



**AUTORITEIT
PERSOONSGEGEVENS**

Autoriteit Persoonsgegevens

Postbus 93374, 2509 AJ Den Haag
Hoge Nieuwstraat 8, 2514 EL Den Haag
T 070 8888 500 - F 070 8888 501
autoriteitpersoonsgegevens.nl

Aangeboden per e-mail: [redacted]@live.nl

Datum

8 april 2024

Ons kenmerk

[redacted]

Uw brief van

19 januari 2024

Contactpersoon

[redacted]

070 8888 500

Onderwerp

Woo-besluit over informatie met betrekking tot de gegevensbeschermingseffectenbeoordeling(en)

Geachte [redacted]

Op 19 januari 2024 heeft u de Autoriteit Persoonsgegevens (AP), met een beroep op de Wet open overheid (Woo), verzocht om informatie en documenten. Uw verzoek ziet, samengevat, op de openbaarmaking van informatie met betrekking tot de gegevensbeschermingseffectenbeoordeling(en). De datum van uw bericht is gelijk aan de datum van ontvangst van uw verzoek.

Op 29 januari 2024 is de ontvangst van het Woo-verzoek per e-mail aan u bevestigd. Vanwege de gecompliceerdheid van uw verzoek, verdaagden wij de beslistermijn met twee weken. Dit hebben wij gedaan met toepassing van artikel 4.4, tweede lid, van de Woo.

In dezelfde e-mail bent u verzocht een tweetal onderdelen van uw verzoek te preciseren.

Op 2 februari 2024 heeft u hierop gereageerd. Aan de hand van uw reactie is de zoekslag verricht.

Ondanks onze inspanningen is het ons helaas niet gelukt om binnen de wettelijke termijn te beslissen op uw verzoek, waarvoor onze excuses.

Besluit

De AP besluit de door u opgevraagde en door ons aangetroffen informatie gedeeltelijk openbaar te maken. U kunt de informatie in het bijgesloten document vinden.

Hieronder licht de AP dit besluit aan u toe.



Datum
8 april 2024

Ons kenmerk
[REDACTED]

Uw Woo-verzoek

Uw verzoek ziet op de volgende documenten:

"Alle informatie inzake de besluitvorming van de vaststelling van het intern gebruikte gegevensbeschermingseffectenbeoordeling zoals bedoeld in artikel 35 van de AVG.

-Alle informatie, waaronder formats, beleidsdocumenten, criteria en werkinstructies voor het opstellen van een interne gegevensbeschermingseffectenbeoordeling.

-Alle uitgevoerde gegevensbeschermingseffectenbeoordelingen."

Ten aanzien van het eerste en derde onderdeel bent u verzocht om precisering.

In uw reactie gaf u aan:

"Ik verzoek alle uitgevoerde gegevensbescherming gegevensbeschermingseffectenbeoordelingen uitgevoerd door de Autoriteit Persoonsgegevens van de afgelopen 3 jaar. Daarbij ook alle werkinstructies, handleidingen, templates en beleid die daarvoor intern gehanteerd worden."

Wettelijk kader

De AP behandelt uw verzoek als een verzoek om openbaarmaking van informatie op grond van de Wet open overheid. Een Woo-verzoek wordt ingewilligd (artikel 4.1, zevende lid, van de Woo), voor zover de AP over de informatie beschikt, de informatie niet al openbaar is en de uitzonderingsgronden van hoofdstuk 5 van de Woo hieraan niet in de weg staan.

Hieronder legt de AP uit wat dit betekent voor uw Woo-verzoek.

Zoekslag

Op basis van uw verzoek en door het uitvoeren van de zoekslag zijn zes documenten aangetroffen.

Motivering bij gedeeltelijke openbaarmaking

Ingevolge artikel 4.1, zevende lid, van de Woo wordt een verzoek om informatie ingediend met inachtneming van het bepaalde in hoofdstuk 5 van de Woo. Het recht op openbaarmaking op grond van de Woo dient uitsluitend het publieke belang van een goede en democratische bestuursvoering en komt iedere burger in gelijke mate toe. Daarom kan ten aanzien van de openbaarheid geen onderscheid worden gemaakt naar gelang de persoon of de bedoeling of belangen van de verzoeker. Bij de belangenafweging worden daarom het algemene belang van openbaarmaking en de te beschermen belangen door de weigeringsgronden betrokken. Het specifieke belang van de verzoeker wordt hierbij niet betrokken. Verder wordt de informatie die aan u openbaar wordt gemaakt ook aan eenieder openbaar gemaakt. In dit licht vinden de onderstaande belangenafwegingen dan ook plaats.

De eerbiediging van de persoonlijke levenssfeer (artikel 5.1, tweede lid, onder e, van de Woo)

In de documenten die gedeeltelijk openbaar worden gemaakt, staan persoonsgegevens. Dit zijn gegevens die, al dan niet in samenhang met andere gegevens, herleidbaar zijn tot een persoon, zoals persoonsnamen, telefoonnummers, e-mailadressen, handtekeningen, initialen en zaaknummers (aangemaakt door de AP). Voor zaaknummers geldt daarbij dat openbaarmaking het risico zou vergroten dat (persoons)gegevens uit dossiers van de AP terecht kunnen komen bij onbevoegden.



Datum
8 april 2024

Ons kenmerk
[REDACTED]

Openbaarmaking van de genoemde (persoons)gegevens zou een inbreuk op de persoonlijke levenssfeer van de betrokkenen maken. Onder de betrokkenen behoren ook ambtenaren. Wij wegen het belang van eerbiediging van de persoonlijke levenssfeer zwaarder dan het belang van openbaarmaking. Deze informatie wordt dan ook niet openbaar gemaakt.

De beveiliging van personen en bedrijven en het voorkomen van sabotage (artikel 5.1, tweede lid, onder h, van de Woo)

Er wordt geen informatie openbaar gemaakt wanneer dit de beveiliging van personen en bedrijven en/of het voorkomen van sabotage belemmert. Dit belang weegt zwaarder dan het belang van openbaarheid. De DPIA's zien op beveiligingsmaatregelen. Hiervan zal de openbaarmaking worden geweigerd. Uit deze DPIA's kan direct of indirect worden afgeleid welke passende technische of organisatorische maatregelen zijn getroffen om sabotage te voorkomen, de systemen veilig te houden, te voldoen aan wet- en regelgeving en welke rollen er toegang hebben tot welke informatie. Wanneer deze gegevens worden geopenbaard, kan dit voor kwaadwillenden sabotage in de hand werken waardoor de veiligheid van de aan de beoordeling onderworpen organisaties in het geding kan komen. De AP vindt het belang om geen zicht te bieden op de beveiligingsmaatregelen zwaarder wegen dan het belang van openbaarheid. Deze informatie wordt niet openbaar gemaakt. In met name document '1. Overzicht DPIA.pdf' wordt deze weigeringsgrond toegepast. De achtergrond hiervan is dat anders de informatiebeveiliging van de AP zelf in het geding kan komen.

Het goed functioneren van de Staat, andere publiekrechtelijke lichamen of bestuursorganen (artikel 5.1, tweede lid, onder i, van de Woo)

Het belang van het goed functioneren van de AP als bestuursorgaan weegt naar het oordeel van de AP zwaarder dan het algemene belang van openbaarheid. Onder verwijzing naar de eerder genoemde overwegingen, kan het goed functioneren van de AP in het geding komen. Dit is het geval als informatie over de genomen beveiligingsmaatregelen van de beoordeelde organisaties openbaar wordt, als gevolg waarvan onbevoegden zich toegang kunnen verschaffen tot de informatie die deze organisaties onder zich hebben. Nadien kan dit met zich meebrengen dat organisaties minder snel geneigd zijn (volledig) mee te werken aan vergelijkbare beoordelingen. Door deze terughoudendheid kan het goed functioneren van de AP in het geding komen. Het belang van het goed functioneren van de AP dient dan ook zwaarder te wegen dan het belang van de openbaarheid. In met name document '1. Overzicht DPIA.pdf' wordt deze weigeringsgrond toegepast. De achtergrond hiervan is dat anders de informatiebeveiliging van de AP zelf in het geding kan komen.

Publicatie

Dit besluit, de inventarislijst en de te openbaren documenten, zal de AP geanonimiseerd publiceren op haar website.



Datum
8 april 2024

Ons kenmerk
[REDACTED]

Bezwaar

Bent u het niet eens met dit besluit? Dan kunt u bezwaar maken. Hieronder leest u hoe u dat kunt doen.

Hoogachtend,
Autoriteit Persoonsgegevens,
[REDACTED]

Rechtsmiddelenclausule

Bent u het niet eens met de inhoud van dit besluit? Dan kunt u binnen zes weken na de verzenddatum van dit besluit digitaal of schriftelijk bezwaar indienen. Op autoriteitpersoonsgegevens.nl/bezwaar-maken leest u hoe u dit doet.

Op autoriteitpersoonsgegevens.nl/bezwaar-maken vindt u het digitale formulier waarmee u uw bezwaar indient.

Als u schriftelijk bezwaar wilt maken, dan moet u uw brief binnen zes weken na de verzenddatum van dit besluit sturen naar het bovenaan deze brief genoemde postadres. Vermeld op de envelop 'Awb-bezwaar' en zet 'bezwaarschrift' in de titel van uw brief. Neem in uw bezwaar ten minste op:

- uw naam en adres;*
- de datum van uw bezwaar;*
- de reden(en) waarom u het niet eens bent met dit besluit;*
- uw handtekening;*
- het bovenaan deze brief genoemde kenmerk of een kopie van dit besluit.*

Document nummer	Bestandsnaam	Weigeringsgrond	Tags
1	1. Overzicht DPIA	5.1.2h, 5.1.2.i	Niet openbaar
2	2. DPIA-20230420-def		Openbaar
3	3. DTIA-20230420-def		Openbaar
4	4. Stroomschema-nieuwe-aangepaste-verwerking-20230420		Openbaar
5	5. Toelichting-Stroomschema-nieuwe-en-aangepaste-verwerking-20230420-def	5.1.2.e	Deels openbaar
6	6. Vragenlijst-Privacy-vs-20230420-def		Openbaar



DPIA

De DPIA dient ingevuld te worden als uit de Pre-DPIA volgt dat dat nodig is. Daarnaast kan de FG ook in andere gevallen adviseren om een DPIA uit te voeren. Bijvoorbeeld als een verwerking kritiek is voor de AP. De DPIA is een aanvulling op de Vragenlijst Privacy.

Naam van de verwerking:

Datum invullen/bijstellen DPIA:

Versienummer:

Datum vaststelling DPIA:

1. Aanvullende vragen op Vragenlijst Privacy

Nr.	Vragen	Antwoorden
1.	Naam contactpersoon en afdeling?	Naam contactpersoon: Afdeling:
2.	Gaat het hier om een nieuwe verwerking met persoonsgegevens die we al hebben of worden er nieuwe persoonsgegevens ontvangen?	Nieuwe verwerking persoonsgegevens: ☐ die wel al hebben ☐ nieuwe persoonsgegevens ontvangen
3.	Beschrijf de dataflow of voeg een plaatje met de dataflow toe?	Beschrijving dataflow: Voeg plaatje dataflow toe:



Nr.	Vragen	Antwoorden
4.	Hoeveel betrokkenen worden geraakt door deze verwerking?	Aantal betrokkenen:
5.	Hoe worden de betrokkenen geïnformeerd over deze verwerking?	Beschrijving hoe betrokkenen worden geïnformeerd:
6.	Zijn de persoonsgegevens van voldoende kwaliteit? Hoe wordt geborgd dat ze van voldoende kwaliteit blijven?	Beschrijf of persoonsgegevens voldoende van kwaliteit zijn: Beschrijf borging kwaliteit:
7.	Benoem alle wet- en regelgeving en beleid met mogelijke gevolgen voor de voorgenomen gegevensverwerkingen. De AVG en de Richtlijn ¹ hoeven niet genoemd te worden	Beschrijf wet- en regelgeving: Beschrijf beleid:

¹ Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad.



Nr.	Vragen	Antwoorden
8.	Beschrijf de procedure waarmee invulling wordt gegeven aan de rechten van de betrokkenen en welke partij verantwoordelijk is voor de uitvoering van de procedure? Als de rechten van de betrokkene worden beperkt, beschrijf op grond van welke wettelijke uitzondering dat is toegestaan?	Beschrijving procedure bij recht: ☐ van inzage: ☐ op rectificatie en aanvulling: ☐ op vergetelheid: ☐ op beperking van de verwerking: ☐ op dataportabiliteit: ☐ niet onderworpen te worden aan geautomatiseerde besluitvorming: ☐ om bezwaar te maken: ☐ op duidelijke informatie Welke wettelijke uitzondering om rechten te beperken:
9.	Is er nog andere relevante informatie die je wilt delen over deze verwerking?	Andere relevante informatie:

2. Risico's voor betrokkenen

Beschrijf en beoordeel de risico's van de gegevensverwerkingen voor de rechten en vrijheden van betrokkenen. Ga hierbij in ieder geval in op:

- welke negatieve gevolgen de gegevensverwerkingen kunnen hebben voor de rechten en vrijheden van de betrokkenen, zoals het verbod op discriminatie;



- b. de oorsprong van deze gevolgen;
- c. de waarschijnlijkheid (kans) dat deze gevolgen zullen intreden;
- d. de ernst (impact) van deze gevolgen voor de betrokkenen wanneer deze intreden.

Beoordeel welke technische, organisatorische en juridische maatregelen in redelijkheid kunnen worden getroffen om de hiervoor beschreven risico's te voorkomen of te verminderen. Beschrijf welke maatregel welk risico aanpakt. Voeg aanvullende informatie in het tekstveld onder de tabellen toe.

Beschrijf ook de restrisico's die nog aanwezig zijn na de uitvoering en/of implementatie van de geïdentificeerde maatregelen. Geef per resterend risico aan wat het niveau is van dit risico.

Gebruik voor de inschatting van de kans, impact en het risico de niveaus 'laag', 'gemiddeld' en 'hoog'. De kans wordt bepaald aan de hand van de formule kans x impact. Maak gebruik van de bijbehorende kleuren.



Nr.	Risico's	Kans	Impact	Risico- inschatting	Mitigerende maatregelen	Restrisico's en risico- inschatting	Eigenaar

Nr.	Restrisico's	Kans	Impact	Risico-inschatting definitief ²



² Indien er een hoog risico overblijft dient er een voorafgaande raadpleging bij de AP geïnitieerd te worden.



Wijze van risico inschatten

Kans / Frequentie	Zeet Groot (ZG)					
	Groot (G)					
	Middel (M)					
	Klein (K)					
	Zeet Klein (ZK)					
		Verwaarloosbaar (V)	Minimaal (Min)	Gemiddeld (Mid)	Maximaal (Max)	Catastrofaal (C)
		Impact				

3. Advies Functionaris Gegevensbescherming

Datum:

Naam:

Advies:

4. Evaluatie DPIA

Datum evaluatie DPIA:



5. Aanvullend advies Functionaris Gegevensbescherming

Datum:

Naam:

Advies:



DTIA (Data Transfer Impact Assessment)

De DTIA wordt ingevuld als uit de Vragenlijst Privacy blijkt dat er gegevens worden gedeeld met partijen buiten de EER en/of partijen buiten de EER toegang hebben tot de gegevens. Zie voor meer informatie [Doorgifte binnen en buiten de EU | Autoriteit Persoonsgegevens](#).

Naam verwerking:

Datum invullen/aanpassen DTIA:

Versienummer:

Nr.	Vragen	Antwoorden
1.	Welke persoonsgegevens worden doorgegeven?	
2.	Aan welk(e) land(en) buiten de EER worden de persoonsgegevens doorgegeven?	
3.	Welk doorgifte instrument wordt gebruikt? Indien er een adequaatheidsbesluit is, hoeft de rest van de DTIA niet ingevuld te worden.	Het doorgifte instrument dat wordt gebruikt is: ☐ Adequaatheidsbesluit, namelijk: ¹ ☐ Standard contractual clauses (SCC) ☐ Binding corporate rules (BCR) ☐ Goedgekeurde gedragscode ☐ Certificeringsmechanisme ☐ Ad hoc contractual clauses ☐ Uitzondering artikel 49 AVG, namelijk:
4.	Beeoordeel het recht en/of de geldende praktijk van de derde landen zoals genoemd bij vraag 2 aan de hand van de WJP Rule of Law Index.	Beeoordeling:
5.	Betrek de CISO en beschrijf de aanvullende maatregelen die nodig zijn om de door te geven gegevens in grote lijnen op het beschermingsniveau te brengen dat voldoen aan de norm die	Beschrijf de aanvullende technische maatregelen: Beschrijf de aanvullende organisatorische maatregelen:

¹ [Adequacy decisions \(europa.eu\)](#).



	geldt in de EER. Zie bijlage 2 van Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data .	Beschrijf de aanvullende contractuele maatregelen:
6.	Welke aanvullende formele procedurele stappen zijn nodig voor de toepassing van de aanvullende maatregelen zoals omschreven bij vraag 5 en hoe worden die toegepast in het doorgifte instrument zoals omschreven bij vraag 3?	Beschrijf aanvullende formele procedurele stappen:
7.	Wanneer wordt de DTIA opnieuw beoordeeld?	Datum evaluatie DTIA:

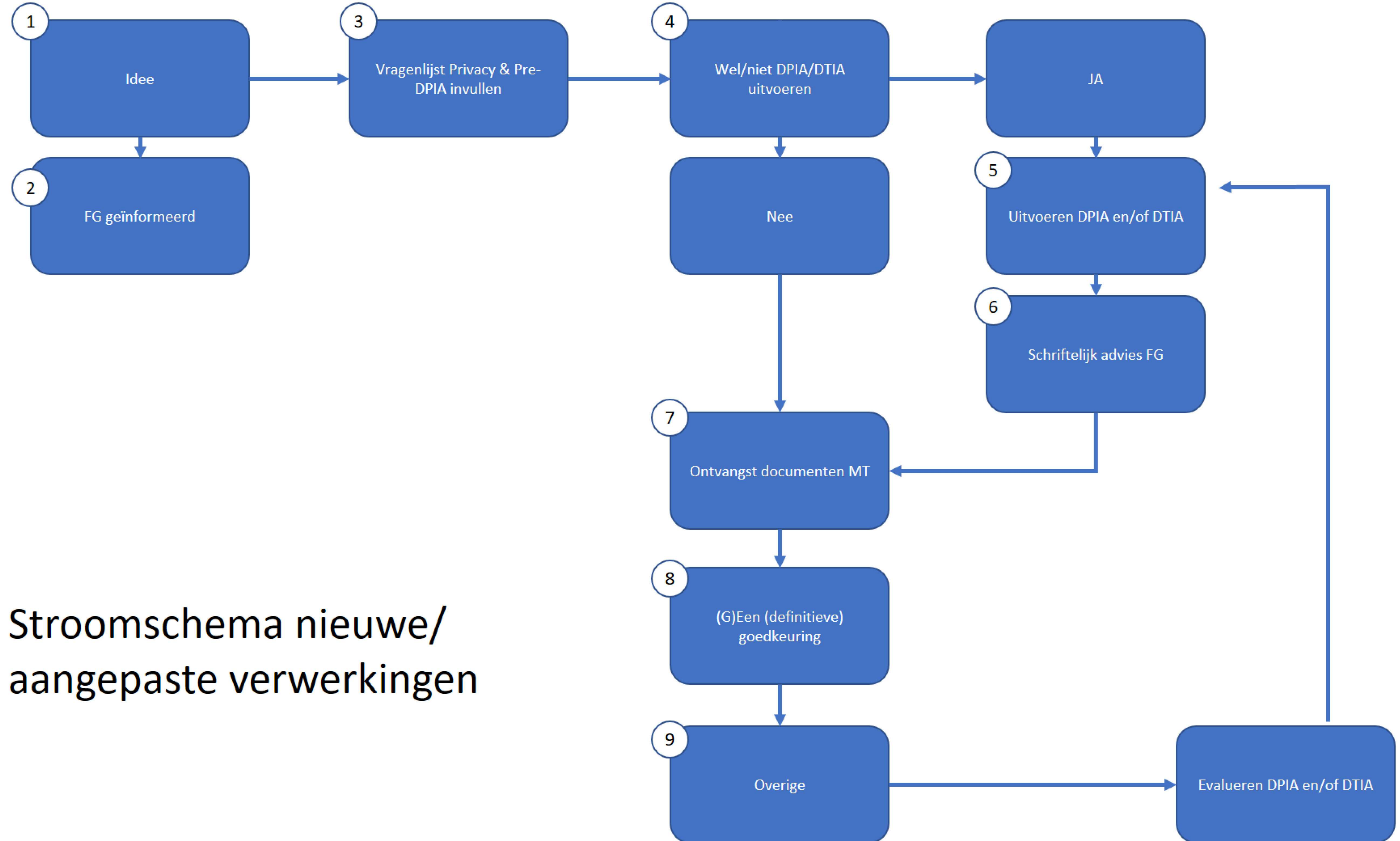
Advies (C)PO (indien noodzakelijk advies FG)

Datum:

Naam:

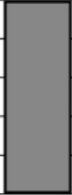
Functie:

Advies:



TOELICHTING STROOMSCHEMA NIEUWE/AANGEPASTE VERWERKING

Versiebeheer

Versie	Datum	Opsteller
V0.1	December 2022	
V0.2	Januari 2023	
V0.3	Januari 2023	
V0.4	Februari 2023	
V0.5	Maart 2023	

De CPO draagt zorg voor het actualiseren van het document. Jaarlijks controleert de CPO of het document herzien dient te worden. De CPO staat genoemd als regiehouder desalniettemin kan de CPO diens taken delegeren aan de PO.

1. Wanneer van toepassing

Het stroomschema is van toepassing als de AP van plan is om¹:

1. Een nieuwe verwerking uit te gaan voeren;
2. Een verwerking wordt aangepast;
3. Een nieuw verwerkingsmiddel aan te schaffen.

Conform artikel 4 lid 2 AVG wordt onder verwerking een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés. Voorbeelden zijn: verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken d.m.v. doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen.

In het kader van deze toelichting wordt onder 'verwerking' verstaan: een *type* verwerking. Concreet betekent dit bijvoorbeeld dat deze wel van toepassing is op het *proces* inhuur van externen, maar vervolgens niet voor elke *individuele* inhuur hoeft te worden ingevuld. Handig hulpmiddel hierbij is dat als het in ons Verwerkingsregister staat en er zijn verder geen afwijkingen ten opzichte van hetgeen daar staat, je dit stroomschema *niet* hoeft te doorlopen. Staat iets niet in ons verwerkingsregister of wijk je er vanaf, dan moet je dit stroomschema wel doorlopen. Bij twijfel: vraag je PO.

Dit stroomschema is daarnaast alleen van toepassing op verwerkingen waar de AP verwerkingsverantwoordelijke is. Als wij verwerker zijn, hoeft dit stroomschema niet gevolgd te worden.

2. Instructie uitvoering

1. Idee.

Wanneer de dossiereigenaar een idee heeft voor een nieuwe of een aangepaste van een verwerking of een nieuw verwerkingsmiddel, dan meldt deze diens voornemen aan de CPO en de PO van de betreffende afdeling. Het aanmelden gebeurt per e-mail naar: [\[redacted\]@autoriteitpersoonsgegevens.nl](mailto:[redacted]@autoriteitpersoonsgegevens.nl) met als onderwerp: nieuwe/aangepaste verwerking/nieuw verwerkingsmiddel + de afdeling waar de verwerking betrekking op heeft.

Actiehouder: dossiereigenaar.

2. FG geïnformeerd.

De CPO informeert de FG dat de organisatie voornemens is een aangepaste of een nieuwe verwerking of een nieuw verwerkingsmiddel te starten.

3. Vragenlijst Privacy en Pre-DPIA invullen.

De dossiereigenaar dient de Vragenlijst Privacy en de Pre-DPIA in te vullen. De PO ondersteunt hierbij en kan tevens advies geven over de verwerking en hoe deze het beste vorm te geven. De Vragenlijst Privacy geeft tevens aan of een DTIA ingevuld moet worden. De Pre-DPIA beantwoordt de vraag of een DPIA uitgevoerd dient te worden. Informatie die je kunt gebruiken om deze vragenlijst in te vullen zijn onder meer het projectplan, de website van contractspartij (privacyverklaring en locatie verwerkingen), een PID, etc.

Actiehouders: PO, CISO en dossiereigenaar. De CPO houdt de regie. De dossiereigenaar is verantwoordelijk voor het proces en het opleveren van de benodigde documenten.

4. Wel/niet DPIA/DTIA uitvoeren.

¹ Dat betekent dat de AP geen uitvoering geeft aan een verwerking voordat het hele proces is doorlopen.

De eindconclusie met onderbouwing om al dan niet een DPIA/DTIA uit te voeren wordt schriftelijk verstrekt aan de CPO door de PO. De CPO stuurt aan de PO een bevestiging van diens conclusie of aanvullend advies met de FG in de cc waarna de dossiereigenaar verder in het proces kan of stuurt met redenen omkleed waarom deze het niet eens met de conclusie. De FG kan hier later op monitoren.

Actiehouders: PO en CPO.

5. Uitvoeren DPIA/DTIA.

Indien dat uit de conclusie blijkt, dient er een DPIA en/of DTIA te worden uitgevoerd. De PO ondersteunt hierbij. De resultaten van de DPIA/DTIA worden versterkt aan de CPO door de PO. Het model voor de DPIA en DTIA zijn te vinden op de Plein-pagina van Privacy & Informatiebeveiliging.

Actiehouders: CPO, PO, CISO en dossiereigenaar. De CPO houdt de regie. De dossiereigenaar is verantwoordelijk dat de DPIA/DTIA wordt ingevuld.

6. Optioneel: schriftelijk advies FG (alleen verplicht bij DPIA/DTIA).

De CPO verstrekt de DPIA/DTIA aan de FG. De FG geeft een schriftelijk advies met betrekking tot de DPIA/DTIA. De FG verstrekt dit advies aan de CPO en de dossiereigenaar.

Actiehouders: CPO en FG.

7. Ontvangst documenten MT.

De Vragenlijst Privacy, de Pre DPIA, (indien uitgevoerd) de DPIA/DTIA en het advies van de FG worden door de CPO verstrekt aan het MT (lid)/Stuurgroep/IV-beraad/bestuur² ter beoordeling.

Actiehouder: dossiereigenaar.

8. (G)een (definitieve) goedkeuring.

Het MT (lid)/Stuurgroep/IV-beraad/bestuur² geeft (g)een (definitieve) goedkeuring. Indien geen (definitieve) goedkeuring wordt gegeven, is het mogelijk om het proces opnieuw te doorlopen.³ De dossiereigenaar informeert de CPO en de FG per e-mail over diens besluit.

Actiehouders: dossiereigenaar.

9. Overige

Indien het MT(lid)/Stuurgroep/IV-beraad, of het bestuur² goedkeuring geeft om het idee uit te voeren, dan dienen **voordat** de verwerking plaatsvindt/verwerkingsmiddel wordt ingezet in ieder geval de navolgende stappen uitgevoerd te worden.

- I. Indien er een verwerker is: afsluiten van de hoofdovereenkomst en de verwerkersovereenkomst. Afsluiten betekent dat beide overeenkomsten zijn ondertekend.

Actiehouders: inkoop. In samenwerking met de dossierhouder, PO en CPO.

- II. Indien er een andere verwerkingsverantwoordelijke is: afsluiten van een (gezamenlijke) verwerkingsverantwoordelijke overeenkomst.

Actiehouders: dossiereigenaar. In samenwerking met staftaken, PO en CPO.

- III. Zodra bovenstaande is geregeld dienen de volgende zaken nog geregeld te worden:

1. Aanpassen van het verwerkingenregister;

Actiehouder: CPO met input van de dossiereigenaar.

2. Privacybeleid en/of privacy verklaring aanpassen;

² Welk van deze gremia is afhankelijk van de vraag wie verantwoordelijk is voor de verwerking.

³ De verwerking wordt in de tussentijd niet gestart.

Actiehouder: dossiereigenaar samen met de CPO en PO.

3. Evt. toestemmingsverklaringen laten ondertekenen en borgen;

Actiehouder: dossiereigenaar met advies van de CPO en PO.

Alle documentatie wordt verstrekt aan de CPO ter registratie, afsluiting en bewaring. Bij documenten waarvoor geen akkoord is gegeven worden deze wel verstuurd aan de CPO. Deze zal de betreffende documenten bewaren, zodat voldaan wordt aan de accountability vereisten.

Het kan voorkomen dat later in het traject, bijvoorbeeld na selectie van een leverancier, meer/andere informatie bekend wordt. Op dat moment moet de dossiereigenaar in overleg met de PO bekijken welke documenten moeten worden aangepast, wat dit betekent voor de risico's van de verwerking en of er nieuwe documenten moeten worden ingevuld (bijvoorbeeld als nog een DPIA of DTIA).

3. Werkwijze DPIA

Als de Autoriteit Persoonsgegevens voornemens is een aangepaste en/of een nieuwe verwerking te starten dan dient ook de Pre-DPIA uitgevoerd te worden. De Pre-DPIA bepaalt of volstaan kan worden met het invullen van de Vragenlijst Privacy of dat een DPIA uitgevoerd moet worden. In veel gevallen zal een DPIA niet nodig zijn.

De DPIA geeft geen antwoord op de vraag of de verwerking conform de AVG is. De DPIA laat zien welke risico's verbonden zijn aan de verwerking. Door die risico's zorgvuldig in kaart brengen en te wegen, kan weloverwogen een keuze gemaakt worden om risico's te beperken/mitigeren dan wel een verwerking al dan niet uit te voeren.

De Pre-DPIA en de DPIA worden ingevuld door de dossiereigenaar, samen met de PO, de CPO en de CISO.

De DPIA is meer omvangrijk. De CPO is regiehouder en bepaalt welke mensen betrokken dienen te worden bij het opstellen van de DPIA. De dossiereigenaar is altijd betrokken. De betrokken personen bij het opstellen van een DPIA kunnen zijn:

- CPO
- PO
- CISO
- Verwerker en/of (gezamenlijk) verwerkingsverantwoordelijke
- Overige inhoudsdeskundige(n)
- FG (voor advies).

4. Werkwijze DTIA

Voor een aantal vragen in de DTIA is het handig om deze website te gebruiken: [WJP Rule of Law Index \(worldjusticeproject.org\)](https://www.worldjusticeproject.org/).



Vragenlijst Privacy (aangepaste en/of nieuwe verwerking/verwerkingsmiddel)

Datum invullen/aanpassen vragenlijst:

Versienummer:

Nr.	Vragen	Antwoorden
1.	Naam contactpersoon en afdeling?	Naam contactpersoon: Afdeling:
2.	Start- en einddatum aangepaste en/of nieuwe verwerking?	Startdatum: Einddatum:
3.	Naam van de verwerking en beschrijf de verwerking?	Naam verwerking: Beschrijving verwerking:
4.	Wat is het doel van de verwerking? - Proportionaliteit: staat de inbreuk op de persoonlijke levenssfeer en de bescherming van de persoonsgegevens van de betrokkenen in evenredige verhouding tot de doeleinden? - Subsidiariteit: kunnen de doeleinden in redelijkheid niet op een andere, voor de betrokkenen minder nadelige wijze, worden verwezenlijkt? - Als 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.	Doel verwerking:



Nr.	Vragen	Antwoorden
5.	Welke van de in de AVG genoemde rechtsgrond is van toepassing? - Indien gekozen wordt voor toestemming: is deze geregistreerd en zo ja, waar? Registratie is verplicht. - Indien gekozen wordt voor wettelijke verplichting of taak van algemeen belang: benoem de wet en het wetsartikel? - Indien gekozen wordt voor gerechtvaardigd belang: vul de gerechtvaardigd belang toets in (zie voor meer informatie https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/mag-u-persoonsgegevens-verwerken#hoe-toetst-u-of-u-zich-mag-baseren-op-de-grondslag-gerechtvaardigd-belang-7531).	☐ <i>Toestemming</i> Geregistreerd: ☐ Ja, waar: ☐ Nee, omdat: ☐ <i>Uitvoering van een overeenkomst</i> ☐ <i>Wettelijke verplichting</i> Benoem wet: Benoem wetsartikel: ☐ <i>Vitale belangen</i> ☐ <i>Taak van algemeen belang</i> Benoem wet: Benoem wetsartikel: ☐ <i>Gerechtvaardigd belang</i> Uitvoeren toets: • Gerechtvaardigd (zijn de belangen van de AP of een derde te kwalificeren als gerechtvaardigd?): • Noodzakelijk (is het noodzakelijk om dit belang te behartigen?, zie proportionaliteit en subsidiariteit toets bij vraag 4.): • Afweging belangen (afweging tussen de belangen van de AP of derde enerzijds en de belangen van de betrokkene anderzijds?):



Nr.	Vragen	Antwoorden
6.	Benoem de categorieën van betrokkenen?	Categorieën betrokkenen:
7.	Benoem de categorieën van persoonsgegevens? - Indien bijzondere, gevoelige of strafrechtelijke persoonsgegevens: benoem welke en uitzonderingsgrond aanwezig?	Categorieën persoonsgegevens: Gevoelige persoonsgegevens: ☐ Gegevens over elektronische communicatie ☐ Locatiegegevens ☐ Financiële gegevens ☐ Anders, namelijk: Bijzondere persoonsgegevens: ☐ Ras of etnische afkomst ☐ Politieke opvattingen ☐ Religieuze of levensbeschouwelijke overtuigingen ☐ Lidmaatschap vakbond ☐ Genetische gegevens ☐ Biometrische gegevens ☐ Gezondheidsgegevens ☐ Seksueel gedrag of seksuele gerichtheid Strafrechtelijke persoonsgegevens: ☐ Strafrechtelijke veroordelingen en strafbare feiten Benoem wet en wetsartikel als er sprake is van een uitzonderingsgrond verwerken bijzondere persoonsgegevens:



Nr.	Vragen	Antwoorden
8.	Benoem de categorieën van ontvangers en de namen van de ontvangers?	Categorieën ontvangers: Namen ontvangers:
9.	Worden de gegevens gedeeld met partijen buiten de EER en/of hebben partijen buiten de EER toegang tot de gegevens? - Zo ja, is er een DTIA uitgevoerd?	Partijen buiten de EER: ☐ Ja, welke: ☐ Nee Partijen buiten EER toegang tot gegevens: ☐ Ja, welke: ☐ Nee DTIA uitgevoerd: ☐ Ja ☐ Nee
10.	Wat is de bewaartermijn van de persoonsgegevens en per wanneer gaat de bewaartermijn in? - Als er geen wettelijke grondslag van toepassing is, dan dient een uitleg toegevoegd te worden ter onderbouwing van de bewaartermijn	Bewaartermijn: Ingangsdatum bewaartermijn: Wettelijke grondslag aanwezig: ☐ Ja, welke: ☐ Nee, uitleg:
11.	Wat zijn de genomen beveiligingsmaatregelen en is dit afgestemd met de CISO? - Zo ja, voeg diens schriftelijke advies toe.	Beveiligingsmaatregelen: Afgestemd met CISO:



Nr.	Vragen	Antwoorden
	- Zo nee, stem met CISO af.	☐ Ja: voeg schriftelijk advies toe: ☐ Nee: stem met CISO af en voeg schriftelijk advies alsnog toe.
12.	Wordt voor de verwerking gebruik gemaakt van een verwerker en subverwerkers? - Zo ja, is er een verwerkersovereenkomst nodig en/of afgesloten? - Benoem de contactgegevens van de FG of contactpersoon van de verwerker.	Verwerker: ☐ Ja, verwerkersovereenkomst nodig/afgesloten: ☐ Nee Contactgegevens FG of contactpersoon verwerker: Subverwerkers: ☐ Ja, namen partijen: ☐ Nee
13.	Wordt er gebruik gemaakt van geautomatiseerde besluitvorming of profilering? - Zo ja, vul een DPIA in.	Geautomatiseerde besluitvorming: ☐ Ja, vul een DPIA in ☐ Nee Profilering: ☐ Ja, vul een DPIA in ☐ Nee
14.	Wordt er gebruik gemaakt van een (nieuwe) applicatie? - Zo ja, hoe heet deze applicatie en waar vindt de verwerking van persoonsgegevens plaats?	(Nieuwe) applicatie: ☐ Ja: Naam: Waar vindt verwerking persoonsgegevens plaats:



Nr.	Vragen	Antwoorden
		☐ Nee
15.	Hoe komt de AP aan de persoonsgegevens?	Beschrijf:
16.	Heb je rekening gehouden met privacy by Design & privacy by Default? - Zo ja, hoe? - Zo nee, waarom niet?	Rekening gehouden met Privacy by Design & Privacy by Default: ☐ Ja, hoe: ☐ Nee, omdat:
17.	Wat is de uitkomst van de pre-DPIA?	Uitkomst pre-DPIA:

Advies (C)PO (indien noodzakelijk advies FG)

Datum: Naam: Functie: Advies:
--