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

Certificaathouders (CN) analyse IH

Dit template is gebaseerd op "***Model Gegevensbeschermingseffectbeoordeling Rijksdienst***"; versie 0.2 voorportalen CIO-beraad, IOWJZ, ICBR; 24 Ju[illegible]17.

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 met behulp van een PKI-overheidscertificaat. Op deze wijze maken we inzichtelijk welke certificaathouder opvallende patronen heeft in de reeks aangiften die van deze certificaathouder afkomstig is. 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 en** de **SBR-rapportages van Logius**. **Velden**: Naam Certificaathouder 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, ordenen, structureren, opvragen, raadplegen, gebruiken. Verstrekken dmv 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 door een bepaalde certificaathouder. We vergelijken deze patronen met het algemene beeld van de hele doelgroep en de certificaathouder die sterk afwijken van het gemiddelde komen daarmee in beeld. Afhankelijk van de mate waarin de certificaathouder van het gemiddelde afwijkt dan wel het aantal keren dat deze certificaathouder 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 betrokkenen 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 zijn opgeslagen 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 certificaathouder 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 gebruik. 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.

b. 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.

c. 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***

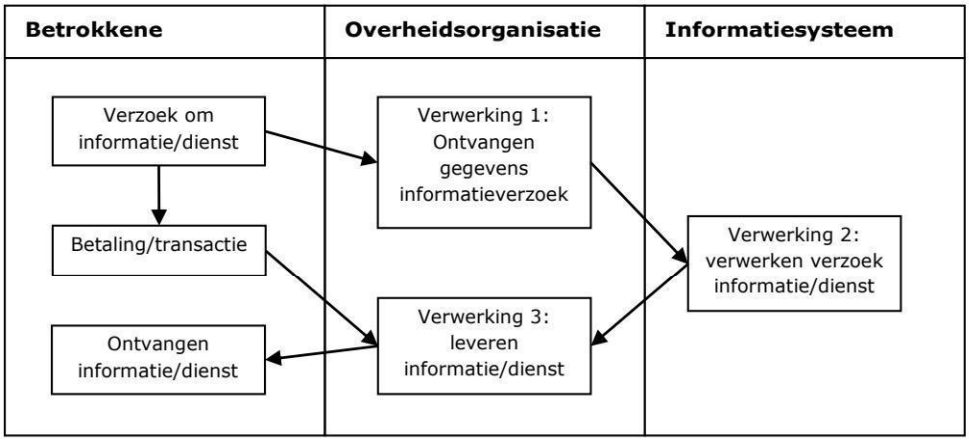
Benoem tot slot de categorieën van betrokkenen: dat zijn degenen op wie de persoonsgegevens betrekking hebben. Denk hierbij aan: medewerkers, consumenten, cliënten, patiënten, zakelijke contacten, bezoekers, gebruikers of ingezetene van een gemeente. De omvang en soort betrokkene heeft invloed op de 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.

Anti Fraude

Gegegevensbeschermingseffectbeoordeling Rijksdienst

De beantwoording van de 14 punten in dit model kan meer of minder gedetailleerd zijn afhankelijk van het niveau van wetgeving (wet in formele zin, AMvB, of ministeriële regeling), of als sprake is van een GEB voor overheidsverwerkingen. Wel is het in alle gevallen noodzakelijk om alle punten na te gaan en de gemaakte afweging per punt op te schrijven.

Deze GEB/PIA dient door de verwerkingsverantwoordelijke ingevuld te worden. Wie is dat? Toeslagen?
De antwoorden in dit document zijn gebaseerd obv 'de PIA van Surf' en een document van het SOC. De rode teksten zijn vragen die nog beantwoord moeten worden om meer scherpte en duidelijkheid te krijgen.

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 GEB op ziet op hoofdlijnen en baken dit af.	Antwoord: De PIA heeft betrekking op: 1. **Anti-fraude monitoring**. Vanuit het hoger management van de Belastingdienst (KPD) is mondeling opdracht gegeven het gebruik van de OLDV-portalen (Mijn Belastingdienst, Mijn toeslagen, Voor ondernemers) en SBR/BAPI te monitoren en analyses uit te voeren op de data. Met als doel afwijkend gedrag op de portalen voortijdig te detecteren. Alle acties (elke muisklik) worden opgeslagen en 'afwijkend gedrag' wordt gezien als gedrag waar niet direct een logische verklaring voor te geven is. Het BSN en/of IP met dit gedrag wordt verder geanalyseerd. Zo kan de Belastingdienst, indien nodig, sneller optreden, nog voordat er tot uitbetaling wordt overgegaan.

		Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ("de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of	**Categorie:** Gewoon/bijzonder/strafrechtelijk	**Op wie betrekking** - eigen personeel of - belastingplichtige

		indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon		
2.	**Persoonsgegevens** Som alle persoonsgegevens op die worden verwerkt. Deel deze persoonsgegevens in onder de categorieën: gewoon, bijzonder of strafrechtelijk. Geef per persoonsgegeven tevens aan op wie die betrekking hebben	Antwoord: https://mijn.toeslagen.nl 1. IP-adres 2. URL 3. HTTP methode 4. User agent[1] 5. Timestamp (datum + tijd) 6. Burger Service Nummer (BSN) 7. Gemachtigde https://mijn.belastingdienst.nl 1. Timestamp (datum + tijd) 2. IP-adres 3. Aantal informatieve kenmerken omtrent het bezoek (wat doet de gebruiker), zoals; a. Dienstcode b. Berichtsoort c. Actie van gebruiker d. Resultaat van actie e. Belastingjaar f. Regeling 4. BSN, natuurlijk persoon	Antwoord: 1. Gewoon 2. Nvt 3. Nvt 4. Nvt 5. Nvt 6. Gewoon 7. Gewoon *In samenhang kunnen de "nvt"-gegevens ook persoonsgegevens zijn!* 1. Nvt 2. Gewoon 3. Nvt 4. Gewoon	Antwoord: Deze persoonsgegevens hebben betrekking op de Belastingplichtige

[1] De user agent bevat informatie over de gebruikte browser, het besturingssysteem en type apparaat

		https://mijn.belastingdienst.nl/ppa/ 1. Timestamp (datum + tijd) 2. IP-adres 3. HTTP methode 4. URL 5. URL referer 6. User agent 7. BSN 8. Beconnummer, beconsofi 9. KvK nummer 10. Gegevens van het PKI-certificaat (aanvrager, plaats etc.) 11. Algemene informatie omtrent bezoek, o.a. berichtsoort (bijv. OB, Aangifte_LH), status, retourbericht BRP (Basisregistratie Personen) 1. Geboortedatum 2. Overlijdensdatum 3. Woonadres 4. Correspondentie adres 5. Eerste nationaliteit 6. Tweede nationaliteit[2] 7. Aantal BSNs ingeschreven op adres FSV (Fraude Signalering Voorziening)[3] 1. BSN 2. Partner BSN 3. Middel 4. Belastingjaar 5. Bron van detectie 6. IP-adres	1. Nvt 2. Gewoon 3. Nvt 4. Nvt 5. Nvt 6. Nvt 7. Gewoon 8. Gewoon 9. Gewoon 10. Gewoon 11. Gewoon Afkomstig uit RAM, bron is EHI 1 t/m 6: Gewoon	

[2] wordt niet meer bijgewerkt, laatst bekende wordt nog gebruikt maar dit wordt steeds minder waardevol naarmate het ouder wordt

[3] BSNs die fraude in het verleden hebben gepleegd worden bijgehouden in een administratie (FSV). Gegevens van de FSV worden gekoppeld aan het BSN.

		7. Soort fraude
		8. Rol van subject
		9. Sofinummer
		10. Sofinummer_p (NNP of sofinr)
		
		SBR (Standard Business Reporting)[4]
		1. Timestamp (datum + tijd)
		2. Belanghebbende
		3. BSN
		4. Beconnummer
		5. Beconsofi
		6. KvK nummer
		7. Gegevens van het PKI-certificaat (aanvrager, plaats etc.)
		8. Verschillende kenmerken van het verstuurde bericht (soort belasting, status, retourbericht, timestamp en status retourbericht)
		
		Elke maand wordt er door SAF een lijst met IP-BSN-telefoonnummer samengesteld uit een IP-BSN-lijst en een BSN-tel-lijst, en opgestuurd naar EHI.
		
		Externe bronnen
		Tevens worden bepaalde elementen verrijkt met open bronnen die te benaderen zijn via het internet.
		• Verrijking van het IP-adres
		  • WHOIS informatie
		  • Maxmind GeoIP informatie (betaalde versie)
		  • Hostnaam informatie
		  • TOR exit nodes
			Dit zijn Toezicht gegevens van (mogelijke) fraude gevallen. Mogelijk raakt dit opsporing (FIOD); sfeerovergang.
			
			1. Nvt
			2. Gewoon
			3. Gewoon
			4. Gewoon
			5. Gewoon
			6. Gewoon
			7. ?
			8. Nvt
			
			IP-adressen worden verrijkt met	

[4] SBR is een methode voor het samenstellen en aanleveren van financiële berichten. Veelal financiële dienstverleners maken gebruik van SBR om wijzigingen door te geven bij de Belastingdienst.

		• Emerging Threats IP List **OB-blauwdruk** In 2016 is, op verzoek van het Combiteam Aanpak Facilitators (CAF), begonnen met een OB-blauwdruk als apart project. De financiële OB-data (alle data van een aangifte: o.a. OB-nummer, bedrijf, branche, opgegeven bedragen) wordt ook opgeslagen in HeidiSQL. Het betreft persoonsgegevens van natuurlijke personen met name éénmanszaken (incl. ZZP-ers) **Vastgoed** In 2016 is, op verzoek van MKB, begonnen met een project over vastgoedtransacties. De data bevat alle gegevens (o.a. BSN's, financiële data) van vastgoedtransacties.	geografische locatie, mobiel netwerk of niet, hostnaam (meestal Internet Service Provider) om de IP-informatie waardevoller te maken voor de klanten. Hier is geen specifieke opdracht voor gegeven. Hiermee kan o.a. worden gekeken of de locatie in de buurt is van de adressen van de BSN's. Is CAF bevoegd? Volgt, er wordt een opdracht geformuleerd. De (schriftelijke) opdracht dient afgegeven te worden door de Directeur van het Dienstonderdeel. Is MKB bevoegd? Deze opdracht is gestopt en aantoonbaar verwijderd.	

		"**verwerking**": een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals 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	
3.	**Gegevensverwerkingen** Geef alle voorgenomen gegevensverwerkingen weer.	Antwoord:	Ja/Nee
		Verzamelen / Vastleggen / Opslaan	Ja
		Ordenen / Structureren	Ja
		Bijwerken of wijzigen	Ja
		Opvragen / Raadplegen / Gebruiken	Ja
		Verstrekken dmv doorzending / Verspreiden	Ja, intern Belastingdienst
		Combineren	Ja
		Afschermen	Ja, alleen bevoegde medewerkers kunnen bij de gegevens in HeidiSQL
		Wissen of vernietigen	Nee

		Hoofddoeleinden	**Nevendoeleinden**
4.	**Verwerkingsdoeleinden** Beschrijf de hoofd- en nevendoeleinden van de gegevensverwerkingen.	Antwoord: **Anti-fraude monitoring**: voorkomen van onterechte uitbetalingen (Toeslagen) door voortijdig afwijkend gedrag op de portalen te detecteren. **OB Blauwdruk**: d.m.v. data-analyse opsporen van opmerkelijkheden in de OB-aangiften.	Antwoord: Achteraf de activiteiten van verdachte BSN's, IP-adressen op de portalen in kaart brengen, als deze BSN's en IP-adressen via andere wegen zijn opgevallen.

		Betrokken organisaties	**Categorie:** verwerkingsverantwoordelijke, verwerker of ontvanger	**Soort verwerkingen:** verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, combineren, afschermen, wissen of vernietigen

5a.	**Betrokken partijen** Benoem welke organisaties betrokken zijn bij welke gegevensverwerkingen. Deel deze organisaties per gegevensverwerking in onder de categorieën: verwerkingsverantwoordelijke, verwerker en ontvanger.	Antwoord:	Antwoord:	Antwoord:
		Belastingdienst	Verwerkingsverantwoordelijke	
		Persoonsgegevens	Verwerkingsverantwoordelijke	
		SOC Anti Fraude	Interne Verwerker/beheerder	Verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken, combineren, afschermen, wissen of vernietigen
		Toeslagen	Ontvanger	Raadplegen, gebruiken, combineren
		EHI (Expertisecentrum Handhaving en Intelligence)	Ontvanger	Raadplegen, gebruiken, combineren
		FIOD	Ontvanger	Raadplegen, gebruiken, combineren
		CAF (Combiteam Aanpak Facilitators)	Verwerker	Raadplegen, gebruiken, combineren, bijwerken
		ID-Belastingdienst (Inlichtingendienst Belastingdienst)	Interne Ontvanger	Raadplegen, gebruiken, combineren

		Betrokken organisaties	**Betrokken functionarissen per organisatie**	**Persoonsgegevens waartoe hij/zij toegang heeft**
5b.	**Betrokken functionarissen** Benoem tevens welke functionarissen binnen deze organisaties toegang krijgen tot welke persoonsgegevens.	Antwoord:	Antwoord:	Antwoord:
		SOC Anti Fraude	Analisten SOC Anti Fraude	Alle onder vraag 2 genoemde gegevens
		Overige onder 5a genoemde partijen (Toeslagen, EHI, FIOD, CAF en ID-Belastingdienst)	Analisten (deze hebben een persoonlijk account binnen Heidi SQL)	Alle onder vraag 2 genoemde gegevens

		Betrokken organisaties Naam organisatie + Categorie (verwerkingsverantwoordelijke, verwerker of ontvanger)	**Belangen bij de gegevensbewerking**
6.	**Belangen bij de gegevensverwerking** Beschrijf de belangen (lees: de waarde of de voordelen) die de verwerkingsverantwoordelijke of een derde heeft bij de gegevensverwerkingen.	1. SOC Anti Fraude	Verwerker/beheerder in opdracht van…
		2. Toeslagen	Mogelijke fraude signalen afgeven, voordat er tot uitbetaling wordt overgegaan
		3. EHI (Expertisecentrum Handhaving en Intelligence)	Mogelijke fraude signalen afgeven
		4. FIOD	Het in opdracht reconstrueren/ bewijsvoering van in het verleden plaatsgevonden (mogelijk) frauduleus gedrag gerelateerd aan IP en/of BSN-nummers in opdracht van FIOD en/of Toeslagen
		5. CAF (Combiteam Aanpak Facilitators)	Mogelijke fraude signalen afgeven
		6. ID-Belastingdienst (Inlichtingendienst Belastingdienst)	Mogelijke fraude signalen afgeven

		Betrokken organisaties	**Verwerkingslokatie:** Land waar de gegevensverwerking plaats vindt (Nederland, EU of derde landen)
7.	**Verwerkingslocaties** Benoem in welke landen de gegevensverwerkingen plaatsvinden.	Antwoord:	Antwoord:
		Zie vraag 5a	Alle in Nederland

		Toelichting:

		"**profilering**": 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
8a.	**Techniek van gegevensverwerking: geautomatiseerde besluitvorming, profilering en big data (grootschalige gegevensverwerking)** Beschrijf op welke wijze en met gebruikmaking van welke (technische) middelen de persoonsgegevens worden verwerkt.	Antwoord: De systemen en applicaties van de Belastingdienst sturen de loginformatie naar een centraal logmanagement systeem. De software die voor de het centrale logmanagement systeem wordt gebruikt is Splunk. Binnen Splunk wordt de data opgeslagen in indexen. Elke soort systeem/applicatie heeft zijn eigen index. Autorisaties worden per index toegekend. Waarbij de indexen die niet als vertrouwelijk worden aangemerkt voor elke Splunk gebruiker te benaderen zijn. Het SOC heeft een eigen index waarin vertrouwelijke data die alleen door het SOC mag worden ingezien wordt opgeslagen. Verder heeft het SOC een eigen search cluster. De zoekopdrachten (die ook persoonsgegevens kunnen bevatten) zijn zodoende niet door anderen in te zien.
8b.	Benoem of sprake is van geautomatiseerde besluitvorming, profilering of big data.	Antwoord: Er is geen sprake geautomatiseerde besluitvorming (selectie); op basis van business rules worden alerts verstuurd met BSN's en/of IP-adressen die het waard zijn extra bekeken te worden. Er worden geen beslissingen genomen o.b.v. deze business rules. Ja, er is sprake van profilering en big data.

9.	**Juridisch en beleidsmatig kader** Benoem de wet- en regelgeving, anders dan de AVG, en het beleid met mogelijke gevolgen voor de gegevensverwerkingen.	Antwoord: • Voorschrift Informatiebeveiliging Rijksoverheid • Voorschrift Informatiebeveiliging Rijksoverheid, Bijzondere informatie (VIR-BI) • Baseline Informatiebeveiliging Rijksoverheid, Technisch Normen Kader (BIR-TNK) • Handboek Beveiliging Belastingdienst (HBB) • ISO27001 / ISO27002 • AVR • Uitvoeringsbesluiten Toeslagen • Uitvoeringsbesluiten Douane

		Bewaartermijn	**Motivatie**

10.	**Bewaartermijnen** Bepaal en motiveer de bewaartermijnen van de persoonsgegevens aan de hand van de verwerkingsdoeleinden.	Antwoord: Logbestanden Splunk https://mijn.toeslagen.nl is 18 maanden. Logbestanden Splunk https://mijn.belastingdienst.nl is 18 maanden. Logbestanden Splunk https://mijn.belastingdienst.nl/ppa/ is 18 maanden.	Antwoord: Elke dag wordt vanuit Splunk de data van de dag daarvoor opgehaald en verwerkt in het eigen Anti-Fraude netwerk (o.a. Heidi SQL, een SQL-database). Op dit moment wordt binnen het Anti-Fraude netwerk alles bewaard en hebben we geen bewaartermijn. Gezien het feit dat er sinds 2013 wordt gelogd, is er sprake van circa 4 jaar aan data.

B. Beoordeling gegevensverwerkingen

Beoordeel de grondslag en de noodzaak van de voorgenomen gegevensverwerkingen. Indien sprake is van een verdere verwerking, beoordeel tevens of deze verenigbaar is met de doeleinden waarvoor de persoonsgegevens zijn verzameld.

11.	**Grondslag: noodzaak en evenredigheid**	
11a.	Bepaal op welke van de volgende zes grondslagen de gegevensverwerking wordt gebaseerd: 1. toestemming van de betrokkene, noodzakelijk voor 2. de uitvoering van een overeenkomst, 3. de nakoming van een wettelijke verplichting, 4. de bescherming van een vitaal belang, 5. een goede vervulling van een publieke taak en/of ~~6. de behartiging van gerechtvaardigd belangen.~~	Antwoord: 3. de nakoming van een wettelijke verplichting (WIV) 5. een goede vervulling van de publieke taak Bijvoorbeeld: De Directie Toeslagen dient er op toe te zien dat de toeslagen op een rechtmatige wijze worden toegekend en uitgekeerd én dat onterechte uitkeringen worden voorkomen.

11b.	Ga in op de vraag of ieder persoonsgegeven noodzakelijk is voor het verwezenlijken van de doeleinden? a. Subsidiariteit: kunnen de verwerkingsdoeleinden niet op een andere, voor de betrokkene minder nadelige wijze, worden verwezenlijkt? **b.** Evenredigheid: staat de inbreuk op de persoonlijke levenssfeer van betrokkenen (elke verwerking kwalificeert op zichzelf als een inbreuk) in evenredige verhouding met de verwerkingen voor de te dienen doeleinden?	Antwoord: a. Nee er is bewust voor gekozen om deze werkzaamheden bij een gespecialiseerd en gecentraliseerde onderdeel van CIE te concentreren. Alternatieven zijn overwogen, maar waren geen optie gezien de gevoeligheid van de te verwerken gegevens. Uitsluitend gegevens noodzakelijk voor de verwerkingsdoeleinden worden verwerkt. Bijvoorbeeld: • BRP: Woon- en correspondentieadres worden gebruikt om te bekijken of bepaald gedrag vanaf een bepaalde locatie verklaarbaar is. • FSV: Bron van detectie is geen persoonsgegeven, bijvoorbeeld balie, faillissement, collega, query, rapport. Rol van subject is o.a. dader/slachtoffer, dit is relevant voor het beoordelen van een BSN. b. Ja, o.b.v. de business rules wordt uitsluitend informatie van potentiële fraudeurs (middels HeidiSQL) doorgezet naar de SOC-analist cq. opdrachtgever.

12.	**Doelbinding**	**Toelichting:** Beoordeel of de verwerkingsdoeleinden voldoende welbepaald, uitdrukkelijk omschreven en gerechtvaardigd (lees: rechtmatig) zijn en of de persoonsgegevens niet op een met die doeleinden onverenigbare wijze worden verwerkt.
		Antwoord: De verwerkingsdoeleinden voor de persoonsgegevens die gebruikt worden om toeslagenfraude te voorkomen (mijn.belastingdienst.nl, mijn.toeslagen.nl en BRP) zijn uitdrukkelijk omschreven. @@Hier zou duidelijkheid moeten komen of de verwerkingen mogen plaatsvinden op basis van de oorspronkelijke bronnen en de bijbehorende doelen. De verwerkingsdoeleinden voor de persoonsgegevens uit FIOD, FSV, SBR, OB-blauwdruk en Vastgoed zijn onvoldoende omschreven.

C. Beoordeling risico's voor de rechten en vrijheden betrokkene	D. Beschrijving voorgenomen maatregelen
Beschrijf en beoordeel de risico's van de voorgenomen gegevensverwerkingen voor de rechten en vrijheden van betrokkene. Houd hierbij rekening met de aard,	*Beschrijf de voorgenomen maatregelen om de*

omvang, context en doelen van de gegevensverwerking. *Voor het beantwoorden van de risico's kunt u gebruik maken van de bijlage.* *Uiteraard moet u ook beoordelen of er nog aanvullende risico's van toepassing zijn.*	*hiervoor beschreven risico's van de voorgenomen gegevensverwerkingen voor de vrijheden en rechten van betrokkene aan te pakken.* *Voor het beantwoorden van de maatregelen kunt u gebruik maken van de bijlage. Uiteraard moet u ook beoordelen of er nog aanvullende maatregelen van toepassing zijn.*

KANS

	Kans verhogende aspecten	Toelichting	Risico-score	Mitigerende maatregel	Rest-risico
1	Er is onvoldoende onderbouwing over de rechtmatigheid van de verwerking	Wie is opdrachtgever? De opdrachtgever dient een schriftelijke opdracht voor anti fraude monitoring te verstrekken.	Hoog	Stel vast of de verwerking noodzakelijk is voor de vervulling van een taak van algemeen belang. Zo nee: stoppen met de verwerking.	
2	Er is onvoldoende duidelijkheid over de noodzaak van de verwerking van de data(-elementen)	De verwerkingsdoeleinden voor de persoonsgegevens uit FSV, SBR, OB-blauwdruk en Vastgoed zijn onvoldoende omschreven.	Hoog	Stel per data-element vast of deze binnen het doel van de gegevensverzameling valt (doelbinding). Zo nee, data-element niet opnemen of het doel aanscherpen.	
3	Gebruik van bijzondere persoonsgegevens		N.v.t.	Pas Privacy-by-design[5] toe	N.v.t.
4	Onvoldoende onderbouwing van data behoefte		Midden	Per data-element doel omschrijven.	
5	Beveiliging van de data onvoldoende op orde of het inzicht hierover ontbreekt		N.v.t.	Zorg dat je voldoet aan het Informatiebeveiligingsbeleid (BIR, VIR, etc.)	N.v.t.
6	Gebruik van nieuwe technologieën		N.v.t.	Huur expertise in en/of laat je informeren door een onafhankelijke deskundige	N.v.t.
7	Betrokkenheid meerdere (ook externe)partijen		N.v.t.	Afspraken met derde partijen contractueel vastleggen (juridisch normenkader kan hierbij helpen; zie ook normenkader voor SAAS-	N.v.t.

[5] Privacy by design bestaat uit de stappen: Anonimiseren, dataminimalisatie, pseudonimiseren, encryptie, acces control, data protection by default, verwijderen/bewaartermijnen en/of faciliteren rechten van betrokkene

				/CLOUD-toepassingen)	
8	Betrokkenheid van externe partijen van buiten de EU/EER		N.v.t.	1. Pas privacy-by-design toe 2. Afspraken met derde partijen contractueel vastleggen (juridisch normen kader kan hierbij helpen; zie ook normenkader voor SAAS-/CLOUD-toepassingen)	N.v.t.
9	De data van de betrokkenen wordt buiten het eigen datacenter opgeslagen		N.v.t.	1. Pas privacy-by-design toe 2. Afspraken met derde partijen contractueel vastleggen (juridisch normen kader kan hierbij helpen; zie ook normenkader voor SAAS-/CLOUD-toepassingen)	N.v.t.
10	Gegevens kunnen de basis zijn voor beoordeling van gedrag of prestatie van het individu	Gegevens worden uitsluitend gebruikt voor het voorkomen en opsporen van mogelijke fraude	Hoog	1. Plaats de gegevens binnen de eigen organisatie 2. Pas Privacy-by-design toe	Laag
11	Gegevens kunnen gebruikt worden voor identiteitsfraude		Laag	1. Plaats de gegevens binnen de eigen organisatie 2. Pas Privacy-by-design toe	Laag
12	Aantal personen dat toegang heeft tot de data/informatie		Laag	Authenticatie en autorisaties op basis van least privileges (minimale rechten)	Laag
13	De betrokkene is onvoldoende geïnformeerd over welke informatie over hem verzameld wordt		Hoog	Zorg dat de informatie over het verzamelen van de data en het doel ervan helder en transparant is (bijv. gepubliceerd op de website) Tekst op de website dient aangepast te worden.	
14	De mate waarin geautomatiseerde besluitvorming plaats vindt		Laag	Uitsluitend geautomatiseerde besluitvorming mag niet, tenzij Nederland dit uitdrukkelijk wel toestaat (zoals bijvoorbeeld geregeld bij de 'Kinderbijslag').	Laag
15	De mate waarin de gegevens binnen de organisatie verspreid worden		Laag	Authenticatie en autorisaties op basis van least privileges (minimale rechten)	Laag
16	De mate waarin de gegevens buiten de organisatie verspreid worden	Gegevens worden uitsluitend binnen BD gebruikt	N.v.t.	Opstellen privacybeleid en werkinstructies voor verwerkers van persoonsgegevens	N.v.t.
17	De mate waarin persoonsgegevens zijn opgenomen in (management)rapportages		N.v.t	1. Persoonsgegevens in (management)rapportages dienen zoveel	N.v.t.

				2. mogelijk geanonimiseerd en/of geaggregeerd te worden 3. Pas dataminimalisatie toe (alleen die gegevens opnemen die noodzakelijk of (wettelijk) vereist zijn	
18	De mate waarin er duidelijkheid is over de bewaartermijnen van de persoonsgegevens	18 maanden	Laag	Stel vooraf de bewaartermijnen van de persoonsgegevens vast	Laag
19	De mate waarin het geregeld is dat de persoonsgegevens conform de bewaartermijnen geautomatiseerd worden verwijderd/vernietigd. Geldt voor HeidiSQL en Splunk	Het ontbreekt aan geautomatiseerde en handmatige vernietiging	Top/Hoog	1. Pas Privacy-by-design toe 2. Indien geautomatiseerd niet mogelijk is: • Stel procedures voor handmatige verwijdering/vernietiging van persoonsgegevens op • Beperk de toegang (acces control) tot strikt noodzakelijk • controleer (aantoonbaar) of dit ook nageleefd wordt	
20	*Door het ontbreken van een opdrachtgever (gemandateerde verwerkingsverantwoordelijke) bestaat de kans dat het SOC onrechtmatig bezig is*	Stel vast wie de opdrachtgever(s) is(zijn) voor de verschillende anti fraude monitoringswerkzaamheden (Directeur Toeslagen, Directeur dienstonderdeel waartoe CAF behoort, ??)	Top	*De opdrachtgever(S) (gemandateerde verwerkingsverantwoordelijke) geeft/geven een schriftelijke opdracht voor de monitoring*	
21	Voor de BRP-gegevens wordt RAM als bron gebruikt	RAM is, op dit moment, een informele bron. Onbekend hoelang deze nog 'in de lucht' blijft	Hoog	Haal de gegevens rechtstreeks uit BRP (of EHI)	
22	*[eventuele andere risico's die onderkent worden, toevoegen]*				

	13b. Impact verhogende aspecten	**Toelichting**	**Risico-score**	**14b. Mitigerende maatregel**	**Rest-risico**
1	Imagoschade		Midden	Communicatiestrategie op orde brengen voor	

				het geval dat er 'iets' misgaat	
2	Niet voldoen aan AVG (Compliance) -> Imagoschade		Hoog	Zorg dat je voldoet aan de AVG en specifiek: - Implementeren mitigerende maatregelen (minimaal Prio Top en Hoog) uit deze PIA - Openstaande opmerkingen/vragen in deze PIA beantwoorden	
3	Beveiliging niet op orde -> Imagoschade		Laag	Zorg dat je voldoet aan het Informatiebeveiligingsbeleid (BIR, VIR, etc.)	Laag
4	De mate waarin het gebruik verenigbaar is met het oorspronkelijke verzameldoel		laag	Zorg dat de informatie over het verzamelen van de data en het doel ervan helder en transparant is (bijv. gepubliceerd op de website)	Laag
5	De mate waarin de integriteit en kwaliteit van de gegevens (actueel, juist, volledig) gewaarborgd is		Midden	1. Geef de betrokkene inzicht in de eigen gegevens 2. Zorg voor een klachtenprocedure 3. Inzicht en eventueel muteren op basis van least privileges (minimale rechten)	
6	De mate van vertrouwelijkheid van de gegevens		Midden	1. Sluit aan op de bestaande authenticatie en autorisatie infrastructuur 2. Pas waar gewenst/nodig 2-factor authenticatie toe 3. Definieer autorisatie profielen op basis van least privileges (minimale rechten)	
7	De mate waarin beslissingen genomen worden over betrokkenen	De gegevens worden gebruikt om potentiële frauduleuze handelingen te signaleren. Voor de uiteindelijke (definitieve) beslissingen wordt door de opdrachtgever nader onderzoek verricht	Midden	Zorg voor transparantie over de herkomst van de gebruikte gegevens en het beslisproces	
8	De mate waarin de kwaliteit van de dienstverlening, interne bedrijfsvoering en besluitvorming afhankelijk is van de gegevens	De kwaliteit van de potentiële frauduleuze 'gevallen' wordt bepaald door de inputgegevens en de business rules	Hoog	Zorg voor een goede AO die de kwaliteit van de data garandeert	

9	*[eventuele andere risico's die onderkent worden, toevoegen]*				
10					

Belastingdienst

memo

Privacy Impact Assessment (PIA) ten behoeve van het Platform verhuur woningen/kamers

Expertisecentrum Handhaving en Intelligence (EHI)

Herman Gorterstraat 55
3511 EW UTRECHT
Postbus 18200 3
511 EW UTRECHT
-

Contactpersonen

Persoonsgegevens

Datum
08 juni 2017

Versienummer
1

Auteurs
Persoonsgegevens

Aan
Wbp-team

Afschrift
MT EHI, Platform verhuur woningen/kamers

Bijlagen
3

1 Inleiding

Op 12 augustus 2016 heeft het CDO2 opdracht gegeven om een handhavingsstrategie uit te werken ten aanzien van de (kortstondige) verhuur van woningen/kamers via (digitale) platforms specifiek gericht op particulieren. Dit heeft geleid tot het plan van aanpak Platform verhuur woningen/kamers[1]. Voorafgaand aan de uitvoering van dit plan van aanpak is, op basis van de beschikbare gegevens, een Privacy Impact Assessment (hierna: PIA) uitgevoerd. De PIA treft u hierbij aan.

Kort samengevat wordt in deze PIA aangeven of en onder welke voorwaarden de gegevens die in 2015 en 2017 verzameld zijn, gebruikt mogen worden in de handhaving. Te beginnen met de in 2017 uit te voeren steekproef. Hierbij zal tevens worden ingegaan op mogelijke aandachtspunten en risico's.

In hoofdstuk 2 zal de voorgeschiedenis en het plan van aanpak worden beschreven. Hoofdstuk 3 ziet op de PIA en in hoofdstuk 4 zijn enkele aandachtspunten en aanbevelingen opgenomen.

2 Platform verhuur woningen/kamers

2.1 Voorgeschiedenis

De tijdelijke verhuur van woonruimte via verhuurplatforms op het internet heeft de afgelopen jaren een forse ontwikkeling doorgemaakt. Naar aanleiding van toenemende media-aandacht en Kamervragen is door het Expertisecentrum Handhaving en Intelligence (EHI) een verkenning interneteconomie uitgevoerd[2]. In deze verkenning stonden de volgende deelvragen centraal:

- Wat zijn de digitale ontwikkelingen en welke daarvan zijn in dit verband relevant?
- Tot welke veranderingen in producten en diensten leiden die digitale ontwikkelingen?
- Met welk kader kunnen we de handhavingsvraagstukken duiden?
- Wat zijn handhavingsvraagstukken?
- Hoe kun je die vraagstukken verder uitdiepen/oppakken?
- Welke kansen biedt het internet de handhaving van belastingen?
- Internet als bron van informatie, wat kan de Belastingdienst daarmee?

2.1.1 Werkwijze verkenning 2015

Door middel van 'scraping' zijn in 2015 de op internet beschikbare gegevens, waaronder voornaam, straat en woonplaats, van de website van een van de twee grootste platforms verzameld. Op deze manier zijn ongeveer 22.000 objecten verzameld welke door ongeveer 17.500 aanbieders worden aangeboden. De verzamelde locatiegegevens, voornamen en accommodatiegegevens konden niet zonder meer worden herleid tot een natuurlijk persoon (belastingplichtige). Daarom was identificatie noodzakelijk.

[1] Plan van aanpak Platform verhuur woningen/kamers, 1 februari 2017, Persoonsgegevens
er Persoonsgegevens
[2] Verkenning Interneteconomie, 17 mei 2016, Expertisecentrum Handhaving.

In een eerste geautomatiseerde identificatieslag zijn de uit openbare bron gescrapete NAW-gegevens vergeleken met interne gegevens uit de Basisregistratie Personen. Indien een (voor)naam van de aanbieder werd gevonden, vond onderzoek plaats in BVR en RAM om vast te stellen of iemand voorkwam met die (voor)naam als bewoner van een woning in die straat. Vervolgens heeft er een handmatige identificatieslag plaatsgevonden. Hierbij werden aanvullende gegevens verzameld via o.a. Streetview, Google en/of sociale mediaplatforms om identificatie mogelijk te maken. Op grond van artikel 18 Wbp zijn deze "bijzondere gegevens" (foto's) verwerkt, omdat dit voor dit doel onvermijdelijk is. Het is namelijk in veel gevallen onmogelijk om zonder de "bijzondere gegevens" de belastingplichtige te identificeren. Hierbij dient vermeld te worden dat de aanbieder het bijzondere gegeven (foto's) zelf openbaar heeft gemaakt door het op het internet te plaatsen.

2.1.2 Resultaten en aanbevelingen verkenning 2015

Uit de verkenning is gebleken dat in ongeveer 75% van de gevallen geen tijdelijke verhuuropbrengst in het jaar 2015 is aangegeven, terwijl er wel een object werd aangeboden. Van de overige personen is zonder aanvullend onderzoek geen uitspraak te doen, o.a. omdat het mogelijk is dat de in box 3 aangegeven woning fiscaal aanvaardbaar is of omdat de inkomsten onder ROW zijn aangegeven. Het risico van het niet aangeven van tijdelijke huurinkomsten is als 'hoog' gekwalificeerd.

Daarnaast is geconcludeerd dat massale identificatie van de aanbieders een moeilijk begaanbare weg is. De belangrijkste bron van beschikbare gegevens zijn, op dit moment, de gegevens beschikbaar op internet via de website van de aanbieder. De onderzoeksmethode (OSINT[3]) is een goed toepasbaar instrument, mits de website vrij toegankelijk is[4].

Een van de aanbevelingen uit de verkenning was om toezicht voor te bereiden waaraan met het plan van aanpak c.q. de voorgenomen steekproef nu een invulling/verdieping wordt gegeven. Met het oog op deze verdieping zijn de verzamelde gegevens na afloop van de verkenning bewaard om ze te zijner tijd naast de aangiften inkomstenbelasting 2015 te kunnen leggen.

2.2 Uitwerking opdracht van CDO2

Het toenemend gebruik van het internet, de explosieve groei van deze platforms en de publieke belangstelling voor de verhuur van woningen/kamers via platforms heeft ertoe geleid dat de Belastingdienst heeft besloten de gevolgen voor zowel de belastingheffing als de handhaving te onderzoeken. De opdracht vanuit het CDO2 is om een handhavingsstrategie uit te werken ten aanzien van de (kortstondige) verhuur van woningen/kamers via (digitale) platforms, specifiek gericht op particulieren. Deze opdracht is nader uitgewerkt in een plan van aanpak.

Plan van aanpak:
Uit het plan van aanpak blijkt de keuze voor de uitvoering van een steekproef met als doel inzicht te verkrijgen in het fiscaal belang en de oorzaken van het (mogelijke) nalevingstekort. Om de steekproef uitvoerbaar te houden en rekening te houden met het level playing field, richt de steekproef zich op de twee grootste platforms die actief zijn op de digitale markt van tijdelijke verhuur van woonruimten. Aan de hand van de inzichten van de steekproef zal het projectteam aanbevelingen en voorstellen doen om tot een effectieve handhavingsstrategie te komen.

---

[3] OSINT = Open Source Intelligence: het met specifieke technieken verzamelen, verwerken en analyseren van openbaar beschikbare informatie voor intelligencedoeleinden.
[4] Het is niet nodig om een account aan te maken om de gegevens op de site te benaderen.

Waarom steekproef op basis van de via internet verzamelde gegevens?
Het projectteam kiest voor een steekproef onder de verhuurders – op grond van de via internet verzamelde gegevens - omdat de twee grootste platforms niet in Nederland zijn gevestigd, en derhalve niet administratieplichtig zijn in de zin van de Algemene Wet inzake Rijksbelastingen (hierna: AWR). Het stellen van vragen op grond van art. 53 AWR aan de platforms is dus niet mogelijk. De Belastingdienst heeft daarnaast nog de mogelijkheid om via de weg van wederzijdse bijstand serievragen te stellen aan het EU-land waar het platform is gevestigd, echter het stellen van vragen via wederzijdse bijstand is alleen toegestaan indien de eigen mogelijkheden voldoende zijn benut. Bovendien moet een inlichtingenverzoek voldoende identificeerbaar zijn. Een zogenoemde 'fishing expedition' is dus niet toegestaan. In dit dossier hebben we geen informatie beschikbaar die het mogelijk maakt om een identificeerbaar informatieverzoek aan het buitenland te richten, behalve de via internet verzamelde gegevens. Alleen de via internet verzamelde gegevens maken het dus mogelijk om het projectdoel te realiseren. Aangezien op grond van artikel 47 AWR de mogelijkheid bestaat om de verhuurders om informatie te verzoeken en we eerst inzichtelijk willen krijgen wat het fiscaal belang en de oorzaken van het (mogelijke) nalevingstekort zijn, moeten we allereerst de mogelijkheden van een steekproef onder de verhuurders verkennen.

Steekproef 2017:
Teneinde meer inzicht te krijgen in het fiscaal belang en de oorzaken van het (mogelijke) nalevingstekort zijn door middel van een aselecte steekproef circa 300 posten getrokken uit de in 2015 verzamelde populatie. De steekproefposten zijn vervolgens op dezelfde wijze geïdentificeerd als bij de verkenning in 2015. Allereerst is voor zover mogelijk geautomatiseerd geïdentificeerd en vervolgens heeft een veel arbeidsintensievere, handmatige identificatie met het 'geoefend oog' plaatsgevonden. Hierbij zijn circa 85% van de verhuurders geïdentificeerd. De objecten welke geen deel uitmaken van de steekproef worden op dit moment niet geïdentificeerd.

De steekproefposten zullen, aan de hand van de ingediende aangiften over 2015 intensief worden behandeld. Afhankelijk van de feiten en omstandigheden van het individuele geval volgt een passende klantbehandeling. Het is uitdrukkelijk niet de bedoeling om in het kader van deze steekproef de aanbieder van het platform te benaderen om aanvullende informatie te verkrijgen. Dit omdat voorafgaand aan het stellen van vragen via wederzijdse bijstand de eigen mogelijkheden voldoende benut moeten worden. Indien verhuurders welke deel uitmaken van de steekproef weigeren informatie aan te leveren, overweegt het projectteam om in dat stadium het verhuurplatform te benaderen om de ontbrekende gegevens aan te leveren. In dat stadium is er geen sprake meer van een fishing expedition maar kunnen gerichte vragen worden gesteld.

Voorafgaand aan de steekproef in 2017 is in 2017 de site van het in 2015 gescrapete verhuurplatform opnieuw gescraped. Ook is een ander (het op één na grootste) verhuurplatform gescraped. Op deze wijze wordt voorkomen dat er sprake is van cherry picking, de steekproef is namelijk niet uitsluitend op een verhuurplatform gericht. Bovendien wordt de zorgvuldigheid van de steekproef gewaarborgd door op 2 momenten te scrapen, namelijk een nulmeting in 2015 en een tweede, vergelijkbare meting in 2017.

De wijze van scraping en de beweegredenen voor de scraping zijn voor de scraping in 2015 en 2017 gelijk. Daarom ziet deze PIA op zowel de scraping welke in 2015 heeft plaatsgevonden als de scraping in 2017. Let wel, de steekproef ziet uitsluitend op de in 2015 gescrapete gegevens, omdat in dit stadium uitsluitend de aangifte inkomstenbelasting 2015 voorhanden is.

3 Privacy Impact Assessment (PIA)

3.1 Algemeen

Een PIA is een hulpmiddel om privacy risico's in kaart te brengen. Het PIA-instrument voor de Belastingdienst wordt ingezet bij nieuwe maatregelen waarbij aspecten van gegevensbescherming spelen, zoals bij nieuwe vormen van procesondersteuning die op eigen initiatief worden ontwikkeld of bij het opzetten van een andere wijze van toezicht. De PIA heeft de vorm van een vragenlijst. Door middel van deze vragenlijst zullen kernbegrippen uit de Wet bescherming persoonsgegevens (Wbp) worden toegelicht. Daarnaast is de PIA ook richtinggevend en corrigerend. De Wbp is van toepassing bij het verzamelen van de benodigde gegevens ter uitvoering van de steekproef. Kernelementen binnen de Wbp bij gegevensverwerking zijn rechtmatige verwerking, doelbinding, proportionaliteit (dataminimalisatie) en subsidiariteit.

Daarnaast heeft de Hoge Raad op 24 februari jl. uitspraak gedaan over het gebruik van ANPR-beelden voor de controle van de rittenregistraties in het kader van privé gebruik auto[5]. In dit hoofdstuk wordt de afweging gemaakt of deze arresten van invloed zijn op de privacy waarborging van de voorliggende steekproef.

3.2 Beoordeling

3.2.1. Internetscraping

Voor de beoordeling van de privacy aspecten is het begrip 'scraping' van groot belang. Scraping is het op een geautomatiseerde manier verzamelen van data die op het browserscherm wordt weergegeven. De data die zichtbaar is op het scherm wordt gekopieerd en vervolgens opgeslagen in een database zodat verdere verwerking en analyse mogelijk is.

Hetzelfde resultaat had bereikt kunnen worden door deze data handmatig te verzamelen. Doch ongeveer 22.000 keer de webpagina opslaan en vervolgens de informatie van de webpagina kopiëren is niet efficiënt. Daarom is vanuit efficiency oogpunt gekozen voor scraping.

De term internetscraping geeft zodoende uitsluitend aan dat de informatie automatisch is verkregen. De webpagina's die hierbij zijn gescraped zijn webpagina's die zichtbaar zijn zonder dat op de website van het platform wordt ingelogd c.q. een account is aangemaakt. Het betreft openbare informatie die voor iedereen zichtbaar is.

Het gebruiken van de websitegegevens van het verhuurplatform is te vergelijken met het gebruiken van openbare gegevens verzameld door medewerkers van de Belastingdienst. Te denken valt aan het raadplegen van advertenties in de krant. Voor het raadplegen van openbare informatie door de Belastingdienst is geen specifieke wettelijke basis vereist. Er is hooguit een beperkte inbreuk op de privacy, waarvoor geen wettelijke grondslag vereist is[6].

---

[5] ECLI:NL:HR:2017:288, 287 en 286.

[6] Zie ook AG Niessen (7.27), In de rechtspraak wordt aangenomen dat bij kortstondige waarnemingen op de openbare weg de persoonlijke levenssfeer niet in het geding is, althans niet in die mate dat dit gebaseerd moet zijn op een speciale bevoegdheid (EHRM, Peck v. Verenigd Koninkrijk, 44647/98, 28 januari 2003; HR 20 april 2004, LJN AL8449).

3.2.2. Rechtmatige verwerking

Artikel 6 Wbp
Persoonsgegevens worden in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze verwerkt.

Voor de verwerking van de persoonsgegevens is in art. 8 Wbp een limitatieve opsomming gegeven van de grondslagen waarop de verwerking moet berusten.

Artikel 8 Wbp
Persoonsgegevens mogen slechts worden verwerkt indien:
Sub e. de gegevensverwerking noodzakelijk is voor de ***goede vervulling van een publiekrechtelijke taak*** *door het desbetreffende bestuursorgaan dan wel het bestuursorgaan waaraan de gegevens worden verstrekt.*

De persoonsgegevens welke middels internetscraping worden verwerkt zijn noodzakelijk voor de goede vervulling van een publiekrechtelijke taak. De opkomst en groei van het internet heeft ertoe geleid dat er een digitale economie is ontstaan waarvoor nog geen geijkte kaders bestaan waarbinnen gewerkt wordt. De deeleconomie (de verhuur van woningen/kamers via platforms) maakt deel uit van de digitale economie. Gezien de verandering van de economieën is het niet meer dan logisch dan dat de bron waarvan het bestuursorgaan haar informatie verkrijgt ook verandert. Het verzamelen van openbare data op het internet is in de huidige samenleving vanzelfsprekend. Voor de uitvoering van de steekproef verwerkt het bestuursorgaan uitsluitend de persoonsgegevens die noodzakelijk zijn om de belastingheffing ten aanzien van de deeleconomie te waarborgen.

3.2.3. Doelbinding

Persoonsgegevens mogen alleen voor welbepaalde, vooraf uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en vervolgens alleen verder worden verwerkt voor doeleinden die daarmee verenigbaar zijn.

Het doel van het verzamelen van de gegevens door middel van scraping is het verkrijgen van inzicht in het fiscaal belang en de oorzaken van het (mogelijke) nalevingstekort dat is ontstaan als gevolg van de verhuur van woningen en kamers met tussenkomst van een platform. Te beginnen met de in 2017 uit te voeren steekproef. Hierbij dient uitdrukkelijk vermeld te worden dat de steekproef posten intensief behandeld worden en waar nodig ook belasting correcties worden doorgevoerd. Aan de hand van het verkregen inzicht zal het projectteam aanbevelingen en voorstellen doen om tot een effectieve handhavingsstrategie te komen.

3.2.4. Proportionaliteit

De proportionaliteit van de gegevensverwerking richt zich op de vraag of de gegevensverwerking in verhouding staat tot het doel dat wordt gediend en niet meer gegevens worden verwerkt dan strikt noodzakelijk (dataminimalisatie).

Het doel van het verzamelen van de gegevens door middel van scraping is het verkrijgen van inzicht in het fiscaal belang en de oorzaken van (mogelijke) nalevingstekorten die zijn ontstaan als gevolg van de verhuur van woningen en kamers met tussenkomst van een platform. De gescrapete gegevens zijn allen noodzakelijk om identificering van de verhuurders mogelijk te maken. Zonder de middels internetscraping verzamelde gegevens kan de Belastingdienst op dit

terrein haar taken niet adequaat uitvoeren waardoor nieuwe verdienmodellen niet onderzocht kunnen worden.

3.2.5. Subsidiariteit

Subsidiariteit wil zeggen dat de gegevensverstrekking op de voor de betrokkenen minst privacy belastende manier ingericht moet worden. Kan de informatievoorziening op een andere, voor de betrokkene minder inbreukmakende manier laten verlopen, dan moet voor die manier worden gekozen.

Het is in dit stadium niet mogelijk de benodigde gegevens op een andere manier te verkrijgen. De andere voor de hand liggende mogelijkheid, zijnde een verzoek om informatie aan het verhuurplatform is in dit stadium niet mogelijk. Alvorens een verzoek om informatie aan het verhuurplatform gedaan kan worden, moet de Belastingdienst namelijk eerst haar eigen mogelijkheden om aan informatie te komen benutten.

3.2.6. Van belang zijnde aspecten m.b.t. privacy:
Het is de vraag of het scrapen van de gegevens van de website van de aanbieder van woonruimte een inbreuk is op de privacy. Hierbij achten wij het volgende van belang:

* Het betreft publiek toegankelijke bronnen. De gegevens zijn voor iedereen raadpleegbaar. Hierbij is het niet nodig om een account aan te maken om de gegevens op de site te benaderen (men hoeft niet in te loggen). Van het maken van accounts/ inloggen is bij het scrapen van het internet dan ook geen sprake geweest.

* Het enige wat vanuit het project wordt gedaan, is de openbare informatie koppelen aan onze interne gegevens (BVR e.d.). Op deze wijze kunnen de verhuurders geïdentificeerd worden. Identificatie is niet mogelijk met uitsluitend de openbare informatie van de platformwebsites.

* Aanbieders plaatsen zelf hun informatie op het verhuurplatform en beogen daarmee deelname aan het economisch verkeer. Deelname aan het economisch verkeer kan verschillende fiscaal belaste feiten met zich mee brengen. Slechts de internetgegevens van personen die hun woning ter verhuur aanbieden worden verzameld. In veel gevallen speelt bij tijdelijke verhuur van woonruimte een fiscaal belang.

* De Belastingdienst is transparant over het gebruik van internetinformatie. Op de website van de Belastingdienst staat het volgende gepubliceerd:

  a) "De Belastingdienst scant regelmatig het internet om zicht te krijgen op (nieuwe) ondernemersactiviteiten. Daarbij kijken we of en hoe een ondernemer bij ons geregistreerd staat en op welke manier hij aan zijn fiscale verplichtingen voldoet [7]."

  b) "De Belastingdienst volgt de ontwikkelingen in de deeleconomie waar Airbnb ook onder valt. Kenmerk in de deeleconomie is dat bezittingen uit de privésfeer in het ruilverkeer worden gebracht. Dit kan zich ontwikkelen tot het feitelijk deelnemen aan het economisch verkeer met gevolgen voor de fiscale behandeling. Het aantal

[7] Belastingdienst, <https://www.belastingdienst.nl/wps/wcm/connect/bldcontentnl/belastingdienst/zakelijk/ondernemen/internetondernemers/>

activiteiten is divers, zowel naar aard als omvang. De sterke groei van de deeleconomie is aanleiding voor een nadere positiebepaling. Alle partijen, inclusief de Belastingdienst, anticiperen hierop. De Belastingdienst verricht op specifieke onderwerpen een eigen onderzoek, waarbij eerst een inschatting gemaakt wordt van het financiële belang. Bij voldoende relevantie kan daarna een vervolgonderzoek plaatsvinden. Op dit moment loopt in dat kader een verkenning naar de inkomsten uit de verhuur van een woning via Airbnb[8]."

Bovengenoemde berichten waren reeds openbaar voordat de websites van de verhuurplatforms zijn gescraped.

* Er worden geen systematische bewegingspatronen van belastingplichtigen vastgelegd. In plaats daarvan hebben twee statische meetmomenten plaatsgevonden. Te weten in september 2015 en in januari 2017. Op een vaste datum zijn de op dat moment aanwezige gegevens vastgelegd van degenen die op dat moment via het verhuur platform woonruimte aanbieden. Het verzamelen van deze gegevens t.a.v. de betrokkenen is dus geen systematische aangelegenheid en is wezenlijk anders dan het systematisch fotograferen van een auto (incl. inzittenden) langs de openbare weg.

* De explosieve groei van deze platforms en de publieke belangstelling voor de verhuur van woningen/kamers via platforms maakt het noodzakelijk dat de Belastingdienst zichtbaar is. De maatschappelijke druk is enorm. De samenleving verlangt van de Belastingdienst dat zij handhaaft ten aanzien van dit groeiende fenomeen. De Belastingdienst dient zicht te hebben op de omvang van het aantal verhuurders dat niet aan hun fiscale verplichtingen voldoet. Dit om negatieve prikkels aan de verhuurders die wel aan hun fiscale verplichtingen voldoen te voorkomen en de compliance te bevorderen.

3.2.7 Gevolgen ANPR-arresten

De ANPR-casus spreekt over het systematisch verzamelen, vastleggen, bewerken en jarenlang vastleggen van gegevens over bewegingen van voertuigen op diverse plaatsen in Nederland. In het voorliggende geval van scraping van gegevens is eveneens sprake van het verzamelen, vastleggen, bewerken en bewaren van gegevens van te huur aangeboden objecten.

De inbreuk op de belangen van betrokkenen is in dit geval, zoals geschetst, echter niet op één lijn te stellen met de inbreuk die is gemaakt in de ANPR-casus, vanwege het feit dat de gegevens door de aanbieders zelf op het internet zijn geplaatst en omdat de informatie vrij raadpleegbaar is voor iedereen. De geplaatste informatie heeft direct fiscale relevantie, omdat deelname aan het economisch verkeer hierbij wordt beoogd, wat verschillende fiscale feiten met zich mee kan brengen. Daarnaast is ook geen sprake is van het vastleggen van bewegingen van belastingplichtigen. In plaats daarvan hebben twee statische meetmomenten plaatsgevonden. Te weten in september 2015 en in januari 2017. Op deze twee vaste data zijn de op dat moment aanwezige gegevens vastgelegd van degenen die op dat moment via het verhuur platform woonruimte aanbieden. Het verzamelen van deze gegevens t.a.v. de betrokkenen is dus geen systematische aangelegenheid en is wezenlijk anders dan het systematisch fotograferen van een auto (incl. inzittenden) langs de openbare weg.

[8] Belastingdienst, juni 2015, <https://belastingdienst-in-beeld.nl/verkenning-naar-inkomsten-uit-verhuur-via-airbnb/>

Zoals geschetst is de mate van inbreuk op de belangen van betrokkenen gering en rechtvaardigt het doel van de steekproef deze inbreuk. Daarnaast is het in dit stadium niet mogelijk om de gegevens op een andere manier te verkrijgen omdat voor een verzoek van wederzijdse bijstand de eigen mogelijkheden allereerst voldoende benut moeten worden.

Het scrapen van de gegevens in deze casus kent teveel verschillen met de ANPR-casus en wordt derhalve niet geraakt door de uitspraak.

3.2.8. Concluderend
Volgens ons is geen sprake van inbreuk op de privacy, althans niet in die mate dat daarvoor een speciale bevoegdheid vereist is. De verwerking voldoet volgens ons aan de beginselen van proportionaliteit en subsidiariteit. Het gebruiken van de digitale gegevens van het verhuurplatform valt te vergelijken met het gebruiken van openbare gegevens verzameld door medewerkers van de Belastingdienst. Voor het raadplegen van openbare informatie door de Belastingdienst is geen specifieke wettelijke basis vereist. Er is hooguit een beperkte inbreuk op de privacy, waarvoor geen wettelijke grondslag vereist is. Het gebruik van dergelijke informatie zou echter geschaard kunnen worden onder de algemene taakomschrijving van de Belastingdienst[9].

3.3 Vragenlijst PIA

I. Basisinformatie: type persoonsgegevens, type verwerking en noodzaak/gegevensminimalisering

1. Wilt u als verantwoordelijke persoonsgegevens gaan gebruiken voor de verwerking die u voorziet? Zo ja, van welk type?

> *Ja, zie voor een overzicht van de gebruikte gegevens bijlage 1 en 2. De meeste externe gegevens die hiervoor worden gebruikt zijn afkomstig van de websites van de twee grootste verhuurplatforms. Deze gegevens zijn speciaal voor dit doel verzameld. Daarnaast is nader internetonderzoek noodzakelijk om aan de hand van geschrapte gegevens en onze interne gegevens de verhuurders te identificeren. Dit gebeurt aan de hand van o.a. Google, Streetview en social media kanalen. Ook hier wordt wederom geen account aangemaakt c.q. ingelogd, het betreft uitsluitend openbare internetinformatie. De gegevens uit de interne bronnen werden oorspronkelijk voor de primaire processen van de Belastingdienst ingezet. Het is niet ongebruikelijk dat ze worden ingezet voor identificatie- en onderzoeksdoeleinden. Het gebruik van de interne gegevens is met het oorspronkelijke doel verenigbaar omdat de gegevens gebruikt worden om te controleren of er sprake is van een juiste belastingheffing hetgeen deel uitmaakt van de primaire processen.*

2. Andere specifieke persoonsgegevens?

> *Zie voor overzicht van de gehanteerde persoonsgegevens bijlage 1 en 2. Er kan sprake zijn van verwerking van bijzondere persoonsgegevens in de vorm van beeldmateriaal uit sociale media en van de betrokken websites. In veel gevallen zal dit beeldmateriaal bestaan uit foto's van verhuurders die door hen zelf zijn geplaatst. Dit beeldmateriaal is noodzakelijk en uitsluitend bedoeld voor de identificatie van de verhuurders. Bovendien is het beeldmateriaal door de aanbieder zelf op het internet geplaatst.*

[9] Artikel 11 – 20 AWR

2a. Is het de bedoeling om gegevens over de financiële of economische situatie van betrokkenen, of andere gegevens die kunnen leiden tot stigmatisering of uitsluiting te verwerken?

Nee. De gegevens worden gebruikt om inzicht te krijgen in het fiscale belang om vervolgens de handhavingsstrategie te bepalen voor deze doelgroep.

2b. Is het de bedoeling om gegevens over kwetsbare groepen of personen te verwerken?

Nee.

2c. Is het de bedoeling gebruikersnamen, wachtwoorden en andere inloggegevens te verwerken?

Nee. Daarnaast wordt opgemerkt dat er niet wordt ingelogd op de websites van de verhuurplatforms of social media e.d.

2d. Is het de bedoeling om uniek identificerende gegevens, zoals biometrische gegevens, te verwerken?

Nee.

2e. Is het de bedoeling om het BSN-nummer, of een ander persoonsgebonden nummer te verwerken?

Ja. Het BSN-nummer heeft bij de verwerkingen een rol gespeeld om gevonden externe gegevens te kunnen koppelen aan Belastingdienstgegevens. Een ander te verwerken persoonsnummer is het btw-nummer.

3. Kan van elk van de onder vraag I.1 en vraag I.2 opgevoerde typen persoonsgegevens worden gesteld dat zij beleidsmatig of technisch direct van belang en onontbeerlijk zijn voor het bereiken van de beleidsdoelstelling? Wat zou er precies niet inzichtelijk worden als ervoor wordt gekozen bepaalde gegevens niet te verwerken? Licht per te verwerken persoonsgegeven toe.

De beleidsdoelstelling van de gegevensverwerking is om zicht te krijgen op het fiscaal belang om vervolgens de handhavingsstrategie te kunnen bepalen. De combinatie van gegevens leidt tot een betere identificatie van de verhuurder. Hierdoor heeft elk gegeven zijn eigen rol binnen de aangifte en is dus noodzakelijk om de verhuurders te identificeren en zicht te krijgen op de omvang van het fiscaal belang. In de bijlagen is per persoonsgegeven de relevantie aangegeven. Er wordt aangegeven waarvoor het gegeven wordt gebruikt, zodat de noodzaak van het gebruik duidelijk wordt gemaakt.

4. Kan, als het gaat om gevoelige persoonsgegevens, hetzelfde beleidseffect of technisch resultaat worden bereikt op een van de volgende wijzen: (a) door (gecombineerd) gebruik van normale persoonsgegevens, (b) door gebruik van geanonimiseerde of gepseudonimiseerde gegevens?

Nee, identificatie op persoonsniveau is noodzakelijk om het fiscaal belang inzichtelijk te krijgen. Het fiscaal belang wordt vastgesteld op basis van de resultaten van de intensieve klantbehandeling. Voor de klantbehandeling is het niet mogelijk om met geanonimiseerde of gepseudonomiseerde gegevens

te werken. De presentatie van de onderzoeksresultaten zal zoveel mogelijk geanonimiseerd plaatsvinden.

5. In welk breder wettelijk, beleidsmatig of technisch kader wordt het voorziene beleid/databestand/informatiesysteem ontwikkeld en wat voor soort(en) verwerking(en) van persoonsgegevens gaan hiervan deel uitmaken bij het voorziene traject? Wordt hierbij gebruikt gemaakt van (nieuwe) technologie of informatiesystemen?

Voor het uitvoeren van haar publiekrechtelijke taken, gebaseerd op de AWR, dient de Belastingdienst op de hoogte te zijn over nieuwe verdienmodellen die zich ontwikkelen op het internet. Met name het feit of de nieuwe verdienmodellen leiden tot de juiste heffing en afdracht van de diverse belastingen is relevant. Om een adequate handhavingsstrategie te ontwikkelen, is het van belang te weten of en in welke mate er op dit moment aan de belastingverplichtingen wordt voldaan met betrekking tot deze nieuwe mogelijkheden. Om de gegevens van het verhuurplatform op internet te verzamelen, is in 2015 en 2017 gebruikt gemaakt van 'scraping'.

II. Doelbinding, koppeling, kwaliteit en profilering

Doeleinden/doelbinding en koppeling

1. Hebt u het/de specifieke doel(en) waarvoor u de persoonsgegevens gaat verwerken in detail vastgesteld? Geldt hiervoor één en hetzelfde specifieke doel?

Het doel van het verwerken van de persoonsgegevens is het verkrijgen van inzicht in het fiscaal belang en de oorzaken van het (mogelijke) handhavingstekort dat is ontstaan als gevolg van de verhuur van woonruimte met tussenkomst van een verhuurplatforms.

2 en 3. Gaat het bij het project/systeem om gebruik van nieuwe persoonsgegevens voor een bestaand doel, of bestaande doelen binnen al bestaande systemen? (scenario toevoeging nieuwe persoonsgegevens). Gaat het bij het project/systeem om het nastreven van nieuwe/aanvullende doeleinden door bestaande persoonsgegevens, of verzamelingen daarvan, te gebruiken, vergelijken, delen, koppelen of anderszins verder te verwerken? (scenario toevoeging doeleinden).

Zo ja, hebben alle personen/instanties/systemen die betrokken zijn bij de verwerking dezelfde doelstelling met de verwerking van de desbetreffende persoonsgegevens of is daarmee spanning mogelijk gelet op hun taak of hun belang? Gelden dezelfde doelen voor het hele proces?

Er wordt gebruikt gemaakt, naast de lijst van reeds gemelde persoonsgegevens, van nieuwe persoonsgegevens (namelijk de gescrapete gegevens). Het in kaart brengen van het fiscaal belang is geen nieuw doel van de Belastingdienst waarvoor gegevens worden verzameld. Voor het gehele proces geldt hetzelfde doel.

4. Indien u positief hebt geantwoord op vragen II.2 of II.3, hoe wordt een dergelijk voorgenomen gebruik (d.w.z. gebruik van nieuwe persoonsgegevens in bestaande systemen of van bestaande persoonsgegevens voor nieuwe doeleinden) gemeld aan: (a) de functionaris voor de gegevensbescherming, of (b) de Autoriteit Persoonsgegevens indien er geen FG is?

(a) Melding FG.

5. Indien u positief geantwoord hebt op vragen II.2 of II.3, welke (nadere) controles op een dergelijk gebruik (d.w.z. gebruik van nieuwe persoonsgegevens in bestaande systemen of van bestaande persoonsgegevens voor nieuwe doeleinden) zijn voorzien?

Het projectteam is verantwoordelijk voor het gebruik van de persoonsgegevens. De middels internetscraping verzamelde internetgegevens zijn uitsluitend toegankelijk voor het projectteam. Uitsluitend de informatie ten aanzien van de 300 steekproefposten wordt uitgezet bij de behandelaars die de steekproefposten zullen gaan behandelen.

6. Welke periodieke en incidentele controles zijn voorzien om de juistheid, nauwkeurigheid en actualiteit van de in het beleidsvoorstel, wetsvoorstel op overheids ICT-systeem verwerkte persoonsgegevens na te gaan?

Er is geen sprake geweest van periodieke en incidentele controles sinds 2015. De deskundigheid van de onderzoeker speelt een rol in het waarderen van de juistheid, nauwkeurigheid en actualiteit van de gehanteerde internetgegevens. Het koppelen van sociale media en gegevens uit BVR/RAM ziet toe op vaardigheden en kwaliteiten van de onderzoeker. Er wordt een betrouwbaarheidsscore gegeven aan de gekoppelde gegevens. Het verdient aanbeveling om hiervoor objectieve criteria vast te stellen en een stappenplan op te stellen. Voor de identificering van de verhuurders is inmiddels een richtlijn opgesteld (bijlage 3). De gehanteerde Belastingdienstgegevens vallen binnen de algemene controlesystematiek van de Belastingdienst.

Profilering

7. Zullen de verzamelde/verwerkte persoonsgegevens gebruikt worden om het gedrag, de aanwezigheid of de prestaties van mensen in kaart te brengen en/of te beoordelen en/of te voorspellen? Zijn de betrokkenen daarvan op de hoogte? Zijn de gegevens die hiervoor worden gebruikt, afkomstig uit verschillende (eventueel externe) bronnen en zijn zij oorspronkelijk voor andere doelen verzameld?

De scraping heeft plaatsgevonden op twee vaste meetpunten, hierdoor kunnen geen bewegingen van natuurlijke personen in kaart gebracht worden. Desalniettemin worden op basis van de gescrapete gegevens vragen gesteld om de mate van naleving van fiscale verplichtingen van de steekproefposten te beoordelen. Hierbij zal, indien van toepassing, ook belasting gecorrigeerd/ nagevorderd worden. Op de website van de Belastingdienst wordt vermeld dat de Belastingdienst regelmatig het internet scant om zicht te krijgen op (nieuwe) ondernemersactiviteiten[10]. Bovendien heeft de Belastingdienst in juni 2015 openbaar gemaakt dat zij een onderzoek naar het grootste platform is gestart[11]. De betrokkenen worden zodoende geacht op de hoogte te zijn. Bovendien worden betrokkenen door middel van een uniforme vragenbrief benaderd op het moment dat de PIA is goedgekeurd en de klantbehandeling ten aanzien van dit onderwerp wordt opgestart.

[10] Belastingdienst, <https://www.belastingdienst.nl/wps/wcm/connect/bldcontentnl/belastingdienst/zakelijk/ondernemen/internetondernemers/>
[11] Belastingdienst, juni 2015, <https://belastingdienst-in-beeld.nl/verkenning-naar-inkomsten-uit-verhuur-via-airbnb/>

De verzamelde gegevens worden gebruikt voor het verkrijgen van inzicht in het fiscaal belang en de oorzaken van het handhavingstekort. In 2015 zijn, met het oog op een nadere verdieping, de verzamelde gegevens bewaard om ze op een later tijdstip te kunnen vergelijken met de ingediende aangiften inkomstenbelasting over 2015. Dit is echter niet specifiek vastgelegd[12]. Het doel van het vervolgonderzoek (de steekproef 2017) ligt echter in lijn met het oorspronkelijk doel waarvoor de gegevens zijn verwerkt. Hierdoor is sprake van een rechtmatige verwerking.

8. Wordt bij deze analyse/beoordeling/voorspelling gebruik gemaakt van vergelijking van persoonsgegevens die technisch geautomatiseerd is (d.w.z. niet door mensen zelf wordt uitgevoerd)? Zo ja, hoe wordt geregeld dat, indien dit geautomatiseerde proces tot een beoordeling of voorspelling over een bepaalde persoon leidt, hierop pas concrete actie wordt ondernomen na tussenkomst en (tweede) controle van (menselijk) personeel?

Ja, voor de identificatie van de verhuurders wordt allereerst een technisch geautomatiseerde vergelijking gemaakt van persoonsgegevens (uit BVR/RAM). De controle op de resultaten van deze geautomatiseerde vergelijking gebeurt door menselijke tussenkomst. Vervolgens wordt er aan de op deze wijze verkregen persoonsgegevens belastingdienstinformatie gekoppeld om uitspraken te kunnen doen over het fiscale belang.

III. Betrokken instanties/systemen en verantwoordelijkheid

1. Welke interne en externe instantie(s) en/of systemen is/zijn betrokken bij de voorziene verwerking in elk van de onder I.5 onderscheiden fasen? Welke verstrekkers zijn er en welke ontvangers? Welke bestanden of deelbestanden en welke infrastructuren?

Zie tabel IV: Stappen procedure vaststellen omvang fiscaal belang verhuurders van accommodaties in bijlage 1.

2. Is (in ieder stadium) duidelijk wie verantwoordelijk is voor de verwerking van de persoonsgegevens? Zo ja, is deze persoon of organisatie daarop voldoende voorbereid en geëquipeerd wat betreft de nodige voorzieningen en maatregelen, waaronder middelen, beleid, taakverdeling, procedures en intern toezicht?

Zie tabel IV: Stappen procedure vaststellen handhavingstekort verhuurders van accommodaties in bijlage 1.

3. Wie binnen uw organisatie, en elk van de andere betrokken organisaties, krijgen precies toegang tot de persoonsgegevens?

De gegevens van internet zijn voor iedereen vrij toegankelijk: het betreft publiek toegankelijke bronnen. De Belastingdienstgegevens zijn alleen voor geautoriseerde personen toegankelijk. Hiervoor geldt het beleid van de Belastingdienst. De middels internetscraping verzamelde internetgegevens zijn uitsluitend toegankelijk voor het projectteam.

4. Geldt voor een of meer van de betrokken instanties een beperking van de mogelijkheid om persoonsgegevens te verwerken als gevolg van geheimhoudingsverplichtingen (in verband met functie/wet)?

Art. 67 AWR is van toepassing voor de Belastingdienst.

[12] De vastlegging hiervan had moeten plaatsvinden in een PIA m.b.t. de scraping in 2015.

5. Zijn alle stappen van de verwerking in de zin van soorten gegevens en uitwisselingen, in kaart gebracht of te brengen, zodanig dat daardoor voor de betrokkenen inzichtelijk is bij wie, waarom en hoe de persoonsgegevens worden verwerkt?

Zie tabel IV: Stappen procedure vaststellen handhavingstekort verhuurders van accommodaties in bijlage 1.

6. Zijn er beleid en procedures voorzien voor het creëren en bijhouden van een verzameling van de persoonsgegevens die u wilt gaan gebruiken? Zo ja, hoe vaak en door wie zal de verwerking worden gecontroleerd? Omvat de verzameling een verwerking die namens u wordt uitgevoerd (bijvoorbeeld door een onderaannemer)?

Verwerking wordt niet uitbesteed. Binnen de Belastingdienst bestaat de notitie Juridisch Kader Internetonderzoek waarin is neergelegd dat gespecialiseerde teams, zoals het ISC, persoonsgegevens mogen creëren. Het ISC is daarom ook de partij die de internetscraping heeft uitgevoerd.

7. Is er sprake van overdracht van persoonsgegevens naar een (overheids)instantie buiten de EU/EER? Heeft dit land een niveau van gegevensbescherming dat als passend is beoordeeld door een besluit van de Europese Commissie of de Minister van Veiligheid en Justitie? Worden daarbij alle of een gedeelte van de persoonsgegevens doorgegeven?

n.v.t.

IV. Beveiliging en bewaring/vernietiging

Beveiliging

1. Is het beleid met betrekking tot gegevensbeveiliging binnen uw organisatie op orde? Zo ja, wie/welke afdeling(en) is/zijn binnen de organisatie verantwoordelijk voor het opstellen, implementeren en handhaven hiervan? Is dit beleid specifiek gericht op gegevensbescherming en gegevensbeveiliging?

Beveiliging is als onderdeel van integraal management en bedrijfsvoering een verantwoordelijkheid van het lijnmanagement op de diverse niveaus in de organisatie. Op het hoogste niveau binnen de Belastingdienst geldt de volgende verdeling van beveiligingsverantwoordelijkheden:

- *de eindverantwoordelijkheid ligt bij* Persoonsgegevens *alsook de verantwoordelijkheid voor bedrijfscontinuïteit;*
- *de verantwoordelijkheid voor personele veiligheid en integriteit bij de* Persoonsgegevens *het concernpersoneelsbeleid;*
- *de verantwoordelijkheid voor informatiebeveiliging bij* Persoonsgegevens Persoonsgegevens
- *de verantwoordelijkheid voor fysieke beveiliging bij het verantwoordelijke MT-lid van de Facilitaire Dienst*

Verantwoordelijk voor het opstellen van beleid is het directoraat-generaal Belastingdienst. In het Handboek Beveiliging Belastingdienst (HBB) is dit beleid vertaald in concrete acties en stappen om de informatiebeveiliging daadwerkelijk te realiseren. Voor implementatie van het beleid is het lijnmanagement verantwoordelijk. Het management wordt hierbij ondersteund door o.a. een adviseur informatiebeveiliging. Het beleid is gericht op het borgen van de gegevensveiligheid.

2. Indien (een deel van) de verwerking bij een bewerker plaatsvindt, hoe draagt u zorg voor de gegevensbeveiliging, en het toezicht daarop, bij die bewerker?

N.v.t.

3. Welke technische en organisatorische beveiligingsmaatregelen zijn getroffen ter voorkoming van niet-geautoriseerde of onrechtmatige verwerking/misbruik van (a) gegevens die in een geautomatiseerd format staan (bv. wachtwoord-bescherming, versleuteling, encryptie) en (b) gegevens die handmatig zijn opgetekend bv. sloten op kasten)? Is er een hoger beschermingsniveau om gevoelige persoonsgegevens te beveiligen?

De dienst is alleen toegankelijk voor gebruikers van wie het account is geverifieerd. Alleen geautoriseerde Belastingdienstmedewerkers hebben toegang tot de dienst. De middels internetscraping verzamelde internetgegevens zijn toegankelijk voor het projectteam. Deze gegevens zijn opgeslagen in een beveiligde omgeving. De behandelaars van de steekproef hebben uitsluitend toegang tot de informatie van de geselecteerde steekproefposten.

4. Welke procedures bestaan er in geval van inbreuken op beveiligingsvoorschriften, en voor het detecteren ervan? Is er een calamiteitenplan om het gevolg van een onvoorziene gebeurtenis waarbij persoonsgegevens worden blootgesteld aan onrechtmatige verwerking of verlies van persoonsgegevens af te handelen?

Interne Procedure Melding Datalek, te raadplegen via: http://intranet.belastingdienst.nl/belastingtelefoon-algemeen/files/2013/12/Procedure-Datalekken-Belastingdienst-versie-2.0.pdf

Bewaring/vernietiging

5. Hoe lang worden de persoonsgegevens bewaard? Geldt dezelfde bewaartermijn voor elk van de typen van verzamelde persoonsgegevens? Is het project onderworpen aan enige wettelijke/sectorale eisen met betrekking tot bewaring?

De reguliere archiefwettelijke bewaartermijnen zijn van toepassing (zie Selectielijst Belastingdienst). De lengte van de bewaartermijn is o.m. afhankelijk van het belastingmiddel waarvoor het betreffende persoonsgegeven is gebruikt.

6. Op welke beleidsmatige en technische gronden is deze termijn van bewaring vereist?

Zie vraag 5.

7. Welke maatregelen zijn voorzien om de persoonsgegevens na afloop van de bewaartermijn te vernietigen? Worden alle persoonsgegevens, inclusief log-gegevens, vernietigd? Is er controle op de vernietiging, en door wie?

Het projectteam is verantwoordelijk voor de vernietiging van alle verzamelde gegevens na afloop van de bewaartermijn.

V. Transparantie en rechten van betrokkenen

Transparantie

1.Is het doel van het verwerken van de gegevens bij de betrokkenen bekend of kan het bekend gemaakt worden? Wat is de procedure om betrokkenen indien nodig te informeren over het doel van de verwerking van hun persoonsgegevens?

Informatie over de verwerking van persoonsgegevens door de belastingdienst is te vinden op

https://download.belastingdienst.nl/belastingdienst/docs/belastingdienst_wet_bescherming_persoonsgegevens_al5331z2pl.pdf

https://www.rijksoverheid.nl/onderwerpen/persoonsgegevens

Op het moment dat de klantbehandeling aanvangt worden de betrokkenen d.m.v. een vragenbrief op de hoogte gebracht.

2. Indien u de persoonsgegevens direct van de betrokkenen verkrijgt, hoe stelt u hen van uw identiteit en het doel van de verwerking op de hoogte vóór het moment van verwerking?

Algemene verstrekking van informatie via

https://download.belastingdienst.nl/belastingdienst/docs/belastingdienst_wet_bescherming_persoonsgegevens_al5331z2pl.pdf

https://www.rijksoverheid.nl/onderwerpen/persoonsgegevens

3. Indien u de persoonsgegevens via een andere (overheids)organisatie verkrijgt, hoe zullen de betrokkenen van uw identiteit en het doel van de verwerking op de hoogte worden gesteld op het moment van verwerking?

N.v.t.

Rechten van betrokkenen

4. Indien u toestemming tot verwerking van persoonsgegevens aan de betrokkene vraagt (opt-in), kan de betrokkene deze toestemming dan op een later tijdstip weer intrekken (opt-out)? Bij een weigering toestemming te geven, of bij een dergelijke intrekking, wat is dan de implicatie voor de betrokkene?

N.v.t.

5. Via welke procedure hebben betrokkenen de mogelijkheid zich tot de verantwoordelijke te wenden met het verzoek hen mede te delen of hun persoonsgegevens worden verwerkt? Hoe worden derden, die mogelijk bedenkingen hebben tegen een dergelijke mededeling, in de gelegenheid gesteld hun zienswijze te geven?

Informatie over de verwerking van persoonsgegevens door de belastingdienst is te vinden op

https://download.belastingdienst.nl/belastingdienst/docs/belastingdienst_wet_bescherming_persoonsgegevens_al5331z2pl.pdf

https://www.rijksoverheid.nl/onderwerpen/persoonsgegevens

6. Hoe kan een verzoek van een betrokkene tot verbetering, aanvulling, verwijdering of afscherming van persoonsgegevens in behandeling worden genomen?

Informatie over de behandeling van een verzoek tot verbetering, aanvulling, verwijdering of afscherming van persoonsgegevens is te vinden op

https://download.belastingdienst.nl/belastingdienst/docs/belastingdienst_wet_bescherming_persoonsgegevens_al5331z2pl.pdf

https://www.rijksoverheid.nl/onderwerpen/persoonsgegevens

4 Aandachtspunten en aanbevelingen

Uit de beantwoording van de vragen blijken enkele aandachtspunten en aanbevelingen.

4.1 Identificatie

Het verdient aanbeveling om voor de identificatie een stappenplan op te stellen waarin objectieve criteria zijn opgenomen om de betrouwbaarheid (juistheid, nauwkeurigheid en actualiteit) te vergroten. Hiermee kunnen fouten worden voorkomen als gevolg van bijvoorbeeld te weinig gegevens, tussenpersonen of het gebruik van fake-namen.

In dat stappenplan zou eveneens moeten worden omschreven op welke manier en met welke diepgang sociale media mag worden ingezet bij de identificatie. Het projectteam heeft inmiddels gehoor gegeven aan deze aanbeveling en richtlijnen voor identificatie opgesteld (bijlage 3).

4.2 Gebruik gegevens Verkenning 2015

Voor de steekproef 2017 zullen in 2015 'gescrapete' gegevens worden gebruikt. Het doel van de verkenning in 2015 was een beeld te krijgen van de omvang van het handhavingstekort. Destijds zijn, met het oog op een nadere verdieping, de verzamelde gegevens bewaard om ze op een later tijdstip te kunnen vergelijken met de ingediende aangiften inkomstenbelasting over 2015. Dit is toen niet specifiek vastgelegd. Echter, aangezien het doel van het vervolgonderzoek (de steekproef 2017) in lijn ligt met het oorspronkelijk doel waarvoor de gegevens zijn verwerkt, is sprake van een rechtmatige verwerking.

4.3 Overige punten

- De gegevens van de steekproef moeten op een vaste plaats worden opgeslagen en dienen alleen toegankelijk te zijn voor de onderzoekers. De resultaten van het vervolgonderzoek worden zoveel mogelijk geanonimiseerd gepresenteerd;

Voor de steekproef dienen op voorhand afspraken gemaakt over het bewaren en vernietigen van gebruikte gegevens.

BIJLAGE 1

Tabel I: Gegevensverwerking persoonsgegevens scraping platformwebsite Airbnb 2015

Veldnamen	Betekenis	Nodig voor oa.:	Indien persoonsgegeven waarom noodzakelijk	Wat wordt niet inzichtelijk bij weglaten item?
Kamer Id	Nummer aan accommodatie toegekend op Webpagina	Accommodatie- aanduiding	Noodzakelijk voor koppeling aan gegevens webpagina	Geen koppeling meer met webpaginagegevens, geen bewijs meer, geen toerekening meer aan accommodatie mogelijk
Locatie	Plaats, Provincie, Land	Lokatiebepaling, identificatie	Noodzakelijk bij identificatie	Identificatie niet mogelijk
Straat	Straat	Lokatiebepaling, identificatie	Idem	Idem
Plaats	Plaats	Lokatiebepaling, identificatie	Idem	Idem
Provincie	Provincie	Lokatiebepaling, identificatie	Idem	Idem
Land	Land	Lokatiebepaling, identificatie	Idem	Idem
Prijs Per Nacht	Prijs per nacht in €	Omzetbepaling	Noodzakelijk bij omzet/inkomstenbepaling	Geen/moeilijke bepaling omzet/inkomsten
Aanbieder	Naam aanbieder (veelal (fake-) voornamen)	Identificatie	Idem	Idem
Verhuurder Id	Nummer aan Verhuurder toegekend op Webpagina	Koppeling met originele gegevens webpagina	Noodzakelijk voor koppeling aan gegevens	Geen koppeling meer met webpaginagegevens, geen bewijs meer, geen toerekening meer aan persoon mogelijk
Lid Sinds	Ingeschreven als aanbieder sinds <maand en jaar>	Omzetbepaling	Noodzakelijk bij omzet/inkomstenbepaling	Geen/moeilijke bepaling omzet/inkomsten
Aantal Personen	Aantal personen mogelijk in aangeboden accomodatie	Omzetbepaling	Idem	Idem
Weekprijs	Prijs accommodatie per week in €. Niet altijd ingevuld	Omzetbepaling	Idem	Idem
Prijs Per Maand	Prijs accommodatie per Maand in €. Niet altijd ingevuld	Omzetbepaling	Idem	Idem
Extra Personen	Prijs per nacht (na eerste persoon) in €. Of "geen kosten"of niet ingevuld	Omzetbepaling	Idem	Idem
Borg	Bedrag borg. Niet altijd ingevuld	Mogelijke aanwijzing verhuur	Idem	Idem
Schoonmaakkosten	Schoonmaakkosten in €. Niet altijd ingevuld	Mogelijke aanwijzing verhuur	Idem	Idem
Annulering	Annuleringsmogelijkheden: Streng, gemiddeld of flexibel	Bijzonderheid bewijs geen verhuur	Idem	Idem
Aankomst	Welkomsttijdstip eerste dag	Bijzonderheid	Idem	Idem
Vertrek	Uiterste vertrektijdstip laatste dag	Bijzonderheid	Idem	Idem
Slaapkamers	Aantal beschikbare slaapkamers	Omzetbepaling	Noodzakelijk bij omzet/inkomstenbepaling	Idem
Badkamers	Aantal beschikbare badkamers. Niet altijd ingevuld	Bijzonderheid	Idem	Idem
Bedden	Aantal beschikbare bedden. Niet altijd ingevuld	Omzetbepaling/Bijzonderheid	Noodzakelijk bij omzet/inkomstenbepaling	
Bed Type	Soort bed: echt bed, matras, luchtbed, slaapbank, sofa of niet ingevuld	Aanwijzing soort accommodatie	Idem	Idem
Aantal OBJ per verhuurder	Aantal objecten per verhuurder	Omzetbepaling	Noodzakelijk bij omzet/inkomstenbepaling	Idem

Tabel II: Verwerking persoonsgegevens i.v.m. identificatie verhuurder

Veldnamen	Voorbeelden	Nodig voor oa.:	Indien persoonsgegeven waarom noodzakelijk?	Wat wordt niet inzichtelijk bij weglaten item?
Verhuurders ID	1234567	Koppeling met de webpaginagegevens	Noodzakelijk voor koppeling met de webpaginagegevens	Geen koppeling meer met webpaginagegevens
Aantal objecten (in Excel)	93	Bepaling grootte belang		
Aantal objecten (op webpagina)	107	Idem		
Verschil in objecten	14	Idem		
URL profiel	https://www.airbnb.nl/users/show/123456	Identificatie	Bewijs voor identificatie	Geen bewijs identificatie
URL advertentie	https://www.airbnb.nl/rooms/123456	Identificatie	idem	Idem
Identificeerbaar?	Ja	Waarneming		
Nauwkeurigheid	100%	Nauwkeurigheid mate van identificatie (subjectief)		
Type subject	Ondernemer	Indicatie voor belastingheffing		
Na(a)(men) voluit subject(en)	Kees Klaas Douwe	Identificatie	idem	Idem
Naam onderneming	KeyNotOkay	Identificatie	idem	Idem
URL onderneming	https://www.keyNotokay.nl/	Identificatie	idem	Idem
Dossiernummer B.V.	123456789	Op basis van identificatiegegevens toegevoegd uit BVR? Of van de ondernemerssite afgehaald? Nodig voor koppeling aan de BD gegevens.	Koppeling met BD-ondernemers-systemen	Geen koppeling meer naar BD-ondernemerssysteme n mogelijk
Adres onderneming	Grote Gartmanplantsoen 35-6, Amsterdam	Identificatie	Bewijs identificatie	Geen bewijs identificatie
Telefoonnummer onderneming	+31(0)20 123456	Identificatie	Bewijs identificatie	Geen bewijs identificatie
Locatie (Google maps)	Hier (met maptoegang)	Identificatie	Bewijs identificatie	Geen bewijs identificatie
Informatie over Belastingheffing?	Indien aanwezig op site(s) van deze ondernemer	Aandacht voor heffingsinfo op ondernemerssite?		
BSN	<invullen>	Op basis van identificatiegegevens toegevoegd uit BVR. Nodig voor koppeling aan de BD gegevens.	Koppeling met BD-bestanden	Geen koppeling met BD-bestanden meer mogelijk
Fiscale toelichting	<invullen>	Eventuele fiscale opmerkingen voor verduidelijking fiscale positie		

Tabel III: Interne en externe bronnen van de toegevoegde gegevens

Naam bestanden	*Omschrijving inhoud*	*Ontvangers*	*Persoonsgegevens*	*Feitelijk doel van de gegevens*	*Wat wordt niet inzichtelijk bij weglaten item?*
Interne bronnen					
BVR (GBA)	Familierelaties (ingangs- en einddatum), rechtsvormcode, sofinummers, percentage aandeelhouderschap, NAW-gegevens, geboortedatum, overlijdensdatum, KVK-nummer, RSIN, beconnummers.	Pilotteamlid ISC	Ja	Identificatie	Geen identificatie
RAMbestanden	Aangiftegegevens OB, IH, VPB over 2014	Pilotteamtlid ISC	Ja	Omzetbepaling	Geen omzetbepaling
Externe bronnen					
Internetbronnen	Facebook, google, streetview enz.	Projectteamlid ISC	Ja	Identificatie	Geen identificatie

Tabel IV: Stappen procedure vaststellen handhavingstekort verhuurders van accommodaties

Stap	Tools/Dmv./reden/gevolg	Opmerkingen	Uitvoerder
Instellen scraper en uitvoeren scraping. Totaalbestand Nederland aangemaakt met gegevens uit de verhuurplatform-site	HTTrack, Outwit (Hub), WebDataExtractor	In 2015 uitgevoerd.	Pilotteamlid ISC
Willekeurige posten kiezen (300)	Excel	Testbestand samenstellen met willekeurige posten	idem
Willekeurige posten verrijken om identificatie mogelijk te maken	Internetonderzoek, Facebook, google Maps enz.	Hierbij is in een pilot in 2015 gebruik gemaakt van internetonderzoek naar identificatiemogelijkheden van de verhuurder. Een subjectief betrouwbaarheidspercentage geeft een indicatie over de betrouwbaarheid van de identificatieslag. Risico!! Koppeling mogelijk foutief ivm o.a. te weinig gegevens, tussenpersonen en fake-voornamen. Betrouwbaarheidstoets invoeren op objectieve punten	idem
Geïdentificeerde willekeurige posten koppelen aan dossiernummer/BSN/omzetgegevens/aangiftegegevens	Identificatie!	Van de 20 willekeurige posten die in 2015 zijn geselecteerd zijn 17 posten geïdentificeerd Ook omzet- en aangiftegegevens zijn toegevoegd.	idem
Beslissing verdiepingsslag ja/Nee	Interpretatie resultaten onderzoek willekeurige posten	Adhv de resultaten is het besluit genomen verder te gaan met het onderzoek naar het nalevingstekort.	idem
Posten geselecteerd voor verdiepingsslag		21739 objecten geselecteerd	idem
Koppeling met BVR ogv Voornaam, Straatnaam, woonplaats	13.685 hits met een BSN gekoppeld	Uiteindelijk 1818 treffers uniek op voornaam geselecteerd. Risico!!: Geen controle op de koppeling meer uitgevoerd!	Idem, Ehi Ci Team Data & Informatieanalyse
Ca. 300 posten koppelen met inkomsten/aangiftegegevens uit RAM (IH aangifte 2014)	Voor bepaling behandelaanpak/ nalevingstekort	**maatwerk**	Pilotteamlid
Taxgap/ Handhavingstekort vastgesteld		Afhankelijk van de uitslag vervolgactiviteiten ingesteld.	Idem.

BIJLAGE 2

Uitleg koppelingen verdiepingsslag

Op de velden uit de scrape-actie

VOORNAAM
STRAATNAAM
WOONPLAATS

Heeft de koppeling met BVR-gegevens plaatsgevonden, waarbij de volgende velden zijn gekoppeld:

SOFINUMMER
GEBOORTEDATUM
GESLACHT
VOORNAMEN
EERSTE_LETTER_VOORNAAM
EERSTE_VOORNAAM_BVR
NP_GEG_VOORLETTERS
EERSTE_VOORLETTER
VOORVOEGSELS
ACHTERNAAM
ADRES_STRAATNAAM
ADRES_HUISNR
ADRES_HUISNR_TOEV
ADRES_POSTCODE
ADRES_WOONPLTS

Hieraan zijn de volgende velden uit RAM gekoppeld:

JAAR	BRC_ENT	ONTVDATUM	
SOFINR	BRC_OMS_EN	DA_DAGTEK	
SOFINAAM	ECON_BRC	PC_HSNR	
DOSNR	BRC_OMS_FI	VA_PC_HSNR	
DOSNAAM	RV_CODE	WA_PC_HSNR	
SOFINR_P	RV_OMSCHR	VA_WA_GELK	
SOFINR_P_AG	RV_GROEP	UNIEK_SOFI	
TEAM_INDEL	VIP	UNIEK_DOS	
TEAMNW	BRONDATUM	BEC_AANG	
REGIOCODE	VERV_DOSFI	BEC_NM	
KANTID	SOFINRVERV	LTSTE_BEC	
KANTOOR	NATNR1	BEC_NMLTST	
KANT_O_WAS	NATNR2	EHI_SUBCAT	
DATUM_O_TM	VPB_BEGIN	EHI_SUBACT	
KANT_P_WAS	VPB_EIND	EHI_INDKO	
DATUM_P_TM	VOLGNROND	EHI_WEGING	
VERZ_GEBD	VPB_CODE	+ 863 velden met aangifte IH, VPB, OB gegevens 2014	

Hieruit is het volgende extract gebruikt om het zicht te krijgen op het fiscaal belang:

SOFINR	
SOFINAAM	
MC_03837	Woning waarde totaal 11xx (Box 3 woning)
MC_03838	Totaalwaarde overige onroerende zaken (Box 3 overige OZ)
MC_00146	Bruto resultaat uit "overige" werkzaamheden (ROW)
MC_03652	Verkoopprijs verkochte woning minus verkoopkosten
MC_02777	Eigen woningschuld verkochte eigen woning
MC_03653	Overwaarde verkochte eigen woning
MC_03654	Aankoopprijs gekochte woning
MC_03655	Kosten onderhoud verbouwing eigen woning
MC_00181	Totaal eigen woningschuld
MC_00186	Totaal huurwaardeforfait eigen woning (HWF)
MC_03694	Kapitaalverzekering spaarrekening beleggingsrekening eigen woning
MC_00184	Inkomsten uit tijdelijk verhuur eigen woning (Verhuuropbrengst)
MC_00182	Saldo inkomsten eigen woning
MC_00174	EW rente schulden kosten geldlening
MC_00177	Ew periodieke betalingen erfpacht

	opstal
MC_00173	Saldo aftrekposten eigen woning
MC_00172	Saldo EW
MC_00171	Saldo inkomsten kosten eigen woning (saldo EW)
MC_03695	Aandeel aangever in inkomsten eigen woning
MC_03695	Vrijstelling kapitaalverzekering spaar-beleggingsrekening eigen woning