EH&I	LSI (landelijke	Sturing aanpak, probleem	SAS Script / ACL	Ja	Eenmalig / op afroep	Persoonsgegevens gedelegee
EH&I	Gruff	Onder Gruff wordt	Teradata SQL Data-	Ja	Ja	Continue beschikbaar	Geautoriseerde medewer
EH&I	Anbi profiling	risicomodel ANBI, beheer en				ANBI – Persoonsgegevens
EH&I	Centrale selectie MKB	ondersteuning MKB met				MKB – Persoonsgegevens
EH&I	Gruff	technisch onderhoud				MT EHI – Persoonsgegevens
EH&I	LAA verwonderadressen	analysemodel adresfrau				CAP – Persoonsgegevens
						Persoonsgegevens
EH&I	risicovolle adressen	vastleggen risicovolle				MT EHI – Persoonsgegevens
EH&I	Stivers	afgeleide van ANBI risicomod				MT MKB – Persoonsgegevens
EH&I	Teradata administrator	technische ondersteu				MT EHI – Persoonsgegevens
EH&I	verhuurderheffing onderhou	risicomodel verhuurd				Persoonsgegevens
EH&I	WMK toetsen maken	beoordelen AVG onderhan				MT EHI – Persoonsgegevens
EH&I	ZVP	analysemodel ZVP met hun				GO – Persoonsgegevens Persoonsgegevens

~~BVR,~~ ~~DIA~~
~~LH,OB,~~
~~Vpb, IH,~~
~~BvR~~ ~~ISC~~
~~(NAW,~~
~~relaties,~~

~~heet LAA~~
~~verwonde~~
~~radressen~~

Project A4, Project NIT*, werkzaamheden vanaf 15 december 2018

*(onderaan dit document is een afkortingenlijst opgenomen)

Aanleiding/inleiding

Samen met de business MKB werken we aan een Nieuwe Intelligence voorziening Toezicht.
De afgelopen maanden is er binnen het project NIT gewerkt aan een MVP wat bestaat uit een eindproduct in de vorm van een roze laag (drie roze tabellen). Daarnaast is binnen het project gewerkt aan de bouw van een subjectgericht datafundament, dat input is voor de roze laag.

Met het MVP kan de business haar huidige werk doen, echter niet volledig. Gedurende de ontwikkeling van het MVP is door business aangegeven dat ze een uitgebreider MVP willen hebben. Daarbij is het MVP een tijdelijk product, en werken we toe aan ander soortig eindproducten. Om de eindproducten te kunnen realiseren is de verwachting dat het subjectgericht datafundament dient te worden verrijkt met data.

Deze opdracht A4 beschrijft hoe het vervolg van project NIT er voor de komende maanden uit komt te zien.

Het doel en scope van het project na 15 december 2018

Waar bestaat het project uit?

Project NIT bestaat na 15 december uit vier onderdelen:

1. **Wegwerken technische schuld op Subjectgericht datafundament**

Het opleveren van het MVP per 15 december 2018 kent een harde deadline. Om deze deadline te halen is het subjectgericht datafundament gebruiksklaar gemaakt. Echter, om te kunnen voldoen aan de richtlijnen van DF&A dienen er nog werkzaamheden uitgevoerd te worden.

In hoofdlijnen omvat dit het volgende:

- Validatie van business rules waardoor het DF voor alle middelen is in te zetten (generiek maken;
- Afstemming over hoe het datafundament kan aansluiten bij de architectuureisen
- Waar nodig verplaatsen van business rules / attributen naar de juiste plaats in het lagenmodel (onderkant of bovenkant paars in SBJ of in een ander datafundament dan SBJ).
- Data die vanwege tijdsdruk via een brievenbuslevering is ontsloten, opnemen vanuit de bron.
- Vooronderzoek naar de behoefte aan een datafundament subject bij DF&A (en eventueel daarbuiten), bijvoorbeeld Inzicht.
- De bevindingen uit dit vooronderzoek verwerken opdat een generiek datafundament subject wordt gemaakt.
- Eventueel een andere manier van historisatie, mede afhankelijk van de behoeften die leven bij de afdeling.
- Documenteren
- Van A naar P omgevingIn beheername

Het wegwerken van de technische schuld bij het datafundament TZT en bij CNV (onderdeel van CLC) vallen buiten de scope van dit project.

De totale doorlooptijd hiervan wordt ingeschat op 6 maanden. Benodigde resources staan vermeld in Onderdeel XX van deze opdracht A4. Er is een aanvullend document wat gedetailleerder ingaat op de inhoud.

2. **Uitbreiden van Subjectgericht datafundament = onderdeel van punt 4**

MKB heeft een grotere diversiteit aan databronnen nodig, ten aanzien van onderwerpen als nalevingsbeelden en verdieping op thema's. Het MVP is niet volledig genoeg voor MKB om deze werkzaamheden uit te kunnen voeren. Dit geldt ook voor het datafundament subject.

De aanpak hierin is voor het datafundament subject als volgt:

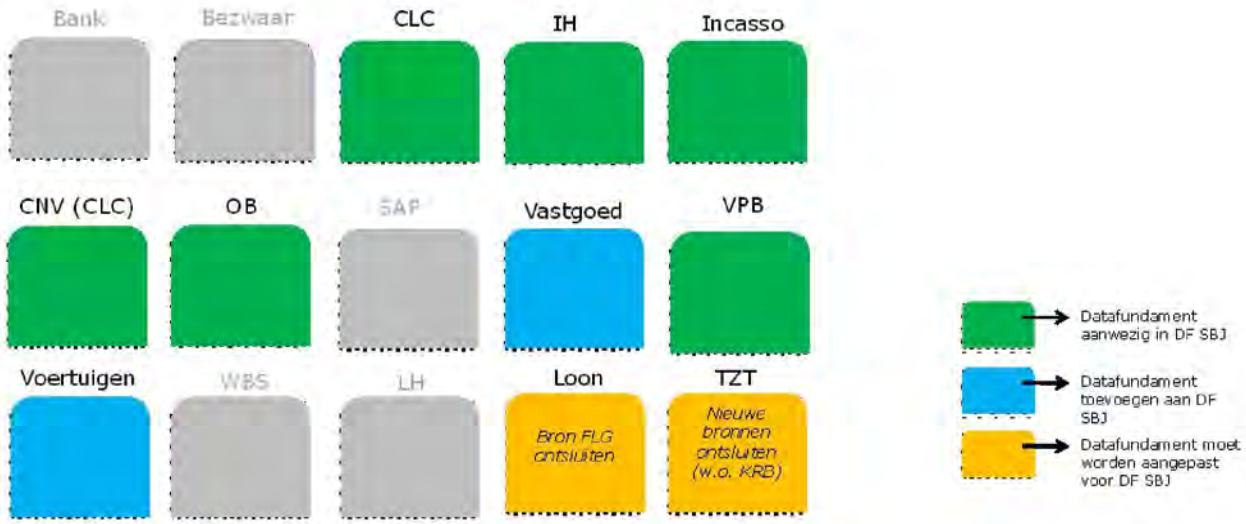
- Er wordt uitgevraagd aan welke data MKB precies behoefte heeft (eindproducten), zodat we vooraf inzichtelijk hebben waar het om gaat. Ook wordt gevraagd voor welke doeleinde de hoeveelheid data nodig is;
- Vaststellen welke informatie in het datafundament subject moet komen om aan de informatiebehoefte van de eindproducten (roze laag) te voldoen.
- Vaststellen hoe de benodigde informatie in het datafundament subject moet worden opgenomen (het datafundament subject bouwt zelf niets op):
    - Informatie is aanwezig in een bestaand datafundament en dit datafundament is al opgenomen in het datafundament subject.
    - Informatie is aanwezig in een bestaand datafundament, die nog niet is opgenomen in een datafundament.
    - Informatie is nog niet aanwezig en moet worden opgenomen in een bestaand datafundament.
    - Informatie zit in een bron die nog niet is ontsloten door een datafundament.
- Het logisch datamodel datafundament subject uitbreiden.
- Een business datamodel maken voor datafundament subject.
- Het subjectgerichte datafundament wordt aangevuld met bovenstaande databronnen;

Het gaat in ieder geval om de volgende databronnen:

- Auto
- Vastgoed

- Loon

Plaatje met informatie over welke fundamenten reeds aanwezig zijn in het datafundament subject en welke nog niet (voor zover nu bekend; een compleet overzicht hebben we pas als we na 15 december de totale wens van MKB hierin inzichtelijk maken):



De totale doorlooptijd hiervan wordt ingeschat op 8 maanden. Benodigde resources staan vermeld in Onderdeel XX van deze opdracht A4. Er is een aanvullend document wat gedetailleerder ingaat op de inhoud.

3. Wegwerken technische schuld op roze laag

Op het MVP (de roze laag) die op 15 december 2018 wordt opgeleverd, dienen nog werkzaamheden te worden uitgevoerd conform richtlijnen van DF&A. Deze werkzaamheden zijn:

- XX
- XX

De totale doorlooptijd hiervan wordt ingeschat op XX maanden. Benodigde resources staan vermeld in Onderdeel XX van deze opdracht A4. Er is een aanvullend document wat gedetailleerder ingaat op de inhoud.

4. Ontwikkeling van eindproducten

Er wordt samen met de business gewerkt aan eindproducten. De eindproducten worden ontwikkeld ten behoeve van centrale regie collega's binnen het MKB. Voorbeelden zijn producten voor

Het is nog onbekend hoe deze producten er exact uit komen te zien. Denk hierbij aan een dashboard, risicomodel/analysetechnieken, self service BI dashboard, enz.

Tevens wordt nog onderzocht of er naast bovenstaande doeleinden nog meer typen producten nodig zijn.

Selectielijsten vervangen voor boekenonderzoeken

Iteratief ontwikkelen, minimaal product ontwikkelen en testen/valideren

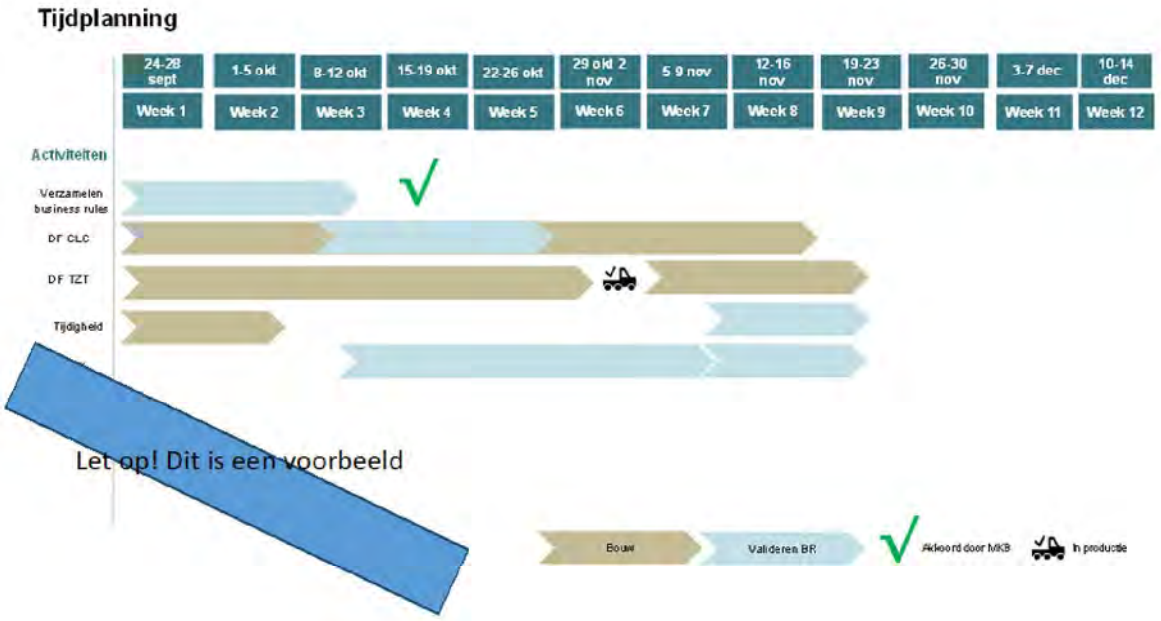
Wat valt buiten scope

- Er dient besluitvorming te komen over gebruik van data op spoor 2. Dit omdat er een negatieve WMK toets ligt. Dit onderwerp wordt door Persoonsgegevens en Persoonsgegevens uitgewerkt en voorgelegd bij Persoonsgegevens en Persoonsgegevens Spoor 2 staat los van de werkzaamheden binnen dit project

- Er is door MKB structureel toegang gevraagd tot data (tot/met onderkant paars). Dit is een bestuurlijke besluitvorming, en wordt door MKB via het portfolio proces ingebracht. Dit valt buiten het project NIT

- Het MVP is ontwikkeld uit nood ivm het uitzetten van de Apandu 06, 07 en 22 op 15 december 2018. Het MVP bestaat voor een deel uit het nabouwen van RAM om de business hiermee te ondersteunen. Het MVP is geen blijvend product, het doel is ten aanzien van centrale regie MKB innovatieve, datagedreven, eindproducten te ontwikkelen conform DF&A structuur en richtlijnen. DF&A ziet de meerwaarde van de reeds door EH&I/MKB ontwikkelde producten, en gebruikt deze input om vernieuwing toe te voegen.

Tijdplanning



Samengevat, wat is het verwachte resultaat op XX

1. Een robuust subjectgericht datafundament en MVP;
2. Het Subjectgerichte datafundament is verrijkt met aanvullende data en generiek gemaakt;
3. Er zijn in een labfase twee eindproducten ontwikkeld en deze zijn klaar om getest te worden met productiedata.

Benodigde resources

De volgende resources zijn benodigd voor het datafundament subject:

Naam	Rol	Wegwerken technische schuld DF SBJ		Uitbreiden DF SBJ	
		FTE	Doorlooptijd	FTE	Doorlooptijd
Persoonsgegevens	Modelleur/bouwer	0,3	6 maanden	0,2	8 maanden
	Modelleur/bouwer	0,3	6 maanden	0,2	8 maanden
	Bouwer/business expert	0,4	6 maanden	0,1	8 maanden
	Bouwer/business expert	0,4	6 maanden	0,1	8 maanden
	Bouwer	0,6	6 maanden	0,4	8 maanden
	Bouwer	0,6	6 maanden	0,4	8 maanden
	Business analist	0,6	6 maanden	0,2	8 maanden
?	Projectleider datafundamenten	0,3	6 maanden	0,2	8 maanden

1. Wegwerken technische schuld MVP			
Naam	Rol	FTE	Doorlooptijd
Persoonsgegevens			
XX			
XX			
?	Overall projectleider		

2. Ontwikkeling van eindproducten			
Naam	Rol	FTE	Doorlooptijd
Persoonsgegevens			
XX			
XX			
?	Overall projectleider		

Opdrachtgever en opdrachtnemer

Opdrachtgever: Persoonsgegevens

Aanspreekpunten gedelegeerd opdrachtgever: Persoonsgegevens (MKB), Persoonsgegevens (DF&A)

Contactpersonen business (MKB):

Persoonsgegevens

Persoonsgegevens

Looplijnen bij Escalatie:

Vanuit MKB: Persoonsgegevens

Vanuit DF&A: Persoonsgegevens

Versiehistorie

Naam	Versienr	Betreft
Persoonsgegevens	0.1	Concept
	0.3	Aanvulling
	0.3	Aanvulling
		Aanvulling

Afkortingenlijst

NIT	Nieuwe intelligence voorziening toezicht
SBJ	Subjectgericht datafundament
MVP	Minimal viable product
GTK	Generieke
MKB	Midden- klein bedrijf
DF&A	Datafundamenten & Analytics

GEGEVENSBESCHERMINGSEFFECTBEOORDELING RIJKSDIENST

IP analyse IH

Dit template is gebaseerd op "***Model Gegevensbeschermingseffectbeoordeling Rijksdienst***"; versie 0.2 voorportalen CIO-beraad, IOWJZ, ICBR; 24 Juli 2017.

Onderwerp van deze GEB

Inhoud

I. INLEIDING

Het model bestaat uit 17 punten verspreid over vier onderdelen. Onderdeel A behandelt de feiten van de voorgenomen gegevensverwerkingen. De beoordeling van de feiten aan het juridische kader komt aan de orde in onderdeel B. Onderdeel C gaat over risico's voor de rechten en vrijheden van betrokkenen en onderdeel D gaat over de beoogde maatregelen om die risico's aan te pakken. Deze opzet is ontleend aan de privacyregelgeving[1]. Het maken van een GEB is een dynamisch proces. Denkbaar is dat antwoorden in onderdeel A (moeten) worden aangepast nadat een beoordeling (onder B) is verricht en de risico's (onder C) en maatregelen (onder D) in kaart zijn gebracht.

De beantwoording van de 17 punten in dit model kan meer of minder gedetailleerd zijn afhankelijk van de aard en omvang van de voorgenomen regelgeving of verwerkingen door de overheid. Wel is het in alle gevallen noodzakelijk om alle punten van het model na te gaan en de gemaakte afweging per punt op te schrijven.

[1] Artikel 35, zevende lid, AVG en artikel 27, tweede lid, Richtlijn.

II. VRAGENLIJST GEGEVENSBESCHERMINGSEFFECTBEOORDELING

A. Beschrijving algemene kenmerken gegevensverwerkingen

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

1. Voorstel

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

. . In het MT Belastingen van 19-8-2013 is, naar aanleiding van wat bekend is geworden als de Bulgarenfraude besloten om het CAF in te richten. Dit combiteam heeft als opdracht om op basis van reeksen aangiften opvallende patronen in beeld te brengen die duiden op systematische fraude en/of misbruik en vervolgens de betrokkenen aan te pakken. De methode van werken heeft zich in de afgelopen jaren zodanig bewezen dat middels een MT besluit van 17 juli 2017 besloten is deze werkwijze een structurele plek te geven in de organisatie In de notitie doorontwikkeling CAF 2.0 is aangegeven dat het maken van scherpe analyses nog op veel meer terreinen kan plaatsvinden en dat bij het bestrijden van fraude en/of misbruik meer gedaan kan worden met het binnenhalen van contra informatie.

Dit specifieke GEB document ziet op de analyse van het aangiften gedrag van aangiften IH die gedaan zijn via een bepaald IP adres. Op deze wijze maken we inzichtelijk vanaf welk IP adres aangiften worden gedaan met opvallende patronen. Op deze wijze kunnen we fraude en/of misbruik detecteren. Momenteel beperkt deze analyse zich nog tot een aantal velden in de aangifte IH. Het doel is deze analyse op termijn verder uit te breiden naar ook andere elementen in de aangiften IH.

2. Persoonsgegevens

Som alle categorieën persoonsgegevens op die worden verwerkt en deel ze in onder de typen: gewoon, bijzonder of strafrechtelijk en wettelijk identificatienummer. Geef per persoonsgegeven aan op wie het betrekking heeft.

Gewone persoonsgegevens

Veldnaam	Bron	Betrekking op
De informatie wordt geleverd vanuit **RAM**. **Velden**: Aantal ingediende aangiften IH { JAAR} , Som van Aftrek specifieke zorgkosten aangever, Aantal van Aftrek specifieke zorgkosten aangever, Gemiddeld bedrag Aftrek specifieke zorgkosten aangever, Percentage aangiftes met Aftrek specifieke zorgkosten aangever, Som van saldo Aftrekbare giften aangever, Aantal van saldo Aftrekbare giften aangever, Gemiddeld bedrag Aftrekbare giften aangever, Percentage aangiftes met Aftrekbare giften aangever, Som van Aftrek uitgaven voor onderhouds-verplichtingen, Aantal van Aftrek uitgaven voor onderhouds-verplichtingen, Gemiddeld bedrag Aftrek uitgaven voor onderhouds-verplichtingen, Percentage aangiftes met Aftrek uitgaven voor onderhouds-verplichtingen, Som van Aftrekbaar bedrag scholingsuitgaven aangever, Aantal van Aftrekbaar bedrag scholingsuitgaven aangever, Gemiddeld bedrag Aftrekbaar bedrag scholingsuitgaven		

aangever, Percentage aangiftes met Aftrekbaar bedrag scholingsuitgaven aangever,Som van uitgaven voor inkomens-voorzieningen, Aantal van uitgaven voor inkomens-voorzieningen, Gemiddeld bedrag Uitgaven voor inkomens-voorzieningen, Percentage Aangiftes met Uitgaven voor inkomens-voorzieningen, Aantal rose velden.		

Bijzondere persoonsgegevens

Veldnaam	Bron	Betrekking op

Strafrechtelijke gegevens

Veldnaam	Bron	Betrekking op

Wettelijk identificatienummer

Veldnaam	Bron	Betrekking op

3. Gegevensverwerkingen

Geef alle voorgenomen gegevensverwerkingen weer.

Verzamelen, vastleggen, opslaan, Ordenen, Structureren, Opvragen, Raadplegen, Gebruiken, Verstrekken door middel van doorzending, Combineren, Afschermen

4. Verwerkingsdoeleinden

Beschrijf de hoofd- en nevendoeleinden van de voorgenomen gegevensverwerkingen.

Met behulp van deze analyse kunnen we opvallende patronen opsporen in de reeks aangiften die gedaan zijn vanaf een bepaald IP adres. We vergelijken deze patronen met het algemene beeld van de hele doelgroep en de adressen die sterk afwijken van het gemiddelde komen daarmee in beeld. Afhankelijk van de mate waarin een IP van het gemiddelde afwijkt dan wel het aantal keren dat het adres van het gemiddelde afwijkt (bekeken over een reeks van velden in de aangifte IH) wordt daarmee het risico ingeschat of sprake is van mogelijke fraude en/of misbruik. De analyse wordt zowel gebruikt om adressen in beeld te brengen die nader onderzocht moeten worden, maar tevens ook om jaarlijks het gedrag en de tendensen daarin te kunnen meten van de betreffende doelgroep.

5. Betrokken partijen

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

Belastingdienst
Combiteam Aanpak Facilitators

6. Belangen bij de gegevensverwerking

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

Afgeven van signalen die kunnen duiden op fraude en/of misbruik, de behandeling daarvan alsmede resultaat/effectmeting

7. Verwerkingslocaties

Benoem in welke landen de voorgenomen gegevensverwerkingen plaatsvinden.

Apeldoorn, Utrecht, via een beveiligde server

8. Technieken en methoden van de gegevensverwerkingen

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 dataverwerkingen en, zo ja, beschrijf waaruit een en ander bestaat.

Op basis van reeksen van aangiften opvallende patronen in beeld brengen die duiden op systematische fraude en/of misbruik bij het doen vaan aangiften inkomensheffing

9. 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 voorgenomen gegevensverwerkingen.

AVG bepaling en Awr 47 e.v

10. Bewaartermijnen

Bepaal en motiveer de bewaartermijnen van de persoonsgegevens aan de hand van de verwerkings-doeleinden.

De bewaartermijn van de data leveringen aan CAF stellen we in lijn met de navorderings/naheffingstermijn op 5 jaar.

Dit heeft tevens als voordeel dat alle CAF produkten voorzover die tot op heden zijnopgeslagen nog binnen deze termijn vallen nu het CAF nog geen 5 jaar bestaat. Aan het einde van ieder jaar, te beginnen eind 2018 wordt de CAP map doorgelopen door de secretaris van het CAF om te beoordelen welke bestanden verwijderd kunnen worden.

Mocht een bestand ouder zijn dan 5 jaar, dan zal dit worden verwijderd, tenzij er een aantoonbare reden is om het bestand alsnog voor een langere tijd vast te houden. Een aantoonbare reden zou kunnen zijn een lopende strafzaak, lopend hoger beroep of cassatie etc. Mocht hiervan sprake zijn, dan zal een document in de betreffende map worden geplaatst waarin de redenen van de verlenging van de termijn zullen worden vermeld. Op deze wijze hopen voor het CAF werk ten behoeve van de bewaartermijn een eenduidige alsmede overzichtelijke en eenvoudig beheersbare werkwijze te creëren.

Beveiliging:

Voor het verrichten van de becon analyses zelf zijn slechts een beperkt aantal CAF specialisten geautoriseerd. Deze medewerkers kunnen de uitkomsten van de analyses zo nodig doorzetten naar de beveiligde CAF map (q schijf). Tot deze map hebben alleen medewerkers toegang die zowel door de teamleider CAF als de teamleider FIOD account midden en vervolgens door toepassingsbeheer van de FIOD geautoriseerd zijn. Periodiek wordt beoordeeld of de autorisatietabel moet worden aangepast

B. Beoordeling rechtmatigheid gegevensverwerkingen

Beoordeel de rechtsgrond, noodzaak en doelbinding van de voorgenomen gegevensverwerkingen en rechten van de betrokkene.

11. Rechtsgrond

Bepaal op welke rechtsgronden de gegevensverwerkingen worden gebaseerd.

AVG bepaling en Awr 47 e.v

12. 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 dit is toegestaan.

13. 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.

de nakoming van een wettelijke verplichting (WIV)
een goede vervulling van de publieke taak

14. Noodzaak en evenredigheid

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

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

Noodzakelijkheid:

Alle CAF vragen zien op het onderkennen, detecteren en monitoren van specifieke patronen in aangiften en of toeslaggegevens die duiden op misbruik, oneigenlijk gebruik en/of fraude.

Uit de Europese verordening komt de volgende voor CAF relevante tekst:

De betrokkene dient het recht te hebben niet te worden onderworpen aan een louter op geautomatiseerde verwerking gebaseerd besluit, dat een maatregel kan behelzen — over persoonlijke hem betreffende aspecten, waaraan voor hem rechtsgevolgen zijn verbonden of dat hem op vergelijkbare wijze aanmerkelijk treft, zoals de automatische weigering van een online ingediende kredietaanvraag of van verwerking van sollicitaties via internet zonder menselijke tussenkomst. Een verwerking van die aard omvat „profilering", wat bestaat in de geautomatiseerde verwerking van persoonsgegevens ter beoordeling van persoonlijke aspecten van een natuurlijke persoon, met name om kenmerken betreffende beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren of interesses, betrouwbaarheid of gedrag, locatie of verplaatsingen van de betrokkene te analyseren of te voorspellen, wanneer daaraan voor hem rechtsgevolgen zijn verbonden of dat hem op vergelijkbare wijze aanmerkelijk treft.
Besluitvorming op basis van een dergelijke verwerking, met inbegrip van profilering, dient echter wel mogelijk te zijn wanneer deze uitdrukkelijk is toegestaan bij Unierecht of lidstatelijk recht dat op de verwerkingsverantwoordelijke van toepassing is, onder meer ten behoeve van de controle en voorkoming van belastingfraude en -ontduiking overeenkomstig de regelgeving, normen en aanbevelingen van de instellingen van de Unie of de nationale voor oversight bevoegde instanties, en om te zorgen voor de veiligheid en betrouwbaarheid van een dienst die door de verwerkingsverantwoordelijke wordt verleend, of noodzakelijk voor de sluiting of uitvoering van een overeenkomst tussen de betrokkene en een verwerkingsverantwoordelijke, of wanneer de betrokkene zijn uitdrukkelijke toestemming heeft gegeven. In ieder geval moeten voor dergelijke verwerking passende waarborgen worden geboden, waaronder specifieke informatie aan de betrokkene en het recht op menselijke tussenkomst, om zijn standpunt kenbaar te maken, om uitleg over de na een dergelijke beoordeling genomen besluit te krijgen en om het besluit aan te vechten. Een dergelijke maatregel mag geen betrekking hebben op een kind.

De verwerking is alleen rechtmatig indien en voor zover aan ten minste een van de onderstaande voorwaarden is voldaan:

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. De eerste alinea, punt f), geldt niet voor de verwerking door overheidsinstanties in het kader van de uitoefening van hun taken.

Volgens de autoriteit persoonsgegevens mag verondersteld worden dat fraudedetectie (misbruik / oneigenlijk gebruik) impliciet tot de opdracht van de Belastingdienst behoort. De bevoegdheden van de Belastingdienst zijn beschreven in de AWR artikel 47 e.v. Daarnaast is wetgeving in de maak die nog explicieter aangeeft hoe de invulling van de bevoegdheden kan worden uitgevoerd. Daarnaast is bij de oprichting van het CAF bepaald dat bij de aanpak van systeemfraude breed moet worden gekeken. Dit behelst daarom zowel de Belastingmiddelen als Toeslagen. Deze opdracht (aanpak van systeemfraude) wordt voor de belastingmiddelen ingevuld op basis van de Awr en voor Toeslagen op basis van de Awir.

Proportionaliteitstoets:

De data die CAF opvraagt liggen in alle gevallen in lijn met de opdracht om patronen in reeksen van gegevens te detecteren en/of resultaten/effecten daarin te meten. Niet in alle gevallen zal sprake zijn van misbruik, oneigenlijk gebruik of fraude, maar om in beeld te krijgen of de risico's zich voordoen en in welke mate is het wel onontbeerlijk om de analyse uit te voeren. We vragen daarbij niet meer gegevens op dan die voor de analyse en/of voor het vervolgtraject daarvan relevant kunnen zijn. Bij ieder verzoek wordt de proportionaliteit afgewogen om te voorkomen dat niet teveel gegevens geleverd worden.

Subsidiariteitstoets:

Er is geen alternatief voor dit type analyse denkbaar. Als je minder zou doen, dan ga je het zicht op deze patronen niet krijgen dan wel niet volledig.

15. Rechten van de betrokkenen

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

In brede zin wordt aan betrokkenen en intermediairs/facilitators uitgelegd dat de Belastingdienst let op patronen in reeksen van aangiften. Dit is meermalen gepubliceerd in de media, beschreven op bijvoorbeeld het forum fiscaal dienstverleners en bijvoorbeeld toegelicht op de intermediairdagen

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 voorgenomen gegevensverwerkingen.

16. Risico's

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

a. welke negatieve gevolgen de gegevensverwerkingen kunnen hebben voor de rechten en vrijheden van betrokkene;
b. de oorsprong van deze gevolgen;
c. de waarschijnlijkheid (kans) dat deze gevolgen zullen intreden en
d. de ernst (impact) van deze gevolgen voor de betrokkene wanneer deze intreden.

Hou bij elk aspect rekening met de aard, omvang, context en doelen van de gegevensverwerking.

a. Mogelijke negatieve gevolgen op de rechten en vrijheden van de betrokkene

Er lijkt sprake van een onevenredige grote inbreuk op de rechten van betrokkene; Dit wordt mede ingegeven door de vrij grote gegevensset die momenteel wordt gebruikt. Voor de detectie van systematische fraude en/of misbruik is deze werkwijze echter onontbeerlijk.

a. Oorsprong van de mogelijke negatieve gevolgen

Dit wordt mede ingegeven door de vrij grote gegevens set die momenteel wordt gebruikt. Zo wordt er tot maximaal 6 jaar teruggekeken, ook worden er diverse koppelingen tussen IH data en gegevens omtrent de mogelijke indiener aangebracht. Probleem is dat op voorhand alle beschreven data benodigd zijn om een goede analyse te kunnen maken en dat pas achteraf na analyse duidelijk wordt of de uitkomsten proportioneel zijn in verhouding tot de omvang van de dataset. Aan de andere kant zegt het ook veel als bijvoorbeeld uit analyse blijkt dat bepaalde risico's zich bijvoorbeeld niet voordoen. In die gevallen blijft het ook bij die constatering, wordt de dataset ook verder niet meer actief ergens voor gebruikt en zijn er ook geen gevolgen voor welke betrokkene dan ook. Betrokkenen waarvan is komen vast te staan dat zij misbruik hebben gemaakt worden voor een langere periode gevolgd teneinde vast te kunnen stellen of het gedrag al dan niet verbetert dan wel of aanvullende maatregelen noodzakelijk zijn.

a. Waarschijnlijkheid (kans) dat de gevolgen zullen intreden

Dit kan voorkomen worden door hier transparant over te zijn. Niet over hoe er exact wordt gedetecteerd, maar wel over het feit dat er gelet wordt op patronen in reeksen van aangiften en dat betrokkenen waarvan is vastgesteld dat zij onjuiste aangiften indienen over een langere periode kunnen worden gemonitord.

b. Ernst (impact) van de gevolgen voor de gevolgen als deze intreden.

De vraag is wat in deze gevallen moet prevaleren. Het belang van de betrokkenen versus het belang van de samenleving in detectie van patronen die duiden op systematische fraude en/of misbruik.

D. Beschrijving voorgenomen maatregelen

Beschrijf de voorgenomen maatregelen om de hiervoor beschreven risico's van de voorgenomen gegevensverwerkingen voor de vrijheden en rechten van betrokkene aan te pakken.

17. 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.

Systematisch inregelen van de autorisaties tot de CAF map. Jaarlijks vast moment kiezen om de afspraken inzake de bewaartermijnen te borgen en te zorgen dat dataverzamelingen die buiten de gestelde bewaarperiode vallen en niet meer nodig zijn worden verwijderd.
Op de website van de Belastingdienst kan en mag in algemene bewoordingen worden aangegeven dat de Belastingdienst analyse verricht op opvallende patronen in reeksen van aangiften in het kader van de bestrijding van fraude en misbruik.

III. Bijlage, achtergrond en bronnen

1. Achtergrond

Een GEB is een instrument om van voorgenomen regelgeving of projecten waarbij persoonsgegevens worden verwerkt, de effecten voor betrokkenen op een gestructureerde en gestandaardiseerde wijze in kaart te brengen en te beoordelen. Op basis hiervan worden maatregelen getroffen om deze effecten voor betrokkenen te voorkomen of verkleinen.

De GEB Rijksdienst vervangt het Toetsmodel Privacy Impact Assessment Rijksdienst van 2013. Dit model is gebaseerd op de nieuwe Europese regelgeving, de Algemene verordening gegevensbescherming (AVG), de Richtlijn gegevensbescherming opsporing en vervolging (Richtlijn)3 en de mede daarop gebaseerde nationale regelgeving. In dit model zijn ook de richtsnoeren van de Europese privacytoezichthouders betrokken.4 Het model is gericht op de ontwikkeling van beleid en regelgeving waaruit verwerkingen van persoonsgegevens voortvloeien en op de verwerking van persoonsgegevens door of in opdracht van een onderdeel van de Rijksdienst en is bedoeld voor toepassing op alle beleidsgebieden en binnen alle rechtsdomeinen.

Deze vragenlijst is onderdeel van het Model Gegevensbeschermingseffectbeoordeling Rijksdienst. Dit document bestaat uit drie onderdelen:

I. Het eerste deel geeft een algemene inleiding op het instrument gegevensbeschermingseffectbeoordeling (GEB) – voorheen Privacy Impact Assessment (PIA) – en beschrijft het proces van het uitvoeren van een GEB/PIA.
II. Het tweede deel bevat het model om een GEB/PIA uit te voeren bestaande uit 17 punten.
III. In het derde deel wordt per punt van het model de achtergrond geschetst en een toelichting gegeven, uitgesplitst naar een GEB/PIA van voorgenomen regelgeving en van door de overheid voorgenomen gegevensverwerkingen (hierna: overheidsverwerkingen).

Dit model wordt gebruikt in de Rijksdienst en het is de opvolger van het Toetsmodel Privacy Impact Assessment Rijksdienst dat sinds 2013 beschikbaar is.

Het staat organisaties vrij om dit model zelf aan te vullen met organisatiespecifieke onderdelen. Door dergelijke onderdelen toe te voegen, wordt het instrument beter bruikbaar voor de eigen organisatie en daarmee gebruiksvriendelijker.

2. Bronnen

Het Model Gegevensbeschermingseffectbeoordeling Rijksdienst is gebaseerd op de volgende bronnen:

1. Grondslag voor het PIA 2013: *Kamerstukken II 2012/13, 26 643, nr. 282, herdruk 1*.

2. Algemene verordening gegevensbescherming (AVG): *Verordening (EU) 679/2016 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming)(PbEU 2016, L 119/1)*.
   Zie ook https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/europese-privacywetgeving/algemene-verordening-gegevensbescherming

3. Richtlijn *Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad.*
   Zie ook:
4. Richtsnoeren *Richtsnoeren van 4 april 2017, WP 248*.

In dit proceskader wordt achtereenvolgens in gegaan op de volgende vragen:

1. Wat is een GEB?
2. Waarom een GEB uitvoeren?
3. In welke gevallen is een GEB verplicht?
4. Hoe verhoudt de GEB zich tot andere instrumenten?
5. Wie is verantwoordelijk voor het uitvoeren van een GEB?
6. Wanneer in het proces moet ik een GEB uitvoeren?
7. Hoe voer ik een GEB uit?
8. Hoe verantwoord ik de uitkomst van een GEB?

1. Wat is een GEB?

De GEB Rijksdienst is een instrument om van voorgenomen regelgeving of projecten waarbij persoonsgegevens worden verwerkt, de privacyrisico's op een gestructureerde en gestandaardiseerde wijze in kaart te brengen. Op basis hiervan kunnen maatregelen worden getroffen om deze risico's te voorkomen of verkleinen. Het instrument is bedoeld om een transparante afweging mogelijk te maken tussen de privacyrisico's van verschillende alternatieven en om te rapporteren over de impact die het voorstel heeft voor de privacy van betrokkenen. Gebruik van het instrument vergroot mede het privacybewustzijn bij betrokken instanties in de beleidsontwikkelingsfase.

De GEB Rijksdienst is nadrukkelijk geen instrument om te beoordelen of bij een gegevensverwerking wet- en regelgeving wordt nageleefd (compliance tool). Het doel van een GEB is om de bescherming van persoonsgegevens onderdeel te maken van het afwegingsproces. Het heeft daarnaast doelen op het vlak van verantwoording en draagvlakvergroting.

Het model is gebaseerd op nationale en Europese regelgeving waaronder de Algemene verordening gegevensbescherming (AVG)[2], de Richtlijn gegevensbescherming opsporing en vervolging (Richtlijn)[3] en de daarop gebaseerde wetgeving, te weten de Uitvoeringswet Algemene verordening gegevensbescherming, de Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens. Het model is gericht op gegevensverwerkingen door of in opdracht van een onderdeel van de Rijksdienst en is bedoeld voor toepassing op alle beleidsgebieden en binnen alle rechtsdomeinen.

Een voltooide GEB Rijksdienst bestaat uit:

A. een systematische beschrijving van de voorgenomen verwerkingen en de verwerkingsdoeleinden;
B. een beoordeling van de noodzaak, evenredigheid en verenigbaarheid van de verwerkingen met betrekking tot de doeleinden;
C. een beoordeling van de risico's voor de rechten en vrijheden van betrokkenen; en
D. de beoogde maatregelen om deze risico's aan te pakken.[4]

2. Waarom een GEB uitvoeren?

Door het uitvoeren van een GEB kan de bescherming van persoonsgegevens op een gestructureerde manier onderdeel uitmaken van de belangenafweging en besluitvorming van voorgenomen regelgeving, beleid of (ICT-)projecten binnen de Rijksdienst. Door een GEB vroeg in het proces van wetgevings-voorbereiding of beleids- of systeemontwikkeling uit te voeren vormt het beschermen van de privacy een uitgangspunt en wordt daarmee gestimuleerd dat bij verwerking van persoonsgegevens een zo klein mogelijke inbreuk op de persoonlijke levenssfeer wordt gemaakt.

---

[2] Verordening (EU) 679/2016 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming)(PbEU 2016, L 119/1).
[3] Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad.
[4] Zie artikel 35, zevende lid, van de AVG.

Een GEB is in de eerste plaats richtinggevend. Door het model te volgen kunnen relevante privacyrisico's die eerder in de wetgevingsvoorbereiding of bij de beleids- of systeemontwikkeling niet zijn onderkend aan het licht komen. Als dat het geval is, is het noodzakelijk om deze aspecten alsnog in de voorbereiding mee te nemen. Een GEB helpt zo met het identificeren en beheersen van risico's maar ook met het vermijden van onnodige kosten (in de zin dat problemen in een later stadium moeten worden opgelost).

Een GEB is ook corrigerend. Het kan tijdens het uitvoeren van de GEB nodig zijn eerdere keuzes te heroverwegen, en vervolgens voor een andere (minder inbreukmakende) oplossing te kiezen. Het kan dus voorkomen dat in een eerder stadium overwogen opties en oplossingen bij nadere beschouwing niet goed genoeg kunnen worden onderbouwd vanwege de hiermee gepaard gaande privacyrisico's. Vanwege het richtinggevende en corrigerende karakter van een GEB kan het uitvoeren van de GEB een dynamisch proces zijn, waarbij beoogde (beleids)oplossingen of het ontwerp van een systeem geleidelijk worden aangescherpt.

Het uitvoeren van een GEB kan op deze manier zorgen voor vertrouwen in de voorgenomen maatregel, binnen en buiten de organisatie. Het verzamelen van de informatie voor het beantwoorden van de vragen helpt medewerkers en leidinggevenden bij de besluitvorming en het afleggen van verantwoording daarover. Het uitvoeren van een GEB als zodanig stimuleert privacybewustwording binnen de Rijksoverheid.

3. In welke gevallen is een GEB verplicht?

Staand kabinetsbeleid bepaalt dat bij de ontwikkeling van beleid en wetgeving waaruit gegevensverwerkingen voortvloeien, evenals bij de bouw van ICT-systemen en de aanleg van grote databestanden, een GEB moet worden uitgevoerd.

Dat beleid volgt uit de op 11 mei 2013 door de Eerste Kamer aangenomen motie-Franken en het regeerakkoord Rutte-II.[5] De ministerraad heeft in juni 2013 besloten dat binnen de Rijksoverheid per 1 september 2013 bij de ontwikkeling van beleid en wetgeving, evenals bij de bouw van ICT-systemen en de aanleg van grote databestanden het Toetsmodel PIA Rijksdienst moet worden gehanteerd.[6] Het Toetsmodel PIA Rijksdienst is daartoe opgenomen in het IAK (Integraal afwegingskader voor wetgeving en beleid) en het Handboek Portfolio Management.

Vanaf 25 mei 2018 verplichten artikel 35 van de AVG en artikel 27 van de Richtlijn tot het uitvoeren van een GEB voor gegevensverwerkingen met een hoog risico voor de rechten en vrijheden van natuurlijke personen.

Een GEB is op grond van de AVG in ieder geval vereist in de volgende gevallen:[7]

a. een systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen, die is gebaseerd op geautomatiseerde verwerking, waaronder profilering, en waarop besluiten worden gebaseerd waaraan voor de natuurlijke persoon rechtsgevolgen zijn verbonden of die de natuurlijke persoon op vergelijkbare wijze wezenlijk treffen;
b. grootschalige verwerking van bijzondere categorieën van persoonsgegevens of van gegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten;
c. stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten.
d. wanneer de AP heeft geoordeeld dat een GEB verplicht is.

Een GEB is op grond van de AVG *niet* verplicht in de volgende gevallen:[8]

a. de verwerking zijn grondslag vindt in een wettelijke verplichting of publieke taak,[9] en in het kader van het vaststellen van deze grondslag reeds een GEB is verricht;

[5] *Kamerstukken I* 2010/11, 31 051, nr. D.
[6] *Kamerstukken II* 2012/13, 26 643, nr. 282, herdruk 1 (brief van 21 juni 2013, aanbieding toetsmodel PIA Rijksdienst aan Tweede Kamer).
[7] Artikel 35, derde en vierde lid, van de AVG.
[8] Artikel 35, vijfde en tiende lid, van de AVG.
[9] In de AVG wordt gesproken van 'een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag'.

b. wanneer de AP heeft geoordeeld dat een GEB niet verplicht is.

Het kabinetsbeleid dat voorschrijft in welke gevallen een GEB verplicht is, gaat verder dan de AVG en de Richtlijn. Allereerst omdat de AVG niet verplicht tot het verrichten van een GEB op wetgeving. Daarnaast omdat de AVG enkel bij risicovolle verwerkingen een GEB vereist. Het kabinetsbeleid dat is ingezet in 2013, wordt voortgezet met dit instrument GEB Rijksdienst. Daarbij is voor de vereisten waaraan een GEB moet voldoen wel aangesloten bij de AVG en Richtlijn.

4. Hoe verhoudt de GEB zich tot andere instrumenten?

Een GEB moet worden gehanteerd naast, en zo nodig in afstemming met andere hulpmiddelen voor ontwikkeling van wetgeving en beleid en de bouw van ICT-systemen en aanleg van databestanden. Een GEB komt dus niet in de plaats van deze bestaande instrumenten.

Bij voorgenomen beleid en wetgeving kan daarbij gedacht worden aan instrumenten uit het IAK waarmee gevolgen van voorgenomen beleid en wetgeving in kaart worden gebracht zoals de bedrijfseffectentoets (BET) en de uitvoerbaarheids- en handhaafbaarheidstoets (U&H-toets) of toetsing van voorgenomen wetgeving aan hoger recht, waaronder een constitutionele toets.

Bij de bouw van ICT-systemen en aanleg van databestanden kan daarbij gedacht worden aan het Voorschrift Informatiebeveiliging Rijksdienst 2007 (VIR 2007) en het Besluit voorschrift informatiebeveiliging rijksdienst – bijzondere informatie 2013 (VIRBI 2013). In het kader van informatiebeveiliging volgt uit het VIR 2007 dat voor een informatiesysteem maatregelen op basis van een risicoafweging zullen worden getroffen, met als doel te borgen dat de beveiliging van informatie binnen het systeem geborgd is. De genoemde risicoafweging wordt idealiter gemaakt in een risicoanalyse, waarbij de impact van verlies aan informatieveiligheid op het bedrijfsproces wordt bepaald (soms genoemd: *business impact analyse* (BIA)).

Zowel in het VIR 2007 als in de AVG wordt gesteld dat de verantwoordelijke een controlcyclus (plan-do-check-act (PDCA)) heeft ingericht om te borgen dat incidenten de juiste opvolging krijgen en maatregelen eventueel worden bijgesteld. Uit bovenstaande beschouwing volgt dat het van belang is beide aspecten in samenhang bij elkaar te brengen. Om te voldoen aan de van toepassing zijnde wet- en regelgeving zal een verantwoordelijke alle relevante aspecten integraal moeten beschouwen teneinde te borgen dat de uiteindelijk te treffen set van maatregelen in organisatie en techniek adequaat is. Om redenen van efficiency kan worden overwogen de genoemde processtappen waar mogelijk te integreren, zodat een BIA gelijktijdig met de GEB wordt uitgevoerd en alsook de keuze voor te treffen maatregelen.

5. Wie is verantwoordelijk voor het uitvoeren van een GEB?

a. Bij wetgeving en beleid

De beleidsdirectie die verantwoordelijk is voor het beleid en de daaruit voortvloeiende wetgeving is verantwoordelijk voor het uitvoeren van de GEB.

b. Bij overheidsverwerkingen (IT/uitvoering)

Formeel is de minister de verwerkingsverantwoordelijke voor de gegevensverwerking. In de praktijk zal de bevoegdheid om te beslissen of en op welke wijze persoonsgegevens worden verwerkt zijn gemandateerd aan een directeur-generaal of een directeur. De gemandateerde functionaris is dan verantwoordelijk voor de uitvoering van een GEB.

Het onderdeel van de Rijksdienst dat optreedt als verwerker in de zin van de AVG – dat wil zeggen degene die persoonsgegevens verwerkt namens/in opdracht van een verwerkingsverantwoordelijke – is niet verantwoordelijk voor de GEB. Wel is de verwerker verplicht de verwerkingsverantwoordelijke desgevraagd bijstand te verlenen. Veelal zal de betrokkenheid van de verwerker nodig zijn om de GEB te kunnen uitvoeren.

6. Wanneer in het proces moet ik een GEB uitvoeren?

a. Vroegtijdig

Het uitvoeren van een GEB in een vroegtijdig stadium is het meest effectief. Op dat moment is het mogelijk om met open vizier na te denken over de risico's en bestaat er nog voldoende gelegenheid om de uitgangspunten van voorgenomen beleid en wetgeving of van de bouw van ICT-systemen en aanleg van databestanden te wijzigen zonder grote nadelige consequenties. Dit voorkomt ook kostbare latere aanpassingen in processen, herontwerp van systemen of zelfs stopzetten van een project.

b. Bij wetgeving en beleid

De GEB moet in ieder geval voorafgaande aan de (internet)consultatie zijn verricht zodat de uitkomsten van de GEB meegenomen kunnen worden bij de consultatie.

c. Bij overheidsverwerkingen (IT/uitvoering)

De GEB moet in ieder geval voorafgaand aan de voorgenomen verwerkingen zijn verricht.

Een GEB kan meermaals en op verschillende momenten worden uitgevoerd. Bij wijziging van beleid en wetgeving waarmee verwerking van persoonsgegevens gemoeid is, wordt (opnieuw) een GEB uitgevoerd. In dat geval wordt de wijziging beoordeeld in samenhang met de bestaande verwerkingen. Ook bij de wijziging of aanpassing van ICT-systemen en databestanden kunnen nieuwe risico's aan de orde zijn. Indien de gegevensverwerking (bijvoorbeeld indien meer persoonsgegevens dan voorheen worden verwerkt) of de risico's die daarmee gepaard gaan significant veranderen, dient de GEB te worden geactualiseerd.

7. Hoe voer ik een GEB uit?

De uitvoering van een GEB beslaat de volgende processtappen:

1. Verzamel alle relevante informatie over de voorgenomen regelgeving of het projectvoorstel waarbij persoonsgegevens worden verwerkt.
2. Bespreek de punten van het model bij voorkeur in een verband, waar diverse relevante expertises deel van uitmaken. Betrokkenheid van meerdere personen met verschillende achtergronden en expertises – denk aan expertise op het gebied van het betreffende beleidsterrein, wetgeving, (informatie)beveiliging, ICT – resulteert in een betere GEB. Voor het uitvoeren van een GEB dient in ieder geval iemand met privacydeskundigheid te worden betrokken. Naast dat medewerkers van het betreffende project betrokken zijn, kan het wenselijk zijn om iemand van buiten het project te betrekken. De ideale omvang en diversiteit van de groep hangt af van de aard en omvang van de voorgenomen gegevensverwerking.
3. Leg de bevindingen schriftelijk in een rapport vast.
4. Consulteer waar passend de personen van wie persoonsgegevens worden verwerkt, de organisatie die hen vertegenwoordigen of andere belanghebbenden. Het betrekken van belanghebbenden stelt de uitvoerders van de GEB in staat om de zorgen die spelen in kaart te brengen en tegelijkertijd transparant te zijn over de persoonsgegevens die verwerkt zullen gaan worden en de redenen daarvoor.[10] Voor zover persoonsgegevens worden verwerkt van eigen personeel dient op grond van de Wet op de Ondernemingsraden de departementale of groepsondernemingsraad te worden betrokken.[11]
   Indien de GEB betrekking heeft op een voorstel voor wet- of regelgeving, kan consultatie achterwege blijven. Conform het draaiboek voor de regelgeving zal namelijk advies over het voorstel worden ingewonnen bij officiële adviescolleges en via internetconsultatie.
5. Wanneer uit de GEB blijkt dat de verwerking een hoog risico zou opleveren indien de verwerkingsverantwoordelijke geen maatregelen neemt om het risico te beperken, moet de AP worden geraadpleegd voorafgaande aan de verwerking.[12] Dit is slechts anders ingeval de GEB betrekking heeft op wet- of regelgeving, in welk geval het wetsvoorstel altijd ter consultatie moet worden toegestuurd aan de AP.[13]

[10] Artikel 35, negende lid, van de AVG.
[11] Artikel 27, eerste lid, onder k en l, van de Wet op de ondernemingsraden.
[12] Artikel 36, eerste lid, van de AVG.
[13] Artikel 36, vierde lid, van de AVG.

6. Leg het GEB-rapport ter advisering voor aan de functionaris voor gegevensbescherming (FG). Op grond van de AVG dient verplicht advies ingewonnen te worden bij de FG.[14]
7. Indien de gegevensverwerking gepaard gaat met de bouw van een ICT-systeem of het aanleggen van een databestand, moet de departementale Chief Information Officer (CIO) worden geconsulteerd. Leg de GEB in dat geval ter advisering voor aan de CIO. Deze geeft een oordeel bij de start of tussentijdse wijziging van een project, zoals opgenomen in de I-strategie. Onderdeel hierin is de beoordeling of in het projectplan is opgenomen of er binnen het project sprake is van het opnemen van privacygevoelige gegevens of van het koppelen of verrijken van data, en of daarbij beargumenteerd is of een GEB gewenst is. Indien de GEB wordt uitgevoerd in het kader van ontwikkeling van beleid waarmee (ook) de aanleg van databestanden of de bouw van ICT-systemen wordt voorzien, moet ook rekening worden gehouden met de beheersmaatregelen zoals beschreven in het handboek portfoliomanagement Rijk voor projecten met een grote ICT-component.

8. Hoe verantwoord ik de uitkomst van een GEB?

a. Bij wetgeving en beleid

Bij wetgeving wordt over GEB-resultaten een passage opgenomen in de memorie of nota van toelichting. Daarin wordt een samenvatting gegeven van de belangrijkste afwegingen en keuzes in de GEB. Het ligt voor de hand deze passage toe te voegen aan de al standaard op te nemen beschouwing over het grondrechtelijke kader en de toetsing aan de AVG. Hoewel een volledig gestandaardiseerde verantwoordingsparagraaf niet kan worden gegeven, zou een modelelement van deze paragraaf kunnen zijn:

"Gezien de aard van dit voorstel is in de fase van beleidsontwikkeling een GEB uitgevoerd (verwijzing naar kabinetsbesluit GEB). Met behulp hiervan is de noodzaak van gegevensverwerking bekeken, en zijn op gestructureerde wijze de implicaties van de maatregel(en)/het systeem op gegevensbescherming in kaart gebracht. Hierbij is in het bijzonder aandacht besteed aan de beginselen van gegevensminimalisering en doelbinding, het vereiste van een goede beveiliging en de rechten van de betrokkenen. [Beschrijving specifieke aspecten en de in dit geval gemaakte belangenafweging]"

In aansluiting op het beleid over het actief openbaar maken van uitvoerings- en effecttoetsen, moet de uitkomst van een GEB gepubliceerd worden op de voor iedereen toegankelijke wetgevingskalender.[15]

b. Bij overheidsverwerkingen (IT/uitvoering)

Neem de uitkomsten van de GEB op in het departementale register van de verwerkingsactiviteiten.

9. Organisatiespecifieke GEB

Het staat organisaties vrij om het Rijksbrede GEB model zelf aan te vullen met organisatiespecifieke vragen. Door dergelijke vragen toe te voegen, wordt het instrument beter bruikbaar voor het eigen organisatieonderdeel en dus gebruiksvriendelijker.

[14] Artikel 35, tweede lid, van de AVG.
[15] *Kamerstukken II* 2016/17, 33 009, nr. 39 en *Kamerstukken II* 2012/13, 29 362, nr. 224.

IV. Bijlage 2, voorbeelden Gegevensbeschermingseffectbeoordeling

Het model voor de GEB Rijksdienst volgt het stramien van artikel 35, zevende lid, AVG en artikel 27, tweede lid, Richtlijn. Het model bestaat uit 16 punten verspreid over vier delen. Deel A beschrijft de feiten van de voorgenomen gegevensverwerkingen. De beoordeling van de feiten aan het juridische kader komt aan de orde in deel B. Deel C gaat over risico's voor de rechten en vrijheden van betrokkenen en deel D gaat over de beoogde maatregelen om die risico's aan te pakken.

A. Beschrijving algemene kenmerken gegevensverwerkingen

Onder A wordt de eerste stap beschreven van de GEB. Dat betreft een overzicht van de relevante feiten. Pas als de feiten vaststaan, kan worden overgegaan tot een beoordeling van de rechtmatigheid gegevensverwerkingen. Zo worden de feiten gescheiden van de beoordeling. Als de feiten onduidelijk zijn, werkt dit door in de beoordeling. Vandaar dat daar eerst moet worden begonnen met een beschrijving van de relevante feiten.

1. Voorstel

Beschrijf het voorstel waar de gegevensbeschermingseffectbeoordeling op ziet op hoofdlijnen.

Om een GEB te kunnen verrichten moet duidelijk zijn op welk onderwerp/object deze betrekking heeft. Met een korte en bondige beschrijving van het voorstel waar de GEB op ziet, wordt tevens voorkomen dat bij het nalopen van de 16 punten hier verschillend over wordt gedacht. Ten behoeve van de duidelijkheid kan het soms ook nuttig zijn om expliciet aan te geven waar de GEB niet over gaat.

Bij conceptregelgeving kan voor deze beschrijving van het voorstel aansluiting worden gezocht bij de inleidende paragraaf van de memorie of nota van toelichting bij het voorstel, voor zover deze betrekking heeft op verwerkingen van persoonsgegevens.

Bij een overheidsverwerking (IT/uitvoering) kan in hoofdlijnen worden beschreven hoe het systeem van gegevensverwerking er uit zal zien. Als dat er is kan worden aangesloten bij het projectvoorstel.

2. Persoonsgegevens

Som alle categorieën persoonsgegevens op die worden verwerkt. Deel deze persoonsgegevens in onder de typen: gewoon, bijzonder of strafrechtelijk. Geef per categorie persoonsgegevens tevens aan op wie die betrekking hebben.

a. Persoonsgegevens

Stel allereerst alle te verwerken categorieën persoonsgegevens vast. Onder persoonsgegevens wordt verstaan: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (artikel 4, eerste onderdeel, AVG). 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.

Voorbeelden van persoonsgegevens zijn: naam, voorvoegsel, adres, telefoonnummer, e-mailadres, leeftijd, geboortedatum en -plaats, geslacht, woonplaats, nationaliteit, IP-adres, MAC-adres, KvK-nummer, winst eenmanszaak, bankrekeningnummer en -saldo, IQ, functie, opleiding, inkomens- en vermogensgegevens, kredietwaardigheid, persoonlijke voorkeuren, loonschaal, verslag van een functioneringsgesprek en wangedrag. 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.

b. Typen

Stel vervolgens de aard van de te verwerken categorieën 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 het persoonsgegevens, hoe groter de privacyrisico's voor de betrokkene zijn.

c. Bijzondere persoonsgegevens

Artikel 9, eerste lid, AVG geeft een limitatieve opsomming van categorieën bijzondere persoonsgegevens:

- ras of etnische afkomst;
- politieke opvattingen;
- religieuze of levensbeschouwelijke overtuigingen;
- het lid maatschap 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 in bepaalde situaties ook bijzondere persoonsgegevens, zoals ras of medische gesteldheid, worden afgeleid.

➢ *Genetische gegevens*

Genetische gegevens zijn persoonsgegevens over overgeërfde of verworven genetische kernmerken van een persoon die unieke informatie verschaffen over zijn fysiologie of gezondheid (artikel 4, dertiende onderdeel, AVG). Denk hierbij aan: DNA en gegevens over erfelijke ziekten.

➢ *Biometrische gegevens*

Biometrische gegevens zijn persoonsgegevens die het resultaat zijn van een specifieke technische verwerking met fysieke, fysiologische of gedragsgerelateerde kenmerken van een persoon op grond waarvan identificatie mogelijk is (artikel 4, veertiende onderdeel, AVG). Denk hierbij aan: vingerafdrukken, irispatroon, gezichtsprofiel, toetsaanslaganalyse, looppatroon, stemgeluid en slaapritme.

➢ *Gegevens over gezondheid*

Gezondheidsgegevens zijn alle persoonsgegevens over de fysieke of mentale gezondheid van een persoon (artikel 4, vijftiende onderdeel, AVG). Denk hierbij aan: gewicht, hartslag, handicap of verleende gezondheidsdiensten.

➢ *Strafrechtelijke persoonsgegevens*

Strafrechtelijke gegevens zijn persoonsgegevens over strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen (artikel 10 AVG). Voorbeelden hiervan zijn: strafblad, relaas verhoor en aanvraag voor een toevoeging in een strafzaak. Dit is een apart type gegevens. In de AVG zijn strafrechtelijke gegevens (anders dan in de Wbp) geen bijzondere persoonsgegevens. Wel gelden speciale eisen voor de verwerking ervan (zie punt 11 hierna).

d. Gewone persoonsgegevens

Alle overige persoonsgegevens die niet kwalificeren als bijzonder of strafrechtelijk zijn gewone persoonsgegevens. Gewone persoonsgegevens wil overigens niet zeggen dat geen sprake kan zijn van een hoog privacyrisico of dat de wetgever geen aanvullende vereisten aan de verwerking daarvan heeft gesteld. Zulks is namelijk het geval bij wettelijk voorgeschreven persoonsidentificerende nummers en bij persoonsgegevens die de AP als 'anderszins gevoelig' aanmerkt.

➢ *Persoonsidentificerende nummers*

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), BIG-nummer (beroepen in de individuele gezondheidszorg), A-nummer (basisregistratie personen), onderwijsnummer,

strafrechtketennummer en kenteken. Het gaat hierbij enkel om in de wet voorgeschreven persoonsidentificerende nummers.

➢ ***Anderszins gevoelige persoonsgegevens:***

De AP heeft in de richtsnoeren beveiliging van persoonsgegevens (Stcrt. 2013, nr. 5174, p. 14) bepaalde persoonsgegevens aangemerkt als 'anderszins gevoelige persoonsgegevens', omdat de gevolgen bij onrechtmatige verwerking van deze persoonsgegevens ernstiger kunnen zijn dan bij andere gewone persoonsgegevens. Dit is geen apart type gegevens in de AVG, anders dan de bijzondere en strafrechtelijke persoonsgegevens. Het gaat om de volgende persoonsgegevens:

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

➢ ***Betrokkenen: personen waarop de gegevens betrekking hebben***

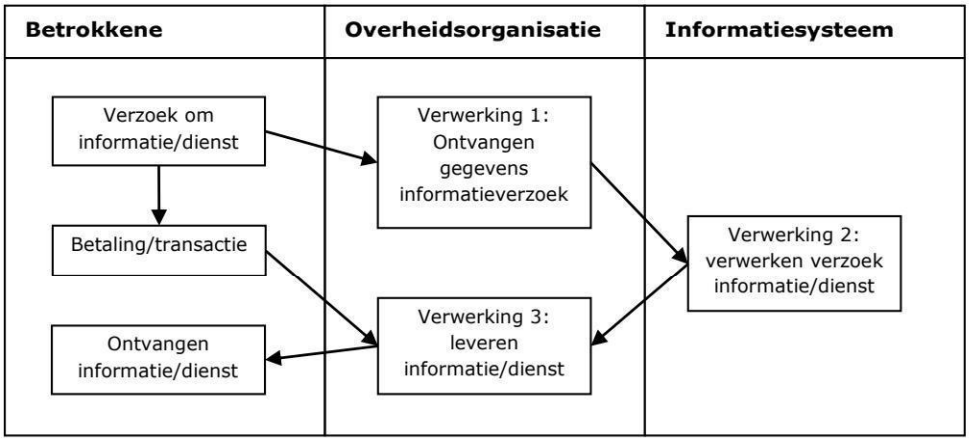
Benoem tot slot de categorieën van betrokkenen: dat zijn degenen op wie de persoonsgegevens betrekking hebben. Denk hierbij aan: medewerkers, consumenten, cliënten, patiënten, zakelijke contacten, bezoekers, gebruikers of ingezetene van een gemeente. De omvang en soort betrokkene heeft invloed op de privacyrisico's. Bepaalde betrokkenen zijn kwetsbaarder dan anderen. Met kwetsbaar wordt bedoeld dat de negatieve gevolgen van een onrechtmatige gegevensverwerking groter kunnen zijn voor bepaalde betrokkene 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.

3. Gegevensverwerkingen

Geef alle voorgenomen gegevensverwerkingen weer.

Om de rechtmatigheid van de voorgenomen gegevensverwerkingen te kunnen beoordelen, is het noodzakelijk om alle gegevensverwerkingen in beeld te hebben. Onder verwerking wordt verstaan: elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens (artikel 4, tweede onderdeel, AVG). Denk hierbij aan: het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens. Met andere woorden, het begrip omvat het gehele proces dat een persoonsgegeven doormaakt, vanaf het moment van verzamelen tot het moment van vernietigen.

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



➢ *Herkomst*

Tevens is het noodzakelijk om de herkomst van persoonsgegevens te herleiden. De AVG geeft namelijk als beginsel dat persoonsgegevens niet verder mogen worden verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen (artikel 5, eerste lid, onder b, AVG). 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 14 hieronder). Met verdere verwerking wordt gedoeld op gebruik van persoonsgegevens die al eerder voor een bepaalde doel zijn verzameld. Denk hierbij aan verstrekkingen van persoonsgegevens aan een andere organisatie die niet oorspronkelijk was beoogd.

4. Verwerkingsdoeleinden

Beschrijf de hoofd- en nevendoeleinden van de voorgenomen gegevensverwerkingen.

De AVG geeft als beginsel dat persoonsgegevens enkel voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden mogen worden verzameld (artikel 5, eerste lid, onder b, AVG). 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 privacyrisico's (onder C) te voorkomen of verkleinen (onder D). Omschrijf per voorgenomen gegevensverwerking de verwerkingsdoeleinden zo specifiek mogelijk.

Bij verwerkingsdoeleinden kan gedacht worden aan: beveiliging, behandeling van personeelszaken, opsporing, direct marketing, het innen van vorderingen, het doen van leveringen en bestellingen, identificatie, het voorbereiden en nemen van Awb-besluiten en het behandelen van geschillen. Denk ook aan eventuele nevendoeleinden van de gegevensverwerking, zoals: wetenschappelijk, statistisch of historisch onderzoek, archiefbeheer, declaratiedoeleinden, rapportagedoeleinden, verbetering van dienstverlening of (door)ontwikkeling van beleid. De verwerkingsdoeleinden moeten zoveel mogelijk worden toegespitst op de concrete gegevensverwerking, 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.

Bij conceptregelgeving wordt het doel van de gegevensverwerking in de regeling zelf vastgelegd (wet, algemene maatregel van bestuur of ministeriële regeling) of op zijn minst benoemd in de memorie of nota

van toelichting (artikel 6, derde lid, AVG). Een wettelijke doelomschrijving bevordert de rechtszekerheid omdat hierdoor een nadere invulling is gegeven aan het beoordelingskader.

Bij overheidsverwerkingen (IT/uitvoering) stelt de verwerkingsverantwoordelijke het doel van de gegevensverwerkingen zelf vast. Bij overheidsverwerkingen ter uitvoering van wet- en regelgeving moet binnen het doel worden gebleven dat daarin is vastgesteld.

5. Betrokken partijen

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

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 (artikel 4, zevende onderdeel, AVG). 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 verwerkingsverantwoordelijken (artikel 26, eerste lid, AVG).

Verwerker is de natuurlijke persoon, de rechtspersoon of het overheidsorgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt (artikel 4, achtste onderdeel, AVG). 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 instelling.

Ontvanger is de natuurlijke persoon, de rechtspersoon of het overheidsorgaan aan wie/waaraan de persoonsgegevens worden verstrekt (artikel 4, negende onderdeel, AVG). Verstrekker is de natuurlijke persoon, de rechtspersoon of het overheidsorgaan van wie/waarvan de persoonsgegevens worden ontvangen.

Bij conceptregelgeving kan het wenselijk zijn om daarin de hoedanigheid van de betrokken organisaties vast te leggen. Bijvoorbeeld: indien een specifieke regeling wordt opgesteld ten behoeve van een publiekrechtelijke taak, dient 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 wettelijke 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 (IT/uitvoering) 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 hoedanig de persoonsgegevens verwerkt. Tevens zal moeten worden bepaalde, voor zover eveneens niet wettelijk voorgeschreven, welke functionarissen binnen deze organisaties toegang krijgen tot welke persoonsgegevens, bijvoorbeeld aan de hand van een autorisatiematrix. Hierin kan tevens worden bepaald in welke gevallen en onder welke voorwaarden deze functionarissen toegang krijgen.

6. Belangen bij de gegevensverwerking

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

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. Denk hierbij bijvoorbeeld aan: bedrijfs- en commerciële belangen, zoals meer gepersonaliseerde dienstverlening, 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 gegevensverwerking werkt door in de toets van de noodzaak (zie punten 11 en 13 hierna).

7. Verwerkingslocaties

Benoem in welke landen de voorgenomen gegevensverwerkingen plaatsvinden.

De locaties waar de voorgenomen gegevensverwerkingen plaatsvinden, kunnen aanvullende privacyrisico's met zich brengen en daarom onderworpen zijn aan strengere regels of extra maatregelen vereisen. Tevens heeft de verwerkingslocatie invloed op de competentie van de (leidende) toezichthoudende autoriteit (artikel 55 en 56 AVG).

Om te borgen dat de regels betreffende de bescherming van de persoonlijke levenssfeer niet omzeild worden door persoonsgegevens in een ander land te verwerken, bepaalt de AVG dat gegevensverwerkingen buiten de Europees Economische Ruimte (EU, Liechtenstein, Noorwegen en IJsland) enkel onder bepaalde omstandigheden zijn toegestaan (artikel 44 AVG). Dit is bijvoorbeeld het geval indien het derde land naar het oordeel van de Europese Commissie een passend beschermingsniveau heeft (een adequaatheidsbesluit, artikel 45 AVG) of indien gebruik wordt gemaakt van passende waarborgen om de betrokkene te beschermen (artikel 46 AVG). Daarnaast geeft de AVG een aantal specifieke situaties waarin gegevensverwerkingen in een derde land toch zijn toegestaan ondanks het ontbreken van een passend beschermingsniveau en passende waarborgen, zoals uitdrukkelijke toestemming van de betrokkene (artikel 49 AVG).

Naast de AVG kunnen andere wettelijke regels of beleid invloed hebben op de locaties waar persoonsgegevens kunnen worden verwerkt. Denk hierbij aan het VIRBI 2013 inzake gerubriceerde overheidsinformatie en situaties waarin opslag in een overheidsdatacenter geëigend is.

De GEB is niet specifiek bedoeld om te toetsen of de doorgifte is toegestaan op grond van de AVG of richtlijn, maar om de privacyrisico's in kaart te brengen. Indien het beschermingsniveau in een ander land minder hoog is dan in de Europese landen, zullen de privacyrisico's waarschijnlijk groter zijn.

8. Techniek van gegevensverwerking: geautomatiseerde besluitvorming, profilering en big data

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

Gebruikmaking van bepaalde technieken van gegevensverwerking kunnen aanvullende privacyrisico's met zich brengen en daarom onderworpen zijn aan strengere regels of extra maatregelen vereisen. Zulks is onder meer het geval bij geautomatiseerde besluitvorming, profilering en big data.

a. Geautomatiseerde besluitvorming

De betrokkene heeft het recht niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking, waaronder profilering, gebaseerd besluit waaraan voor hem rechtsgevolgen zijn verbonden of dat hem anderszins in aanmerkelijke mate treft (artikel 22, eerste lid, AVG). Dit verbod is enkel niet van toepassing indien het besluit:

1. noodzakelijk is voor de totstandkoming of de uitvoering van een overeenkomst tussen de betrokkene en een verwerkingsverantwoordelijke;
2. 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
3. berust op de uitdrukkelijke toestemming van de betrokkene (artikel 22, tweede lid, AVG).

b. 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 (artikel 4, vierde onderdeel, AVG).

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.

Voorbeelden profilering

Het bouwen van dure en ingewikkelde systemen is geen voorwaarde voor het inzetten van profilering. 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 bij de grens;
- gebruik wordt gemaakt van de gegevens die websitebezoekers achterlaten om de doelgroep van de website mee vast te stellen.

c. Big Data

Big Data is als zodanig niet gedefinieerd in de AVG, 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 (Wetenschappelijk Raad voor het Regeringsbeleid, rapport nr. 95, p. 21 en 35). Toepassing van Big Data brengt specifieke risico's mee en vergt daarom ook specifieke maatregelen (zie onder D).

9. Juridisch en beleidsmatig kader

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

Naast of in de plaats van de AVG en de Richtlijn kan (sectorale) wet- en regelgeving de mogelijkheden voor gegevensverwerkingen creëren, conditioneren of beperken. Voorbeelden van dergelijke wetten zijn: Wet algemene bepalingen burgerservicenummer, Wet gebruik burgerservicenummer in de zorg, Wet basisregistratie personen, Archiefwet, Telecommunicatiewet, Kadasterwet, Handelsregisterwet, Kieswet, Wet bijzondere maatregelen grootstedelijke problematiek, Wet op de geneeskundige behandelovereenkomst, Wet op de Jeugdzorg, Wet maatschappelijke ondersteuning, Participatiewet, Politiewet 2012, Wet justitiële en strafvorderlijke gegevens.

Er kan ook departementaal of rijksbreed beleid zijn die de mogelijkheden voor de voorgenomen gegevensverwerkingen conditioneert of beperkt. Bijvoorbeeld ten aanzien van de opslag en beveiliging van persoonsgegevens.

Aan de hand van deze inventarisatie kan bij onderdeel B beoordeeld worden of de voorgenomen gegevensverwerkingen rechtmatig zijn en bij onderdeel D of specifieke maatregelen voorgeschreven zijn.

10. Bewaartermijnen

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

De AVG 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 doeleinden waarvoor zij worden verwerkt, noodzakelijk is (artikel 5, eerste lid, onder e, AVG). Op dit beginsel van opslagbeperking maakt de AVG een uitzondering indien de persoonsgegevens uitsluitend worden verwerkt ten behoeve van archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden. Hieraan stelt artikel 89 wel de eis dat passende maatregelen worden getroffen om de betrokkenen te beschermen.

Bij conceptregelgeving zal moeten bepaald en gemotiveerd of het al dan niet wenselijk is om bij 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 (IT/uitvoering) moet worden nagegaan of wet- en regelgeving een bewaartermijn voorschrijven. Indien zulks het geval is, moet de verwerkingsverantwoordelijke zich aan die termijn houden. Indien geen wettelijke bewaartermijn is voorgeschreven, moet de verwerkingsverantwoordelijke zelf een bewaartermijn vaststellen. Uitgangspunt is: indien het voor de verwezenlijking van de verwerkingsdoeleinden niet meer noodzakelijk is de persoonsgegevens te bewaren, moeten deze worden verwijderd of geanonimiseerd (zodanig dat de betrokkene niet meer identificeerbaar is).

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

Categorie Persoons-gegeven	Ingang bewaartermijn	Termijn van bewaring	Motivatie bewaring	Verantwoordelijkheid 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

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 grondslag, noodzaak en doelbinding van de gegevensverwerkingen. Voor dit onderdeel van de GEB is in het bijzonder juridische expertise nodig.

1. Grondslag

Bepaal op welke grondslagen de gegevensverwerkingen worden gebaseerd.

De AVG geeft als beginsel dat persoonsgegevens moeten worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is (artikel 5, eerste lid, onder a, AVG). Dit beginsel van rechtmatigheid is uitgewerkt in artikel 6, eerste lid, AVG. Hierin is geregeld dat een gegevensverwerking alleen rechtmatig is indien deze gebaseerd kan worden op ten minste één van de volgende zes grondslagen:

1. de betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden;
2. 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;

3. de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust;
4. de verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen;
5. 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;
6. 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.

Een conceptregelgeving zal veelal tot gevolg hebben dat de verwerkingsverantwoordelijke de gegevensverwerking kan baseren op de grondslag genoemd onder c (wettelijke verplichting). Zulks zal het geval zijn 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 het tot gevolg hebben dat een bestuursorgaan de gegevensverwerking kan baseren op de grondslag genoemd onder e (publieke taak). De publieke taak wordt wettelijke vastgelegd. En voor de goede vervulling daarvan zal het noodzakelijk zijn om persoonsgegevens te verwerken. In een wetsvoorstel kan ook worden voorgeschreven dat toestemming van de betrokkene vereist is om persoonsgegevens te verwerken, en daarmee de andere grondslagen uitsluiten.

Bij overheidsverwerkingen (IT/uitvoering) zal het bestuursorgaan de voorgenomen gegevensverwerkingen moeten baseren op één van de zes grondslagen. De grondslag genoemd onder f geldt niet voor gegevensverwerkingen in het kader van de uitoefening van publieke taken. In veel situaties zal de grondslag genoemd onder a (toestemming) evenmin kunnen dienen als grondslag voor gegevensverwerkingen door bestuursorganen, omdat de betrokkene in de gegeven situatie niet vrijelijk toestemming kan geven (artikel 4, elfde onderdeel, AVG). Indien de gegevensverwerking gebaseerd wordt op de grondslag 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 wegens dan de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of de derde.

11. Bijzondere en strafrechtelijke persoonsgegevens

Indien bijzondere of strafrechtelijke persoonsgegevens worden verwerkt, bepaal of één van de wettelijke uitzonderingen op het verwerkingsverbod van toepassing is op de voorgenomen gegevensverwerkingen.

De AVG verbiedt de verwerking van bijzondere persoonsgegevens, tenzij de wet in een uitzondering op dit verbod (artikel 9, eerste lid, AVG; zie voor definitie van bijzondere persoonsgegevens de toelichting bij punt 2). Deze uitzonderingen zijn te vinden in de overige leden van artikel 9 AVG, alsook in de Uitvoeringswet Algemene verordening gegevensbescherming en in sectorale wet- en 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 (artikel 10 AVG; zie voor de definitie van strafrechtelijke gegevens de toelichting bij punt 2). De Uitvoeringswet Algemene verordening gegevensbescherming regelt een aantal gevallen waarin dit is toegestaan.

12. 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.

De AVG 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 (artikel 5, eerste lid, onder b, AVG). Dit beginsel van doelbinding is uitgewerkt in artikel 6, vierde lid, AVG. Hierin is geregeld dat de verdere verwerking in ieder geval verenigbaar is indien de verdere verwerking berust op toestemming van de betrokkene of op een specifiek wettelijk voorschrift. Tevens acht de wetgever de verdere verwerking ten behoeve van archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden als verenigbaar met de oorspronkelijke doeleinden. Hieraan stelt artikel 89 AVG wel de eis dat passende maatregelen worden getroffen om de betrokkene te beschermen.

In alle andere gevallen moet de verwerkingsverantwoordelijke zelf beoordelen of de verdere verwerking 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. het kader 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 of bijzondere categorieën van persoonsgegevens worden verwerkt of persoonsgegevens over strafrechtelijke veroordelingen en strafbare feiten worden verwerkt;
d. de mogelijke gevolgen van de voorgenomen verdere verwerking voor de betrokkene;
e. het bestaan van passende waarborgen, waaronder eventueel versleuteling of pseudonimisering.

Bij conceptregelgeving moet worden beoordeeld of het noodzakelijk is om wettelijk te regelen dat verdere verwerking toegestaan is (zie punt 14 hierna).

Bij overheidsverwerkingen (IT/uitvoering) moet de verwerkingsverantwoordelijke aan de hand van het bovenstaande beoordelen of de verdere gegevensverwerking verenigbaar is.

13. Noodzaak en evenredigheid

Beoordeel of de voorgenomen gegevensverwerkingen noodzakelijk zijn voor het verwezenlijken van de nagestreefde doeleinden. Ga hierbij in ieder geval in op:
a. Proportionaliteit: staat de inbreuk op de persoonlijke levenssfeer van betrokkenen in evenredige verhouding tot de met de gegevensverwerkingen nagestreefde doelen?
b. Subsidiariteit: kunnen de verwerkingsdoeleinden niet op een andere, voor de betrokkene minder nadelige wijze, worden verwezenlijkt?

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

Bij proportionaliteit wordt gewogen of de realisatie van de verwerkingsdoeleinden zodanig gewicht hebben dat de gegevensverwerkingen, gelet op de mate waarin deze de privacy beperken, deze rechtvaardigen? (zijn de beperkingen van het grondrecht en het doel dat ermee wordt beoogd met elkaar in balans?) 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?) Bij deze afwegingen worden de doelen, belangen en feiten zoals in beeld gebracht onder A betrokken.

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

C. Beschrijving en beoordeling risico's voor de rechten en vrijheden betrokkene

Beschrijf en beoordeel de risico's van de voorgenomen gegevensverwerkingen voor de rechten en vrijheden van betrokkene. Houd hierbij rekening met de aard, omvang, context en doelen van de gegevensverwerking zoals in onderdeel A en B van de GEB Rijksdienst zijn bepaald, geïdentificeerd en beoordeeld. Het gaat hierbij niet om de risico's van de verwerkingsverantwoordelijke zelf.

2. Risico's

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

Houd bij elk aspect rekening met de aard, omvang, context en doelen van de gegevensverwerking.

Volgens de AVG dient een GEB een beoordeling van risico's voor de rechten en vrijheden van betrokkenen te bevatten (artikel 35, zevende lid, aanhef en onder c, AVG). 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 betrokkene te worden bepaald, zodat op basis van een objectieve beoordeling vastgesteld kan worden of de gegevensverwerking gepaard gaat met een (hoog) risico (overweging 76 AVG). Hiervoor is het nodig om de oorsprong, de aard, het specifieke karakter en de ernst van dat risico te evalueren (overweging 84 AVG).

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 de risicoafweging in het kader van informatiebeveiliging, waartoe artikel 4, aanhef en onder a, van het Besluit voorschrift informatiebeveiliging rijksdienst 2007 (VIR) verplicht. Derhalve zal ook gebruik gemaakt kunnen worden van informatie die daaruit naar voren is gekomen. Anders dan bij deze risicoafweging in de VIR 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 etc.), ziet de risicoafweging in het kader van de GEB specifiek op de risico's voor de betrokkene.

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

Risico's identificeren

De eerste stap is om potentiële privacyrisico's vast te stellen. Een privacyrisico is een (hypothetische) situatie waarin persoonsgegevens (onrechtmatig) verwerkt worden met gevolgen voor de rechten en vrijheden van de betrokkene.

Bij (onrechtmatige) verwerking van persoonsgegevens kan gedacht worden aan het al dan niet opzettelijke:

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

van persoonsgegevens (overweging 83 AVG), of anderszins handelen in strijd met het recht.

Bij rechten en vrijheden van betrokkene 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 natuurlijke personen (overwegingen 75 en 83 AVG). Hierbij kan gedacht worden aan:

- verlies van controle over hun persoonsgegevens of de beperking/schending van hun rechten;
- discriminatie, stigmatisering en uitsluiting;
- (blootstelling aan) identiteitsdiefstal of –fraude;
- gezondheidsschade;
- financiële verliezen;
- ongeoorloofde ongedaanmaking van pseudonimisering;
- reputatie- of anderszins relationele schade;
- verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens; of
- enig ander aanzienlijk economisch of maatschappelijk nadeel voor de natuurlijke persoon in kwestie (overwegingen 75 en 85 AVG).

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 betrokkene. Met andere woorden: wat zijn de gevreesde gevolgen en wat is de impact daarvan op betrokkene? En hoe treden deze in werking en hoe waarschijnlijk is dat? Aan de hand van deze vragen 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 het 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.

Risico's beoordelen
Definieer aanvaardbare risicowaarden en beoordeeld of de risico's aanvaardbaar zijn.

D. Beschrijving voorgenomen maatregelen

In onderdeel D wordt bezien welke maatregelen kunnen worden getroffen om de erkende privacyrisico's in onderdeel C te voorkomen of te verminderen. Welke maatregelen in redelijkheid worden getroffen is een belangenafweging van de wetgever of verwerkingsverantwoordelijke. Voor dit onderdeel van de GEB is in het bijzonder expertise over informatiebeveiliging belangrijk.

14. Maatregelen

Beoordeel welke technische, organisatorische en juridische maatregelen in redelijkheid kunnen worden getroffen om de hiervoor beschreven privacyrisico'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.

De AVG 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 (artikel 5, eerste lid, aanhef en onder f, AVG). Dit beginsel van integriteit en vertrouwelijkheid is nader uitgewerkt in artikel 32 AVG.

Dit artikel schrijft voor dat de verwerkingsverantwoordelijk passende technische en organisatorische maatregelen moet 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 aller zwaarste beveiliging te nemen. De AVG vereist enkel dat maatregelen met het oog op de beschikbare technologie en uitvoeringskosten redelijk zijn (overwegingen 83 en 94 AVG). Deze maatregelen moeten het risico tot een aanvaardbaar niveau brengen. Privacyrisico'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 deze aanvaardbaar wordt geacht.

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

De AVG noemt ter illustratie 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:

- 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 toegekend bevoegdheden
- privacybewustzijn- en beveiligingstrainingen
- managementrapportages over risicobeheer
- beperken inzageniveau
- periodiek een audit, hack of penetratietest uitvoeren
- richtlijnen inzake gebruik ICT-hulpmiddelen, zoals versleutelde USB-sticks en beveiligde opslagplekken
- responsible disclosurebeleid
- geheimhoudingsverklaringen
- service level argreements (met boeteclausules)
- verwerkersovereenkomsten
- screening personeel en VOG-verklaring

Bij conceptregelgeving: ook op het niveau van wet- en 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 toepassing van Big Data (zie punt 10) 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 (*Kamerstukken II* 2016/17, 26 643, nr. 426, p. 7-10):

- 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 er nuttige informatie aan betrokkenen kan worden verschaft over de gebruikte logica achter de analyse en dat voor toezicht en rechterlijke toetsing voldoende inzicht kan worden gegevens in gebruikte algoritmen en analysemethoden.

GEGEVENSBESCHERMINGSEFFECTBEOORDELING RIJKSDIENST

OB Blauwdruk

Dit template is gebaseerd op "***Model Gegevensbeschermingseffectbeoordeling Rijksdienst***"; versie 0.2 voorportalen CIO-beraad, IOWJZ, ICBR; 24 Juli 2017.

Onderwerp van deze GEB

Inhoud

I. INLEIDING

Het model bestaat uit 17 punten verspreid over vier onderdelen. Onderdeel A behandelt de feiten van de voorgenomen gegevensverwerkingen. De beoordeling van de feiten aan het juridische kader komt aan de orde in onderdeel B. Onderdeel C gaat over risico's voor de rechten en vrijheden van betrokkenen en onderdeel D gaat over de beoogde maatregelen om die risico's aan te pakken. Deze opzet is ontleend aan de privacyregelgeving[1]. Het maken van een GEB is een dynamisch proces. Denkbaar is dat antwoorden in onderdeel A (moeten) worden aangepast nadat een beoordeling (onder B) is verricht en de risico's (onder C) en maatregelen (onder D) in kaart zijn gebracht.

De beantwoording van de 17 punten in dit model kan meer of minder gedetailleerd zijn afhankelijk van de aard en omvang van de voorgenomen regelgeving of verwerkingen door de overheid. Wel is het in alle gevallen noodzakelijk om alle punten van het model na te gaan en de gemaakte afweging per punt op te schrijven.

[1] Artikel 35, zevende lid, AVG en artikel 27, tweede lid, Richtlijn.