppelvlakken met andere informatiesystemen zijn:	NCP
Processen die gebruik maken van het informatiesysteem zijn:	Primaire CCMO kernprocessen met ondersteuning door o.a. 'National Collaboration Platform' en overige informatiesystemen

Detailbeschrijving informatiesysteem: CTIS

Naam van het informatiesysteem	CTIS
Informatiesysteemeigenaar	EMA
De gebruikers van het informatiesysteem zijn:	Intern: Ca. 50 Extern: Buiten scope
De output van het informatiesysteem is:	
Koppelvlakken met andere informatiesystemen zijn:	NCP
Processen die gebruik maken van het informatiesysteem zijn:	Primaire CCMO kernprocessen met ondersteuning door o.a. 'National Collaboration Platform' en overige informatiesystemen

Detailbeschrijving informatiesysteem: Research Portaal

Naam van het informatiesysteem	Research portaal
Informatiesysteemeigenaar	Directeur CCMO
De gebruikers van het informatiesysteem zijn:	Intern: Enkele (functioneel) beheerders bij DICTU Extern: > 10.000
De output van het informatiesysteem is:	
Koppelvlakken met andere informatiesystemen zijn:	NCP
Processen die gebruik maken van het informatiesysteem zijn:	Primaire CCMO kernprocessen met ondersteuning door o.a. 'National Collaboration

	Platform’ en overige informatiesystemen

5. **Inhoud**

1. Contactgegevens..... 2
2. Managementsamenvatting..... 3
3. Inleiding..... 5
4. Resultaten per onderdeel..... 7
5. Inhoud..... 10
6. Analyse Te Beschermen Belangen (TBB)..... 11
7. Analyse Algemene Verordening Gegevensbescherming (AVG)..... 15
   B. Beginselen voor verwerking (hoofdstuk II AVG)..... 15
   V. Verwerkingsverantwoordelijke en Verwerker (hoofdstuk IV AVG)..... 21
   R. Rechten van de betrokkene (hoofdstuk III AVG)..... 25
   E. Extra vragen t.b.v. AVG register..... 26
8. QuickScan BIO..... 28
9. Analyse Betrouwbaarheidsniveaus voor digitale dienstverlening..... 31

Bijlage 1: TBB Categorieën (Vraag 5 TBB)..... 35
Bijlage 2: TBB Classificatie (Vraag 5 TBB)..... 36
Bijlage 3: AVG Toelichting (Vraag B1 t/m E7 AVG)..... 38
Bijlage 4: AVG Logische gegevensverwerkingsgroepen (Vraag B4 AVG)..... 47
Bijlage 5: BIO Proces-classificatie (Vraag 1 BIO)..... 48
Bijlage 6: BIO Informatiesysteem-classificatie (Vraag 1 BIO)..... 50
Bijlage 7: BIO Beschikbaarheid-classificatie (Vraag 2 BIO)..... 51
Bijlage 8: BIO Integriteit-classificatie (Vraag 2 BIO)..... 52
Bijlage 9: BIO Vertrouwelijkheid-classificatie (Vraag 2 BIO)..... 53
Bijlage 10: BIO Basisbeschermingsniveau (BBN) (Vraag 10 BIO)..... 54
Bijlage 11: ICV Toelichting..... 57
Bijlage 12: eIDAS Toelichting..... 58
Bijlage 13: Toelichting categorieën persoonsgegevens..... 63

6. 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(gegevensset), 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 informatiebeveiliging.

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: **Primaire CCMO kernprocessen met ondersteuning door o.a. 'National Collaboration Platform' en overige informatiesystemen**

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	De schade is m.n. op het financiële gebied omdat het om medicijnontwikkeling gaat. De ontwikkeling van medicijnen en hoe dit te doen staat volledig beschreven in de informatie die een ontwikkelaar aanlevert. Denk hierbij aan een patent dat op straat komt te liggen, etc. De kans op een rechtszaak met claim/boete is echter heel klein. Daarnaast is er een kans op diplomatieke schade omdat Nederland niet in een vacuüm opereert t.o.v. medicijnenonderzoek. Als Nederland, middels CCMO, fouten maakt in de toetsing, kan Nederland met name op Europees niveau iets uit te leggen hebben.

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 uitvoering van de processen binnen CCMO vindt geen letselschade plaats. Benadrukt moet hierbij worden dat het om de processen binnen CCMO gaat, niet de daadwerkelijke onderzoeken naar medicijnen.

3	**Is de dienstverlening aan burgers of bedrijven in belangrijke mate afhankelijk van het proces?**	Schade aan vitale processen van de samenleving 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 Financiële schade voor de economie **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	Als het Research Portal langdurig offline gaat, wordt de dienstverlening aan individuele academische onderzoekers of farmaceutische bedrijven gehinderd. Er is dan tenminste een verlies van zekerheid van continuïteit. De CCMO kan tijdelijk overschakelen op indiening per e-mail. We schatten in dat in een dergelijk geval de financiële schade minder is dan 50 miljoen euro.

4	**Zijn belangrijke processen binnen mede-overheden afhankelijk van het proces?**	Schade voor vitale processen medeoverheden **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	Hoewel er wel enige afhankelijkheid binnen VWS is (bv. CBG en IGJ), is dit niet naar mede-overheden het geval.

5	**Wat is de exclusiviteitswaarde van de informatie die binnen het proces wordt verwerkt?**	VIR-BI informatie-rubricering n.v.t.: Geen *bijzondere informatie* **4: Departementaal VERTROUWELIJK (Dep.V.)** 3: Staatsgeheim CONFIDENTIEEL (Stg.C) 2: Staatsgeheim GEHEIM (Stg.G) 1: Staatsgeheim ZEER GEHEIM (Stg.ZG) EU informatie-rubricering **n.v.t. : EU unclassified** 4: EU restricted 3: EU confidential 2: EU secret 1: EU top secret

		NATO informatie-rubricering **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 informatie die aanwezig is in de processen kan departementaal vertrouwelijk zijn (Dep. V.) aangezien het openbaar worden van deze informatie schade kan toebrengen aan één of meer ministeries. De informatie kan onder andere vertrouwelijke informatie omtrent medicijnen bevatten. Dit is bedrijfsvertrouwelijke informatie die bedrijven financiële schade kan toebrengen indien dit openbaar wordt. Deze schade zou dan weer op VWS verhaald kunnen worden. EU rubricering wellicht bekend bij de EMA, maar niet bij ons bekend.

Conclusie QS-TBB

Bepaal hoogste niveau van vraag 1-5	**Classificatie (Bijlage 2)**
Niveau 4	Laag

7. 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 verwerkingenregister.

Resultaten QS-AVG

Proces: **Primaire CCMO kernprocessen met ondersteuning door o.a. 'National Collaboration Platform' en overige informatiesystemen**

Lijst ondersteunende informatiesystemen:
Geef aan indien er sprake is van (semi-)geautomatiseerde besluitvorming, profilering of big data-verwerkingen in de informatiesystemen.

NCP
OMON
CTIS
Research Portaal

Resultaten AVG analyse voor het proces: Primaire CCMO kernprocessen met ondersteuning door o.a. 'National Collaboration Platform' en overige informatiesystemen

B. Beginselen voor verwerking (hoofdstuk II AVG)

Vraag		**Toelichting**	
B1	Is er al eerder een QS AVG uitgevoerd?	Indien Ja: Datum en vindplaats van de documenten aangeven	**Ja**
Datum		**Vindplaats**	
29-01-2019 11-07-2019 13-01-2022		CCMO/Bedrijfsvoering/Integriteit & informatiebeveiliging/Informatiebeveiliging/Audits/2019	

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 (Nieuw: Bijlage 13)	**Ja**
Betrokkene			
Leden en externe adviseurs medisch ethische toetsingscommissies (CCMO / METC's)			
Opdrachtgever onderzoek (sponsor)			
Uitvoerders onderzoek (aanvrager, indiener, hoofdonderzoeker)			
Medewerkers CCMO / METC's			
Deelnemers onderzoek			

! 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**
Gegevens van aanvrager, indiener, opdrachtgever		Contactgegevens	Gewone persoonsgegevens
Gegevens hoofdonderzoeker		Contactgegevens en zakelijke CV	Gewone persoonsgegevens
Gegevens leden CCMO en METC's		Contactgegevens, zakelijke CV's, Verklaring van belangen,	Gewone persoonsgegevens

	geheimhoudingsverklaring, aanwezigheidsregistratie	
Gegevens medewerkers CCMO en METC's	Rol in beoordelingsproces	Gewone persoonsgegevens
Deelnemers onderzoek	Bijzondere persoonsgegevens / gezondheidsgegevens (gepseudonimiseerd)	Bijzondere 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**
Gegevens van aanvrager, indiener, opdrachtgever	Contactgegevens	**Ja**	
Gegevens hoofdonderzoeker	Contactgegevens en CV	**Ja**	
Gegevens leden CCMO en METC's	Contactgegevens, CV's, Verklaring van belangen, geheimhoudingsverklaring, aanwezigheidsregistratie	**Ja**	
Gegevens medewerkers CCMO en METC's	Contactgegevens, rol in beoordelingsproces	**Ja**	
Deelnemers onderzoek	Bijzondere gegevens / gezondheidsgegevens (gepseudonimiseerd)	**Ja**	

!

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-verwerkins groep	**Betrokkene**	**Soort gegevens**	**Toelichting verwerking**
AAN01	Gegevens van aanvrager, indiener, opdrachtgever	Contactgegevens	Logische gegevens verwerkingsgroep
ONZ01	Gegevens hoofdonderzoeker	Contactgegevens en zakelijke CV	Logische gegevens verwerkingsgroep
LED01	Gegevens leden CCMO en METC’s	Contactgegevens, CV’s, Verklaring van belangen, geheimhoudingsverklaring, aanwezigheidsregistratie	Logische gegevens verwerkingsgroep
MWK01	Gegevens medewerkers CCMO en METC’s	Contactgegevens, rol in beoordelingsproces	Logische gegevens verwerkingsgroep
DNM01	Deelnemers onderzoek	Bijzondere persoonsgegevens / gezondheidsgegevens (gepseudonimiseerd)	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**	**Toelichting**
AAN01		**Nee**	
ONZ01		**Nee**	
LED01		**Nee**	
MWK01		**Nee**	
DNM01		**Ja**	Gegevens over gezondheid (gepseudonimiseerd)

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**	**Toelichting register**
AAN01		**Ja.**	M4926 1a Beoordeling van protocollen medisch-wetenschappelijk onderzoek met mensen M4929 1b Beoordeling veiligheidsinformatie goedgekeurde, lopende onderzoeken M7443 Beoordeling van protocollen pilot EU-verordening 2017/745 en 2017/746 M7440 Beoordeling van protocollen pilot EU-verordening 536/2014
ONZ01		**Ja**	M4926 1a Beoordeling van protocollen medisch-wetenschappelijk onderzoek met mensen M4929 1b Beoordeling veiligheidsinformatie goedgekeurde, lopende onderzoeken M7443 Beoordeling van protocollen pilot EU-verordening 2017/745 en 2017/746 M7440 Beoordeling van protocollen pilot EU-verordening 536/2014
LED01		**Ja**	M4926 1a Beoordeling van protocollen medisch-wetenschappelijk onderzoek met mensen M4929 1b Beoordeling veiligheidsinformatie goedgekeurde,

		lopende onderzoeken M7443 Beoordeling van protocollen pilot EU-verordening 2017/745 en 2017/746 M7440 Beoordeling van protocollen pilot EU-verordening 536/2014
MWK01	**Ja**	M4926 1a Beoordeling van protocollen medisch-wetenschappelijk onderzoek met mensen M4929 1b Beoordeling veiligheidsinformatie goedgekeurde, lopende onderzoeken M7443 Beoordeling van protocollen pilot EU-verordening 2017/745 en 2017/746 M7440 Beoordeling van protocollen pilot EU-verordening 536/2014
DNM01	**Ja**	M4926 1a Beoordeling van protocollen medisch-wetenschappelijk onderzoek met mensen M4929 1b Beoordeling veiligheidsinformatie goedgekeurde, lopende onderzoeken M7443 Beoordeling van protocollen pilot EU-verordening 2017/745 en 2017/746 M7440 Beoordeling van protocollen pilot EU-verordening 536/2014

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**	**Toelichting doelen**
AAN01, ONZ01, LED01, MWK01, DNM01		**Ja**	Zie vraag B6

Vraag		**Toelichting**	
B8	Zijn de grondslagen van de verwerking vastgesteld?	Geef per gegevensverwerkingsgroep aan Ja/Nee. Bij Ja: geef een uitgebreide toelichting bij de grondslagen (zie Bijlage 3 voor een nadere uitleg).	
Gegevensverwerkingsgroep		**Grondslagen**	**Toelichting grondslagen**
AAN01, ONZ01, LED01, MWK01, DNM01		**Ja**	Zie vraag B6

Vraag		**Toelichting**
B9	Is er wet- en regelgeving	Benoem de wet- en regelgeving, met uitzondering van de

	en/of beleid dat gevolgen heeft voor de verwerkingen?	AVG en de Richtlijn, en het beleid met mogelijke gevolgen voor de gegevensverwerkingen (zie Bijlage 3 voor een nadere uitleg).	
Gegevensverwerkingsgroep		**Wet- en regelgeving**	**Toelichting juridische en beleidsmatige kaders**
AAN01		**Ja**	WMO, Embryo wet, CTR, MDR, IVDR. Op termijn komt WZL erbij, wet is er nog niet en ligt al 10 jaar in concept.
ONZ01		**Ja**	WMO, Embryo wet, CTR, MDR, IVDR. Op termijn komt WZL erbij, wet is er nog niet en ligt al 10 jaar in concept.
LED01		**Ja**	WMO, Embryo wet, CTR, MDR, IVDR. Op termijn komt WZL erbij, wet is er nog niet en ligt al 10 jaar in concept.
MWK01		**Nee**	
DNM01		**Ja**	WMO, Embryo wet, CTR, MDR, IVDR. Op termijn komt WZL erbij, wet is er nog niet en ligt al 10 jaar in concept.

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		**Bewaartermijn**	**Toelichting bewaartermijn**
AAN01, ONZ01, LED01, MWK01, DNM01		**Ja**	Zie vraag B6 Zie Concernbrede selectielijst van het ministerie van Volksgezondheid, Welzijn en Sport.pdf (nationaalarchief.nl) hierin is de CCMO opgenomen. V20 MDR, V25 WMON V30 WMON/MDR/CTR na beëindiging van studie

V. Verwerkingsverantwoordelijke en Verwerker (hoofdstuk IV AVG)

Vraag		**Toelichting**	
V1	Wie is de verwerkingsverantwoordelijke?	Geef per gegevensverwerkingsgroep aan Functieaanduiding/organisatieonderdeel.	
Gegevensverwerkingsgroep		**Verwerkingsverantwoordelijke**	**Organisatie**
AAN01, ONZ01, LED01, MWK01, DNM01		Algemeen Secretaris/Directeur	CCMO

Vraag		**Toelichting**
V2	Welke verwerkers zijn er?	Geef per gegevensverwerkingsgroep aan verwerkers/ organisatie.

Gegevensverwerkingsgroep	Verwerker	Organisatie
AAN01, ONZ01, LED01, MWK01, DNM01	DICTU, voor research portaal	Ministerie van EZ
AAN01, ONZ01, LED01, MWK01, DNM01	DICTU (OMON)	Ministerie van EZ
AAN01, ONZ01, LED01, MWK01, DNM01	n.n.t.b. voor het NCP	CCMO

! 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/ afspraak**
AAN01, ONZ01, LED01, MWK01, DNM01		DICTU (OMON)	Min. Van EZ	**Ja (voor OMON)**
AAN01, ONZ01, LED01, MWK01, DNM01		DICTU (Research Portaal)	Min. Van EZ	
AAN01, ONZ01, LED01, MWK01, DNM01		n.n.t.b. (NCP)		

Vraag		Toelichting		
V4	Is de verwerking aangesloten op het proces 'Melden Datalekken'?	Geef per gegevensverwerkingsgroep – verwerker aan Ja/Nee.		
Gegevensverwerkingsgroep		**Verwerker**	**Aangesloten**	**Toelichting aansluiting**
AAN01, ONZ01, LED01, MWK01, DNM01		DICTU	**Ja**	

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**
AAN01, ONZ01, LED01, MWK01, DNM01		**Ja**	Zit in het DNA van de opdracht en de organisatie. 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**
AAN01		**Nee**	
ONZ01		**Nee**	
LED01		**Nee**	
MWK01		**Nee**	
DNM01		**Ja**	Bijzondere persoonsgegevens

!

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**
DNM01		**Ja**	Datum: 11-07-2019

Vraag		Toelichting	
V8	Worden de gegevens door gegeven aan andere verwerkingsverantwoordelijken?	Geef per gegevensverwerkingsgroep aan Ja/Nee. Bij Ja: aan wie (organisatie)	
Gegevensverwerkingsgroep		**Doorgifte**	**Organisatie**
AAN01		**Ja**	IGJ, CBG, indien van toepassing

ONZ01	**Ja**	IGJ, CBG, indien van toepassing
LED01	**Nee**	
MWK01	**Nee**	
DNM01	**Nee**	

!

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 verwerkingsverantwoordelijke?	Geef per gegevensverwerkingsgroep – organisatie aan Ja/Nee Bij Ja: Toelichting m.b.t. de afspraken (o.a. vindplaats documenten)		
Gegevensverwerkingsgroep		**Organisatie**	**Afspraken**	**Toelichting afspraken**
AAN01		IGJ, CBG	**Ja**	Marjolein: CCMO > Bedrijfsvoering > Integriteit & Informatiebeveiliging > Geheimhouding
ONZ01		IGJ, CBG	**Ja**	Marjolein: CCMO > Bedrijfsvoering > Integriteit & Informatiebeveiliging > Geheimhouding
LED01, MWK01, DNM01		N.v.t.		

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**
AAN01		IGJ, CBG	NL
ONZ01		IGJ, CBG	NL
LED01, MWK01, DNM01		N.v.t.	

Vraag		Toelichting	
V11	Worden de gegevens door gegeven aan andere verwerkingsverantwoordelijk en buiten de EU?	Geef per gegevensverwerkingsgroep aan Ja/Nee/N.v.t.. Bij Ja: welk land	
Gegevensverwerkingsgroep		**Buiten EU**	**Land**
AAN01		**Nee**	
ONZ01		**Nee**	
LED01, MWK01, DNM01		**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**	**Beschrijf informatie naar betrokkene**
AAN01		**Nee**	
ONZ01		**Nee**	
LED01		**Nee**	
MWK01		**Nee**	
DNM01		**Ja**	

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**	**Toelichting proces**

AAN01, ONZ01, LED01, MWK01, DNM01	**Ja**	Dit is een CCMO deelproces.

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**	**Is dit gedocumenteerd**
AAN01, ONZ01, LED01, MWK01, DNM01		**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**	**Toelichting**
AAN01		**Betrokkene**	
ONZ01		**Aanleverende Partij**	
LED01		**Aanleverende Partij**	
MWK01		**Aanleverende Partij**	
DNM01		**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**	**Toelichting**
AAN01		**Ja**	Anders kan het onderzoek niet worden ingediend c.q. beoordeeld/gevalideerd.
ONZ01		**Ja**	Anders kan het onderzoek niet worden ingediend c.q. beoordeeld/gevalideerd.
LED01		**Nee**	
MWK01		**Nee**	
DNM01		**Ja**	Anders kan de deelnemer niet meedoen aan het onderzoek.

Vraag		**Toelichting**
E3	Zijn de persoonsgegevens gepseudonimiseerd?	Geef per gegevensverwerkingsgroep aan of deze gepseudonimiseerd zijn.

		Bij Ja: Toelichting m.b.t. de pseudonimisering	
Gegevensverwerkingsgroep		**Pseudonimisering**	**Toelichting**
AAN01		**Nee**	
ONZ01		**Nee**	
LED01		**Nee**	
MWK01		**Nee**	
DNM01		**Ja**	

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**	**Toelichting**
AAN01, ONZ01, LED01, MWK01, DNM01		**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 electronische weg verzonden**	**Toelichting**
AAN01, ONZ01, LED01, MWK01, DNM01		**Ja**	Ja, grotendeels via een publiek netwerk, maar wel via de informatiesystemen.

8. 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, bedrijfs-kritisch 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: **Primaire CCMO kernprocessen met ondersteuning door o.a. 'National Collaboration Platform' en overige informatiesystemen**
Informatiesysteem: **NCP**
OMON
CTIS
Research Portaal

1 – Classificatie

Classificatie van het proces	Strategisch
Argumentatie van de gekozen classificatie van het proces	Het betreft het primaire proces van CCMO en er is een wettelijke basis voor de beoordeling van de onderzoeksvoorstellen. Het proces is voor de ZBO CCMO daarmee strategisch. Voor het ministerie is het proces bijdragend. Er is een indirecte relatie met de hoofdactiviteiten van het ministerie. Als ZBO heeft CCMO verder een meer zelfstandige positie ten opzichte van het ministerie.
Classificatie van het informatiesysteem	Belangrijk
Argumentatie van de gekozen classificatie van het informatiesysteem	De informatiesystemen zijn de afgelopen jaren belangrijker geworden. De combinatie van het NCP en het research portaal is een belangrijke koppeling waarbij CCMO niet zonder de éne of de andere kan werken. De laatste optie is

	om alles terug te zoeken in de e-mails, hierdoor zou je kunnen zeggen dat 'belangrijk' de classificatie is, maar dit zorgt voor zo'n enorm onevenredige inspanning dat dit tegen een vitaal informatiesysteem aanzit.

2 – Betrouwbaarheidseisen

Beschikbaarheid	Midden
Argumentatie van de gekozen beschikbaarheid	Maximaal één dag uitval is aanvaardbaar (geen deadlines bijvoorbeeld), maar meer dan een dag zorgt voor verstoring van de processen. Verschilt ook per informatiesysteem.

Integriteit	Laag
Argumentatie van de gekozen integriteit	Indien er schade optreedt is dit met name op het proces en de doorloop ervan. Als niet alle documenten worden aangeleverd, zal de CCMO bijvoorbeeld geen beoordeling doen. De focus ligt voor de CCMO op de documenten en niet de juistheid van de informatie binnen de documenten.

Vertrouwelijkheid	Hoog
Argumentatie van de gekozen vertrouwelijkheid	Het betreft gerubriceerde (Departementaal vertrouwelijk) en of vertrouwelijke informatie (persoonsgegevens of bedrijfsgevoelige informatie) die in de gedeelde dossiers en documenten staat. De gevoelige informatie ligt bijvoorbeeld aan de informatie die farmaceuten aanleveren. Daarin zit ook gevoelige bedrijfsinformatie die tot significante financiële schade voor bedrijven kan leiden.

BBN-niveau	BBN 2+
Toelichting gekozen BBN-niveau	Vanwege de classificatie Midden – Laag – Hoog (zonder dreiging van statelijke actoren) is de conclusie BBN 2+.

	Er is overwogen of het BBN 3 betreft, denk bijvoorbeeld aan de hack van het EMA door vermoedelijke Russische en of Chinese hackers. Maar de CCMO is tot zover geen doelwit van dit soort aanvallen, daarom is gekozen voor BBN 2+. Hiermee is het aan te raden extra strict om te gaan met de implementatie van de BIO maatregelen op de systemen en te overwegen of deze voldoende veiligheid verschaffen.

Resultaten ICV-classificatie

Proces: **Primaire CCMO kernprocessen met ondersteuning door o.a. 'National Collaboration Platform' en overige informatiesystemen**

Informatiesysteem: NCP **+ RP**

Informatiesysteemclassificatie conform TBB

TBB proces-classificatie	QS-BIO Informatiesysteem-classificatie
4	Belangrijk

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 NCP + RP is:
niet Kritiek en niet Bedrijfskritisch in relatie tot het proces (zie Bijlage 11).

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**
Toelichting	Het research portaal is voor registratie en indiening van al het medisch-wetenschappelijk onderzoek met mensen, dat niet via het CTIS-portaal of het toekomstige EudaMED-portaal wordt ingediend.

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 persoonsgegevensverwerking?	
	eIDAS-betrouwbaarheids-niveau	**Substantieel**
	Toelichting	In het Research Portaal worden op bij alle typen indiening op één na alleen openbare contactgegevens verwerkt die geen risico opleveren voor betrokkenen. Echter bij verschillende type veiligheidsmeldingen worden gezondheidsgegevens van onderzoek deelnemers aan de CCMO ter beoordeling overlegd. Dit zijn bijzondere persoonsgegevens en vandaar is het betrouwbaarheidsniveau van het Research Portaal substantieel.

Vraag		
1.2	Wordt het BSN verwerkt door de digitale dienst?	Nee
	eIDAS-betrouwbaarheids-niveau	**Geen**
	Toelichting	Er worden geen Burgerservicenummers verwerkt.

2. Rechtsgevolg

Vraag		
2.1	Heeft het gebruik van de dienst rechtsgevolgen?	Ja
	eIDAS-betrouwbaarheids-niveau	**Substantieel**
	Toelichting	Onderzoek dat onder de Wet medisch-wetenschappelijk onderzoek met mensen (WMO) valt moet in Nederland vooraf door een erkende METC of de CCMO worden getoetst. Onderzoek dat niet onder WMO valt, moet wel gemeld worden bij een erkende METC. Al deze indieningen zullen plaatsvinden via het Research Portaal. Ook niet-WMO studies worden ingediend via het Research Portaal. Vandaar heeft deze dienst rechtsgevolgen en is het betrouwbaarheidsniveau van het Research Portaal substantieel.

3. Gegevenswijzigingen basisregistraties

Vraag		
3.1	Worden er gegevens in de basisregistraties gewijzigd?	Nee
	eIDAS-betrouwbaarheids-niveau	**Geen**
	Toelichting	Er worden geen basisregistratie gebruikt of gewijzigd.

4. Economisch belang

Vraag		
4.1	Wat is het economisch belang van de dienst?	
	eIDAS-betrouwbaarheids-niveau	**Laag**
	Toelichting	Het economisch belang van deze dienst is gering. Als het Research Portal langdurig offline gaat dat wordt de dienstverlening aan individuele academische onderzoekers of farmaceutische bedrijven gehinderd. Er is dan tenminste een verlies van zekerheid van continuïteit. De CCMO kan tijdelijk overschakelen op indiening per e-mail. We schatten in dat in een dergelijk geval de economische schade minder is dan 50 miljoen euro.

5. Publiek belang

Vraag		
5.1	Wat is (potentieel) van toepassing betreft publicitaire onrust?	
	eIDAS-betrouwbaarheids-niveau	**Laag**
	Toelichting	Als het Research Portal langdurig offline gaat dat wordt de dienstverlening aan individuele academische onderzoekers of farmaceutische bedrijven gehinderd. Er is dan tenminste een verlies van zekerheid van continuïteit. De CCMO kan tijdelijk overschakelen op indiening per e-mail. We schatten in dat in een dergelijk geval er door aanvragers klachten kunnen worden ingediend en bij langdurige uitval berichten in de media kunnen komen.

Vraag		
5.2	Wat is (potentieel) van toepassing betreft maatschappelijke ontwrichting?	
	eIDAS-betrouwbaarheids-niveau	**Laag**
	Toelichting	Als het Research Portal langdurig offline gaat dat wordt de dienstverlening aan individuele academische onderzoekers of farmaceutische bedrijven gehinderd. Er is dan tenminste een verlies van zekerheid van continuïteit. De CCMO kan tijdelijk overschakelen op indiening per e-mail. Deze verstoringen kunnen door de CCMO in samenwerking met haar leveranciers worden opgelost.

6. Correctiefactoren

Vraag		
6.1	Zijn er risicoverhogende factoren van toepassing?	
		Nee
	Toelichting	We zien geen risico verhogende factoren.

Vraag		
6.2	Zijn er risicoverlagende factoren van toepassing?	
		Nee
	Toelichting	

Resultaten eIDAS-analyse

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

Vraag	
Betreft het een digitale dienst aan een burger of bedrijven?	**Ja**
eIDAS-betrouwbaarheids-niveau	**Substantieel**
Toelichting	Vanwege de verwerking van gezondheidsgegevens van onderzoekdeelnemers en de rechtsgevolgen is het betrouwbaarheidsniveau van het Research Portaal substantieel. Echter het Research Portaal is technisch nog niet geschikt om authenticatie met de huidige toegelaten voor burgers en bedrijven inlogmiddelen met betrouwbaarheidsniveau substantieel, te weten DIGID, eHerkenning en eIDAS, te ondersteunen. Aanvragers zullen in het Research Portaal worden verplicht om in te loggen met behulp van multifactor authenticatie, wat valt onder het betrouwbaarheidsniveau laag. De CCMO heeft hier in het verleden bewust voor gekozen om de drempel voor indieningen via het Research Portaal door academische onderzoekers laag te houden. Voorafgaand aan de mogelijke aansluiting van de CCMO op het nieuwe Stelsel Toegang zullen we nagaan of de gekozen uitzonderingsgrond voor authenticatie in het Research Portaal stand kan houden of dat de CCMO alsnog organisatorische en technische maatregelen moeten nemen om aan te sluiten op het Stelsel Toegang en de erkende inlogmiddelen.

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. Er zijn alternatieven of adequate	Van schade is sprake indien kennisneming door niet-gerechtigden, aantasting, verlies kan leiden tot een dusdanig nadelig effect op het

MIDDEN	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 V6: 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. Profilering

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 heef 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 beschikbaarheidseis overstijgt het standaardniveau 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 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.
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, geheim-houdingsplicht 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 imagorisico 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.

Bijlage 13: Toelichting categorieën persoonsgegevens

Categorieën persoonsgegevens

Persoonsgegevens die de gebruikers in de applicatie verwerken

Content-gegevens (inhoudelijke gegevens)

Denk hierbij aan: - persoonsgegevens van betrokkenen bij het doelgebruik van de applicatie (bijvoorbeeld medewerkers, afnemers van diensten/producten van de organisatie, leveranciers van de organisatie etc.)

Persoonsgegevens van de gebruikers/beheerders van de applicatie

Account-gegevens

Denk hierbij aan: - account-gegevens van eindgebruikers
- account-gegevens van systeembeheerders

Contact-gegevens

Denk hierbij aan: - contact-gegevens van personen die bij de applicatie betrokken zijn

Authenticatie/Licentie-gegevens

Denk hierbij aan: - authenticatie/licentie-verificatiegegevens van eindgebruikers
- authenticatie/licentie-verificatiegegevens van systeembeheerders

Financiële gegevens

Denk hierbij aan: - financiële gegevens (o.a. verplichtingen, ontvangsten, betalingen) m.b.t. de applicatie/dienstverlening die persoonsgegevens bevatten

Support-gegevens

Denk hierbij aan: - inhoudelijke gegevens (content-gegevens) over een issue/bug/error die persoonsgegevens bevatten
- diagnostische gegevens over een issue/bug/error die persoonsgegevens bevatten

Diagnostische gegevens

Denk hierbij aan: - telemetrie-gegevens van eindgebruikers
- telemetrie-gegevens van systeembeheerders
- logging-gegevens die persoonsgegevens bevatten

Website/Cookies-gegevens

Denk hierbij aan: - Website/Cookies-gegevens die worden opgeslagen op de website/server van de dienstenleverancier die persoonsgegevens bevatten.