



Gegevensbeschermingseffectbeoordeling (PIA)

FSV (Fraude Signalering Voorziening)

Ministerie van Financiën

Belastingdienst/Midden- en KleinBedrijf (MKB)

Utrecht, 21 januari 2019



Vaststelling verwerkersverantwoordelijke: Selecteer/typ datum

Naam: de Minister van Financiën, namens deze, mr. MKB

Advies Selecteer/typ datum

Naam:

Advies Selecteer/typ datum

Naam:

Gegevensbeschermingseffectbeoordeling (GEB/PIA)

Ministerie van Financiën
Belastingdienst/Midden- en KleinBedrijf (MKB)

Contact:

Ministerie van Financiën, directie Belastingdienst/CAP
Cluster Gegevens
Unit Inwinnen en Verstrekken van Gegevens

Team Juridisch Advies Gegevens

06	
	@belastingdienst.nl

Materiedeskundigen:

			FSV
			(MKB)
		TSL;	
		TSL;	
		DF&A	
		PDB (w.o. IH Systeemfraude)	
		AVG MKB /	

Versie: 1.0 November 2018

Inhoudsopgave

A. Beschrijving kenmerken gegevensverwerkingen.....	6
1. Voorstel.....	6
2. Persoonsgegevens.....	6
3. Gegevensverwerkingen.....	8
4. Verwerkingsdoeleinden.....	8
5. Betrokken partijen.....	9
6. Belangen bij de gegevensverwerking.....	9
7. Verwerkingslocaties.....	10
8. Techniek en methode van gegevensverwerking.....	10
9. Juridisch en beleidsmatig kader.....	12
10. Bewaartermijnen.....	12
B. Beoordeling rechtmatigheid gegevensverwerkingen.....	13
11. Rechtsgrond.....	13
12. Bijzondere persoonsgegevens.....	13
13. Doelbinding.....	14
14. Noodzaak en evenredigheid.....	17
15. Rechten van de betrokkene.....	18
C. Beschrijving en beoordeling risico's voor de betrokkenen.....	19
16. Risico's.....	19
D. Beschrijving voorgenomen maatregelen.....	21
17. Maatregelen.....	21

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.

Aanleiding voor deze GEB is een opdracht van de directie MKB (MT MKB besluit van 20 augustus 2018) om op basis van de uitkomst van een uitgevoerde WMK-toets (april 2018) een GEB op de applicatie dagboek FSV en het bijbehorende proces uit te voeren. MKB is business en product owner van FSV.

De applicatie Dagboek FSV (Fraude Signalering Voorziening, hierna FSV genoemd) is sinds begin 2014 bestemd voor de registratie van (fraude-)signalen, tips & kliks van derden, informatieverzoeken en hierop gebaseerde projecten¹. FSV is bij ingebruikname gevuld met de data uit de per 2014 uitgefaseerde applicatie dagboek Persoonsgericht Intensief Toezicht (PIT). Historische gegevens in PIT (dossiers <2010) en de gegevens die tussen 2010 en 2014 in behandeling waren zijn 1 op 1 overgenomen in FSV,

Het betreft registratie van signalen van (vermoedens van) systeemfraude voor meerdere belastingmiddelen en verschillende Toeslagen. Daarnaast wordt de applicatie ook gebruikt voor de registratie van tips & kliks, projecten (per segment, regionaal, plaatselijk) in het subjectgerichte toezicht. FSV wordt ook ingezet voor de registratie van (bijzondere, wettelijke) verzoeken of vorderingen om informatie². Door het vastleggen van deze gegevens, kunnen over een bepaalde periode wellicht bepaalde trends in beeld worden gebracht, bestuurlijke informatie worden verstrekt, en mogelijke andere relevante informatie worden verzameld.

FSV wordt ook gebruikt als bron (middels dumps van de database) voor het voeden van risicomodellen en datafundamenten van DF&A voor bv. IVT en OB-carrouselfraude. Ook voor Toeslagen geldt dat een vermelding in FSV bij inschatting van het risico voedend werkt. Tevens is het een onderdeel van de periodiek toegepaste risicocategorisering. Het procesverloop en in het bijzonder de applicatie dagboek FSV, vormen de scope van deze GEB op een bestaande gegevensverwerking vanuit een eerdere risicoschatting in de voornoemde GEB Informatieloketten. FSV kent vier hoofd-verwerkingsvormen (tabbladen) die waar nodig onderscheiden beoordeeld zullen worden in deze PIA. Dit betreft:

1. Aanmaken/bewerken aangiftefraude³.
2. Aanmaken/behandelen informatieverzoek.
3. Aanmaken/behandelen Tip/Klikmelding.

¹ Registratie van signalen en informatieverzoeken in FSV binnen MKB is verplicht, op basis van een besluit van het MT-MKB d.d. 24-5-2017.

² Er is een directe relatie met de facultatieve GEB Informatieloketten van mei 2018.

³ Hoewel de titel anders doet vermoeden, betreft het een signaal dat een (*vermoeden van*) mogelijke fraude waaronder aangiftefraude vastlegt. Ook Toeslagen gebruikt deze functionaliteit maar dan voor vermoedens van mogelijke fraude met Toeslagen.

4. Aanmaken/behandelen project.

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 persoonsgegevens. 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 gedragssgerelateerde 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 privacyregelgeving 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 conceptregelgeving 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.

In FSV worden van de volgende categorieën betrokkenen persoonsgegevens verwerkt:

1. Belastingplichtigen (al dan niet beschreven) / toeslaggerechtigden;
2. Partner / kinderen van categorie 1;
3. Fiscaal dienstverleners (NP; natuurlijke personen);
4. Inhoudingsplichtigen (NP);
5. Gastouders (NP); in geval van LRK nummer gastouder.
6. Tip/Klik-meldende personen (al dan niet anoniem);
7. Medewerkers van de Belastingdienst;
8. Medewerkers van andere overheidsdiensten.

	Categorie (detailuitwerking in bijlage 1)	Type
1	NAW gegevens over de persoon	Gewoon
	Gegevens over hardware(locatie) (IP, MAC-adres)	Gewoon
	BSN/RSIN	Wettelijk identificerend
	Sanctie-gerelateerde informatie (bv fiscale boetes)	Strafrechtelijk
	Financiële / fiscale gegevens feiten en objectieve kwalificaties (Negatieve Norm OB; rekenregeluitkomst)	Gewoon / gevoelig
	Strafrechtelijke informatie (van FIOD, OM, Politie)	Strafrechtelijk
	Risico-indicerende kwalificaties mbt voornoemde persoonsgegevens ('besmet adres')	'Zwarte lijst'
	Vrije tekstvelden + bijlagen (ongestructureerde data)	(mogelijk) Gewoon, strafrechtelijke, bijzonder
2	Naamgegevens Partner	Gewoon
	BSN	Wettelijk identificerend
3	Naamgegevens Fiscaal dienstverlener	Gewoon
	BSN	Wettelijk identificerend
4	Naamgegevens Inhoudingsplichtige (NP)	Gewoon
	LH-nr (omvat mogelijk BSN)	Gewoon / Wettelijk identificerend
5	Gastouder(s) ; LRK nummer (Gastouders KOT)	Wettelijk identificerend
6	Naam/info over de Melder/bron Tip/Klik (niet anoniem NP)	Gewoon
7	Naam medewerkers van de Belastingdienst	Gewoon
8	Naam medewerkers van de andere overheidsorganisaties	Gewoon

2. Gegevensverwerkingen

Geef alle voorgenomen gegevensverwerkingen weer.

Het proces en de voorziening FSV in eerste instantie gericht op de **registratie** van signalen. Primaair doel is de **vastlegging** van signalen (tips en kliks, MMA, e.d.), (externe) informatieverzoeken. Hiervan afgeleid ontstaan er mogelijk projecten die met behulp van FSV kunnen worden vastgelegd. FSV wordt belastingdienstbreed gebruikt. Wel wordt er per bedrijfsonderdeel een verschillend gebruik gemaakt (zie 5. Betrokken partijen) en zijn er binnen bedrijfsonderdelen verschillen in het gebruik. Bijvoorbeeld enkele MKB-EOS-teams die alleen algemene signaalinformatie in FSV opvoeren en de (extra vertrouwelijk geachte) details elders **registreren** (bijv. OPO-tool, besloten CP-communities).

Naast registratie van door de Belastingdienst **ontvangen** informatie (denk aan tip/klik signalen) of door medewerkers aangebrachte signalen, wordt FSV ook gebruikt voor signalen die als afgeleide ontstaan van een andere vorm van (persoons)gegevensverwerking bv. de opvraag van fiscale (persoons)gegevens door een andere overheidsinstantie (bv. het OM) die aanleiding geeft om hierover ook een signaal in FSV te **registreren**. FSV heeft een 'signaalfunctie' die bij het opvoeren van een nieuwe signaal aangeeft of er al items in FSV voorkomen. Bij opname van het BSN of RSIN, volgt de melding: "BSN komt x voor in FSV". Afhankelijk van het aantal, is het aan degene die een nieuw item opvoert, wat hij/zij doet met de reeds eerder opgenomen informatie⁴.

Na registratie vormen **raadplegen, muteren, sorteren, kopiëren** ten behoeve van het primaire proces (individuele klantbehandeling, klantbehandeling toeslagen) en **rapportage-doeleinden** (BI) mogelijke maar, in geval van rapportage/BI, niet veel voorkomende verwerkingen. **Verwijderen, archiveren en vernietigen** is op dit moment alleen gevals-/casusgewijs mogelijk via reguliere systeemfunctionaliteit.

Er zijn tijdens het assessment voorbeelden genoemd van *niet voorgenomen/bedoelde* verwerkingsvormen die functioneel wel mogelijk zijn en worden gebruikt: het **raadplegen** van de werkvoorraad van collega's en het maken van een **'systeemdump'** via de excel-exportfunctie.

Het gebruik van FSV binnen de verschillende bedrijfsonderdelen is niet uniform. Er is een handleiding beschikbaar die een uniforme werkwijze mogelijk maakt.

3. 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

⁴ Het idee hierachter is, dat 1 klik is geen klik; 2 kliks kan een aanleiding zijn voor (nader) onderzoek, of een richting aangeven aan het behandelen van het nieuwe item.

Awb-besluiten en het behandelen van geschillen. Denk ook aan eventuele nevendoelende van de gegevensverwerking, zoals: wetenschappelijk, statistisch of historisch onderzoek, archiefbeheer, declaratiedoeleinden, rapportagedoeleinden, verbetering van dienstverlening of (door)ontwikkeling van beleid. De verwerkingsdoelstellingen 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 privacyreggeving 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 **conceptreggeving** 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 reggeving moet binnen het doel worden gebleven dat daarin is vastgesteld. Het verdient de voorkeur de verwerkingsdoelstellingen zoveel mogelijk op het niveau van werk- en organisatieprocessen te enten.

Voor het uitvoeren van zijn taken op het gebied van uitvoering van heffing en inning, waaronder risicovinding⁵, toezicht en handhaving voortvloeiend uit de taken in de Algemene Wet inzake Rijksbelastingen, de Invorderingswet 1990, de Algemene Wet Inkomensafhankelijke regelingen, de Wet aanscherping handhaving en sanctiebeleid SZW-wetgeving 2013 en specifieke (fiscale) middelwetgeving zoals de Wet Inkomstenbelasting 2001, moet de Belastingdienst kunnen beschikken over informatie om de mate van compliantie van belastingplichtigen en toeslaggerechtigden.

FSV draagt bij aan het verrijken van de al beschikbare gegevens, om zodoende te

⁵ bv. OB-carrouselfraude, Combiteam Aanpak Facilitators (CAF)

helpen bepalen de mate van compliantie te beoordelen met als doel de mate van (fiscale) aandacht voor een belastingplichtige/ toeslaggerechtigde te bepalen en in voorkomend geval de informatiepositie te verrijken en beter te onderbouwen. De gegevens in FSV hebben het karakter van contra-informatie c.q. renseignements.

Een tweede doel wordt gevormd door de bestuurlijke informatie en operationele sturingsinformatie die met behulp van FSV kan worden gegenereerd om de inzet van capaciteit, opbrengsten en andere kengetallen inzichtelijk te maken respectievelijk capaciteit zo effectief en efficiënt mogelijk in te zetten. Gebruik (en de mate) hiervan bij de onderscheiden directies, is divers.

Een derde doel vloeit voort uit het voldoen aan wettelijke verplichtingen jegens andere overheidsorganisaties op het gebied van informatieverstrekking⁶.

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.

⁶ Voor MKB: zie hiervoor de afgeronde GEB op de informatieloketten.

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.

De Minister van Financiën is in beginsel verantwoordelijk voor deze verwerking.

De (algemeen) directeur(en) MKB, Toeslagen, PDB, FIOD en Douane zijn als gedelegeerd verwerkingsverantwoordelijken aangewezen voor de respectievelijke wettelijke taken.

GO, Douane en FIOD raadplegen FSV voornamelijk. Toeslagen, PDB en MKB raadplegen en muteren in FSV.

De taken in FSV worden feitelijk uitgevoerd door:

- Regiocoördinatoren systeemfraude en IH heffers regionaal
- (fiscale) Baliemedewerkers
- MKB Fraude-EOS-teammedewerkers
- Heffers fiscale middelen en Toeslagen
- Managers heffing en Inning en Toeslagen
- Fraudezorgmedewerkers (vorm van slachtofferhulp_ / Stella-teams
- Bezwaren/beroepsprocedure - medewerkers
- Invorderings- en LIC-medewerkers (met name raadplegen)
- AFB (Adviesteam Fraudebestendigheid, voorheen AntiFraudeBox, kan over alle gegevens beschikken);
- DF&A waaronder (voorheen) EHI; (kan over alle gegevens beschikken);
- Douane-medewerkers (2 autorisaties)

De voorziening wordt beheerd door functionele en technische beheerders. In zijn totaliteit zijn ongeveer 5000 gebruikers geregistreerd (waaronder ruim 400 inactieve gebruikers). Dit aantal neemt nog steeds toe.

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).

Vanuit het belang van een zorgvuldige en juiste heffing en inning respectievelijk het beoordelen van de rechtmatigheid van de aanvraag en toekenning van toeslagen, worden in FSV signalen vastgelegd. Door het vastleggen van deze gegevens, kunnen over een bepaalde periode (systeem)fraudetrends in beeld worden gebracht, kan bestuurlijke informatie worden verstrekt en relevante informatie op casus- of projectniveau worden verzameld of ter beschikking worden gesteld aan de behandelaar(s). Gedurende het assessment is niet expliciet gebleken dat FSV (consequent) vanuit dit belang wordt gebruikt⁷. De informatieverzoeken worden geregistreerd mede vanuit het belang van zorgvuldig, rechtmatig en doortastend handelende overheid cq andere overheidspartijen veelal met een financiële/materiele invalshoek, bv. binnen een strafproces (OM) of ten aanzien van uitkeringen (UWV) of alimentatieverplichtingen (LBIO).

4. Verwerkingslocaties

Benoem in welke landen de voorgenomen gegevensverwerkingen plaatsvinden.

Nederland.

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.

⁷ De (voormalige) AntiFraudeBox (AFB) is om deze reden destijds geautoriseerd. Idem EHI.

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

- a. noodzakelijk is voor de totstandkoming of de uitvoering van een overeenkomst tussen de betrokkene en een verwerkingsverantwoordelijke;
- b. 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.

De signalen/gegevens worden voornamelijk casusgewijs ingevoerd en opgeslagen in een centrale (SQL)database. Massale invoer van gegevens is mogelijk voor de (platform)beheerder en senior behandelaars voor de 'thema's': aangiftefraude, bijwerken aangiftefraude en project/overig. Het raadplegen en muteren gebeurt primair via systeemfunctionaliteit. Wel is het voor technisch beheerders mogelijk om rechtstreeks de database te benaderen/muteren. Dit wordt niet gelogd en gemonitord.

Er wordt gewerkt met een via IMS-geïmplementeerde autorisatiematrix die de volgende rollen kent:

Baliemedewerker	Senior behandelaar
Medewerker raadplegen	Platform gebruiker / beheerder
Medewerker raadplegen aangiftefraude	Special (BCA)
Medewerker raadplegen B.I.	Behandelaar aangiftefraude
Behandelaar	Senior behandelaar

Er is geen sprake van geautomatiseerde besluitvorming; óf de verwerkte gegevens worden door tussenkomst van een individuele medewerker verwerkt of vormen input voor een verdere verwerking (DF&A, bv. de risicomodellen OB) die niet rechtstreeks leidt tot een geautomatiseerd besluit. De gegevens worden ingezet in big-data-verwerkingsvormen binnen DF&A ten behoeve van de risicomodellen OB (o.m. BTW carouselfraude). Er is op dit moment binnen de Belastingdienst geen sprake van profilering doordat de Belastingdienst subjectgericht toezicht houdt, in principe gebaseerd op risicoselectie aan de hand van objectieve kenmerken.

Profielen op basis van dergelijke kenmerken worden ingezet voor selectie van dossiers voor toezicht of klantbehandeling. Dergelijke profielen zijn geen product van profilering in de zin van de AVG⁸. Enkele van de binnen FSV verwerkte elementen⁹ én het feit dat er ook niet zondermeer objectief getoetste of toetsbare signalen worden geregistreerd, maken dat het karakter van sommige verwerkingsvormen binnen FSV als profilering inclusief 'zwarte lijst'-achtige effecten kunnen gelden. Het überhaupt voorkomen van een betrokkene in FSV wordt bijvoorbeeld gebruikt als signaal in bv. afnemende 'systemen' / verdere verwerkingen (DF&A, mogelijk IVT), zonder dat dit op basis van een objectief aangetoond (verhoogd) risico is gebaseerd (risico van waardering als.. 'waar rook is, is vuur'). Het onderscheid tussen een signaal en een informatievraag wordt bij verdere verwerking ook niet of niet juist gewogen. Niet ieder informatieverzoek is op voorhand een fiscaal signaal.

Er is op dit moment sprake van een lange, op dit moment zelfs ongelimiteerde, bewaartermijn van gegevens. In deze context is ook de kwaliteit van de gegevens van belang (juistheid, volledigheid, actualiteitswaarde). Een niet geverifieerd kliksignaal van een anonieme melder heeft een andere waarde en houdbaarheid dan een objectief aangetoond feit of een als onjuist vastgesteld kliksignaal. De FSV-database bevat signalen die zich begeven tussen beide hiervoor genoemde uitersten. Meerdere rollen [] hebben de mogelijkheid, hoewel hiervoor niet bedoeld, om met bestaande systeemfunctionaliteit een export-dump van alle gegevens uit de database te maken. Dit wordt niet gelogd. Vanuit het oogpunt van databeheersing is dit een risico. In totaal zijn 5000+ medewerkers geregistreerd. Daarvan zijn ongeveer 4500 gebruikers actief in FSV, blijkend uit een actuele autorisatie in IMS¹⁰. Dit aantal herbergt ook een beperkt aantal users dat meerdere malen is opgevoerd. Doordat er niet op basis van een uniek gegeven (zoals UserId) wordt geregistreerd, maar op naam, is vervuiling ontstaan.

⁸ Standpunt/beslissing DT BD, verslag 7 juni 2018.

⁹ Zoals risico-scores of mogelijk subjectieve waarderingen uit andere processen: negatieve-norm OB, prioriteit (2 vormen, nader duiden), besmet adres, besmette postcode.

¹⁰ IMS: identity management systeem; registratie in IMS is noodzakelijk voor toegang in FSV.

Er is geen systeemfunctionaliteit voor het afvoeren van gebruikers. Momenteel zijn er 5-6 functioneel beheerders die medewerkers voor FSV autoriseren op verzoek van IM. De beperkte mate waarin een autorisatieverzoek wordt getoetst op juistheid/toepasselijkheid vormt een risico.

Afgedane posten kunnen gemuteerd worden zonder behoud van het origineel, dus zonder historie en zonder logging. Dit geldt ook voor niet afgedane posten. Medewerkers met mutatierechten kunnen ook posten van anderen muteren. Antidatering van gegevens is mogelijk.

5. 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.

AWR, AWIR, Invorderingswet 1990, middelwetgeving (bv. Wet IB 2001), Fraudewetgeving 2013. Specifieke / sectorale wetgeving van andere ministeries die andere overheidspartijen de wettelijke bevoegdheid geeft bij de Belastingdienst gegevens op te vragen (bv. art. 126 nd Sv, art 23 Wlbio, art. 54 WSuwi). De BIR 2017 en het HBB, handboek beveiliging Belastingdienst bevatten het hier toepasselijke beveiligingsbeleid.

5. Bewaartermijnen

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

[Klik hier om infotekst te verbergen](#)

De privacyregelgeving geeft als beginsel dat persoonsgegevens niet langer in een vorm die het mogelijk maakt de betrokkenen te identificeren, mogen worden bewaard dan voor de verwezenlijking van de verwerkingsdoeleinden noodzakelijk is. Met andere woorden: indien het voor de verwezenlijking van de verwerkingsdoeleinden niet meer noodzakelijk is de persoonsgegevens te bewaren, moeten deze worden vernietigd of geanonimiseerd. Op dit beginsel van opslagbeperking maakt de privacyregelgeving een uitzondering indien de persoonsgegevens uitsluitend worden verwerkt ten behoeve van archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden. Hieraan wordt wel de eis verbonden dat passende maatregelen worden getroffen om de betrokkenen te beschermen.

Bij conceptregelgeving zal moeten worden bepaald en gemotiveerd of het al dan niet wenselijk is om een specifieke minimale of maximale bewaartermijn voor te schrijven. Aan de hand van het uitgangspunt dat de bewaartermijn in verhouding moet staan met de verwerkingsdoeleinden, moet de gekozen termijn worden gemotiveerd. Motiveer ook het niet opnemen van een bewaartermijn.

Bij overheidsverwerkingen moet worden nagegaan of regelgeving een bewaartermijn voorschrijft. Indien dat het geval is, moet de verwerkingsverantwoordelijke zich aan die termijn houden. Indien geen wettelijke bewaartermijn is voorgeschreven, moet de verwerkingsverantwoordelijke zelf bewaartermijnen vaststellen of de gegevens periodieke toetsen aan het beginsel van opslagbeperking.

Hierbij moet rekening worden gehouden met andere regelgeving over bewaartermijnen, zoals de Archiefwet 1996.

Voorbeeld opsomming bewaartermijn voor persoonsgegevens bij overheidsverwerkingen (IT/uitvoering):

Persoonsgegevens	bewaartermijn	van bewaring	bewaring	voor verwijdering
Naam	Vanaf moment dat de betrokkene voor het eerst inlogt in het systeem.	365 dagen, als de gebruiker 'onthouden inloggegevens' aanklikt 30 dagen.	Deze persoonsgegevens zijn functioneel: het gegeven zorgt er voor dat je met slechts één handeling inlogt in het verschillende databases.	Functioneel beheerder

Hoewel procesmatig onderkend¹¹ bevat FSV geen voorziening om afgedane posten te archiveren gedurende de resterende bewaartermijn om na afloop van de bewaartermijn, gebaseerd op de relevante selectielijst(en), vernietigd te worden.

Op dit moment is alle data toegankelijk en (rolafhankelijk) zowel raadpleegbaar als muteerbaar.

De historie van de geregistreerde data gaat terug tot 2001. Dit wordt mede veroorzaakt doordat bij de start van FSV in 2014 de database van dagboek PIT is geïmporteerd.

¹¹ En geregistreerd in (Agile)Feature F18.045, Aanpassingen FSV v.0.5, dd. 22-10-2018.

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:

- a. de betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden;
- b. 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;
- c. de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust;
- d. 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.

Algemene bepalingen AWR?

1. Verwerking van de persoonsgegevens door de Belastingdienst ten behoeve van zijn wettelijke taken in de fiscaliteit en toeslagen: artikel 6 lid 1 onder e AVG.
2. Artikel 6 lid 1 onder f AVG; gerechtvaardigd belang; hoewel er beperkt voorbeelden¹² zijn gebleken van inzet van FSV trendanalyses en BI ten behoeve van de bedrijfsvoering, is dit wel een beoogde inzetvorm.
3. Registratie van verstrekking op verzoek van persoonsgegevens door de Belastingdienst aan derden met een wettelijke taak: artikel 6 lid 1 onder c AVG. (de informatieverzoeken). Het volledige proces van de externe informatieverzoeken is behandeld in de GEB Informatieloketten. Hier wordt

¹² Toeslagen gebruikt FSV ook om te raadplegen bij Bibob en Track verzoeken. Omdat Toeslagen in FSV het Gefisnr. (th. PSF) registreert en het boetebedrag en percentage in FSV registreert. Dit valt onder het kopje strafrechtelijke gegevens.

alleen het aspect registratie (en eventuele verdere verwerking) in FSV bedoeld.

7. 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:

- a. de betrokkene heeft uitdrukkelijke toestemming gegeven;
- b. 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;
- c. de verwerking is noodzakelijk ter bescherming van vitale belangen van de betrokkenen of een ander;
- d. de verwerking wordt verricht door een instantie die op politiek, levensbeschouwelijk, godsdienstig of vakbondsgebied werkzaam is;
- e. de verwerking betrekking heeft op persoonsgegevens die kennelijk door de betrokkene openbaar zijn gemaakt;
- f. de verwerking noodzakelijk is voor de instelling, uitoefening of onderbouwing van een rechtsvordering;
- g. de verwerking noodzakelijk is om redenen van zwaarwegend algemeen belang;
- h. 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;
- i. de verwerking noodzakelijk is om redenen van algemeen belang op het gebied van de volksgezondheid;
- j. 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.

1. **Informatieverzoeken** bevatten mogelijk **bijzondere**¹³ persoonsgegevens. De primaire verwerking (het afhandelen van het informatieverzoek) voldoet aan de voorwaarden voor verwerking van art. 9 onder f en g AVG. De verdere verwerking van aangaande het informatieverzoek binnen FSV en evt. andere informatiesystemen moet aanvullend en indien van toepassing herhaald getoetst worden. De context in combinatie met (de betekenis van) de gegevens is bepalend voor de wijze van gebruik. Een informatieverzoek is bv. niet op voorhand / op per definitie een (fraude)signaal en de actualiteitswaarde begrenst. De huidige verwerkingswijze is hierop onvoldoende ingericht.
2. **Tips en kliks**¹⁴ (signalen) ontvangen van derden kunnen **bijzondere** persoonsgegevens bevatten. De Belastingdienst ontvangt en verwerkt deze signalen bij de uitvoering van zijn taken 'spontaan' doordat derden signalen moeten kunnen aanbrengen over andere burgers. De primaire verwerking (het afhandelen van de tip/klik) voldoet aan de voorwaarden voor verwerking van art. 9 onder g AVG. De verdere verwerking is wel aan beperkingen onderhevig incl. dit plicht tot vernietiging bijvoorbeeld bij gebleken onbruikbaarheid of onjuistheid. De huidige verwerkingswijze is hierop onvoldoende ingericht.
3. **Interne en externe**¹⁵ **(fraude) signalen** kunnen **bijzondere** persoonsgegevens bevatten. De primaire verwerking (het afhandelen van de tip/klik) voldoet aan de voorwaarden voor verwerking van art. 9 onder g AVG. In de verdere verwerking speelt de context en kwaliteit van de gegevens een bepalende rol voor de rechtmatigheid en welbepaaldheid van de verdere verwerking. Die is niet voor alle gevallen zondermeer aanwezig. De huidige verwerkingswijze is hierop onvoldoende ingericht. Toeslagen boekt onder "aangifte fraude" de signalen in, op het moment dat er een gerede twijfel is aan de opmaak van documenten (facturen, contracten, etc.) hier is al een kort onderzoek aan vooraf gegaan. Dit kan door een andere afdeling zijn gedaan of afkomstig zijn van externe partijen (zie 4.) of een klikmelding (zie 2.).
4. **Informatieverzoeken** bevatten **strafrechtelijke** persoonsgegevens. De wettelijke uitzondering voor verwerking is primair gelegen in de wettelijke grondslag (lees verplichting) bijvoorbeeld een vordering op grond van art. 126nd Sv. Daarmee voldoet de verwerking 'in enge zin' (ten behoeve van het voldoen aan de vordering) aan de voorwaarden¹⁶ voor verwerking van art. 10 AVG jo art. 23 onder c UAVG. De verdere verwerking binnen FSV en evt. andere informatiesystemen voldoet aan de voorwaarde van 'verwerking onder toezicht van de overheid'. De context van een informatieverzoek in combinatie met (de betekenis van) de gegevens is wel bepalend voor de wijze van gebruik. Een extern informatieverzoek is niet bedoeld te gelden als / niet op voorhand / per definitie een (fraude)signaal en de actualiteitswaarde is begrenst. Toeslagen

¹³ Direct of indirect. Bv. in de context van zorgtoeslag kan een gegeven indirect iets over de gezondheidstoestand van een betrokkene zeggen.

¹⁴ Tips/kliks is een algemeen begrip. In het signaal moet worden opgenomen wat de bron. Via overzichten kunnen aantallen (per periode, kantoor, BSN/RSIN) inzichtelijk worden gemaakt.

¹⁵ Zoals MMA, Track/Justis, FIU, iSZW e.d.

¹⁶ "...verwerkt onder toezicht van de overheid of indien de verwerking is toegestaan bij Unitrechtelijke of lidstaatrechtelijke bepalingen die voldoende waarborgen ... bieden." Zorgtoeslag van Toeslagen is een tegemoetkoming in de kosten voor een zorgverzekering, die inkomensafhankelijk is.

doet bij gerede twijfel eerst onderzoek en voert dan evt. een signaal op. De huidige verwerkingswijze moet ten aanzien van deze aspecten worden verbeterd. De aanpak van Toeslagen kan, indien dit past binnen het uitvoeringsproces, hierbij als uitgangspunt worden genomen.

5. **Tips en kliks** ontvangen van derden kunnen **strafrechtelijke** persoonsgegevens bevatten. De Belastingdienst ontvangt en verwerkt dit 'spontaan' doordat derden signalen moeten kunnen aanbrengen over andere burgers. Ook hier is bij aanvang van de verwerking sprake van de uitzondering 'onder toezicht van de overheid'. De verdere verwerking is wel aan beperkingen onderhevig incl. dit plicht tot vernietiging bijvoorbeeld bij gebleken onbruikbaarheid of onjuistheid. De huidige verwerkingswijze moet ten aanzien van deze aspecten worden verbeterd.
6. **Interne (fraude) signalen** kunnen **strafrechtelijke** persoonsgegevens bevatten (waaronder daarmee gelijkgeschakelde fiscale sanctiegegevens). Ook hier geldt dat bij aanvang van de verwerking strafrechtelijke gegevens sprake is van de uitzondering 'onder toezicht van de overheid'. In de verdere verwerking speelt de context en kwaliteit van de gegevens een bepalende rol voor de rechtmatigheid en welbepaaldheid van de verdere verwerking. Die is niet voor alle gevallen zondermeer aanwezig. De huidige verwerkingswijze moet ten aanzien van deze aspecten worden verbeterd.
7. Bovenstaande geldt ook voor projecten gebaseerd op gegeven zoals besproken onder 1 tot en met 6.
8. Gegevens met een '**zwarte lijst**'-karakter: in FSV ontstaan of worden bestaande gegevenselementen verwerkt die het karakter van een zwarte-lijst-element hebben of krijgen. De mogelijke subjectiviteit ('bias', vooringenomenheid, zelfversterkend effect door stapeling) maakt het verwerken risicovol. Ook het voorkomen in FSV als betrokkene wordt als risicosignaal. Dit brengt ook een aantal risico's met zich mee waaronder een mogelijk 'zwarte lijst'-effect.

8. 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:

- a. het verband tussen de doeleinden waarvoor de persoonsgegevens zijn verzameld en de doeleinden van de voorgenomen verdere verwerking;
- b. de context waarin de persoonsgegevens zijn verzameld, met name wat de verhouding tussen de betrokkene en de verwerkingsverantwoordelijke betreft;
- c. de aard van de persoonsgegevens, met name bijzondere of strafrechtelijke persoonsgegevens;
- d. de mogelijke gevolgen van de voorgenomen verdere verwerking voor de betrokkene;
- e. 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:

- a. de verwerkingsverantwoordelijke overeenkomstig de wet gemachtigd is deze persoonsgegevens voor een dergelijk doel te verwerken; en
- b. 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.

De vraag of de verdere gegevensverwerking verenigbaar is met het oorspronkelijke verzameldoel van de gegevens, speelt met name met betrekking tot de verdere verwerking gegevens in FSV. De initiële vastlegging van persoonsgegevens bij (registratie van) een informatieverzoek of (extern) tip/klik/signaal of intern signaal is namelijk het begin van de verwerking. Vanwege het verschillende karakter worden informatieverzoeken apart behandeld naast de (fraude)signalen.

Informatieverzoeken: In deze afweging zijn de volgende factoren gewogen:

- a. Het verband tussen het oorspronkelijk verzameldoel en de doeleinden van de voorgenomen verdere verwerking;
- b. Het kader waarin de persoonsgegevens zijn verzameld en de redelijke verwachtingen van de ontvanger (de betrokkene) met betrekking tot de voorgenomen verwerking;
- c. De aard van de persoonsgegevens en met name of bijzondere persoonsgegevens worden verwerkt;
- d. De mogelijke gevolgen van de voorgenomen verwerking voor de ontvanger

- (betrokkene);
- e. Het bestaan van passende waarborgen, waaronder versleuteling of pseudonimisering van de gegevens.

Ad a. Het informatieverzoek wordt verwerkt (geregistreerd) wanneer een externe overheidspartij op basis van een wettelijke grondslag inlichtingen vordert. Het verwerkingsdoel is tweeledig:

1. Vastlegging van (een deel van de¹⁷) informatie aangaande het informatieverzoek ten behoeve van een goede verwerking van het verzoek en het creëren van een audit trail.
2. Vastleggen van contra-informatie/reñseignementen vanuit het (ten dele statistisch onderbouwde) ervaringsgegeven¹⁸ dat een significant deel van subjecten waarvan informatie wordt opgevraagd, fiscaal gezien aanvullende aandacht verdient of mogelijkheid dat de betrokkene ook fiscaal nader onderzocht of getoetst moet worden. (Vermoedens van) misbruik doet zich veelal regeling overstijgend voor én er is een wederzijdse relatie doordat inkomen- en vermogen (mede)bepalend is voor aanspraken op diverse regelingen buiten de fiscale context.

De verdere verwerking zal plaatsvinden doordat bij de risico(posten)selectie en/of individuele klantbehandeling FSV direct of indirect (via export van FSV-data naar andere bronnen) wordt geraadpleegd. Het gebruiken van FSV als bron is verenigbaar indien kan worden gegarandeerd dat de gegevens juist, volledig en actueel is en de gegevens inclusief contextinformatie worden verwerkt. Een informatieverzoek heeft bv. een andere context en daardoor betekenis dan een kliksignaal.

Er is vastgesteld dat deze zorgvuldigheid bij de huidige inrichting niet voldoende kan worden gegarandeerd. Zo wordt per bedrijfsonderdeel en daarbinnen per behandelend team (en mogelijk individu) anders omgegaan met de mate van vastlegging in FSV. Ook de verdere verwerking van FSV data in andere informatiesystemen is voldoende fijnmazig. Als het überhaupt voorkomen in FSV als selectiecriteria geldt, wordt geen rekening gehouden met de context en hiervan afgeleid met mogelijk (ontrechte) stigmatisering van betrokkenen als gevolg.

Ad b. Het vastleggen van een informatieverzoek vloeit voort uit een wettelijke plicht. De betrokkene zal in het merendeel van de gevallen hiervan niet (direct) op de hoogte zijn maar via het dossier (strafdossier, alimentatie-dossier LBIO) op enig moment geconfronteerd worden met het feit dat een dergelijke verwerking heeft plaatsgevonden. De Belastingdienst informeert de ontvanger (betrokkene) in zijn algemeenheid door middel van het privacy statement en de brochure "Overzicht verwerkingen van persoonsgegevens door de Belastingdienst".

Ad c. Er worden bijzondere- en strafrechtelijke persoonsgegevens verwerkt evenals een wettelijk identificatienummer (BSN). De aard en het karakter van dit type verwerking brengt dat met zich mee. Dit brengt extra zorgvuldigheidseisen met zich mee uitgaande van wettelijke mogelijkheden (zo niet verplichting) om deze gegevens te verwerken.

Ad d. De gevolgen van de voorgenomen verwerking voor de ontvanger (betrokkene) kunnen groot zijn. Als de enkele registratie van een informatieverzoek in FSV, zonder fiscale relevantie vervolgens meerjarig (tot nu toe zelfs blijvend vanwege het ontbreken van een verwijdermogelijkheid) geldt als variabele in diverse risicoprofielen van de Belastingdienst, dan herbergt dit het risico van te grofmazige risicoselectie en mogelijke stigmatisering.

Ad e. De gegevens worden verwerkt binnen de beveiligde infrastructuur van de Belastingdienst zonder pseudo- of anonimisering. Het relatief grote aantal personen dat toegang heeft tot de gegevens (raadplegen en evt. muteren, rolfafhankelijk) zonder een goed ingerichte need-to-

¹⁷ In veel gevallen wordt in FSV alleen een signaal vastgelegd en worden onderliggende stukken elders opgeslagen. Dit wordt voornamelijk ingegeven door het grote aantal autorisaties op FSV en het daardoor ontstane overschrijden van een need-to-know-toegang tot signaalinformatie.

¹⁸ Bron: DF&A

know-structuur en het ontbreken van logging en monitoring vormt daarbinnen een risico.

(Fraude/klik/tip)Signalen: De signalen vormen de tweede groep die beschouwd zal worden in deze paragraaf. Hoewel verschillend qua typologie vormen ze wel één groep die zich onderscheidt van de informatieverzoeken.

Ad a. De geregistreerde signalen van fraude/misbruik worden gebruikt voor (ruwweg) risicoselectie en de klantbehandeling. Bij signalen van derden ligt het initiatief bij (anonieme) burgers en komen van andere (overheids)Partners af, interne signalen komen op vanuit de verschillende bedrijfsprocessen rondom de klantbehandeling (fiscaal en toeslagen). Verwerking vindt steeds plaats in de context van het bevorderen van compliance van betrokkenen.

Ad b. Hoewel de Belastingdienst de betrokkene in zijn algemeenheid informeert door middel van het privacy statement en de brochure "Overzicht verwerkingen van persoonsgegevens door de Belastingdienst", is de specifieke verwerking van signalen in FSV voor het merendeel van de betrokken onbekend. Indirect wordt een betrokkene hier op enig moment mee bekend doordat er een vorm van (geïntensiveerde) klantbehandeling ontstaat waarin FSV mede bepalend is geweest.

Ad c. Er worden mogelijk en in voorkomend geval bijzondere en strafrechtelijke persoonsgegevens verwerkt evenals het BSN als wettelijk identificatienummer.

Ad d. De gevolgen van de voorgenomen verwerking voor de ontvanger (betrokkene) kunnen groot zijn. Als de enkele registratie van een signaal in FSV leidt vervolgens meerjarig (tot nu toe zelfs blijvend vanwege het ontbreken van een verwijdermogelijkheid) geldt als variabele in diverse risicoprofielen van de Belastingdienst, dan herbergt dit het risico van te grofmazige risicoselectie en mogelijke stigmatisering.

Ad e. De gegevens worden verwerkt binnen de beveiligde infrastructuur van de Belastingdienst. Het relatief grote aantal personen dat toegang heeft tot de gegevens (raadplegen en evt. muteren, rolfafhankelijk) zonder een goed ingerichte need-to-know-structuur en het ontbreken van logging en monitoring vormt daarbinnen een risico.

9. Noodzaak en evenredigheid

Beoordeel of de voorgenomen 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?.**

[Klik hier om infotekst te verbergen](#)

De privacyregelgeving geeft als beginsel dat de gegevensverwerking wordt beperkt tot wat noodzakelijk is voor de verwerkingsdoeleinden. Dit beginsel van minimale gegevensverwerking/dataminimalisatie komt verder tot uitdrukking door het gebruik van het woord 'noodzakelijk' in artikel 6 AVG en artikel 8 Richtlijn. De AVG en Richtlijn eisen hiermee dat de gegevensverwerking noodzakelijk is voor het verwezenlijken van de doeleinden. De gegevensverwerking moet daarbij voorts de toets aan de beginselen van proportionaliteit en subsidiariteit kunnen doorstaan.

Proportionaliteit betekent dat moet worden beoordeeld of de indringendheid van de voorgenomen gegevensverwerking in een redelijke verhouding staat tot het doel. Bij proportionaliteit wordt gewogen of de realisatie van de verwerkingsdoeleinden zodanig gewicht heeft dat de gegevensverwerkingen, gelet op de mate waarin deze de privacy beperken, deze rechtvaardigen (zijn de beperkingen van het grondrecht en het doel dat

met de verwerking wordt beoogd met elkaar in balans?). Daarbij zal onder meer moeten worden gekeken of de voorgenomen gegevensverwerking effectief is om het beoogde doel te bereiken en of de aangevoerde redenen relevant en toereikend zijn om het beoogde doel te bereiken.

Daarbij kunnen empirische onderzoeksresultaten helpen.

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

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

Zo kan in bepaalde gevallen met foto's hetzelfde doel worden bereikt (bijvoorbeeld: identificatie) als met het verwerken van filmbeelden. Het subsidiariteitsbeginsel houdt bijvoorbeeld ook in dat als persoonsgegevens openbaar gemaakt gaan worden, niet automatisch alle persoonsgegevens openbaar worden gemaakt, maar een selectie wordt gemaakt op grond van gerechtvaardigde criteria. Bij deze afwegingen worden de doelen, belangen en feiten zoals in beeld gebracht in onderdeel A betrokken.

Bij conceptregelgeving kunnen de uitkomsten van deze afweging worden meegenomen in de grondrechttoets van het IAK.

a. Proportionaliteit:

Vanwege het verschillende karakter worden ook hier informatieverzoeken onderscheiden behandeld van de (fraude)signalen.

Informatieverzoeken: de inbreuk op de privacy wordt gerechtvaardigd doordat de afhandeling van een informatieverzoek voortvloeit uit een wettelijke plicht. Vanuit een zorgvuldigheidsoogpunt is registratie een noodzakelijke processtap. De noodzakelijkheid van de (verdere) verwerking buiten de 'logistieke' doeleinden van het zorgvuldig afhandelen van een informatieverzoek vraagt om aanvullende, privacy-bevorderende maatregelen. De noodzaak van verdere verwerking van een informatieverzoek als renseignement moet zorgvuldig worden getoetst én vraagt om vastlegging van voldoende (en hierdoor mogelijk verwerking van meer) (persoons)gegevens om bij de verdere verwerking de relevantie te kunnen bepalen. Tevens moet de 'houdbaarheid' voldoende fijnmazig worden bepaald. Ieder (type) informatieverzoek heeft zijn eigen, beperkte, actualiteitswaarde. Er moet een goed evenwicht gevonden worden tussen ervaringsregels als 'een signaal is geen signaal' en 'waar rook is, is vuur' die ieder voor zich leiden tot het verlengen van de bewaartermijnen en de belangen en rechten van betrokkenen. De werkwijze van Toeslagen, waarbij een informatieverzoek wordt 'gewogen' en bij gerede twijfel FSV wordt 'aangevuld' met een signaal lijkt een zuivere scheiding tussen een informatieverzoek en een signaal te kunnen aanbrengen.

(Fraude/klik/tip)Signalen: de inbreuk op de privacy wordt in zijn algemeenheid gerechtvaardigd doordat het ontvangen of intern ontstaan van signalen een logisch gevolg is van de uitvoering van de wettelijke taken van de Belastingdienst. Signalen van derden (tips/kliks en andere signalen) zijn vormvrij, wat maakt dat een uniforme vastlegging georganiseerd moet worden. FSV is hiervoor een instrument. De criteria voor registratie in FSV laten toe dat de mate van 'hardheid', objectiviteit / subjectiviteit, bruikbaarheid en actualiteit per melding verschilt zonder dat dit in de verdere verwerking als objectieve criteria toetsbaar is. Dit vraagt om aanvullende, privacy-bevorderende maatregelen die een betere balans geven in de plicht om een

zo beperkt mogelijke privacy-schending te veroorzaken en tegelijkertijd de noodzaak tot het registreren van (mogelijk) fiscaal relevante signalen blijvend mogelijk te maken.

b. Subsidiariteit:

De verwerkingsdoelen voor beide informatiestromen kunnen met een aangepaste verwerkingwijze in FSV leiden tot hetzelfde resultaat maar met een minder grote inbreuk op de persoonlijke levenssfeer van betrokkenen. De mate waarin dit in de huidige opzet van FSV mogelijk en wenselijk is of bv. in de vorm van een migratie naar een nieuwe omgeving/voorziening, zal nader beoordeeld moeten worden.

De belangrijkste aspecten, grotendeels corresponderend met de hierna in paragraaf 16 te benoemen risico's, zijn: het aanbrengen van een beter onderscheid tussen informatieverzoeken en 'echte' signalen. de bewaartermijn, registratie en meeleveren van metadata (contextinformatie) ten behoeve van de verdere verwerking en need-to-know/have toegang van medewerkers.

10. 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.

Het karakter van de verwerkingsgrondslagen voor opname van (persoons)gegevens in FSV zal er in veel gevallen toe leiden dat bij een eventueel inzageverzoek betrokkene geen specifieke informatie, zoals verwerkt in en vanuit FSV, zal ontvangen. Een wettelijke geheimhoudingsplicht (bijvoorbeeld voortvloeiend uit art. 126nd SV maar ook specifieke signalen zoals MeldMisdadAnoniem) kan hieraan in de weg staan maar ook de voorlopige geheimhouding corresponderend met de wettelijke taken van de (rijks)Belastingdienst. Art. 23 AVG, in het bijzonder letter d en h AVG geldt hier als beperking op de rechten van betrokkene.

Wel informeert de Belastingdienst de ontvanger (betrokkene) in zijn algemeenheid met betrekking tot in FSV registreerde persoonsgegevens door middel van het privacystatement en de brochure "Overzicht verwerkingen van persoonsgegevens door de Belastingdienst".

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.

11. 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 privacyregulering 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.

1. In zijn algemeenheid kan worden geconcludeerd dat **de huidige opzet van FSV geen goede aansluiting (meer) heeft op de verwerkingsbeginselen van art. 5 AVG**. Ten aanzien van elk van de 10 in dit artikel genoemde beginselen zijn een of meer bevindingen gedaan en afgeleid daarvan zijn er privacy risico's signaleerd. Hieronder worden de meest impact hebbende risico's beschreven. De hoofdmaatregel genoemd in .17 sluit overigens specifiek aan op dit eerste 'meta-risico'.
2. **Onvoldoende onderscheid tussen een informatieverzoek en een signaal maar ook betekenis/gewicht van de informatie, leidt tot mogelijke stigmatisering van betrokkene ('zwarte lijst effect').** FSV biedt de

mogelijkheid tot registratie van beide fenomenen wat bij de (verdere) verwerking, afhankelijk van de wijze van verwerking, door de individuele gebruiker (of bedrijfsonderdelen) tot een verschillende en deels risicovolle verwerking leidt. Een afgeleid risico ontstaat doordat er nauwelijks of geen onderscheid wordt gemaakt in de kwalificatie, 'gewicht' en betekenis van een melding. Een informatieverzoek zonder fiscale relevantie 'weegt' even zwaar als een 'vage' klikmelding ('buurman drie keer met een aanhangwagen met 'handel' zien rijden') of een concrete melding van bv. een valse factuur. Zeker wanneer de FSV content integraal (verder) wordt verwerkt en/of de registratie in FSV als risicofactor wordt (mee)gewogen, is de kans groot dat een deel van de betrokkenen onterecht of bovengemiddeld snel/vaak als risicopost wordt aangemerkt met als gevolg een mogelijk meer intensieve klantbehandelvorm dan noodzakelijk is.

3. **De datakwaliteit vormt een risico** doordat registratie in FSV niet uniform geschiedt, het onderscheid tussen objectieve en subjectieve informatie onvoldoende inzichtelijk is en verouderde informatie blijvend wordt verwerkt. De oorzaak van voornoemde voorbeelden is verschillend. Respectievelijk de verschillende werkwijze van bedrijfsonderdelen (én teams en per medewerker), feiten en vermoedens (waaronder het label 'besmet adres') die deels zonder nadere kwalificatie/onderscheid worden verwerkt en het ontbreken van massale-archiverings-/schoningsfunctionaliteit. Dit heeft tot gevolg dat er een incompleet, onjuist en/of gedateerd beeld van betrokkene ontstaat in de (verdere) verwerking van gegevens, ook buiten FSV, zoals de risicopostselectie (bv. bij DF&A) en toetsing in FSV in geval van individuele klantbehandeling. Dit kan aanzienlijke gevolgen hebben voor betrokkenen.
4. **Informatiebeveiligingsissues waaronder onvoldoende garantie ten aanzien van data-integriteit, vormen een risico** door te ruime toegang tot en onvoldoende controle op het gebruik van de gegevens in FSV. Er zijn inmiddels 5000+ medewerkers geautoriseerd¹⁹ voor minimaal raadpleegtoegang tot alle data. Enkele rollen kunnen een export van de volledige database maken zonder zicht op de verdere verwerking van de geëxporteerde data. Er bestaat de mogelijkheid voor medewerkers met muteerrechten tot wijzigen (aanvullen, wijzigen, ante-dateren etc) van alle data in FSV. Dit wordt niet gelogd en gemonitord. Ook leidt voornoemde in zekere zin tot een zgn 'chilling effect'²⁰ doordat meerdere teams FSV slechts beperkt vullen ('hit-no hit-achtig') en een parallelle administratie voeren voor de details van het signaal. Hoewel er geen voorbeelden van incidenten/misbruik bekend zijn, voldoet de huidige verwerkingsvorm niet aan de eisen die, mede vanuit privacy by design/default, aan informatiesystemen worden gesteld. Ook hier bestaat een aanzienlijke kans dat de inbreuk op de privacy groter is dan noodzakelijk en de impact aanzienlijk kan zijn als er (veelal een verdere) verwerking ontstaat door de wijze van registratie in FSV.

¹⁹ Waarvan ongeveer 10% (509) inactief, dd dec 2018.

²⁰ Fenomeen dat ontstaat als personen zich anders gaan gedragen vanwege een mogelijke privacy-impact. Doorgaans betrokkene (belastingplichtigen), in dit geval medewerkers.

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.

12. 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 verwerkingsverantwoordelijke 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. herstelmogelijkheid.

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.

²¹ Mede ingegeven door de constatering dat er functionele wensen bestaan, soms overlappend met de in de PIA geadresseerde issues, die niet (goed) in de huidige applicatie-architectuur kunnen worden uitgewerkt. Kostenefficiëntie speelt mede een rol bij dit advies. Hierbij is aansluiten bij het project (in opstartfase) vanuit het Breed Informatiestroomlijn Overleg (BIO) gewenst. Het BIO heeft directe aansluiting op het concernbrede fraudelandschap (FDO, FPO en de fraudecoördinator).

Als hoofdmaatregel wordt een herontwerp / migratie van FSV naar een nieuwe opzet²¹ geadviseerd. Daarmee kunnen, met als uitgangspunt privacy by design en default, deesignaleerde risico's worden weggenomen. Borg dat de migratie wordt gedaan in combinatie met processuele maatregelen als procesuniformering²², work-flow-management, zicht en zeggenschap op en over de verdere verwerking van data buiten FSV en voldoende controle daarop.

Herontwerpaspecten gerelateerd aan privacy-risico's zijn dan: gegevenskwaliteit (metadatering van de betekenis / waarde van gegevens waaronder het 'gewicht' van een signaal en het onderscheid tussen een signaal en een informatieverzoek), ontwikkelen van systeemfunctionaliteit en vastleggen van meta-data met betrekking tot de bewaar/archiveringstermijn, organiseren en reguleren van (al dan niet geautomatiseerde²³) datadistributie, need-to-know toegang tot data, logging- en monitoring van gebruik.

Mede afhankelijk van het tijdpad van de voorgestelde migratie/herontwerp, moet een aantal voorlopige maatregelen in de huidige opzet van FSV worden genomen, in het bijzonder ten aanzien van:

1. Het toetsen van de bestaande autorisaties (en mogelijk het aantal rollen) op noodzakelijkheid en actualiteit/geldigheid gevolgd door 'schoning' op basis van de uitkomst van de toetsing.
2. Het schonen van een aantal jaarlagen (bv jongste signaal over betrokkene is > x jaar).
3. a. Het aanbrengen van onderscheid tussen een signaal en een informatieverzoek bij verdere verwerking van FSV data in andere informatiesystemen / analyseomgevingen.
b. (indien mogelijk) het zo objectief mogelijk vastleggen van het 'gewicht' van een signaal.
c. Implementeren van een uniforme werkwijze (bv. Conform/analoog proces Toeslagen) om op fiscale relevantie onderzochte informatieverzoeken op te voeren als signaal en deze signalen (verder) te verwerken in plaats van de informatieverzoeken.
4. Het verwijderen/de-activeren (of nader beperken qua gebruikersgroep) van massale en/of integrale exportfunctie(s).
5. Verbeteren van kennis en gebruik van FSV in het bijzonder ten aanzien van de mogelijke privacyrisico's zoals stigmatisering. Hier kan ook worden gedacht aan een Code of Practice/gebruikersinstructie met ethische en privacy uitgangspunten, mogelijk in een breder verband dan FSV.

Maak hierbij gebruik van de al aanwezige informatie in het document 180329 F18.045 Feature aanpassingen Dagboek FSV en eerder vastgelegde oplossingsmogelijkheden voor herbouw.

²¹ Mede Ingegeven door de constatering dat er functionele wensen bestaan, soms overlappend met de in de PIA geadresseerde issues, die niet (goed) in de huidige applicatie-architectuur kunnen worden uitgewerkt. Kostenefficiëntie speelt mede een rol bij dit advies. Hierbij is aansluiten bij het project (in opstartfase) vanuit het Breed Informatiestroomlijn Overleg (BIO) gewenst. Het BIO heeft directe aansluiting op het concernbrede fraudelandschap (FDO, FPO en de fraudecoördinator).

²² Waaronder bredere implementatie van de praktijk bij Toeslagen van weging van een informatieverzoek om vervolgens bij gereede twijfel een (verder te verwerken) signaal op te voeren.

²³ Denk aan opslag in en distributie vanuit datafundamenten ipv handmatig overzetten naar (5+)systemen zoals nu gebeurt.



Maatregelen
nemen

Privacybewustwording

Doelbinding

Noodzaak

Effecten in kaart

PIA
Bescherming van
persoonsgegevens

Risico's

minimaliseren

Richtinggevend

Rechtsgrond

Met open vizier