



Gegevensbeschermingseffectbeoordeling (PIA)

[Ministerie/Onderdeel/Afdeling/Proces]

[Directie]

[Plaats/Datum]



Naam ministerie - Naam directie

Vaststelling verwerkersverantwoordelijke: Selecteer/typ datum

Naam: Typ naam/functie

Advies functionaris voor gegevensbescherming: Selecteer/typ datum

Naam: Typ naam/functie

Advies CIO: Selecteer/typ datum

Naam: Typ naam/functie

Gegevensbeschermingseffectbeoordeling (PIA)

Naam ministerie

Naam directie

Contact:

Ministerie xxx, directie xxx

xxx

xxx

xxx

x

x

x

x

Versie: 1.0 December 2017

Inhoudsopgave

Inleiding.....	4
A. Beschrijving kenmerken gegevensverwerkingen.....	4
1. Voorstel	4
2. Persoonsgegevens	4
3. Gegevensverwerkingen	4
4. Verwerkingsdoeleinden	4
5. Betrokken partijen	4
6. Belangen bij de gegevensverwerking	4
7. Verwerkingslocaties	4
8. Techniek en methode van gegevensverwerking	4
9. Juridisch en beleidsmatig kader	4
10. Bewaartermijnen	4
B. Beoordeling rechtmatigheid gegevensverwerkingen.....	4
11. Rechtsgrond	4
12. Bijzondere persoonsgegevens	4
13. Doelbinding	4
14. Noodzaak en evenredigheid	4
15. Rechten van de betrokkene	4
C. Beschrijving en beoordeling risico's voor de betrokkenen.....	4
16. Risico's	4
D. Beschrijving voorgenomen maatregelen.....	4
17. Maatregelen	4

Inleiding

Voeg hier wanneer gewenst een openingsalinea of inleiding toe. Denk bijvoorbeeld aan:

- Verwijzing naar het privacybeleid of motivatie achter de uitvoering van deze PIA
- Informatie over de manier van opstellen.

A. Beschrijving kenmerken gegevensverwerkingen

Beschrijf op gestructureerde wijze de voorgenomen gegevensverwerkingen, de verwerkingsdoeleinden en de belangen bij de gegevensverwerkingen.

Onder A wordt de eerste stap beschreven van de PIA: een overzicht van de relevante feiten van de voorgenomen gegevensverwerkingen. Als de feiten onduidelijk zijn, werkt dit door in de beoordeling.

1. Voorstel



Beschrijf het voorstel waar de gegevensbeschermingseffectbeoordeling op ziet en context waarbinnen deze plaatsvindt op hoofdlijnen.

aantekeningen:

- *Waar ziet het proces nu op? Waar ziet de DPIA precies op? Graag duidelijk afbakenen.*
- *Wat houden de slachtoffermeldingen in? Zijn deze meldingen onderdeel van het proces en behoort dit tot de DPIA?*
- *Hoe vindt de selectie plaats? Wat voor signalen zijn dat? Wat wordt er door derden toegezonden? Welke partijen zijn die derden?*
- *Is het stukje van de FIOD ook onderdeel van deze DPIA? Er wordt verwezen naar voorwaarden, welke zijn dat?*

Afbakening:

Er worden berichten ontvangen bij het Meldpunt van de afdeling fraude. Berichten kunnen als signaal aangemerkt worden welke in aanmerking komen voor nader onderzoek.

Het proces voor de PIA 'Behandeling fraudesignalen' ziet op het ontvangen van berichten tot de afhandeling van een onderzoek. Onderstaand de processen puntsgewijs weergegeven:

- Ontvangen van berichten
- Registratie van berichten welke als signaal aangemerkt worden
- Rechtmatigheidsonderzoek naar aanleiding van een signaal
- Opzetbepaling naar aanleiding van een rechtmatigheidsonderzoek en/of signaal
- Afhandeling van het onderzoek: geen actie, resultaat rechtmatigheid, bestuurlijke boete, Strafrecht

TEOS-postbus verstuurd melding naar de fraude postbus

Screeningsteam: quickscan TWO overlegt, samenspanning, georganiseerdheid

Rapport sociale recherche

Het proces in stappen ingedeeld:

A. Registratie

1.	Ontvangst melding
i.	Quicksan melding - individueel - samenspanning (uitwerken in HST 8)
ii.	Aanmaken dossier (q-schijf)
iii.	Registreren TVS, BPM
iv.	excelbestand
2.	Prioritering
3.	Categorisering
i.	Melding categoriseren
4.	Slachtoffermelding
5.	Landelijke stuurgroep Interventieteams (LSI)
6.	Output
i.	Aanbod melding opzetbepaling
ii.	Aanbod melding rechtmatigheidsonderzoek / IST
B.	Onderzoek
1.	Rechtmatigheidsonderzoek
i.	Documenteren gegevens (q-schijf)
2.	Resultaat / conclusie
i.	Rechtmatigheid: geen vervolg
ii.	Vermoeden opzet of grove schuld
3.	Output
i.	Verslag rechtmatigheid + onderbouwing onderzoek opzetbepaling
C.	Opzetbepaling
1.	Input
i.	Directe melding vanuit registratie
ii.	Verslag rechtmatigheid + onderbouwing onderzoek opzetbepaling
2.	Onderzoek + onderbouwing
3.	Resultaat / conclusie + controle
i.	Prewaag > controle BFC (Doorzetten naar FIOD)
ii.	Geen vervolg > controle BFC
iii.	Individueel sanctioneren Br.
D.	sanctioneren
1	Output
i.	FIOD / strafrecht (evt. terug voor Br)
ii.	Opleggen passende sanctie
Uitzoeken:	
Welke stukken ontvangen wij en wat doen wij ermee.	
Proces verbaal, na uitspraak.	
Rapport sociale recherche, na bezwaar en beroep termijn. (normaal gegeven?)	

2. Persoonsgegevens



Som alle categorieën van persoonsgegevens op die worden verwerkt. Geef per categorie

van persoonsgegevens tevens aan op wie die betrekking hebben. Deel deze persoonsgegevens in onder de typen: gewoon, bijzonder, strafrechtelijk en wettelijk identificerend.

[Klik hier om infotekst te verbergen](#)

Beschrijf allereerst alle te verwerken categorieën van persoonsgegevens. Onder persoonsgegeven wordt verstaan: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon.

Natuurlijke personen wil zeggen mensen. Informatie over overleden personen, rechtspersonen, dieren, zaken en objecten zijn in beginsel geen persoonsgegeven. Deze informatie kwalificeert weer wel als persoonsgegeven indien die ook betrekking heeft op een levende persoon.

Om te bepalen of iemand identificeerbaar is, moet rekening worden gehouden met alle middelen waarvan redelijkerwijs valt te verwachten dat zij kunnen worden gebruikt om de persoon te identificeren.

Gepseudonimiseerde (ook wel: versleutelde) gegevens worden als persoonsgegevens beschouwd. Onder pseudonisering wordt verstaan: het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens (sleutels) worden gebruikt. Hieraan wordt wel de eis verbonden dat deze aanvullende gegevens apart worden bewaard en maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een persoon worden gekoppeld.

Anonieme en geanonimiseerde gegevens zijn geen persoonsgegevens. Met anoniem en geanonimiseerd wordt bedoeld dat de persoon op wie het gegeven betrekking heeft, niet (meer) identificeerbaar is. Het anonimiseren van persoonsgegevens als zodanig is overigens weer *wel* een verwerking van persoonsgegevens.

Voorbeelden van persoonsgegevens zijn: naam, voorvoegsel, adres, telefoonnummer, e-mailadres, leeftijd, geboortedatum en -plaats, geslacht, woonplaats, nationaliteit, IP-adres, MAC-adres, KvK- nummer, voertuigidentificatienummer, winst eenmanszaak, bankrekeningnummer en -saldo, IQ, functie, opleiding, inkomens- en vermogensgegevens, kredietwaardigheid, persoonlijke voorkeuren, loonschaal, verslag van een functioneringsgesprek en (wan)gedrag. Ook metadata – informatie over informatie – zijn persoonsgegevens als hieruit de identiteit van de betrokkene kan worden herleid. Voorbeelden van metadata zijn: welke browser of telefoon iemand gebruikt, wanneer een document is opgesteld of voor het laatste bewerkt en de geschreven taal. Ook locatie-informatie en geografische informatie kwalificeren als persoonsgegevens als de informatie herleidbaar is tot een persoon. Denk hierbij aan de koppeling van gegevens uit de basisregistratie adressen en gebouwen aan andere gegevens en het monitoren van de locaties van voertuigen.

Typen

Stel vervolgens de aard van de te verwerken categorieën van persoonsgegeven vast. De AVG onderscheidt drie typen van persoonsgegevens – gewone, bijzondere en strafrechtelijke persoonsgegevens – en stelt verschillende eisen aan een rechtmatige verwerking daarvan. De gedachte hierachter is dat hoe gevoeliger de aard van de persoonsgegevens, hoe groter de effecten voor de betrokkenen zijn.

Bijzondere persoonsgegevens

Hieronder een limitatieve opsomming van categorieën van bijzondere persoonsgegevens:

- ras of etnische afkomst;
- politieke opvattingen;
- religieuze of levensbeschouwelijke overtuigingen;
- het lidmaatschap van een vakbond;
- genetische gegevens;
- biometrische gegevens met het oog op de unieke identificatie van een persoon;

- gegevens over gezondheid;
- gegevens over seksueel gedrag of seksuele gerichtheid.

Voorbeelden van bijzondere persoonsgegevens zijn: het adressenbestand van een kerkblad, gegevens die via een apothekers-app worden verwerkt, ziekte- en verzuimgegevens van werknemers, ledenlijst van een politieke partij, relatiestatus op sociale media. Let op: uit beeldmateriaal zoals foto's en camerabeelden kunnen soms ook bijzondere persoonsgegevens, zoals etnische afkomst of medische gesteldheid, worden afgeleid.

Genetische gegevens

Genetische gegevens zijn persoonsgegevens over overgeërfde of verworven genetische kenmerken van een persoon die unieke informatie verschaffen over zijn fysiologie of gezondheid en die met name voortkomen uit een analyse van een biologisch monster van die persoon. Denk hierbij aan: chromosomen, DNA of RNA en erfelijke ziekten.

Biometrische gegevens

Biometrische gegevens zijn persoonsgegevens die het resultaat zijn van een specifieke technische verwerking met fysieke, fysiologische of gedragsgerelateerde kenmerken van een persoon op grond waarvan eenduidige identificatie van die persoon mogelijk is of wordt bevestigd. Denk hierbij aan: vingerafdrukken, irispatroon, gezichtsprofiel, toetsaanslaganalyse, looppatroon, stemgeluid en slaapritme. Foto's vallen overigens alleen onder de definitie van biometrische gegevens wanneer zij worden verwerkt met behulp van bepaalde technische middelen die de unieke identificatie of authenticatie mogelijk maken.

Gegevens over gezondheid

Gezondheidsgegevens zijn persoonsgegevens over de fysieke of mentale gezondheid van een persoon. Denk hierbij aan: gewicht, hartslag, handicap, ziekterisico of verleende gezondheidsdiensten.

Strafrechtelijke persoonsgegevens

Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen (hierna: strafrechtelijke persoonsgegevens) zijn een apart type persoonsgegeven. Het gaat hier zowel om veroordelingen als om verdenkingen van strafbare feiten. Voorbeelden hiervan zijn: proces-verbaal, sepotbeslissing, strafblad, relaas verhoor en aanvraag voor een toevoeging in een strafzaak.

Wettelijke identificatienummers

Nummers ter identificatie van een persoon die bij wet zijn voorgeschreven, mogen slechts worden verwerkt voor doeleinden die bij wet zijn bepaald. De gedachte hierachter is dat persoonsnummers de koppeling van verschillende bestanden aanzienlijk vergemakkelijken en daarmee een extra bedreiging voor de persoonlijke levenssfeer vormen. Denk hierbij aan: een burgerservicenummer (BSN), BIGnummer (beroepen in de individuele gezondheidszorg), A-nummer (basisregistratie personen), onderwijsnummer, strafrechtketennummer en kenteken. Het gaat hierbij enkel om in de wet voorgeschreven persoonsidentificerende nummers.

Overige persoonsgegevens

Alle overige persoonsgegevens die niet kwalificeren als bijzonder of strafrechtelijk worden in dit model aangemerkt als gewone persoonsgegevens. Gewone persoonsgegevens wil overigens niet zeggen dat geen sprake is van een hoog privacyrisico. Bepaalde persoonsgegevens kunnen door de context waarin zij worden gebruikt gevoelig zijn en daardoor een hoog privacyrisico met zich brengen. Hierbij kan gedacht worden aan:

- gegevens over de financiële of economische situatie van de betrokkene;
- gegevens over overtredingen van wettelijke voorschriften, bestuurlijke en/of tuchtrechtelijke maatregelen of sancties;

- (andere) gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene;
- gegevens die betrekking hebben op kwetsbare groepen;
- gebruikersnamen, wachtwoorden en andere inloggegevens;
- gegevens die kunnen worden misbruikt voor (identiteits)fraude;
- communicatie- en locatiegegevens.

Betrokkenen

Benoem tot slot de categorieën van betrokkenen van wie de persoonsgegevens worden verwerkt. Denk hierbij aan: medewerkers, consumenten, cliënten, patiënten, zakelijke contacten, bezoekers, gebruikers of ingezetenen van een gemeente. De omvang en categorie van betrokkenen kunnen invloed hebben op de effecten van het voorstel. Bepaalde betrokkenen zijn kwetsbaarder dan anderen. Met kwetsbaar wordt bedoeld dat de negatieve effecten van een (onrechtmatige) gegevensverwerking groter kunnen zijn voor bepaalde betrokkenen dan voor andere (zie ook de anderszins gevoelige persoonsgegevens). Denk bijvoorbeeld aan: minderjarigen, verstandelijk gehandicapten, mensen die te maken hebben met stalking of die in een blijf-van-mijn-lijfhuis verblijven, medewerkers van inlichtingen- en veiligheidsdiensten, klokkenluiders of informanten van politie of justitie. Betrokkenen hebben op grond van de privacyregulering bepaalde rechten, zoals het inzage- en correctierecht.

De AVG biedt specifieke bescherming aan kinderen, omdat zij zich minder bewust zullen zijn van de effecten van de gegevensverwerking en van hun rechten in dat kader. Die specifieke bescherming geldt met name voor het gebruik van persoonsgegevens van kinderen voor marketingdoeleinden, het opstellen van persoonlijkheids- of gebruikersprofielen en het verzamelen van persoonsgegevens over kinderen bij het gebruik van rechtstreeks aan kinderen verstrekte diensten. Zo is wanneer het kind jonger is dan 16 jaar zo'n verwerking slechts rechtmatig, indien de toestemming of machtiging tot toestemming wordt verleend door de ouder of voogd. Ook heeft de leeftijd van betrokkenen gevolgen voor de wijze waarop hij geïnformeerd moet worden.

In het kader van de Richtlijn kan het onderscheid worden gemaakt tussen:

- a. personen ten aanzien van wie gegronde vermoedens bestaan dat zij een strafbaar feit hebben gepleegd of zullen plegen;
- b. personen die voor een strafbaar feit zijn veroordeeld;
- c. slachtoffers van een strafbaar feit, of personen ten aanzien van wie bepaalde feiten aanleiding geven tot het vermoeden dat zij het slachtoffer zouden kunnen worden van een strafbaar feit; en
- d. andere personen die bij een strafbaar feit betrokken zijn, zoals personen die als getuige kunnen worden opgeroepen in een onderzoek naar strafbare feiten of een daaruit voortvloeiende strafrechtelijke procedure, personen die informatie kunnen verstrekken over strafbare feiten, of personen die contact hebben of banden onderhouden met een van de personen bedoeld onder a en b.

Bij conceptregulering kan het wenselijk zijn om de te verwerken categorieën van persoonsgegevens in de regeling op te nemen. Wanneer de verwerking onder de werkingssfeer van de Richtlijn valt, is het verplicht om de te verwerken categorieën van persoonsgegevens in de regeling op te nemen.

Aantekeningen:

- *Wordt binnen dit proces ook de rechtmatigheid van de aangevraagde toelating beoordeeld? Behoort dit tot de reikwijdte van de DPIA?*
- *Welke contra-informatie? Waar komt dat vandaan? Welke gegevens zijn dat? Waarom is dat noodzakelijk?*
- *Welke derde partijen?*

- *Klik-melding: zie voetnoot 11. Wat wordt er doorgemaid (wat wordt er geregistreerd)? Op welke wijze gebeurt dat?*
- *Volgt men een re-integratietraject: Worden er dan gezondheidsgegevens verwerkt?*

Gewone persoonsgegevens

Id	Veldnaam	Bron 1	Bron 2	Betrekking op	Processtap
1	Naam (achternaam, voorletters, tussenvoegsels)	BVR ¹	AV	AV ² , TP ³ en kinderen	A, B, C
2	Geboortedatum	BVR	AV	AV, TP en kinderen	A, B, C
3	Persoonsrelaties	BVR, IGA ⁴	AV	AV, TP en kinderen	A, B, C
4	Aantal personen op adres	BVR	AV	AV, TP, kinderen en medebewoner ⁵	A, B, C
5	Verblijfstitel ⁶	BVR, IGA		AV, TP, kinderen en medebewoner	A, B, C
6	Geschat inkomen	FLG ⁷ , BRI ⁸	AV, TP	AV, TP	B, C
7	Rekeningnummer	RBG ⁹ , TVS ¹⁰	AV	AV	B, C
7	Opvangsituatie				
7.1	Opvanggegevens: • Naam • Adres • LRK-nummer • KvK-nummer¹¹ • Soort opvang, DO, BSO • Kindercentrum/gastouderopvang • Contactgegevens	KOO ¹² , LRK ¹³	AV	AV, TP en kinderen	A, B, C
7.2	Afgenomen uren	KOO, KOI-vieuwer ¹⁴	AV	AV en kinderen	B, C
7.3	(gemiddeld) uurtarief	KOO	AV	AV en kinderen	B, C
7.4	Ingangs- en einddatum opvang	KOO, KOI-vieuwer	AV	AV en kinderen	B, C

¹ BVR staat voor Beheer Van Relaties en bevat een BRP-kopie (Basisregistratie personen gemeente). BVR vormt de basisregistratie van alle personen die bij de belastingheffing en uitvoering van niet-fiscale regels betrokken (kunnen) zijn. In BVR zijn de algemene gegevens van (bijna) alle burgers vastgelegd, zoals; naam, adres, woonplaats, geboorte- of oprichtingsdatum, relaties tussen de verschillende burgers geregistreerd.

² AV staat voor aanvrager.

³ TP staat voor toeslagpartner

⁴ IGA staat voor Inrijkt Gemeentelijke basis Administratie

⁵ Medebewoner, is degene die op hetzelfde adres staat ingeschreven als de aanvrager en die geen partner of onderhuurder is en ook niet tot het huishouden van de onderhuurder behoort ([artikel 2](#), eerste lid, letter e, Awir). Als de onderhuurder een bloed- of aanverwant in de eerste graad is van de aanvrager of diens partner, dan is deze wel medebewoner.

⁶ Verblijfstitel bepaald recht op toeslag (artikel??)

⁷ FLG staat voor Fiscale Loon Gegevens

⁸ BRI staat voor Basisregistratie Inkomen en levert achteraf het vastgestelde inkomen uit de aanslag IB of de jaaropgaaf loongegevens.

⁹ RBG staat voor registratie bankgegevens.

¹⁰ TVS staat voor Toeslagen verstrekkingen Systeem, onder "Derden betalingen" is zichtbaar of de KOT toekenning rechtstreeks aan de KOO wordt uitbetaald.

¹¹ KvK staat voor Kamer van Koophandel

¹² KOO staat voor kinderopvangorganisatie

¹³ LRK staat voor Landelijk Register Kinderopvang

¹⁴ KOI-vieuwer, daarin staat contra-informatie geleverd door KOO

8	Gegevens om maximum aantal te vergoeden opvanguren vast te stellen				
8.1	Verloonde uren	UWV ¹⁵ , FLG	AV, TP	AV, TP	B, C
8.2	Doelgroepstatus/-periode: ¹⁶ - Student - Inburgeraar - Re-integratie	UWV, DUO ¹⁷ , gemeente, RIS ¹⁸	AV, TP	AV, TP	B, C
8.3	Aard van werkzaamheden: - Werk in loondienst - Winst uit een onderneming - Meewerken in de onderneming van de partner - Inkomsten uit overig werk	ABS ¹⁹ , UWV	AV, TP	AV, TP	B, C
9	Huur - Huurlasten - Woningbezit - Woonobject	Verhuurder, RIS, BAG-vieuwer	AV	AV, TP, kinderen en medewoner	B, C
10	Zorg Zorgverzekerd	Vektis ²⁰	AV, TP	AV, TP	B, C
11	Kindgebonden budget	SVB ²¹	AV	AV, TP	B, C

Bijzondere persoonsgegevens

Id	Veldnaam	Bron 1	Bron 2	Betrekking op	Processtap
1	Gemoedsbezwaarden	Tool gemoedsbezwaarden	AV, TP	AV, TP	B, C
2	Betalingsverkeer	Financiële instellingen	AV, TP, KOO	AV, TP, KOO	B, C
3	Militair	Tool militairen	AV, TP	AV, TP	B, C
5	Verblijfstitel	IND, IGA	AV	AV, TP, kinderen en medebewoner	B, C

Strafrechtelijke gegevens

Id	Veldnaam	Bron 1	Bron 2	Betrekking op	Processtap
1	Begin- en einddatum detentie	Detentietool	AV	AV, TP	B, C
2	Sanctie (strafrecht en boete)	PSF ²²		AV, TP	C
3	Procesverbaal na				

¹⁵ UWV staat voor Uitvoeringsinstituut Werknemersverzekeringen. Het UWV levert de verloonde uren.

¹⁶ Als een AV en/of TP niet werkzaam zijn als bedoeld in artikel 1.6, eerste lid, onderdeel a, Wko, kunnen zij ook als zgn. doelgroep in aanmerking komen voor een kinderopvangtoeslag (zie artikel 1.6, eerste lid, onderdelen c t/m j, Wko)

¹⁷ DUO staat voor Dienst Uitvoering Onderwijs

¹⁸ RIS staat voor Renseignementen Informatie Systeem, geeft informatie op persoonsniveau over studiefinanciering en woning bezit.

¹⁹ ABS staat voor Aanslagbelastingensysteem

²⁰ Vektis staat voor, heeft men een zorgverzekering

²¹ SVB staat voor sociale verzekeringsbank

²² PSF staat voor

	uitspraak				
--	-----------	--	--	--	--

Nationaal identificatienummer

Id	Veldnaam	Bron 1	Bron 2	Betrekking op	Processtap
1	BSN ²³	BVR	AV	AV, TP, kinderen en medebewoner	A, B, C

Aanvullend:

- adreshistorie
- woonobject
- de risicoscores HT en KOT
- actuele schuld toeslagen en blauw
- onderhuurder bij de HT
- inkomensgegevens worden ook uit AIG gehaald (vastgesteld inkomen)

3. Gegevensverwerkingen



Geef alle voorgenomen gegevensverwerkingen weer.

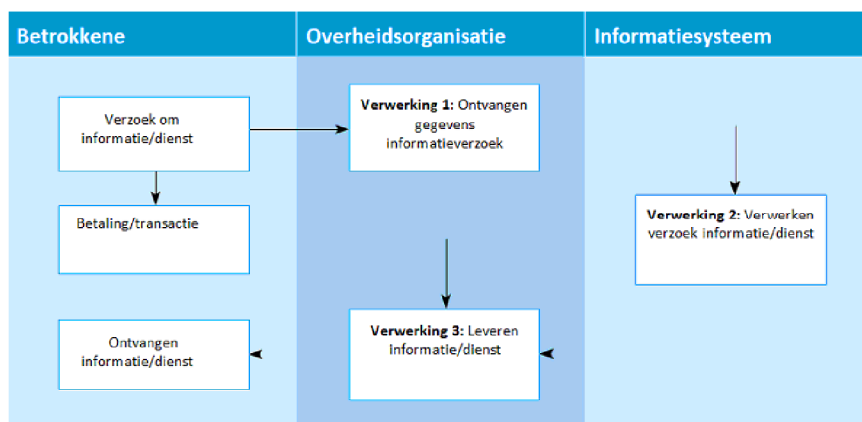
[Klik hier om infotekst te verbergen](#)

Om de rechtmatigheid van de voorgenomen gegevensverwerkingen te kunnen beoordelen, is het noodzakelijk om alle gegevensverwerkingen in beeld te hebben. Onder verwerking wordt verstaan: elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens. Denk hierbij aan:

het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens. Met andere woorden, het begrip omvat het gehele proces dat een persoonsgegeven doormaakt, vanaf het moment van verzamelen tot en met het moment van vernietigen.

Indien mogelijk verdient het aanbeveling om de gegevensverwerkingen te visualiseren, bijvoorbeeld aan de hand van een *input-proces-output* model, *flowchart* of *workflow*.

²³ BSN staat voor Burger Service Nummer



Aantekeningen:

- Welke gegevens worden er verwerkt, op welke wijze en door welke medewerker?
- Welke derden? Welke gegevens worden er opgehaald bij deze derden? Op welke manier gebeurt dat?
- Graag een duidelijk schema van de gegevensverwerking toevoegen, met toelichting waar nodig.
- Welke medewerkers (in rol/functie) kunnen bij deze informatie?
- Waarom worden er IP-analyses gedaan?
- Wat is FSV?

Hele keten in benoemen

Procesplaten in plakken

Zoals bekend wordt een toeslag toegekend op basis van diverse grondslagen. In de voorschotfase bestaat er voor B/T beperkt tot geen zekerheid wat betreft deze grondslagen, dit aangezien deze gegevens veelal na afloop van het toeslagjaar pas volledig kunnen worden vastgesteld. Gedurende de voorschotfase is B/T dus afhankelijk van informatie van derden **wie zijn derden en welke informatie** en de gegevens die door de burger zelf worden aangeleverd bijvoorbeeld door middel van wijzigingen in het Toeslagen Verstrekkingen Systeem (TVS).

Door middel van het raadplegen van gegevens van derden, worden de gegevens welke door de burger aan B/T worden verstrekt voor zover mogelijk gelijk gevalideerd. Naast een vorm van zekerheid, neemt dit ook voor een deel de noodzaak weg om gegevens bij de burger zelf op te vragen ter controle. De burger wordt hierdoor ook niet belast om deze gegevens te verstrekken, daarnaast bestaat ook voor de burger meer zekerheid dat de voorlopige toekenning op de juiste gegevens wordt gebaseerd met als gevolg dat het risico op een terugvordering wordt verkleind.

Het kan echter ook voorkomen dat er om diverse redenen wordt getwijfeld aan de juistheid door de burger verstrekte gegevens. Ook hierbij bestaat de noodzaak om gegevens van derden te raadplegen, enerzijds om eventuele incorrecte grondslagen tijdig te wijzigen en hiermee terugvorderingen voor zover mogelijk te voorkomen dan wel te beperken. Anderzijds om de financiële schade voor B/T te beperken bij vermoedelijk oneigenlijk gebruik van de toeslagen en te bepalen in welke mate de burger verantwoordelijkheid draagt voor het verstrekken van incorrecte gegevens.

Informatie van derden:

Systeem	Te raadplegen gegevens	Benaderbaar door
---------	------------------------	------------------

**** doorstroomschema voor gegevensuitwisseling met andere instantie incl. korte uitleg waarom de gegevens nodig zijn ****

**** gemeente ****

B/T is voor een groot aantal gegevens afhankelijk van de gemeente. De omvang van het Awir-huishouden heeft om diverse redenen invloed op de hoogte van de toeslag. Om de huishoudsamenstelling goed in kaart te kunnen brengen, is het raadplegen van de Basisregistratie Personen (BRP) noodzakelijk. Naast gegevens die helpen bij het vaststellen van de correcte huishoudsamenstelling (zoals adressering en persoonsrelaties), kunnen ook zakelijke relaties worden geraadpleegd. Indien een burger bijvoorbeeld een eigen onderneming heeft – een gegeven dat voor belang kan zijn bij bijvoorbeeld de kinderopvangtoeslag – dan is het mogelijk om deze inschrijving in de BRP te controleren. **** doorstroomschema BRP / IGA voor automatische gegevensverwerking**

****Naast gegevens die automatisch uitgewisseld worden met de gemeente, bestaat er ook de mogelijkheid om direct gegevens bij de gemeente op te vragen. Denk hierbij aan telefonisch, digitaal of schriftelijk contact.**

Als voorbeeld, een van de mogelijke voorwaarden om in aanmerking te komen voor de kinderopvangtoeslag is het volgen van een re-integratietraject. Indien er bijvoorbeeld twijfel bestaat aan de juistheid of volledigheid van de door de burger toegestuurde gegevens, dan kan er vanuit B/T indien noodzakelijk contact opgenomen worden met de desbetreffende gemeente om contra-informatie op te vragen.

**** doorstroomschema informatieverzoeken aan de gemeente en wijze van verwerking/opslag**

****Naast verzoeken om informatie vanuit B/T zelf, bestaat er ook een uitwisseling van rapporten van de Sociale Recherche indien er bijvoorbeeld gedurende een onderzoek is bepaald dat er sprake is van verzwegen samenwoning en deze samenwoning invloed kan hebben op de samenstelling van het huishouden. Dergelijke meldingen worden digitaal doorgestuurd aan het Meldpunt.**

**** doorstroomschema soc.rech. rapporten en verwerking ****

**** terugmelding BRP? De werkopdracht wordt bij ons geregistreerd? LAA?**

****Het kan ook voorkomen dat de inschrijving in de BRP niet overeenkomt met de opgave van de bewoningssituatie voor het adres, dan moet de feitelijke bewoningssituatie op dat adres worden nagegaan. Indien er op basis van controles gerede twijfel bestaat over de juistheid van de bewoningssituatie, dan dient er een tegenmelding aangemaakt te worden waarna de gemeente een onderzoek kan starten. Indien naar aanleiding van een onderzoek de inschrijving in de BRP wordt aangepast, dan wordt B/T hier automatisch van op de hoogte gesteld.**

**** koo's (koo-viewer/automatisch en handmatig) ****

In artikel 11 van de Regeling Wet kinderopvang (Wko) is opgenomen welke gegevens de administratie van kindercentra en gastouderbureaus moet bevatten en welke gegevens de Belastingdienst (op grond van artikel 38 van de Awir en artikel 1a van het Uitvoeringsbesluit Awir) derhalve kan opvragen.

** Verhuurders (proces VHA en handmatig)

**** DUO

**** UWV

**** Blauw/IB (FLG/ABS)

**** DACAS/COA

**** Bankgegevens

**** BRG

**** Heidi **

4. Verwerkingsdoeleinden



Beschrijf de doeleinden van de voorgenomen gegevensverwerkingen.

[Klik hier om infotekst te verbergen](#)

De privacyregelgeving geeft als beginsel dat persoonsgegevens enkel voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden mogen worden verzameld. De vaststelling van de verwerkingsdoeleinden is een noodzakelijk voorwaarde om te kunnen beoordelen of de voorgenomen gegevensverwerkingen rechtmatig zijn (onder B) en om vast te stellen welke maatregelen moeten worden getroffen om de risico's (onder C) te voorkomen of verkleinen (onder D). Omschrijf daarom per voorgenomen gegevensverwerking de verwerkingsdoeleinden zo specifiek mogelijk.

Bij verwerkingsdoeleinden kan gedacht worden aan: beveiligen van gebouwen en objecten, behandelen van personeelszaken, opsporen van strafbare feiten, direct marketing, het innen van vorderingen, het doen van leveringen en bestellingen, identificatie en authenticatie, het voorbereiden en nemen van Awb-besluiten en het behandelen van geschillen. Denk ook aan eventuele nevendoeleinden van de gegevensverwerking, zoals: wetenschappelijk, statistisch of historisch onderzoek, archiefbeheer, declaratiedoeleinden, rapportagedoeleinden, verbetering van dienstverlening of (door)ontwikkeling van beleid. De verwerkingsdoeleinden moeten zoveel mogelijk worden toegespitst op de concrete gegevensverwerking, waarbij het algemene overkoepelende doel kan worden gebruikt als kapstok waaraan verschillende subdoelen kunnen worden gehangen, bijvoorbeeld:

- e-mailadres: noodzakelijk voor communicatie met 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 betrokken partij in aanmerking komt voor een toeslag;
- strafrechtelijke gegevens: noodzakelijk om een screening te kunnen uitvoeren.

Wanneer de persoonsgegevens niet rechtstreeks bij de betrokkene worden verkregen (met andere woorden: de persoonsgegevens zijn afkomstig van een andere persoon of organisatie dan wel uit een bestaand databestand), is het noodzakelijk om de doeleinden waarvoor de gegevens oorspronkelijk zijn verzameld te herleiden. De privacyregelgeving geeft namelijk als beginsel dat persoonsgegevens niet verder mogen worden verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen. Met andere woorden: de verwerking van persoonsgegevens voor andere doeleinden dan die waarvoor de persoonsgegevens aanvankelijk zijn verzameld, mag enkel indien de verwerking verenigbaar is met de doeleinden waarvoor de persoonsgegevens aanvankelijk

zijn verzameld (zie voor de beoordeling van de verenigbaarheid punt 13 hieronder). Met verdere verwerking wordt bedoeld op gebruik van persoonsgegevens die al eerder voor een bepaald doel zijn verzameld. Denk hierbij aan verstrekkingen van persoonsgegevens aan een andere organisatie die niet oorspronkelijk, ten tijde van het verzamelen van de gegevens, was beoogd.

Bij **conceptregelgeving** wordt het doel van de gegevensverwerking in de regeling zelf vastgelegd of op zijn minst benoemd in de memorie of nota van toelichting. Een wettelijke doelomschrijving bevordert de rechtszekerheid omdat hierdoor een nadere invulling is gegeven aan het beoordelingskader.

Bij **overheidsverwerkingen** stelt de verwerkingsverantwoordelijke het doel van de gegevensverwerkingen zelf vast. Bij overheidsverwerkingen ter uitvoering van regelgeving moet binnen het doel worden gebleven dat daarin is vastgesteld. Het verdient de voorkeur de verwerkingsdoeleinden zoveel mogelijk op het niveau van werk- en organisatieprocessen te enten.

Aantekening:

- *Wat is het concrete doel van de verwerking?*

Typ tekst

4. Betrokken partijen



Benoem welke organisaties betrokken zijn bij welke gegevensverwerkingen. Deel deze organisaties per gegevensverwerking in onder de rollen: verwerkingsverantwoordelijke, verwerker, verstrekker en ontvanger. Benoem tevens welke functionarissen binnen deze organisaties toegang krijgen tot welke persoonsgegevens.

[Klik hier om infotekst te verbergen](#)

Om de rechtmatigheid van de voorgenomen gegevensverwerkingen te kunnen beoordelen, moet inzichtelijk zijn welke organisaties (functioneel) betrokken zijn bij welke gegevensverwerking en in welke hoedanigheid: verwerkingsverantwoordelijke, verwerker, verstrekker of ontvanger.

Verwerkingsverantwoordelijk is de natuurlijke persoon, de rechtspersoon of het overheidsorgaan, die/dat het doel van en de middelen voor de gegevensverwerkingen vaststelt. Met andere woorden: degene die formeel bevoegd is te beslissen of persoonsgegevens worden verwerkt, voor welke doeleinden deze worden verwerkt en op welke wijze deze worden verwerkt. Wanneer twee of meer verwerkingsverantwoordelijken gezamenlijk de doeleinden en middelen van de verwerking bepalen, zijn zij gezamenlijke verwerkingsverantwoordelijke en moeten zij onderling vastleggen wie waarvoor verantwoordelijk en aansprakelijk is.

Verwerker is de natuurlijke persoon, de rechtspersoon of het overheidsorgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt. De verwerker verwerkt persoonsgegevens voor de verwerkingsverantwoordelijke, dat wil zeggen volgens diens instructies en onder diens verantwoordelijkheid. De verwerker is een buiten de organisatie van de verwerkingsverantwoordelijke staande persoon of organisatie. De verwerkingsverantwoordelijke en verwerker moeten onderling schriftelijk vastleggen wie waarvoor verantwoordelijk en aansprakelijk is. Om in een concreet geval te bepalen wie de verwerkingsverantwoordelijke is en wie de verwerker is, moet naast de formele taakverdeling zoals partijen die onderling hebben afgesproken ook worden gekeken naar de feitelijke omstandigheden (waarom vindt de verwerking plaats? Wie heeft deze geïnitieerd?). Dat

betekent dat enkel het schriftelijk vastleggen van de taakverdeling niet voldoende is: ook in de praktijk moet de verwerkingsverantwoordelijke zeggenschap hebben over het doel en de middelen van gegevensverwerkingen.

Ontvanger is de natuurlijke persoon, de rechtspersoon of het overheidsorgaan aan wie/waaraan de persoonsgegevens worden verstrekt. Verstrekker is de natuurlijke persoon, de rechtspersoon of het overheidsorgaan die/dat de persoonsgegevens ter beschikking stelt.

Bij **conceptregelgeving** kan het wenselijk zijn om daarin de hoedanigheid van de betrokken organisaties vast te leggen of volgens welke criteria deze wordt aangewezen. Indien een specifieke regeling over gegevensverwerkingen wordt opgesteld ten behoeve van een publiekrechtelijke taak, dient in de regeling de verwerkingsverantwoordelijke te worden aangewezen. Zo is in de Basisregistratie personen vastgelegd wanneer het college van burgemeester en wethouders en wanneer de minister verantwoordelijk is voor het bijhouden van persoonsgegevens in de basisregistratie. In bepaalde gevallen kan het ook wenselijk zijn om wettelijk voor te schrijven dat de toegang tot bepaalde persoonsgegevens beperkt blijft tot een specifieke functionaris, zoals een officier van justitie, vertrouwenspersoon of bedrijfsarts.

Bij **overheidsverwerkingen** zullen, voor zover niet reeds wettelijk voorgeschreven, de organisaties die (functioneel) betrokken zijn bij de gegevensverwerkingen zelf en in onderling overleg moeten bepalen wie in welke hoedanigheid de persoonsgegevens verwerkt. Tevens zal moeten worden bepaald, voor zover eveneens niet wettelijk voorgeschreven, welke functionarissen binnen deze organisaties toegang krijgen tot welke persoonsgegevens, bijvoorbeeld aan de hand van een autorisatiematrix, in relatie tot de doeleinden van de gegevensverwerking. Hierin kan tevens worden bepaald in welke gevallen en onder welke voorwaarden deze functionarissen toegang krijgen tot de persoonsgegevens.

Aantekening:

- *Geen namen noemen van medewerkers. Alleen de rol/functie.*
- *Er wordt gesproken over derden. Graag specificeren.*

Typ tekst

4. Belangen bij de gegevensverwerking



Beschrijf alle belangen die de verwerkingsverantwoordelijke en anderen hebben bij de voorgenomen gegevensverwerkingen.

[Klik hier om infotekst te verbergen](#)

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 (zie punten 11 en 14 hierna).

Aantekening:

- *Wat zijn de belangen concreet voor de betrokkenen?*

Typ tekst

4. Verwerkingslocaties



Benoem in welke landen de voorgenomen gegevensverwerkingen plaatsvinden.

Typ tekst

4. Techniek en methode van gegevensverwerking



Beschrijf op welke wijze en met gebruikmaking van welke (technische) middelen en methoden de persoonsgegevens worden verwerkt. Benoem of sprake is van (semi-)geautomatiseerde besluitvorming, profilering of big data-verwerkingen en, zo ja, beschrijf waaruit een en ander bestaat.

[Klik hier om infotekst te verbergen](#)

Gebruikmaking van bepaalde technieken en methoden van gegevensverwerking kunnen aanvullende privacyrisico's met zich brengen en daarom onderworpen zijn aan strengere regels en aanvullende maatregelen vereisen. Dit is onder meer het geval bij (semi-)geautomatiseerde besluitvorming, profilering en big data-verwerkingen.

Geautomatiseerde besluitvorming

Uitsluitend op geautomatiseerde verwerking gebaseerde besluiten die voor de betrokkenen rechtsgevolgen hebben of hem anderszins in aanmerkelijke mate treffen, zijn in beginsel verboden.

Voor verwerkingen die onder de werkingssfeer van de AVG vallen, geldt dat dit verbod niet van toepassing indien het besluit:

- noodzakelijk is voor de totstandkoming of de uitvoering van een overeenkomst tussen de betrokkene en een verwerkingsverantwoordelijke;
- is toegestaan bij een Unierechtelijke of lidstaatrechtelijke bepaling die op de verwerkingsverantwoordelijke van toepassing is en die ook voorziet in passende maatregelen ter bescherming van de rechten en vrijheden en

- gerechtvaardigde belangen van de betrokkene; of
- c. berust op de uitdrukkelijke toestemming van de betrokkene.

Bij verwerkingen die vallen onder de werkingssfeer van de Richtlijn geldt dit verbod niet indien het besluit:

- a. wettelijk is toegestaan; en
- b. voorziet in passende waarborgen voor de rechten en vrijheden van de betrokkenen, waaronder ten minste het recht op menselijke tussenkomst.

Profilering

Onder profilering wordt verstaan: elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen.

Bepaalde gegevens, zoals de resultaten van een zoekopdracht met een zoekmachine, kunnen in combinatie met elkaar een risicoprofiel doen ontstaan. De kans hierop bestaat vooral wanneer meerdere registers met elkaar worden gecombineerd. Er kan sprake zijn van profilering wanneer:

- op basis van een combinatie van persoonsgegevens, zoals het automerk in combinatie met de leeftijd van de betrokkene wordt besloten iemand extra te controleren;
- gebruik wordt gemaakt van de gegevens die websitebezoekers achterlaten om de doelgroep van de website mee vast te stellen.

Bij verwerkingen die vallen onder de werkingssfeer van de Richtlijn, geldt dat profilering die leidt tot discriminatie op grond bijzondere persoonsgegevens verboden is.

Big data

Big data is als zodanig niet gedefinieerd in de privacyregelgeving, maar hangt als verschijnsel nauw samen met geautomatiseerde besluitvorming en profilering. *Big data* staat voor het verschijnsel dat grote hoeveelheden gestructureerde en ongestructureerde data uit verschillende bronnen worden geanalyseerd waarbij geautomatiseerd naar correlaties wordt gezocht die kennis kunnen opleveren om te kunnen toepassen voor beslissingen op groeps- of individueel niveau. In de kern komt het bij *big data*-analyses neer op het zoeken naar correlatie (onderlinge samenhang tussen twee reeksen van waarnemingen), in tegenstelling tot causaliteit (betrekking van oorzaak en gevolg). Toepassing van *big data* brengt specifieke risico's mee en vergt daarom ook specifieke maatregelen (zie onder D).

Nieuwe technologieën

Ook grote verschuivingen in de werkwijze, de manier waarop persoonsgegevens worden verwerkt en de technologie die daarbij gebruikt wordt, kunnen gevolgen hebben voor betrokkenen. Denk aan: intelligente volgsystemen op basis van GPS, biometrie en nieuwe vormen van identificatie.

Aantekening:

- *Graag de gebruikte systemen/applicaties en de bijbehorende technische- en organisatorische maatregelen beschrijven. Hoe krijgt men toegang tot de gegevens?*

- *Er wordt genoemd dat er geen sprake is van profilering, geautomatiseerde besluitvorming. Wat is de relatie met proces M840? Hoe zit dat met de analyses op IP-adressen?*
- *Wat houdt de uitsluitlijst in? Is dit hetzelfde als een zwarte lijst? Wordt deze lijst gedeeld met anderen?*

Typ tekst

4. Juridisch en beleidsmatig kader



Benoem de wet- en regelgeving, met uitzondering van de AVG en de Richtlijn, en het beleid met mogelijke gevolgen voor de gegevensverwerkingen.

Aantekening:

- *Graag specificeren met wetsartikelen waarin de bevoegdheid m.b.t. het verwerken van gegevens is vastgelegd.*

Het behandelen van fraude signalen heeft als doel toezicht te houden op de naleving van de Awir (artikel 43 Awir). De in hoofdstuk 2 opgesomde gegevens worden verwerkt vanwege de uitvoering van deze wettelijke taak door B/T.

B/T is belast met het toekennen, uitbetalen en terugvorderen van de huurtoeslag en de kinderopvangtoeslag (artikel 11, tweede lid, Algemene wet inkomensafhankelijke regelingen (AWIR); artikel 1.3, eerste lid, Wet kinderopvang (Wko); artikel 1a, tweede lid, Wet op de huurtoeslag). Daarnaast is B/T belast met het uitvoeren van de zorgtoeslag en het kindgebonden budget (artikel 5, eerste lid, Wet op het kindgebonden budget en artikel 5, eerste lid, Wet op de zorgtoeslag).

De kinderopvangtoeslag en de huurtoeslag vallen onder de werking van de Awir (artikel 1.3, tweede lid, Wko en artikel 1a, eerste lid Wet op de huurtoeslag). Ten aanzien van de systematiek van toeslagen is in de Awir het volgende geregeld. In artikel 14, eerste lid, Awir bepaald dat een toeslag op aanvraag wordt toegekend en in artikel 15, vijfde lid, Awir dat een aanvraag geacht wordt ook te zijn gedaan voor de volgende berekeningsjaren.

Na afloop van het berekeningsjaar wordt het recht (definitief) vastgesteld (artikel 19 Awir). Als voorschotten zijn verleend, worden deze verrekend met het definitief vastgestelde bedrag, en deze verrekening kan leiden tot een terug te vorderen bedrag (artikel 24, tweede en derde lid, Awir). Als een voorschot is verleend, is de aanvrager verplicht bepaalde wijzigingen door te geven (artikel 17 Awir jo. artikel 5 Uitvoeringsregeling Awir). Daarnaast is een aanvrager, partner of medebewoner verplicht mogelijk relevante gegevens en inlichtingen te verstrekken, als B/T daarom vraagt (art. 18 Awir).

De hoogte van de toeslagen is onder andere afhankelijk van de draagkracht van de aanvrager, de eventuele toeslagpartner en de eventuele medebewoner. Hiervoor wordt het toetsingsinkomen in aanmerking genomen (artikel 7, eerste lid, Awir; artikel 1.7, eerste lid onderdeel a, Wko; artikel 7 eerste lid, Wet op de huurtoeslag; artikel 1, tweede lid, Wet op het kindgebonden budget en artikel 1, tweede lid, Wet op de zorgtoeslag). Daarnaast is voor de kinderopvangtoeslag de

hoogte afhankelijk van de kosten van kinderopvang, waaronder het aantal uren afgenomen kinderopvang (artikel 1.7, eerste lid onderdeel b, Wko). Voor de huurtoeslag is de hoogte ook afhankelijk van de onder andere de rekenhuur (artikel 21, eerste lid wet op de huurtoeslag). Om die reden dienen relevante wijzigingen in deze omstandigheden binnen vier weken door aan B/T te worden doorgegeven (artikel 5 Uitvoeringsregeling Awir). Als deze wijzigingen echter niet (tijdig) worden doorgegeven, dan kan er een te hoog voorschot zijn verleend, dat door de B/T moet worden teruggevorderd (artikel 26 Awir).

Publiekrechtelijke organisaties, zoals DUO en UWV, en aangewezen andere personen en organisaties zijn verplicht om gegevens en inlichtingen aan B/T te verstrekken waarvan de kennisneming van belang kan zijn voor de uitvoering van de Awir (artikel 38, eerste lid, Awir). In artikel 1a, eerste lid, onderdeel b, van het Uitvoeringsbesluit Awir zijn de kinderopvangorganisaties aangewezen voor de levering van de gegevens, bedoeld in artikel 11, eerste lid, onderdeel b, van de Regeling Wko.

Als uit de gegevens van de publiekrechtelijke organisaties blijkt dat de burger gegevens niet, niet tijdig of onjuist heeft doorgegeven kan B/T het voorschot herzien (artikel 16, vijfde lid Awir). Indien de toeslag reeds definitief is vastgesteld heeft B/T in twee gevallen de bevoegdheid om de toeslag te herzien. Dat is wanneer op grond van feiten of omstandigheden waarvan de Belastingdienst/Toeslagen bij de toekenning redelijkerwijs niet op de hoogte kon zijn en op grond waarvan de tegemoetkoming vermoedelijk tot een te hoog bedrag is toegekend, of indien de tegemoetkoming tot een te hoog bedrag is toegekend en de belanghebbende of zijn partner dit wist of behoorde te weten (artikel 21, eerste lid onder a en b, Awir).

Daarnaast kan bij het niet of niet tijdig verstrekken van gegevens of inlichtingen en het opzettelijk of grof schuldig verstrekken van geen, onjuiste of onvolledige gegevens of inlichtingen er door B/T een bestuurlijke boete worden opgelegd (artikelen 40 en 41 Awir en Besluit Bestuurlijke Boeten/Toeslagen). Met dien verstande dat wanneer er sprake is van vrijwillige verbetering B/T geen bestuurlijke boete kan opleggen (artikel 42 Awir). Bij het opleggen van de boete dient B/T rekening te houden met eventuele straf verminderende omstandigheden (paragraaf 7 Besluit Bestuurlijke Boeten Belastingdienst/Toeslagen). Hiertoe kunnen ook de financiële omstandigheden van de belanghebbende behoren.

Aanmelding voor mogelijke strafrechtelijke afhandeling kan plaatsvinden als sprake is van 'nadeel' van bepaalde omvang (onderdeel 2.1 Protocol AAFD). Dat is het bedrag dat door de in of over de onderzoeksperiode gepleegde feiten die daartoe strekten, te weinig is of zou zijn gegeven of teveel is of zou zijn toegekend als de aangifte of aanvraag van belanghebbende was gevolgd. Ook geldt als nadeel de niet, gedeeltelijk niet, dan wel niet binnen de in de belastingwet gestelde termijn, betaling van belasting welke op aangifte moet worden voldaan of afgedragen. Het begrip nadeel sluit aan bij – en heeft dezelfde inhoud als – het 'strekingsvereiste' in artikel 69 Algemene wet inzake rijksbelastingen.

Volledigheidshalve wordt opgemerkt dat voor het vaststellen van de omvang van het fiscaal nadeel ook rekening wordt gehouden met een (te hoog) aangegeven verlies dat in het desbetreffende (boek)jaar geleden zou zijn.

Bij een nadeelbedrag van € 100.000 of meer, wordt de zaak aangemeld voor mogelijke strafrechtelijke afhandeling als sprake is van een vermoeden van opzet (Wetboek van Strafvordering in artikel 27 lid 1). Bedraagt het nadeel minder dan € 100.000, dan wordt de zaak voor mogelijke strafrechtelijke afhandeling aangemeld als sprake is van een vermoeden van opzet en als een of meerdere van de aanvullende wegingscriteria daartoe aanleiding geeft (onderdeel 2.2 Protocol AAFD).

Als sprake is van een vermoeden van het begaan van één van de feiten zoals beschreven in de artikelen 69 en 69a AWR, dan bespreken de Belastingdienst en het Openbaar Ministerie de mogelijkheid van het opleggen van een fiscale strafbeschikking in een afstemmingsoverleg (onderdeel 3 Protocol AAFD).

5. Bewaartermijnen



Bepaal en motiveer de bewaartermijnen van de persoonsgegevens aan de hand van de verwerkingsdoeleinden.

Aantekening:

- Wat wordt er vernietigd? Hoe gaat dat?

Typ tekst

B. Beoordeling rechtmatigheid gegevensverwerkingen

Beoordeel aan de hand van de feiten zoals vastgesteld in onderdeel A of de voorgenomen gegevensverwerkingen rechtmatig zijn. Het gaat hier om de beoordeling van de juridische rechtsgrond, noodzaak en doelbinding van de gegevensverwerkingen. Beoordeel tevens de wijze waarop invulling wordt gegeven aan de rechten van de betrokkenen. Voor dit onderdeel van de PIA is in het bijzonder juridische expertise nodig.

6. Rechtsgrond



Bepaal op welke rechtsgronden de gegevensverwerkingen worden gebaseerd.

[Klik hier om infotekst te verbergen](#)

De AVG geeft als beginsel dat persoonsgegevens moeten worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is. Als uitwerking van dit beginsel is geregeld dat een gegevensverwerking alleen rechtmatig is indien deze gebaseerd kan worden op ten minste één van de volgende zes rechtsgronden:

- de betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden;
- de verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen;
- de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust;
- de verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon

te beschermen;

- e. de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen;
- f. de verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is.

Of de gegevensverwerkingen noodzakelijk zijn, wordt beoordeeld onder punt 14.

Ten aanzien van de rechtsgronden c (wettelijke plicht) en e (taak van algemeen belang) geldt dat deze moet worden vastgesteld bij of krachtens de wet. De wettelijke verplichting (rechtsgrond c) hoeft niet noodzakelijkerwijs te bestaan uit een expliciete verplichting om persoonsgegevens te verwerken. Ook is mogelijk dat de verwerking van persoonsgegevens een basis vindt in een ruimer geformuleerde zorgplicht of wettelijke verplichting. Zonder verwerking van de persoonsgegevens moet het uitvoeren van een wettelijke verplichting redelijkerwijs niet goed mogelijk zijn. Met betrekking tot rechtsgrond e (de taak van algemeen belang) geldt dat deze taak zal moeten blijken uit regelgeving die op de verwerkingsverantwoordelijke van toepassing is. Niet noodzakelijk is dat in de regelgeving ook expliciet is opgenomen dat ten behoeve van de vervulling van de wettelijke taak gegevens verwerkt mogen worden. Indien het noodzakelijk is om voor de uitvoering van de publieke taak persoonsgegevens te verwerken, kan de wettelijke grondslag voor de publieke taak tevens worden beschouwd als grondslag voor de verwerking van persoonsgegevens.

De Richtlijn gegevensbescherming opsporing en vervolging voor dat een gegevensverwerking door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid alleen rechtmatig is indien die verwerking gebaseerd is op de wet.

Bij **conceptregelgeving** zal de regeling veelal tot gevolg hebben dat de verwerkingsverantwoordelijke de gegevensverwerking kan baseren op de rechtsgrond genoemd onder c (wettelijke verplichting). Dit is het geval indien de gegevensverwerking noodzakelijk is ter uitvoering van de wettelijke verplichting en indien de verwerkingsverantwoordelijke belast is met de uitvoering van de wettelijke plicht. Daarnaast kan regelgeving tot gevolg hebben dat een overheidsorgaan de gegevensverwerking kan baseren op de rechtsgrond genoemd onder e (taak van algemeen belang). De publieke taak wordt (of is reeds) wettelijk vastgelegd waarbij, naast andere onderwerpen, volgens de Aanwijzingen voor de regelgeving ook aandacht moet worden geschonken aan de daarbij noodzakelijke gegevensverwerkingen. In regelgeving kan ook worden voorgeschreven dat toestemming van de betrokkene vereist is om persoonsgegevens te verwerken, en daarmee de andere rechtsgronden uitsluiten.

Bij **overheidsverwerkingen** zal het overheidsorgaan de voorgenomen gegevensverwerkingen moeten baseren op één van de zes rechtsgronden. De rechtsgrond genoemd onder f geldt niet voor gegevensverwerkingen in het kader van de uitoefening van publieke taken. Wel kan deze rechtsgrond gebruikt worden voor gegevensverwerkingen in de bedrijfsvoering, zoals cameratoezicht, bezoekersregistratie en toegangscontrole. In veel situaties zal de rechtsgrond genoemd onder a (toestemming) evenmin kunnen dienen als rechtsgrond voor gegevensverwerkingen door overheidsorganen, omdat de betrokkene in de gegeven situatie niet vrijelijk toestemming kan geven.

Indien de gegevensverwerkingen gebaseerd worden op de rechtsgrond genoemd onder f (het gerechtvaardigd belang van de verwerkingsverantwoordelijke of een derde), dan stelt de AVG als eis dat de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene niet zwaarder mogen wegen dan de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of de derde.

Aantekening:

- *Worden er i.v.m. toelagen niet meer bijzondere persoonsgegevens verwerkt zoals gezondheidsgegevens en religieuze gegevens?*

Typ tekst

6. Bijzondere persoonsgegevens



Indien bijzondere of strafrechtelijke persoonsgegevens worden verwerkt, beoordeel of één van de wettelijke uitzonderingen op het verwerkingsverbod van toepassing is. Bij verwerking van een wettelijk identificatienummer beoordeel of dat is toegestaan.

[Klik hier om infotekst te verbergen](#)

De AVG verbiedt de verwerking van bijzondere persoonsgegevens. Op dit verwerkingsverbod gelden de volgende uitzonderingen:

- de betrokkene heeft uitdrukkelijke toestemming gegeven;
- de verwerking is noodzakelijk met het oog op de uitvoering van verplichtingen en de uitoefening van specifieke rechten op het gebied van arbeids- en sociaalzekerheidsrecht;
- de verwerking is noodzakelijk ter bescherming van vitale belangen van de betrokkenen of een ander;
- de verwerking wordt verricht door een instantie die op politiek, levensbeschouwelijk, godsdienstig of vakbondsgebied werkzaam is;
- de verwerking betrekking heeft op persoonsgegevens die kennelijk door de betrokkene openbaar zijn gemaakt;
- de verwerking noodzakelijk is voor de instelling, uitoefening of onderbouwing van een rechtsvordering;
- de verwerking noodzakelijk is om redenen van zwaarwegend algemeen belang;
- de verwerking noodzakelijk is voor preventieve en arbeidsgeneeskunde, voor de beoordeling van de arbeidsgeschiktheid, medische diagnoses, het verstrekken van gezondheidszorg of sociale diensten of behandelingen dan wel het beheren van gezondheidszorgstelsels en –diensten of sociale stelsel en diensten;
- de verwerking noodzakelijk is om redenen van algemeen belang op het gebied van de volksgezondheid;
- de verwerking noodzakelijk is met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden.

Verdere uitzonderingen zijn te vinden in nationale regelgeving.

De AVG bepaalt daarnaast dat verwerking van strafrechtelijke gegevens alleen is toegestaan door of onder toezicht van de overheid of als dit bij wet geregeld is (zie voor de definitie van strafrechtelijke gegevens de toelichting bij punt 2).

De verwerking van nationale identificatienummers is alleen toegestaan ter uitvoering van de wet of voor doeleinden die bij wet zijn bepaald. Overheidsorganen kunnen bij de uitvoering van hun publieke taak gebruik

maken van het burgerservicenummer, zonder dat daarvoor nadere regelgeving vereist is.

De Richtlijn schrijft voor dat verwerking van bijzondere persoonsgegevens slechts is toegestaan wanneer de verwerking strikt noodzakelijk is, geschiedt met inachtneming van passende waarborgen voor de rechten en vrijheden van betrokkene, en:

- a. wettelijk is toegestaan;
- b. noodzakelijk is om vitale belangen van de betrokkene of een andere natuurlijke persoon te beschermen; of
- c. die verwerking betrekking heeft op gegevens die kennelijk door de betrokkene zelf openbaar zijn gemaakt.

Bij conceptregelgeving kan van het verbod op de verwerking van bijzondere of strafrechtelijke persoonsgegevens worden afgeweken, mits passende waarborgen worden geboden ter bescherming van persoonsgegevens en andere grondrechten van de betrokkene.

Aantekening:

- Worden er ook niet gezondheidsgegevens verwerkt?

Typ tekst

6. Doelbinding



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.

[Klik hier om Infotekst te verbergen](#)

De privacyregelgeving geeft als beginsel dat persoonsgegevens voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden moeten worden verzameld en vervolgens niet verder mogen worden verwerkt op een met die doeleinden onverenigbare wijze.

De AVG regelt dat de verdere verwerking voor een ander doel toegestaan is indien de verdere verwerking berust op toestemming van de betrokkene of op een specifiek wettelijk voorschrift, dat een noodzakelijke en evenredige maatregel is in een democratische samenleving ter waarborging van een belangrijke doelstelling van algemeen belang, bijvoorbeeld de nationale veiligheid, de openbare veiligheid, monetaire, budgettaire of fiscale aangelegenheden. Daarnaast wordt de verdere verwerking ten behoeve van archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden als verenigbaar geacht met de oorspronkelijke doeleinden. Hieraan wordt wel de eis verbonden dat passende maatregelen worden getroffen om de betrokkene te beschermen.

Bij conceptregelgeving moet worden beoordeeld of het noodzakelijk is om wettelijk te regelen dat verdere verwerking toegestaan is (zie ook punt 14 hierna), bijvoorbeeld in verband met de doorbreking van een geheimhoudingsplicht.

Binnen het hierboven geschetste kader voor verwerking voor een ander doel bestaat ruimte voor een wettelijke

regeling op grond waarvan sets van persoonsgegevens van meerdere partijen uit meerdere domeinen worden gecombineerd ten behoeve van een big data analyse, waarbij gegevens worden verwerkt ten behoeve van een in die wettelijke regeling vastgesteld doeleinde, dat niet met het oorspronkelijke doel waarvoor de gegevens zijn verzameld, verenigbaar is. Dit laat onverlet dat de verwerkingsverantwoordelijke die beslissingen neemt ten aanzien van individuele personen of een groep van personen op basis van de uitkomsten van die analyse zelfstandig moet voldoen aan alle eisen voor rechtmatige gegevensverwerking. Een dergelijke verwerking dient op een eigen rechtsgrond te berusten (zie punt 11).

Bij **overheidsverwerkingen** moet de verwerkingsverantwoordelijke zelf beoordelen of de verdere gegevensverwerking voor een ander doel toegestaan en verenigbaar is aan de hand van:

- het verband tussen de doeleinden waarvoor de persoonsgegevens zijn verzameld en de doeleinden van de voorgenomen verdere verwerking;
- de context waarin de persoonsgegevens zijn verzameld, met name wat de verhouding tussen de betrokkene en de verwerkingsverantwoordelijke betreft;
- de aard van de persoonsgegevens, met name bijzondere of strafrechtelijke persoonsgegevens;
- de mogelijke gevolgen van de voorgenomen verdere verwerking voor de betrokkene;
- het bestaan van passende waarborgen.

De Richtlijn staat de verdere verwerking van persoonsgegevens toe voor een doelstelling die binnen het toepassingsgebied van de Richtlijn valt, niet zijnde die waarvoor zij zijn verzameld, voor zover:

- de verwerkingsverantwoordelijke overeenkomstig de wet gemachtigd is deze persoonsgegevens voor een dergelijk doel te verwerken; en
- de verwerking noodzakelijk is en in verhouding staat tot dat andere doel.

De verdere verwerking voor andere doeleinden is enkel op basis van de wet toegestaan. Wanneer de persoonsgegevens voor zulke andere doeleinden worden verwerkt, is de AVG van toepassing.

Aantekening:

- *Wat is het doel van het verzamelen van de gegevens? Is dit doel gelijk aan het originele verwerkingsdoel? Worden deze gegevens vervolgens verwerkt voor een ander doel dan het originele verwerkingsdoel?*
- *Er wordt aangegeven dat na een query/data-analyse meerdere gegevens worden onderzocht. Welke gegevens zijn dat? Waarom is dat?*
- *Wat is de grondslag waarop het BSN wordt verwerkt?*
- *Hoe werkt dat met de toezichtlijst?*
- *Op welke manier worden posten verwijderd van de toezichtlijst? Wie beoordeelt dat?*

Typ tekst

6. Noodzaak en evenredigheid



Beoordeel of de voorgenumen gegevensverwerkingen noodzakelijk zijn voor het verwezenlijken van de verwerkingsdoeleinden. Ga hierbij in ieder geval in op proportionaliteit en subsidiariteit.

- a. Proportionaliteit: staat de inbreuk op de persoonlijke levenssfeer en de bescherming van de persoonsgegevens van de betrokkenen in evenredige verhouding tot de verwerkingsdoeleinden?**
- b. Subsidiariteit: kunnen de verwerkingsdoeleinden in redelijkheid niet op een andere, voor de betrokkene minder nadelige wijze, worden verwezenlijkt?.**

Aantekening:

- *Het verwerkingsdoel is niet gespecificeerd.*
- *Hoe zit het de toezichtlijst?*
- *Is het analyseren van IP-adressen in verhouding met het doel? Is deze verwerking noodzakelijk? Er worden nog meer analyses gedaan hoe zit het daarmee. Daarnaast worden er meer gegevens verwerkt dan gespecificeerd in de DPIA.*
- *Wat is de reikwijdte van het inzien van strafrechtelijke gegevens van een burger? Tot hoever kan/wordt er terug gekeken? Wie kan dit inzien? Worden deze exacte gegevens bijgehouden/geregistreerd?*

Typ tekst

6. Rechten van de betrokkene



Geef aan hoe invulling wordt gegeven aan de rechten van betrokkenen. Indien de rechten van de betrokkene worden beperkt, bepaal op grond van welke wettelijke uitzonderingen dat is toegestaan.

[Klik hier om infotekst te verbergen](#)

Betrokkenen hebben op grond van de privacyregelgeving diverse rechten, waarin ook staat op welke wijze en onder welke omstandigheden zij die rechten kunnen uitoefenen. Het betreft het recht op informatie, het recht van inzage, het recht op rectificatie, het recht op gegevenswissing, het recht op beperking van de verwerking, een kennisgevingsplicht inzake rectificatie of wissing van persoonsgegevens, het recht op overdraagbaarheid van gegevens, het recht van bezwaar en het recht om niet onderworpen te worden aan een uitsluitend op geautomatiseerde verwerking gebaseerd besluit. Er zijn uitzonderingen mogelijk op de uitoefening van deze rechten, op voorwaarde dat de wezenlijke inhoud van de grondrechten en fundamentele vrijheden niet wordt aangetast en dat het gaat om noodzakelijke en evenredige maatregelen ter waarborging van enkele expliciet opgesomde belangrijke doelstellingen van algemeen belang. Uitzonderingen moeten altijd op een nationale wet berusten, direct zijn toegestaan op grond van de bepalingen in de Europese privacyregelgeving.

Indien in conceptregelgeving een uitzondering wordt gemaakt op de rechten van betrokkenen moet worden beoordeeld of dit is toegestaan op in de privacyregelgeving genoemde gronden én moeten specifieke bepalingen worden opgenomen met betrekking tot ten minste:

- a. de verwerkingsdoeleinden;
- b. de categorieën van persoonsgegevens;

- c. het toepassingsgebied van de ingevoerde beperkingen;
- d. de waarborgen ter voorkoming van misbruik of onrechtmatige toegang of doorgifte
- e. de specificatie van de verwerkingsverantwoordelijke of de categorieën van verwerkingsverantwoordelijken;
- f. de opslagperiodes en de toepasselijke waarborgen;
- g. de risico's voor de rechten en vrijheden van betrokkenen;
- h. het recht van betrokkenen om over de beperking te worden geïnformeerd, tenzij dit afbreuk kan doen aan het doel van de beperking.

Geef bij **overheidsverwerkingen** aan hoe invulling wordt gegeven aan de rechten van betrokkenen, bijvoorbeeld op welke wijze de betrokkenen worden geïnformeerd en hoe wordt omgegaan met een aanvraag voor correctie en wissing van gegevens. Indien de verwerkingsverantwoordelijke uitzonderingen wil maken op de uitoefening van bepaalde rechten van betrokkenen, geef aan waarom dat noodzakelijk is en op welke grond dat is toegestaan.

Aantekening:

- *Waarom wordt de bescherming van de persoonsgegevens ingeperkt?*
- *Graag de rechten op grond van de Avg benoemen. Welke procedure is hiervoor ingericht?*
- *Waarom blijft de burger in FSV (wat is FSV?) staan als deze in het gelijk gesteld is?*

Typ tekst

C. Beschrijving en beoordeling risico's voor de betrokkenen

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 gegevensverwerking zoals in onderdeel A en B zijn beschreven en beoordeeld. Het gaat hierbij overigens niet om de risico's van de verwerkingsverantwoordelijke zelf.

7. Risico's



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

- a. welke negatieve gevolgen de gegevensverwerkingen kunnen hebben voor de rechten en vrijheden van de betrokkenen;**
- 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.**

[Klik hier om infotekst te verbergen](#)

Volgens de privacyregelgeving dient een PIA een beoordeling van risico's voor de rechten en vrijheden van de

betrokkenen te bevatten. Aan de hand van de aard, het toepassingsgebied, de context en de doeleinden van de gegevensverwerking dient de waarschijnlijkheid en de ernst van het risico voor de rechten en vrijheden van de betrokkenen te worden bepaald. Op basis van een objectieve beoordeling kan vastgesteld worden of de gegevensverwerking gepaard gaat met een (hoog) risico. Hiervoor is het nodig om de oorsprong, de aard, het specifieke karakter en de ernst van dat risico te evalueren.

Het gaat hier om een risicogerichte benadering die kan bestaan uit de volgende stappen:

1. risico's identificeren;
2. risico's inschatten/analyseren;
3. risico's beoordelen/evalueren.

Deze benadering zal in grote lijnen vergelijkbaar zijn met een risicoafweging in het kader van informatiebeveiliging. Daarom kan ook gebruik gemaakt worden van informatie die daaruit naar voren is gekomen. Anders dan bij deze risicoafweging die gericht is op de betrouwbaarheidseisen voor informatiesystemen, en daarmee de risico's voor de verantwoordelijke (zoals aanpassing, vertrouwen, publiciteit, toezicht en handhaving, dienstverlening, betrouwbare informatie), ziet de risicoafweging van de PIA op de risico's voor de betrokkenen.

De privacyregelgeving schrijft niet voor op welke wijze de risicoanalyse moet worden uitgevoerd. Het verdient aanbeveling om aan te sluiten bij internationale standaarden, bijvoorbeeld van de International Organization of Standardization (ISO), Eenduidige Normatiek Single Information Audit (ENSIA) en Organisation for Economic Co-operation and Development (OECD).

1. Risico's identificeren

De eerste stap is om potentiële privacyrisico's vast te stellen. Een privacyrisico is een kans op het optreden van een negatief gevolg voor de rechten en vrijheden van de betrokkenen als gevolg van de verwerking van persoonsgegevens.

Bij rechten en vrijheden van de betrokkenen moet in eerste instantie aan het recht op privacy worden gedacht, maar ook aan andere fundamentele rechten en vrijheden, zoals de vrijheid van meningsuiting, de vrijheid van godsdienst en het verbod van discriminatie. Het voordoen van de (hypothetische) situatie kan leiden tot lichamelijke, materiële of immateriële schade voor de betrokkene. Hierbij kan gedacht worden aan de volgende situaties:

- waar de gegevensverwerking kan leiden tot:
 - discriminatie, stigmatisering en uitsluiting;
 - (blootstelling aan) identiteitsdiefstal of -fraude;
 - financiële verliezen;
 - reputatie- of anderszins relationele schade;
 - verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens;
 - ongeoorloofde ongedaanmaking van pseudonimisering;
 - of enig ander aanzienlijk economisch of maatschappelijk nadeel voor de natuurlijke persoon in kwestie;
- wanneer de betrokkenen hun rechten en vrijheden niet kunnen uitoefenen of worden verhinderd om controle over hun persoonsgegevens uit te oefenen;
- wanneer bijzondere of strafrechtelijke persoonsgegevens worden verwerkt;
- wanneer persoonlijke aspecten worden geëvalueerd, om bijvoorbeeld beroepsprestaties, economische

- situatie, gezondheid, persoonlijke voorkeuren of interesses, betrouwbaarheid of gedrag, locatie of verplaatsingen te analyseren of te voorspellen, teneinde persoonlijke profielen op te stellen of te gebruiken;
- wanneer persoonsgegevens van kwetsbare personen, zoals kinderen, worden verwerkt; of
- wanneer de verwerking een grote hoeveelheid persoonsgegevens betreft en gevolgen heeft voor een groot aantal betrokkenen.

2. Risico's inschatten

Vervolgens moeten de benoemde risico's worden gekwalificeerd door het inschatten van de kans dat een dreiging zich voordoet en de mogelijke gevolgen daarvan voor de betrokkenen. Met andere woorden: wat zijn de gevreesde gevolgen en hoe groot is de impact daarvan op de betrokkenen? En hoe treden deze in werking en hoe waarschijnlijk is dat? Deze vragen zijn niet gericht op zwart-wit antwoorden, maar op een afweging. Aan de hand hiervan moet een risiconiveau worden bepaald.

De impact/ernst van de risico's hangt af van de context van de verwerkingen: de aard van de persoonsgegevens, de aard van de verwerkingen en de doeleinden waarvoor de gegevens worden verwerkt.

De kans dat de risico's zich voltrekken is mede afhankelijk van de middelen die de verwerkingsverantwoordelijke gebruikt bij de gegevensverwerking. Alsook van de aard van de persoonsgegevens.

Persoonsgegevens die de sleutel vormen voor toegang tot geldelijke middelen of waarmee een betrokkene te chanteren is, zijn aantrekkelijk voor hackers. Denk hierbij aan de inloggegevens voor DigiD of een datingwebsite.

De kans dat zich gevolgen voordoen voor de rechten en vrijheden van de betrokkenen, kan tevens verband houden met de (mate van) beveiliging van de persoonsgegevens. De al dan niet opzettelijke:

- vernietiging en verlies (beschikbaarheid);
- wijziging (integriteit);
- ongeoorloofde toegang en verstrekking (vertrouwelijkheid);

van persoonsgegevens, kan leiden tot schade voor de betrokkene.

Voor het inschatten van de risico's kan het behulpzaam zijn om de betrokkenen of hun vertegenwoordigers te consulteren.

Big data-verwerkingen kunnen specifieke risico's voor de betrokkene met zich brengen. Zo kan een algoritme een correlatie ontdekken die weliswaar in statistische zin logisch is, maar die kan leiden tot vooroordelen en stereotypering, discriminatie en sociale uitsluiting of anderszins impact heeft op de betrokkenen, bijvoorbeeld bij sollicitaties, het aangaan van leningen en afsluiten van verzekeringen.

Ook bestaat het risico dat de betrokkene onderworpen is aan big data-besluitvorming die hij niet begrijpt en waar hij geen invloed op heeft.

3. Risico's beoordelen

Definieer aanvaardbare risicowaarden en beoordeel of de risico's aanvaardbaar zijn.

Aantekening:

- *Graag de risico's benoemen m.b.t. de verwerkingen.*

- *Punt 1: Zie vorige opmerking. Dit is een overmatige verwerking. Indien een burger in het gelijk gesteld is en toch in dat systeem blijft staan en daar analyses op uitgevoerd worden.*
- *Punt 2: 'ongeacht of dat daadwerkelijk zo is'. Waarom gebeurt dit dan toch? Op basis waarvan wordt: 'die kans is niet groot' beoordeeld?*
- *Punt 3: maar als een burger onterecht in FSV blijft staan is die kans wel groot?*
- *Punt 4: waarom is dat risico niet groot? wat is het risico van het verwerken van deze gegevens?*
- *Punt 5: waarom is dat risico niet groot? Wat is het risico van het verwerken van deze gegevens?*
- *Punt 6: risico registratie in PSF?*

Typ tekst

D. Beschrijving voorgenomen maatregelen

In onderdeel D wordt gezien welke maatregelen kunnen worden getroffen om de in onderdeel C erkende risico's te voorkomen of te verminderen. Welke maatregelen in redelijkheid worden getroffen is een belangenafweging van de wetgever of verwerkingsverantwoordelijke. Voor dit onderdeel van de PIA is, als het gaat om beveiligingsmaatregelen, expertise over informatiebeveiliging belangrijk.

8. Maatregelen



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 en wat het restrisico is na het uitvoeren van de maatregel. Indien de maatregel het risico niet volledig afdekt, motiveer waarom het restrisico acceptabel is.

[Klik hier om infotekst te verbergen](#)

Denk bij maatregelen bijvoorbeeld aan: het extra informeren van de betrokkenen, een extra keuze-, inspraak- of bezwaarmogelijkheid voor de betrokkenen, periodieke controles, toezicht verstevigen, verhogen bewustwording en dataminimalisatie.

Daarnaast kunnen de maatregelen ook beveiligingsmaatregelen omvatten. De privacyregelgeving geeft als beginsel dat persoonsgegevens door het nemen van passende technische en organisatorische maatregelen op een dusdanige manier wordt verwerkt dat een passende beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.

De verwerkingsverantwoordelijk moet passende technische en organisatorische maatregelen treffen om een op het risico afgestemd beveiligingsniveau te waarborgen. In het begrip passend ligt besloten dat de beveiliging in

overeenstemming is met de stand van de techniek. Het begrip passend duidt mede op een proportionaliteit tussen de maatregelen en erkende privacyrisico's. Naarmate de risico's groter zijn, worden zwaardere eisen gesteld aan de beveiliging van de persoonsgegevens. Er is geen verplichting om altijd de zwaarste beveiliging te nemen. Enkel is vereist dat de maatregelen met het oog op de beschikbare technologie en uitvoeringskosten redelijk zijn. Deze maatregelen moeten het risico tot een aanvaardbaar niveau brengen. Beveiligingsrisico's volledig reduceren is niet mogelijk. Dit betekent dat er altijd een restrisico zal overblijven. De verwerkingsverantwoordelijke dient te beschrijven hoe hij tot dit restrisico is gekomen en waarom dit aanvaardbaar wordt geacht. Een passend beveiligingsniveau veronderstelt dat gewerkt wordt met een planning- en controlcyclus (plan-do-check-act) aan de hand waarvan kan worden beoordeeld of de beveiliging steeds adequaat is voor de huidige stand van de techniek en de organisatie.

Voor te treffen maatregelen kan worden aangehaakt bij beveiligingskaders en -standaarden, beste praktijken en goedgekeurde gedragscodes en certificeringsmechanismen.

Ter illustratie noemt de AVG de volgende maatregelen:

- a. pseudonimiseren en versleutelen van persoonsgegevens;
- b. het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;
- c. het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;
- d. een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.

Daarnaast kan worden gedacht aan de volgende maatregelen, mede bedoeld om ervoor te zorgen dat persoonsgegevens, gelet op de doeleinden waarvoor ze worden verwerkt, juist en nauwkeurig zijn:

- fysieke maatregelen voor toegangsbeveiliging en logische toegangscontrole;
- opslag van gegevens in een kluis;
- project-, risico- en incidentenmanagement;
- data opsplitsen;
- dataminimalisatie;
- back-ups;
- integriteitscontroles;
- meerfactor-authenticatie;
- monitoring en logging;
- controle van toegekende bevoegdheden;
- privacybewustzijn- en beveiligingstrainingen;
- managementrapportages over risicobeheer;
- beperken inzageniveau;
- periodiek een audit of hack- of penetratietest uitvoeren;
- richtlijnen inzake gebruik ICT-hulpmiddelen, zoals versleutelde USB-sticks en beveiligde opslagplekken;
- responsible-disclosurebeleid;
- geheimhoudingsverklaringen;
- service level agreements (met boeteclausules);
- verwerkersovereenkomsten;
- screening personeel en VOG-verklaring.

Bij het bepalen van de gepaste maatregelen moet ook rekening gehouden worden met maatregelen die

voortvloeien uit de Baseline Informatiebeveiliging Rijksdienst (BIR).

De Richtlijn noemt tot slot de volgende maatregelen:

- a. controle op de toegang tot de apparatuur;
- b. controle op de gegevensdragers;
- c. opslagcontrole;
- d. gebruikscntrole
- e. controle op de toegang tot gegevens;
- f. transmissiecontrole;
- g. invoercontrole;
- h. transportcontrole; en
- i. herstelbaarheid.

De Richtlijn verplicht tot het bijhouden van logbestanden van bepaalde vormen van verwerkingen, opdat het mogelijk is de reden, datum en het tijdstip van die handelingen te achterhalen en indien mogelijk de identiteit van de persoon die de persoonsgegevens heeft geraadpleegd of bekendgemaakt, en de identiteit van de ontvangers van die persoonsgegevens.

Bij **conceptregelgeving**: ook op het niveau van regelgeving kunnen maatregelen worden getroffen. Denk hierbij aan het voorschrijven van maximum bewaartermijnen, het beperken van inzage in en besluiten over persoonsgegevens tot bepaalde functionarissen of geheimhoudingsverplichtingen.

Big Data

Bij Big data-analyses (zie punt 8) waarbij persoonsgegevens worden verwerkt, dient, gelet op de daarmee gepaard gaande risico's, in het bijzonder aandacht te worden besteed aan het treffen van de volgende maatregelen.

- Zorg ervoor dat naarmate de mogelijkheden van patroonherkenning bij de toepassing van big data minder zijn, een goede validatie door experts op het desbetreffende vakgebied plaatsvindt om het risico van foutieve uitkomsten zoveel mogelijk te reduceren.
- Zorg ervoor dat de data zoveel als met een redelijke inspanning mogelijk is, up to date zijn, de te gebruiken datasets een zo gering mogelijke bias (afwijking) bevatten en dat de te gebruiken algoritmen en analysemethoden deugdelijk zijn.
- Bepaal, rekening houdend met de potentiële impact van de toepassing, de foutmarge die bij de toepassing mag optreden.
- Zorg ervoor dat nuttige informatie aan betrokkenen wordt verschaft over de gebruikte logica achter de analyse en dat voor toezicht en rechterlijke toetsing voldoende inzicht kan worden gegeven in gebruikte algoritmen en analysemethoden.

Bij de toepassing van de uitkomsten van big data-analyses dient aandacht te worden besteed aan het treffen van de volgende maatregelen.

- Zorg voor menselijke tussenkomst in het proces van geautomatiseerde besluitvorming.
- Naarmate de potentiële negatieve impact voor de betrokkene groter wordt, neemt de noodzaak voor een goede validatie en een weging van de uitkomsten navenant toe.

Aantekening:

- *Technische- en organisatorische maatregelen benoemen die van toepassing zijn op dit proces.*
- *Daarnaast dienen de risico's opnieuw bekeken te worden. Aan de hand daarvan dienen aanvullende maatregelen te worden geformuleerd.*

Typ tekst

Hier kunt u aanvullende punten toevoegen: selecteer de tab *Invoegen*, kies *Snelonderdelen*, *Aanvullend punt*

Voeg hier wanneer gewenst een afsluitende alinea toe. Denk bijvoorbeeld aan:

- Lessen uit deze PIA
- Volgende stappen etc.

