Privacy Impact Assessment

[Naam PIA]

Privacy Impact Assessment

Documentbeschrijving

PIA Versiehistorie Template

Versie	Datum	Samenvatting van de wijzigingen
1.0	22-08-2018	Versiehistorie geschoond t.b.v. publicatieversie
1.0	04-09-2018	SVB-template veralgemeniseerd tbv publicatie via CIP[1]

Verspreiding

Versie	Datum	Verspreid naar
1.0	04-09-2018	CIP community (https://cip.pleio.nl/)

PIA Versiehistorie [Naam PIA]

Versie	Datum	Samenvatting van de wijzigingen

[1] Dit PIA template is in 2018 ontwikkeld door de Sociale Verzekeringsbank (SVB) voor eigen gebruik. Ten behoeve van publicatie via de kanalen van CIP is het template veralgemeniseerd.

Privacy Impact Assessment

Reviews

REVIEW		
Akkoord / commitment (toekomstig) proces/data eigenaar	**Eventuele voorwaarden voor akkoord**	**Datum akkoord**
[Naam eigenaar + mail waarin akkoord is gegeven]		
Voor gezien Privacy Coördinator	**Eventuele toelichting**	**Datum van gezien**
[Naam PC + mail waarin deze is doorgezet]		
Voor gezien Functionaris gegevensbescherming	**Eventueel advies**	**Datum van gezien**
[Naam FG + mail waarin deze is doorgezet]		

Privacy Impact Assessment

Inleiding

Een Privacy Impact Assessment (PIA) is een instrument om privacyrisico's van een gegevensverwerking in een vroegtijdig stadium op een gestructureerde en heldere manier in kaart te brengen. Daarnaast is de PIA een middel om verantwoordelijken te stimuleren om zich bewust te zijn van en verantwoordelijkheid te nemen voor een zorgvuldige verwerking van persoonsgegevens. Met een PIA is het mogelijk om een transparante afweging te maken tussen de privacyrisico's van verschillende alternatieven en om te rapporteren over de impact die het voorstel heeft voor de privacy van de betrokkenen. Op deze manier kan de onze organisatie voldoen aan:

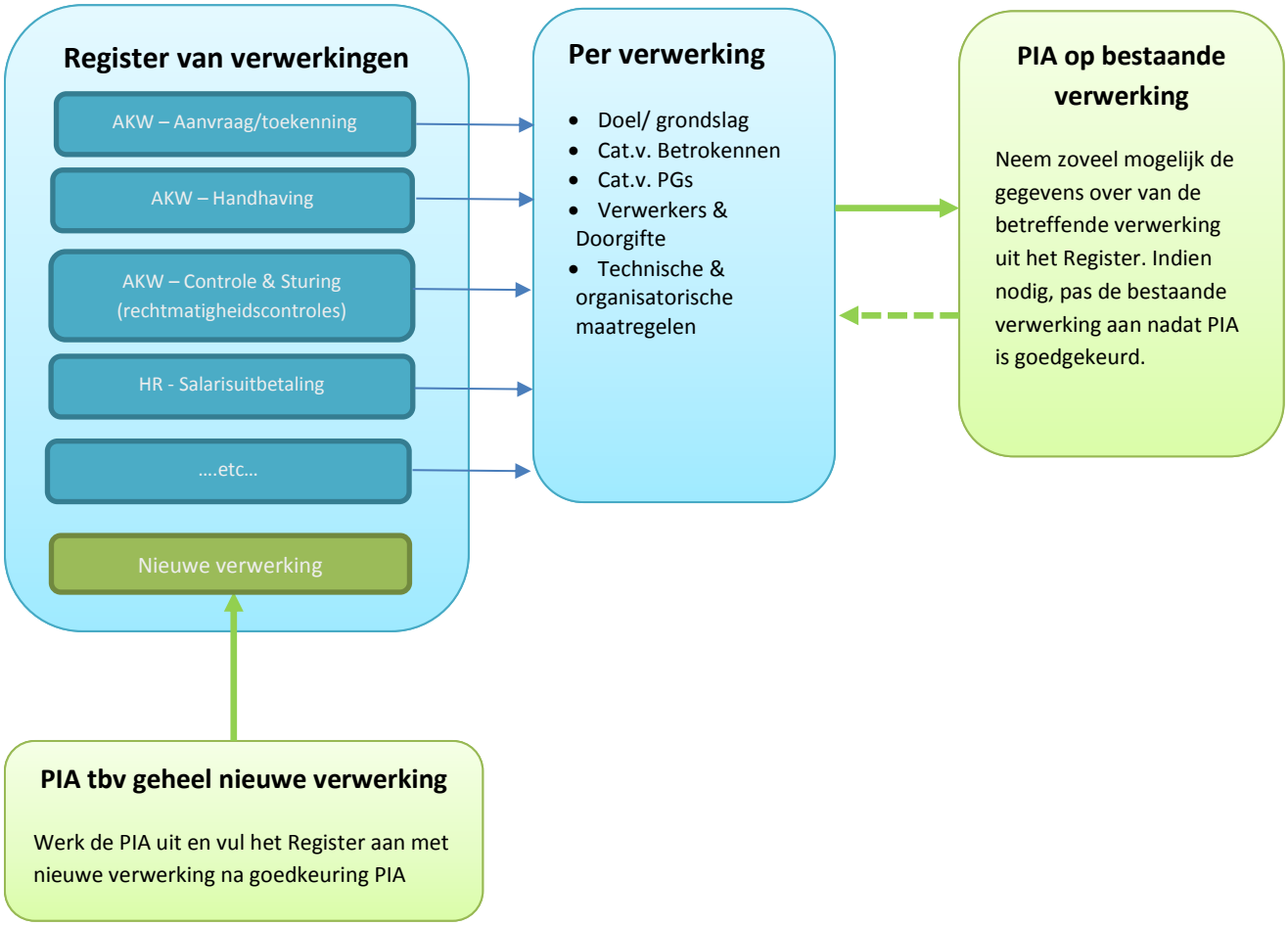
- documentatieplicht, welke afwegingen hebben aan een besluit ten grondslag gelegen en
- verantwoordingsplicht voor het verwerken van persoonsgegevens. Gebruik van een PIA vergroot tevens de privacybewustzijn.

De eerste pagina's van deze PIA template betreft een blanco template. In de bijlage is een versie opgenomen inclusief toelichting. In de bijlage is eveneens het proces opgenomen dat doorlopen dient te worden bij het opstellen van een PIA.

Deze PIA template dient gebruikt te worden bij het uitvoeren van PIA's binnen de onze organisatie. Deze template volgt de opzet zoals deze eveneens voor het Register van verwerkingsactiviteiten wordt gehanteerd. In het geval er een PIA uitgevoerd gaat worden naar aanleiding van een wijziging, kan gestart worden met de huidige vastlegging in het Register en kunnen hier de wijzigingen op doorgevoerd worden. Voor meer informatie over de reeds beschikbare informatie in het Register, neem contact op met de Privacy Coördinator van betreffende Directie waar het voorstel onder valt (voor de "kleinere" directies met de Coördinator Informatiebeveiliging). Zie voor de contactgegevens de contactpagina van IB.

Zie hieronder (volgende pagina) schematische weergave in de relatie tussen de PIA en het Register van verwerkingen en hoe het Register kan ondersteunen bij het uitwerken van de PIA. In veel gevallen zal er een PIA worden uitgevoerd op een bestaande verwerking (aanpassing van systeem, uitbreiding van bestaand proces etc) en dat betekent dat het hierbij handigst is om de bestaande gegevens die we hebben met betrekking tot de verwerking uit het Register op te halen en in de PIA alvast in te vullen.

Privacy Impact Assessment



Privacy Impact Assessment

A. Beschrijving algemene kenmerken gegevensverwerkingen

Beschrijf op gestructureerde wijze de voorgenomen gegevensverwerkingen, de verwerkingsdoeleinden en de belangen bij de gegevensverwerkingen. Indien er sprake is van een wijziging op een bestaande regeling, geef in rode letters aan welke algemene gegevens/aspecten anders of nieuw zijn ten opzicht van de bestaande verwerking.

ALGEMEEN		
1a. Voorstel		
1b. Betreft dit een bestaande verwerking?		
1c. Verwerkingsnaam	**1d. Categorieën verwerkingen**	**1e. Verbonden verwerkingen**
		Nee
1f. Verbonden assessments		
2a. BETROKKEN PARTIJEN		
2b. Verantwoordelijken	**2c. Verwerkers**	**2d. Categorieën betrokkenen**
Onze organisatie		
2f. Uitvoerende entiteiten	**2g. Ontvangers**	

VERWERKTE PERSOONSGEGEVENS			
	Eventueel type pers.geg.		
3a. Persoonsgegevens	**3b. Bijzonder pers.geg.**	**3c. Gevoelig**	**3d. Nat. ID-nummer**
3e. Gegevensbron	**3f. Bewaartermijnen van persoonsgegevens in gegevensbronnen**	**3g. Motivatie bij bewaartermijn**	
3h. Technische en organisatorische maatregelen			

3i. Kenmerken verwerking	
	Geldt een van de volgende kenmerken voor het project/voorstel/beleidsvoornemen:
☐	Geautomatiseerde verwerking/besluitvorming[2], waaronder profilering[3]
☐	Grootschalige[4] verwerking van (bijzondere) persoonsgegevens
☐	Verwerking persoonsgegevens met betrekking tot misdaad
☐	Systematische bewaking van openbare ruimten
☐	Categorie verwerkingen op de lijst van de Autoriteit Persoonsgegevens (nog niet beschikbaar)

JURIDISCHE KWALIFICATIES		
4.a Verwerkingsdoel	**4b. Verwerkingsgrondslagen**	**4c. Internationale overdrachten**

[2] Besluiten die voor de betrokkenen rechtsgevolgen hebben of hem anderszins in aanmerkelijke mate treffen, zijn in beginsel verboden.
[3] Elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd. Dit om zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen.
[4] Analyse van grote hoeveelheden gestructureerde en ongestructureerde data uit verschillende bronnen waarbij geautomatiseerd naar correlaties wordt gezocht die kennis kunnen opleveren om te kunnen toepassen voor beslissingen op groeps- of individueel niveau.

	-	

4d. Toelichting Juridische en beleidsmatig kader

Privacy Impact Assessment

B. Beoordeling gegevensverwerkingen

<table>
<tr><th colspan="3">BEOORDELING</th></tr>
<tr><th colspan="3">5a. Rechtmatigheid: Noodzaak en evenredigheid</th></tr>
<tr><td colspan="3"></td></tr>
<tr><th colspan="3">5b. Risico’s</th></tr>
<tr><td colspan="3"></td></tr>
<tr><th colspan="2">5c. Toepasselijke risico’s</th><th>5d. Overige risico’s</th></tr>
<tr><td>☐</td><td>Gebruik van persoonsgegevens in gevoelige contexten</td><td rowspan="4"></td></tr>
<tr><td>☐</td><td>Gebruik van persoonsgegevens van minderjarigen</td></tr>
<tr><td>☐</td><td>Een groot aantal betrokkenen</td></tr>
<tr><td>☐</td><td>Gebruik van nieuwe technologieën</td></tr>
<tr><th colspan="3">Maatregelen</th></tr>
<tr><th colspan="3">5e. Privacy by design en privacy by default maatregelen</th></tr>
<tr><td colspan="3"></td></tr>
<tr><th colspan="2">5f. Maatregelen voor juistheid</th><th>5g. Mitigeren van risico's</th></tr>
<tr><td colspan="2"></td><td></td></tr>
<tr><th colspan="3">5h. Rechten van de betrokkenen</th></tr>
<tr><td colspan="3"></td></tr>
<tr><th colspan="3">5i. Register</th></tr>
<tr><td colspan="3"></td></tr>
</table>

Privacy Impact Assessment

C. Samenvatting acties

In het overzicht hieronder zijn alle acties opgenomen die in de PIA zijn genoemd.

ACTIES		
Omschrijving	**Actiehouder**	**Deadline oplevering**
3g. Motivatie bij bewaartermijn	-	-
3h. Technische en organisatorische maatregelen	-	-
4c. Internationale overdrachten	-	-
5e. Privacy by design en privacy by default maatregelen	-	-
5f. Maatregelen voor juistheid	-	-
5g. Mitigeren van risico's	-	-
5h. Rechten van de betrokkenen	-	-
5i. Register	-	-

Privacy Impact Assessment
BIJLAGE 1 – TEMPLATE INCLUSIEF TOELICHTING

A. Beschrijving algemene kenmerken gegevensverwerkingen

Proces: De verantwoordelijke voor het betreffende bedrijfsproces of het bedrijfsmiddel of een verantwoordelijke projectmanager/medewerker neemt contact op met de PC/CIB/ISO/ISC voor een Intake. Als onderdeel van de Intake worden de "verwerkingen" besproken om de verantwoordelijke op weg te helpen met het vullen van hoofdstuk A (dit hoofdstuk) en worden de relevante expertises vastgesteld die betrokken worden bij de PIA. Als onderdeel van de Intake worden (waar mogelijk) de tijdslijnen/oplevermomenten vastgesteld en de werkzaamheden al ingepland (een voorlopige afspraak - incl. de relevante expertises - voor het bespreken van hoofdstuk B wordt al ingepland door de PC/CIB/ISO/ISC).

Na de intake verzamelt de verantwoordelijke de relevante informatie voor het vullen van hoofdstuk A en levert een eerste ingevulde versie op aan de PC/CIB/ISO/ISC. De PC/CIB/ISO/ISC beoordeelt de eerste ingevulde versie en stemt af / geeft (eventuele) adviezen ter verbetering. Vervolgens neemt de PC/CIB/ISO/ISC de lead voor het vullen van hoofdstuk "B. Beoordeling gegevensverwerkingen".

Beschrijf op gestructureerde wijze de voorgenomen gegevensverwerkingen, de verwerkingsdoeleinden en de belangen bij de gegevensverwerkingen. Indien er sprake is van een wijziging op een bestaande regeling, geef in rode letters aan welke algemene gegevens/aspecten anders of nieuw zijn ten opzicht van de bestaande verwerking. Bij een volledig nieuwe verwerking hoeft niet alles rood gearceerd te worden, alleen datgene wat dan organisatorisch nieuw zou zijn (bijvoorbeeld een nieuwe verwerker waardoor ook een verwerkersovereenkomst opgesteld moet worden).

Voorbeeld 1: bij een toevoeging van een BSN nummer aan een bestaande verwerking waar voorheen dit gegeven nog niet was opgenomen, arceer in 3a en 3d BSN dan rood. Zodoende is zichtbaar wat er is veranderd. Bij een compleet nieuwe verwerking is het niet noodzakelijk alle velden rood te arceren.

Voorbeeld 2: Bij een compleet nieuwe verwerking moet bij 1b 'nee' worden aangegeven en dan hoeft sectie 3 niet compleet rood te worden gearceerd omdat dan reeds bekend is dat dit een nieuwe verwerking betreft waarbij in theorie alle persoonsgegevens derhalve opnieuw bekeken dienen te worden (voor deze nieuwe verwerking) . Het is wel van belang om dan aan te geven of er organisatorisch iets nieuws is: bijvoorbeeld bij 2c 'verwerkers' om aan te geven dat het een nieuwe verwerker ook betreft.

ALGEMEEN		
1a. Voorstel		
[Beschrijf in hoofdlijnen hoe het project/voorstel/beleidsvoornemen eruit ziet. Geef daarbij aan wie (functie) gedelegeerd verwerkingsverantwoordelijke (bv. proces/data-eigenaar) is voor het project/voorstel/beleidsvoornemen, wie heeft opdracht gegeven?]		
1b. Betreft dit een bestaande verwerking?		
[Geef met Ja of nee aan of dit een bestaande verwerking is, en controleer of de verwerking reeds in het Register is opgenomen. Indien dit en bestaande verwerking is, gebruik bij 1c de naam van de bestaande verwerking uit het Register		
1c. Verwerkingsnaam	**1d. Categorieën verwerkingen**	**1e. Verbonden verwerkingen**
[Korte heldere verwerkingsnaam. I.g.v. SV of PGB domein wordt hier de naam van de Regeling opgenomen. I.g.v. bedrijfsvoering wordt bijvoorbeeld "Loopbaanbegeleiding" opgenomen. Bij bestaande	[Geef een overzicht van de voorgenomen gegevensverwerkingen van het project/voorstel/ beleidsvoornemen. Beschrijf o.a. - het moment van verzamelen, - het moment van vernietigen.	[Geef aan of er verwerkingen zijn vastgelegd die een relatie hebben met deze verwerking. Indien er sprake is van een bestaande registerregel die aangepast wordt

verwerkingen: neem de naam uit het Register over]	- de processtappen die onderkend worden (Verwerken aanvraag, Uitvoeren betaling etc)]	dient hier opgenomen te worden welke regel dit is.]
1f. Verbonden assessments		
[Geef aan of er al PIA's zijn uitgevoerd die een relatie hebben met deze verwerking.]		
2a. BETROKKEN PARTIJEN		
[Geef aan of er andere organisaties zijn betrokken bij de gegevensverwerking. Beschrijf wat de rollen per organisatie zijn, verwerkingsverantwoordelijke[5], verwerker[6], verstrekker en ontvanger. Benoem ook welke functies binnen de onze organisatie (directie, afdeling) en andere organisaties toegang krijgen tot welke persoonsgegevens.]		
2b. Verantwoordelijken	**2c. Verwerkers**	**2d. Categorieën betrokkenen**
Onze organisatie	[Benoem de andere organisaties die zijn betrokken bij het verwerken van de persoonsgegevens namens de ONZE ORGANISATIE als Verwerker. Dit zijn tevens eventuele IT hosting partijen. Overige Verwerkingsverantwoordelijken moeten niet hier opgenomen worden maar onder Betrokken Partijen]	[Van welke categorieën van betrokkenen gaan persoonsgegevens verwerkt worden. Voorbeelden: Aanvrager, Verzekerden, Pensioengerechtigden, Nabestaanden, Kinderen van verzekerden, Medewerker, Slachtoffer, Gemachtigden, Sollicitant]
2f. Uitvoerende entiteiten	**2g. Ontvangers**	
[Binnen welke afdeling wordt de daadwerkelijke verwerking uitgevoerd/wie is data-eigenaar. Bijvoorbeeld DSV – Proceseigenaar V&O; DPGB – Manager Dienstverlening; of HR, I&F – Manager Facilities]	[Een ontvanger is een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, al dan niet een derde, aan wie/waaraan de persoonsgegevens worden verstrekt (niet zijnde de betrokkene). Interne afdelingen dienen niet als ontvangers opgenomen te worden, deze kunnen opgenomen worden bij Uitvoerende entiteiten. Voorbeelden: infrastructuurdienstverlener, Pensioenfondsen, Gemeenten en Zorgkantoren]	

[5] een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen.

[6] een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/ dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt

Privacy Impact Assessment

<table>
<tr><th colspan="4">VERWERKTE PERSOONSGEGEVENS</th></tr>
<tr><td></td><td colspan="3">Eventueel type pers.geg.</td></tr>
<tr><td>3a. Persoonsgegevens</td><td>3b. Bijzonder pers.geg.</td><td>3c. Gevoelig</td><td>3d. Nat. ID-nummer</td></tr>
<tr><td>[Som alle categorieën persoonsgegevens op die worden verwerkt en geef aan of ze vallen onder de typen: bijzonder, gevoelig of wettelijk identificatienummer. Klik op de volgende link naar ‘Checklist Persoonsgegevens’ op de Intranet Pirvacy Portal Voorbeelden: Naw-gegevens, contactgegevens (zoals telefoonnummer, emailadres), Geboortedatum of leeftijd, Burgerlijke staat/leefsituatie, Relatie tot een kind (eigen kind, aangehuwd kind, pleegkind), Inkomensgegevens, schuldstand]</td><td>[Categorieën:
• geg. waaruit ras of etnische afkomst blijkt.
• geg. waaruit politieke opvattingen blijken,
• geg. waaruit religieuze of levensbeschouwelijke overtuigingen blijken,
• geg. waaruit het lidmaatschap van een vakbond blijkt,
• genetische of biometrische gegevens die worden verwerkt met het oog op de unieke identificatie van een persoon,
• gegevens over gezondheid,
• gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid.]</td><td>Gevoelige gegevens betreffen gegevens over de financiële of economische situatie van een betrokkene, gegevens die kunnen leiden tot stigmatisering of uitsluiting van een betrokkene, gegevens die betrekking hebben op kwetsbare groepen, inloggegevens, gebruikersnamen, en gegevens die kunnen worden misbruikt voor (identiteits)fraude.</td><td>Is er sprake van gebruik van BSN of andere internationale ID nummers</td></tr>
<tr><td>3e. Gegevensbron</td><td>3f. Bewaartermijnen van persoonsgegevens in gegevensbronnen</td><td colspan="2">3g. Motivatie bij bewaartermijn</td></tr>
<tr><td>[Middelen die een rol spelen bij de verwerking. Dit kan zijn een applicatie/systeem, bestanden, fysieke dossiers, maar eveneens de betrokkene zelf.]</td><td>[Bepaal en motiveer de bewaartermijnen van de persoonsgegevens aan de hand van de verwerkingsdoeleinden. Kijk daarbij eerst of er een wettelijke plicht bestaat om de gegevens te bewaren. Zo niet, stel de bewaartermijn vast aan de hand van het noodzakelijkheidscriterium (neem hiervoor contact op met Recordmanagement die e.e.a. reeds heeft vastgesteld in de Selectielijst waarin bewaartermijnen zijn gedefinieerd binnen onze organisatie). Bepaal daarvoor de datum waarop het procesdoel is behaald.]</td><td colspan="2">[Bepaal en motiveer of de gegevens gedurende de hele bewaartermijn actueel, juist en volledig gehouden worden. Ga na of de risico’s op ongewenste verspreiding bij langer bewaren klein zijn. Overweeg anonimiseren van de te bewaren gegevens. Hoe wordt geborgd dat gegevens ook inderdaad vernietigd/onbruikbaar gemaakt/geanonimiseerd worden? Noem de functie die hiervoor verantwoordelijk is.]</td></tr>
<tr><td colspan="4">3h. Technische en organisatorische maatregelen</td></tr>
<tr><td colspan="4">[Naast de voor onze organisatie generieke maatregelen (zoals fysieke toegangsbeveiliging pand, geheimhoudingsverklaringen en gedragscodes personeel), welke specifieke maatregelen zijn geïmplementeerd m.b.t. de verwerkingsactiviteit. Denk hierbij aan:
a) Gebruik maken van rollen en functiescheiding (autorisatiemanagement)
b) Medewerkers expliciet toegang verschaffen tot gegevens die ze op dat moment nodig hebben (whitelisting)
c) Logging en controle van alle handelingen m.b.t. persoonsgegevens
d) Periodieke beoordeling van technische kwetsbaarheden (OWASP top 10)
e) Encryptie (versleuteling) van bestanden
f) Beveiliging van externe netwerkverbindingen (bij doorgifte buiten onze organisatie)
g) Pseudonimisering van persoonsgegevens
h) Anonimiseren van persoonsgegevens

Beschrijf op welke wijze en met gebruikmaking van welke (technische) middelen en methoden de persoonsgegevens worden verwerkt en hoe Privacy by Design aspecten zijn meegewogen/geïmplementeerd in de verwerking en/of het</td></tr>
</table>

systeem.

[Voor ondersteuning bij het beantwoorden van deze vraag kan IB en IT betrokken worden.

3i. Kenmerken verwerking	
	Geldt een van de volgende kenmerken voor het project/voorstel/beleidsvoornemen:
☐	Geautomatiseerde verwerking/besluitvorming[7], waaronder profilering[8]
☐	Grootschalige[9] verwerking van (bijzondere) persoonsgegevens
☐	Verwerking persoonsgegevens met betrekking tot misdaad
☐	Systematische bewaking van openbare ruimten
☐	Categorie verwerkingen op de lijst van de Autoriteit Persoonsgegevens (https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/wp248_rev.01_nl.pdf)

JURIDISCHE KWALIFICATIES		
4.a Verwerkingsdoel	**4b. Verwerkingsgrondslagen**	**4c. Internationale overdrachten**
[Beschrijf het doel[10], zowel de hoofd als de nevendoeleinden, van de voorgenomen gegevensverwerkingen. Doe dit voldoende SMART. Voorbeelden nevendoelen: - Emailadres: noodzakelijk voor communicatie met de betrokkene; - IP-adres: noodzakelijk ter verificatie dat alleen vanuit een bepaalde locatie contact wordt gemaakt met het systeem; - Adresgegevens: noodzakelijk om een beschikking naar de betrokkene te kunnen toezenden; - Financiële gegevens: noodzakelijk om vast te stellen of de betrokkene partij in aanmerking komt voor een toeslag; - Strafrechtelijke gegevens: noodzakelijk om een screening te kunnen uitvoeren.] Geef eveneens aan of het gebruik van de persoonsgegevens in lijn is met het doel van het verzamelen. Als de gegevens voor andere doelen of bedrijfsprocessen verwerkt dan waar ze oorspronkelijk zijn verzameld, beoordeel of deze verwerking past bij	[Bepaal (evt. in overleg met JZ) op welke rechtsgronden uit de AVG de gegevensverwerkingen worden gebaseerd. De AVG geeft als beginsel dat persoonsgegevens moeten worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is. De AVG onderkent 6 grondslagen en tenminste 1 van onderstaande dient gekozen te worden. In geval van sub c of e dient het veld 4d. ‘ Toelichting Juridische en beleidsmatig kader” uitgewerkt te worden waarin tenminste de van toepassing zijnde wetsartikelen worden benoemd. - Artikel 6 lid 1 sub a AVG: toestemming - Artikel 6 lid 1 sub b AVG: uitvoering overeenkomst - Artikel 6 lid l sub c AVG: wettelijke verplichting - Artikel 6 lid l sub d AVG: bescherming vitale belangen - Artikel 6 lid 1 sub e AVG: vervulling van een taak van algemeen belang of openbaar gezag - Artikel 6 lid l sub f AVG: gerechtvaardigd belang]	[Is er sprake van doorgifte van persoonsgegevens buiten de EU. Zo ja, benoem in welke Niet-EU-landen de voorgenomen gegevensverwerkingen plaatsvinden. De locaties waar de voorgenomen gegevensverwerkingen plaatsvinden, kunnen aanvullende privacy-risico’s met zich brengen en daarom onderworpen zijn aan strengere regels en aanvullende maatregelen vereisen.]

[7] Besluiten die voor de betrokkenen rechtsgevolgen hebben of hem anderszins in aanmerkelijke mate treffen, zijn in beginsel verboden.
[8] Elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd. Dit om zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen.
[9] Analyse van grote hoeveelheden gestructureerde en ongestructureerde data uit verschillende bronnen waarbij geautomatiseerd naar correlaties wordt gezocht die kennis kunnen opleveren om te kunnen toepassen voor beslissingen op groeps- of individueel niveau.
[10] Persoonsgegevens mogen enkel voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld. De vaststelling van de verwerkingsdoeleinden is een noodzakelijk voorwaarde om te kunnen beoordelen of de voorgenomen gegevensverwerkingen rechtmatig zijn en om vast te stellen welke maatregelen moeten worden getroffen om de risico’s te voorkomen of verkleinen. Omschrijf daarom per voorgenomen gegevensverwerking de verwerkingsdoeleinden zo specifiek mogelijk

het oorspronkelijke doel van verzamelen.		

4d. Toelichting Juridische en beleidsmatig kader

[Benoem i.g.v. verwerkingsgrondslag “wettelijke verplichting” of “taak van algemeen belang of openbaar gezag” de wet- en regelgeving, met uitzondering van de AVG, en het beleid met mogelijke gevolgen voor de voorgenomen gegevensverwerkingen. Noem ook de wetgeving waaruit blijkt dat gebruik van een wettelijk identificatienummer is toegestaan. Voorbeelden:

- Artikel 62 Wet Suwi
- Artikel 64 Participatiewet

Beschrijf i.g.v. verwerkingsgrondslag “algemeen belang” alle belangen die de verwerkingsverantwoordelijke, betrokkene en derden hebben bij de voorgenomen gegevensverwerkingen. Voorbeelden zijn:

- bedrijfs- en commerciële belangen (ten behoeve van gepersonaliseerde dienstverlening),
- handhaving van juridische vorderingen,
- toezicht op medewerkers ten behoeve van veiligheid en management doeleinden,
- (nationale of openbare) veiligheid, zoals de preventie van fraude, misbruik, netwerkbeveiliging en gezondheid.

Bij de noodzaak van gegevensverwerking wordt een afweging gemaakt van belangen en risico’s.]

[Voor ondersteuning bij het beantwoorden van deze vraag kan JZ betrokken worden (raadpleeg de PC/CIB/ISO/ISC indien onbekend is welke personen hierbij te betrekken)]

Privacy Impact Assessment

B. Beoordeling gegevensverwerkingen

Proces: De PIA verantwoordelijke maakt (o.b.v. hoofdstuk A) een eerste aanzet voor de risico's in hoofdstuk B (dit hoofdstuk). De eerste aanzet van hoofdstuk B en hoofdstuk A zijn vervolgens input voor een overleg (dat al gepland kan worden na de intake) waarbij de risico's en noodzakelijke maatregelen in kaart worden gebracht (wat wordt vastgelegd in een nieuwe/aangevulde versie van hoofdstuk B). De PIA verantwoordelijke neemt hierbij de lead en zorgt ervoor dat relevante expertises worden betrokken.

BEOORDELING

5a. Rechtmatigheid: Noodzaak en evenredigheid

[Beoordeel of en waarom de voorgenomen gegevensverwerkingen noodzakelijk zijn voor het verwezenlijken van de nagestreefde doeleinden. Ga hierbij in ieder geval in op:

1. Proportionaliteit: staat de inbreuk op de persoonlijke levenssfeer en de bescherming van de persoonsgegevens van de betrokkenen in evenredige verhouding tot de verwerkingsdoeleinden?
2. Subsidiariteit: kunnen de verwerkingsdoeleinden in redelijkheid niet op een andere, voor de betrokkenen minder nadelige wijze, worden verwezenlijkt? Zijn alle te verzamelen, te leveren gegevens nodig om het doel te bereiken? Kan het verwerken van persoonsgegevens in een beperkte vorm of met minder verwerkingen? Geef per onderdeel aan waarom de gegevens noodzakelijk zijn en wat de toegevoegde waarde is.]

5b. Risico's

[Beschrijf en beoordeel de risico's van de voorgenomen gegevensverwerkingen voor de rechten en vrijheden van de betrokkenen. Houd hierbij rekening met de aard, omvang, context en doelen van de voorgenomen gegevensverwerkingen. Ga in op zowel de risico's voor betrokkenen als de risico's voor de organisatie. Welke redenen zijn er om af te zien van de gegevensverwerking?]

5c. Toepasselijke risico's

- ☐ Gebruik van persoonsgegevens in gevoelige contexten
- ☐ Gebruik van persoonsgegevens van minderjarigen
- ☐ Een groot aantal betrokkenen
- ☐ Gebruik van nieuwe technologieën

[Als er gebruik wordt gemaakt van een nieuwe techniek bestaat er een hoger risico en moeten passende beheersmaatregelen getroffen worden. De risico's kunnen zijn onder andere imagoschade, in gevaar komen van de bedrijfscontinuïteit, handhaving, beperking van verwerking door toezichthouders.]

5d. Overige risico's

[Identificeer de risico's, denk aan de volgende situaties:

1. Heeft het een negatieve invloed op betrekkingen met andere organisaties of het publiek bijvoorbeeld resulterend in negatieve publiciteit?
2. Resulteert het in directe of indirecte verliezen? Niet voldoen aan deel B van deze PIA kan resulteren in een boete van de Autoriteit Persoonsgegevens. Dat is bijvoorbeeld het geval indien de gegevenskwaliteit onvoldoende is.
3. Draagt het bij aan het niet efficiënt opereren van de organisatie of benadeeld goed besturen van (delen van) de organisatie?
4. Ongemak voor een persoon of groep personen eventueel resulterend in een civiele procedure, schadevergoeding, boete of gevangenisstraf?
   - Lichamelijke, materiele of immateriële schade met betrekking tot:
   verlies van controle over de gegevens;
   - Discriminatie, stigmatisering en uitsluiting;
   - Identiteitsdiefstal of –fraude; gezondheidsschade;
   - Financiële verliezen;
   - Ongeoorloofde ongedaan making van pseudonimisering;
   - Reputatie- of anderszins relationele schade;
   - Verlies van vertrouwelijkheid door het beroepsgeheim;
   - Of, enig ander aanzienlijk economisch of maatschappelijk nadeel voor de natuurlijke persoon.
   -Definieer aanvaardbare risicowaarden en beoordeel of de risico's aanvaardbaar zijn.]

Maatregelen

5e. Privacy by design en privacy by default maatregelen

[Geef aan welke Privacy by design en Privacy by default maatregelen worden toegepast. Hierbij kan gedacht worden aan (hieronder betreft een hele korte omschrijving):

1. Anonimiseren (de gegevens op zichzelf geen herleidbare elementen meer omvatten en niet via alternatieve/aanvullende bronnen alsnog herleidbaar zijn naar een persoon);
2. Dataminimalisatie (alleen die gegevens worden verzameld die strikt noodzakelijk zijn voor latere verwerking en

waarvoor een doelbinding/rechtsgrond aanwezig is);
3. Pseudonimiseren (het verbergen van persoonsgegevens die worden verwerkt);
4. Encryptie (ongeautoriseerde toegang tot (persoons)gegevens gedurende opslag, gebruik en/of transport minimaliseren via versleuteling);
5. Access Control (Role based access/need to know // Whitelisting // Logging & monitoring // Fysieke toegang // Veilig wissen van gegevens // Beveiliging t.b.v. ongeautoriseerde toegang van buitenaf);
6. Data protection by default ("privacy-vriendelijke" setting als uitgangspunt en geen "verstopte" privacy-onderwerpen op een plek waar ze niet thuishoren);
7. Verwijderen / bewaartermijnen (op een duurzame wijze bewaren, met voldoende metadata omvat om de context van de betreffende data te kunnen herleiden en vernietigingsmethodiek ingericht rekening houdend met de mogelijkheid om te over te kunnen dragen waar nodig aan het Nationaal Archief);
8. Faciliteren rechten van betrokkenen (het bieden van maximale transparantie met betrekking tot de verwerkingen die worden uitgevoerd).]

5f. Maatregelen voor juistheid	5g. Mitigeren van risico's
[Geef aan hoe invulling wordt gegeven aan het waarborgen van actualiteit, juistheid en volledigheid van de persoonsgegevens.]	[Beoordeel welke technische, organisatorische en juridische maatregelen in redelijkheid kunnen worden getroffen om de hiervoor beschreven risico's te voorkomen of te verminderen. Beschrijf de aandachtspunten voor degene die het systeem/beleid/enzovoort verder gaat ontwikkelen. Beschrijf oplossingsrichtingen in de zin van privacy maatregelen en/of compliance mechanismen. Noem bovendien wie verantwoordelijk is voor de hieronder beschreven maatregelen. Voorbeelden: 1. Limitering van het verzamelen van gegevens: Het verminderen van de hoeveelheid gegevens, door de gegevens niet op te slaan of niet te bewaren. Niet op te nemen in de back-up. 2. Gegevenskwaliteit: Introduceren van geautomatiseerde controles op gegevens. 3. Doelbinding: De doelen voor het verzamelen en verenigbaarheid van verdere verwerking nader specificeren en hierover communiceren. Verwerkersovereenkomsten, responsible disclosurebeleid, SLA's. 4. Limitering van gebruik van gegevens: Het beperken van de mogelijkheid om grote hoeveelheden gegevens in een keer binnen en buiten de organisatie te verspreiden door gefragmenteerde opslag, in plaats van concentreren van alle gegevens in één database. Beperken van inzageniveau. 5. Beveiliging van gegevens: Het toepassen van encryptie en logische of fysieke toegangsbeveiliging. Logging of meerfactor authenticatie. Hack of pentest. 6. Transparantie: Het opstellen van een privacy beleid, gedragscode of het laten certificeren van de verwerking. 7. Rechten van betrokkenen: Betrokkenen zeggenschap geven over zijn gegevens door de invoer van een 'self-service' bijvoorbeeld via een beveiligd internet portal. 8. Verantwoording: Bijvoorbeeld invoeren van periodiek externe controle, melding in jaarverslag, organiseren van hulp na schending privacy. Maar ook werken aan bewustwording en opleiding. Managementrapportage over risicobeheer.]

5h. Rechten van de betrokkenen
[Heeft deze verwerking invloed op de rechten van betrokkenen en zo ja, hoe wordt deze aanvullende verwerking aangehaakt op de bestaande procedures (voorbeeld inzagerecht).]

5i. Register
[Dient deze verwerking toegevoegd te worden aan het Register of dient een bestaande registerregel aangepast,

aangevuld te worden? Zie ook vraag 1b]

Privacy Impact Assessment

C. Samenvatting acties

In het overzicht hieronder zijn alle acties opgenomen die in de PIA zijn genoemd.

ACTIES		
Omschrijving	**Actiehouder**	**Deadline oplevering**
3g. Motivatie bij bewaartermijn	-	-
3h. Technische en organisatorische maatregelen	-	-
4c. Internationale overdrachten	-	-
[indien adequaatheidsbeginsel uitgezocht moet worden]		
5e. Privacy by design en privacy by default maatregelen	-	-
5f. Maatregelen voor juistheid	-	-
5g. Mitigeren van risico's	-	-
5h. Rechten van de betrokkenen	-	-
5i. Register	-	-

Privacy Impact Assessment

BIJLAGE 2 – Uitwerking PIA Proces

AVG – PIA proces

Augustus 2018

Uitgangspunten

- Doorlooptijd is leidend
- Doelstelling is dat het proces drie weken (15 werkdagen) duurt vanaf processtap "PIA Intake" (zowel "aanvrager" als "PC/CIB/ISO/ISC" bewaken dat deze drie weken wordt gerealiseerd); zie detail in tabel volgende slides.
- Doorlooptijd "stopt" indien onvoldoende kwaliteit wordt opgeleverd door een van de partijen (indien dit het geval is zal dit ook expliciet gemaakt moeten worden). Dit proces beschrijft alleen de "happy flow" en beschrijft niet eventuele iteraties bij vragen of beoordelingen door stakeholders.
- Lid van RvB kan bij uitloop (potentiële) risico's accepteren voor nog niet afgeronde PIA.

Privacy Impact Assessment

Randvoorwaarden

- Commitment alle stakeholders
- Op moment van het betrekken van de stakeholders dient de scope van de PIA helder te zijn
- Betrokken stakeholders geven voldoende prioriteit aan het uitvoeren van een PIA en hebben voldoende capaciteit om de oplevertermijnen na te komen.
- Betrokken stakeholders van de Risicobeoordeling komen voorbereid bij het overleg
- Betrokkenen worden éénmaal (op de dag) gerappelleerd (door "ontvanger"). Dag erna escalatie naar bovenliggend management

Doorlooptijdtabel

Processtap	Moment / doorlooptijd	Actiehouder*
PIA Initiële check	Moment X	"aanvrager" + "PC/CIB/ISO/ISC"
Inplannen van afspraak voor bespreken van deel B (Risicobeoordeling)	Uiterlijk X+1 werkdag	"PC/CIB/ISO/ISC"
Aanvullen deel A v/d PIA n.a.v. initiële check	Uiterlijk X+2 werkdagen	"aanvrager"
Uitvoeren quickscan + doorzetten naar de deelnemers van de afspraak Risicobeoordeling (waar mogelijk al aangevuld met de eerste aanzet hoofdstuk B)	Dag van ontvangst	"PC/CIB/ISO/ISC"
Afspraak Risicobeoordeling	Uiterlijk X+8 werkdagen	Allen
Opvolging "uitzoekpunten" n.a.v. het overleg Risicobeoordeling	Uiterlijk X+9 werkdagen	Allen
De ingevulde PIA (deel A, B en C) worden (na goedkeuring door de "proces/dataeigenaar") ter advisering doorgezet naar de FG	Uiterlijk X+10 werkdagen	"aanvrager"
Advies FG	Uiterlijk 5 werkdagen na ontvangst	FG

* Zie slide 7 voor wie de lead heeft bij de processtap

Privacy Impact Assessment

PIA Proces + doorlooptijden

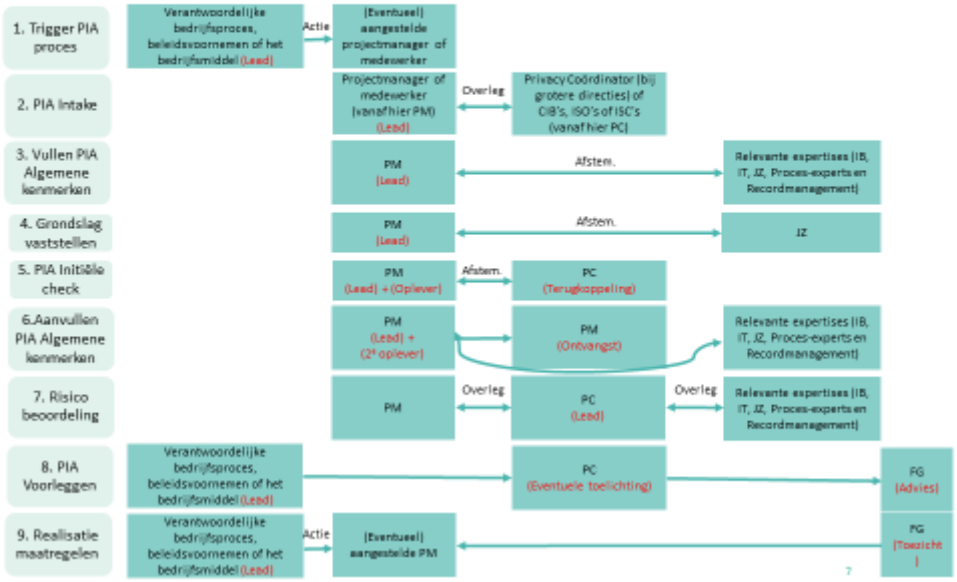
Betrokkenen bij PIA

Betrokkenen

- De PIA wordt ingevuld door of namens degene die verantwoordelijk is voor het doel en de middelen voor de verwerking van persoonsgegevens. Dit is bijvoorbeeld degene die opdracht geeft voor een project voor de implementatie van een taak, aanschaf van een tool, inzetten van een cloudoplossing, etc. Dus de verantwoordelijke voor het betreffende bedrijfsproces, beleidsvoornemen of het bedrijfsmiddel (zie Privacy Beleid op de intranetpagina voor nadere toelichting over de taken en verantwoordelijkheden op vlak van Privacy). Deze verantwoordelijk dient er tevens voor te zorgen dat de maatregelen beschreven in de PIA worden geïmplementeerd en worden uitgevoerd. Of dit wordt gedaan vanuit een projectvorm, binnen het Agile proces of vanuit de lijn zal niet afdoen aan de situatie van verantwoordelijkheden.
- De verantwoordelijke haakt de Privacy Coördinator (bij grotere directies) of CIB's, ISO's of ISC's aan. Ook in geval er twijfel is of een PIA uitgevoerd moet worden kan contact opgenomen worden met de PC/CIB/ISO/ISC.
- Relevante expertises (IB, IT, JZ, Proces-experts en Recordmanagement) worden bij de PIA betrokken.
- De FG kan geraadpleegd worden voor het geven van advies bij de PIA en fungeert als interne toezichthouder op het PIA proces en de daarin geïdentificeerde maatregelen.
- De ingevulde PIA wordt voorgelegd bij de Functionaris Gegevensbescherming (FG) voor advies.

Privacy Impact Assessment

PIA Proces vs betrokkenen



1. Trigger PIA proces

- Een PIA-proces moet in een zo vroeg stadium, bij nieuwe gegevensverwerkingen in de ontwerpfase worden gestart (ook als nog niet alle details van de verwerking bekend zijn).
- PIA maakt onderdeel uit van projectmanagementflow
- [T.z.t. vastleggen hoe van toepassing in Agile methodiek]
- [T.z.t. vastleggen hoe van toepassing bij changes (incl data-analyse verzoeken)]
- Als onderdeel van de PDCA cyclus dient jaarlijks de ingevulde PIA's gereviewd te worden (trigger vanuit PC o.b.v. "geldigheidsdatum" assessment).

Privacy Impact Assessment

2. PIA Intake

2.PIA Intake

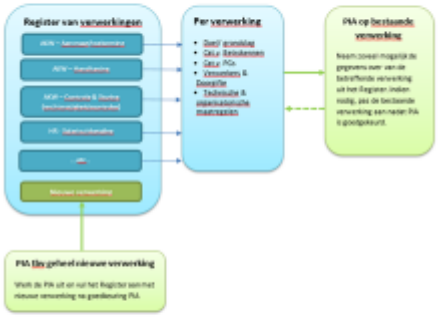
- De verantwoordelijke voor het betreffende bedrijfsproces of het bedrijfsmiddel of een aangestelde projectmanager/medewerker neemt contact op met de PC/CIB/ISO/ISC.
- Als onderdeel van de Intake wordt (aan de hand van de criteria uit de Quickscan) vastgesteld of een PIA noodzakelijk is.
- Als onderdeel van de Intake worden de "verwerkingen" besproken om de verantwoordelijke op weg te helpen met het vullen van hoofdstuk "A. Beschrijving algemene kenmerken gegevensverwerkingen" van de PIA template en welke relevante informatie verzameld dient te worden voor de risicobeoordeling.
- Als onderdeel van de Intake worden de relevante expertises vastgesteld die betrokken worden bij de PIA en wordt commitment van deze expertises vastgelegd.
- Als onderdeel van de Intake worden (waar mogelijk) de tijdslijnen/oplevermomenten vastgesteld en de werkzaamheden al ingepland (een voorlopige afspraak - incl. de relevante expertises - voor het bespreken van hoofdstuk B wordt al ingepland door de PC/CIB/ISO/ISC).

9

3. Vullen PIA Algemene kenmerken

3.Vullen PIA Algemene kenmerken

- De verantwoordelijke verzamelt de relevante informatie voor het vullen van hoofdstuk "A. Beschrijving algemene kenmerken gegevensverwerkingen" van de PIA template.
- In diagram hiernaast is weergegeven hoe de relatie tussen het Register van verwerkingen en de PIA gebruikt kan worden bij het vullen van de PIA. Voor toegang tot het register kan contact worden opgenomen met de Privacy Coördinator.
- Het vaststellen van de grondslag (volgende stap) maakt een onderdeel uit van dit onderdeel.



10

4. Grondslag vaststellen

4. Grondslag vaststellen

- De verantwoordelijke voor het betreffende bedrijfsproces of het bedrijfsmiddel of een aangestelde projectmanager/medewerker neemt contact op met JZ voor het bepalen van de grondslag (een heldere scope en doelstelling van de PIA is hierbij essentieel).
- Het achterhalen van de grondslag wordt geprioriteerd op de backlog van JZ:
  - Bij JZ Beleid wordt de backlog periodiek ter afstemming opgeleverd aan DSV;
  - Bij JZ team Zorg (PGB) vindt prioritering samen met het team plaats bij de prioritering van de tactische onderwerpen;
  - Bij Bedrijfsjuridische dienst wordt gewerkt met "dossiers" (bijvoorbeeld aanbestedingen) die worden toegekend aan medewerkers waarbij de PIA slechts één van de onderdelen is van het dossier. Prioritering vindt op dossierniveau plaats en directe lijnen zijn aanwezig tussen "aanvrager" en JZ.

5. PIA Initiële check

5.PIA Initiële check

- De verantwoordelijke levert een eerste ingevulde versie van hoofdstuk "A. Beschrijving algemene kenmerken gegevensverwerkingen" op aan de PC/CIB/ISO/ISC.
- De PC/CIB/ISO/ISC beoordeelt de eerste ingevulde versie en stemt af / geeft (eventuele) adviezen ter verbetering. Vervolgens neemt de PC/CIB/ISO/ISC de lead voor het vullen van "B. Beoordeling gegevensverwerkingen".

6. Aanvullen PIA Algemene kenmerken

6.Aanvullen PIA Algemene kenmerken

- De verantwoordelijke geeft opvolging aan de (eventuele) adviezen ter verbetering van de PC/CIB/ISO/ISC.
- De verantwoordelijke levert binnen 2 werkdagen een volgende versie op (n.a.v. de adviezen) die gebruikt zal worden bij de Risicobeoordeling.

7. Risicobeoordeling

7.Risico beoordeling

- De PC/CIB/ISO/ISC maakt een eerste aanzet voor de risico's in hoofdstuk "B. Beoordeling gegevensverwerkingen".
- Met als input de door de verantwoordelijk ingevulde versie van hoofdstuk "A. Beschrijving algemene kenmerken gegevensverwerkingen" en de eerste aanzet in hoofdstuk "B. Beoordeling gegevensverwerkingen", zal de PC/CIB/ISO/ISC in samenwerking met de verantwoordelijke een overleg inplannen voor het in kaart brengen van de risico's en noodzakelijke maatregelen (wat wordt vastgelegd in hoofdstuk "B. Beoordeling gegevensverwerkingen"). De PC/CIB/ISO/ISC neemt hierbij de lead.
- Waar nodig wordt bij de beoordeling expertise van andere directies ingewonnen (IB, IT, JZ, proces-experts, Record management) – partijen vastgesteld bij de Intake.

Privacy Impact Assessment

8. PIA voorleggen

8.PIA Voorleggen

- De verantwoordelijke verzamelt de vervolgacties uit hoofdstuk A en B en legt deze vast in hoofdstuk "C. Samenvatting acties" inclusief wie de verantwoordelijke actiehouder is en deadline voor oplevering.
- De proces/data-eigenaar geeft op de ingevulde PIA (hoofdstuk A, B en C gevuld) zijn/haar commitment op juistheid en volledigheid en op de realisatie van de maatregelen.
- Voorzien van een toelichting/overige opmerkingen van de Privacy Coördinator wordt de PIA voorgelegd bij de Functionaris Gegevensbescherming (FG) voor advies.
- PIA wordt indien nodig aangevuld op basis van advies FG (iteratief terug naar eigenaar etc.)
- Als er uit de PIA komt dat de verwerking een hoog risico oplevert en er geen risicobeperkende maatregelen worden genomen dan moet (na raadpleging bij FG) een voorafgaande raadpleging worden aangevraagd bij de AP (waarbij de PIA aan de AP wordt verstrekt). Vóór de raadpleging bij de AP wordt (door de proces/data-eigenaar) een risicoacceptatie voorgelegd bij de RvB.

9. Realisatie maatregelen

9. Realisatie maatregelen

- De proces/data-eigenaar is ervoor verantwoordelijk dat de maatregelen beschreven in de PIA worden geïmplementeerd en worden uitgevoerd.
- In geval van wijzigingen gedurende het project/change waarbij wordt afgeweken van datgene wat is beschreven in de voorgelegd PIA, zal een evaluatie worden uitgevoerd en zal de nieuwe versie wederom door partijen worden "goedgekeurd".
- Als resultaat van de PIA is het mogelijk dat een bestaande verwerking in het Register aangepast/aangevuld moet worden, dan wel dat een nieuwe verwerking erin opgenomen moet worden. Binnen de directies zijn proceseigenaren aangewezen die dienen te zorgdragen dat de register up-to-date blijft. De Privacy Coördinatoren kunnen op verzoek hierbij ondersteuning leveren.
- De FG zal vanuit een toezichtfunctie eveneens toezien op de realisatie van de maatregelen onderkend binnen de PIA's.