

DPIA rapportage RIEC Bibob proces

Versiebeheer

Versie	Datum	Wijzigingen	Wie
0.3	02-09-2021	Oplevering eerste concept	5.1.2.e
1.0	22-12-2021	Oplevering definitieve versie	5.1.2.e

Inhoudsopgave

1. Inleiding.....	3
<i>Aanleiding en onderwerp van de DPIA</i>	<i>3</i>
<i>Doelstelling</i>	<i>3</i>
<i>Scope</i>	<i>3</i>
<i>Opbouw van de analyse</i>	<i>4</i>
2. Managementsamenvatting	5
3. Beschrijving Verwerking	6
<i>Systematische beschrijving van het proces</i>	<i>6</i>
<i>Systematische beschrijving van de verwerking</i>	<i>10</i>
<i>Persoonsgegevens</i>	<i>11</i>
4. Analyse privacy consequenties	13
<i>Inleiding</i>	<i>13</i>
<i>4.1 Governance</i>	<i>13</i>
<i>Inleiding</i>	<i>13</i>
<i>Feiten & analyse</i>	<i>13</i>
<i>Risico's en maatregelen</i>	<i>14</i>
<i>4.2 Grondslag & Doelbinding</i>	<i>15</i>
<i>Inleiding</i>	<i>15</i>
<i>Feiten & analyse</i>	<i>15</i>
<i>Risico's en maatregelen</i>	<i>16</i>
<i>4.3 Juistheid</i>	<i>17</i>
<i>Inleiding</i>	<i>17</i>
<i>Feiten & Analyse</i>	<i>17</i>
<i>Risico's en maatregelen</i>	<i>17</i>
<i>4.4 Dataminimalisatie</i>	<i>18</i>
<i>Inleiding</i>	<i>18</i>
<i>Feiten & Analyse</i>	<i>18</i>
<i>Risico's en maatregelen</i>	<i>19</i>

4.5 Opslag	21
Inleiding	21
Feiten & Analyse.....	21
Risico's en maatregelen	22
4.6 Bescherming.....	24
Inleiding	24
Feiten & Analyse.....	24
Risico's en maatregelen	25
4.7 Transparantie.....	26
Inleiding	26
Feiten & Analyse.....	26
Risico's en maatregelen	26
4.8 Cultuur	28
Inleiding	28
Feiten & analyse.....	28
Risico's en maatregelen	28
4.9 Ethische Aspecten	29
Inleiding	29
Analyse.....	29
Risico's en maatregelen	29
5. Advies en accordering	30
Aanbevelingen voor vervolg	30
Advies FG.....	31
Accordering.....	32
Bijlage A.....	33
A1. Documentatie.....	33
A2. Geïnterviewden	33

1. Inleiding

Aanleiding en onderwerp van de DPIA

Het RIEC is geen zelfstandige entiteit en het personeel werkzaam voor het RIEC is in dienst bij de verschillende convenantpartners¹. Deze convenantpartners zijn gezamenlijk verwerkingsverantwoordelijken in de zin van artikel 26 AVG zodra persoonsgegevens in RIEC-IS worden verwerkt. Voor het Bibob proces bij het RIEC is er sprake van een verwerking van strafrechtelijke en mogelijk bijzondere persoonsgegevens binnen het samenwerkingsverband tussen de convenantpartners. Wegens de gevoeligheid van deze gegevens is een DPIA uitgevoerd op het Bibob proces bij het RIEC.

Een DPIA is een middel om in kaart te brengen welke persoonsgegevens in een proces, systeem of organisatie verwerkt worden en wat hiervan de risico's voor betrokkenen zijn. Op 18 augustus 2021 is een DPIA-workshop gehouden om de benodigde informatie hiervoor op te halen. In Bijlage A is opgenomen wie aan deze bijeenkomst hebben deelgenomen. Dit rapport omvat de resultaten van deze DPIA.

Doelstelling

Deze DPIA rapportage schetst de eventuele privacy risico's van de onderhavige gegevensverwerking, en maatregelen die kunnen worden getroffen teneinde deze risico's te mitigeren.

In de DPIA wordt vooral gekeken naar de geplande maatregelen, waarborgen en mechanismen om de risico's te beperken, de persoonsgegevens te beschermen en aan te tonen dat aan de beginselen voor verwerking uit de AVG is voldaan. Deze DPIA is een momentopname. Bij nieuwe ontwikkelingen, zoals wijzigingen in wetgeving, verandering van processen, inzet van nieuwe technologie e.d. moet de DPIA worden herijkt. Ook dienen uitgevoerde DPIA's periodiek te worden herijkt (iedere 3 jaar).

Scope

5.1.2.d en 5.2.1.i

Buiten scope van de DPIA is de beleidsadvisering (of er een Bibob toets moet worden gedaan of niet), omdat er in dit proces geen persoonsgegevens worden verwerkt. Ook de signaalfunctie (naar aanleiding van door het RIEC verkregen informatie uit een Integrale Casus Analyse een bestuursorgaan te adviseren over de toepassing van de wet Bibob ter zake van een reeds eerder

¹ Alle convenantpartners zijn benoemd in het "Convenant ten behoeve van Bestuurlijke en Geïntegreerde Aanpak Georganiseerde Criminaliteit, Bestrijding Handhavingsschakelpunten en Bevordering Integriteitsbeoordelingen", versie september 2014, van het Landelijk Informatie en Expertise Centrum (LIEC).

verstrekke vergunning) wordt buiten scope gelaten. Deze DPIA ziet ook niet op de processen met betrekking tot uitvoering van de taken van de individuele bestuursorganen ter uitvoering van de Wet Bibob, alleen de verwerkingen die daadwerkelijk binnen het RIEC plaatsvinden vallen binnen scope. Tenslotte valt ook de verwijfsindex buiten de scope. Via de verwijfsindex wordt inzichtelijk gemaakt of een subject en/of object in een casus voorkomt. Dit gebeurt op basis van hit/no hit. Het idee is dat bij een hit contact wordt opgenomen met de desbetreffende RIEC. Hiermee wordt getracht om ‘shoppen’ langs gemeentes door criminelen op deze manier te signaleren. De verwijfsindex is geen onderdeel van de werkprocessen in RIEC Den Haag en wordt dus ook niet of nauwelijks gebruikt. Mogelijk gebruiken wel andere RIEC’s de verwijfsindex om objecten binnen dit proces te zoeken. Tijdens de DPIA sessie is gebleken dat op het gebruik van de verwijfsindex onvoldoende zicht is. Het is daarom raadzaam hier nog een analyse op uit te voeren.

Opbouw van de analyse

Dit document schetst de privacy risico’s binnen bovengenoemde scope en de te nemen maatregelen die het betreffende risico kunnen mitigeren.

De uitvoering van deze DPIA verloopt via de zes beginselen waaraan elke verwerking moet voldoen. Deze zes beginselen zijn Juisheid, Data minimalisatie, Opslag, Bescherming, Transparantie en Grondslag & doelbinding. Daarnaast zijn ook de thema’s ‘Governance’ en ‘Privacycultuur’ van belang.

Deze beginselen vormen de basis voor de uitvoering van deze analyse. Per thema worden eventuele risico’s geanalyseerd en wordt de impact van deze risico’s op de betrokkenen en het RIEC ingeschat. Daarnaast worden de maatregelen om de risico’s tot een acceptabel niveau terug te brengen beschreven. Hierbij wordt rekening gehouden met de haalbaarheid en maakbaarheid van deze maatregelen binnen de context van het RIEC. De eventuele acceptatie van risico’s of restrisico’s is de verantwoordelijkheid van de verwerkingsverantwoordelijke(n).

Voor elk van de thema’s zijn risico’s geïnventariseerd die voor het onderhavige onderwerp relevant kunnen zijn voor de gegevensbescherming binnen het RIEC. De aanwezige deelnemers aan de workshop hebben tijdens het uitvoeren van de risicoanalyse de belangrijkste risico’s benoemd en maatregelen geïdentificeerd.

Leeswijzer

Deze rapportage bestaat uit vijf hoofdstukken:

- Hoofdstuk 1: beschrijft ter inleiding de achtergrond, doelstelling en scope van de DPIA.
- Hoofdstuk 2: ‘managementsamenvatting’ waarin de belangrijkste onderdelen van de rapportage zijn opgenomen.
- Hoofdstuk 3: beschrijft het proces en hoe persoonsgegevens worden verwerkt binnen dat proces.
- Hoofdstuk 4: analyse van de onderhanden gegevensverwerking, inclusief geïdentificeerde risico’s.
- Hoofdstuk 5: aanbevelingen en advies.
- Bijlage A: overzicht van de bestudeerde documentatie en de geïnterviewde personen.

2. Managementsamenvatting

Wat zijn de belangrijkste risico's die in de analyse zijn geconstateerd? Welke maatregelen zijn hierbij van toepassing?

5.1.2.d en 5.2.1.i



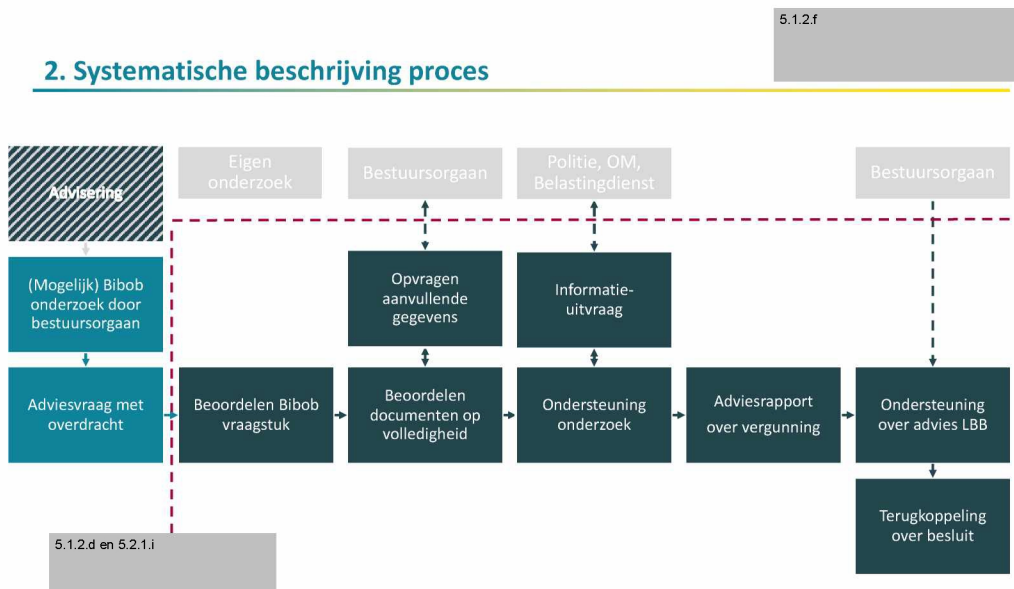
3. Beschrijving Verwerking

Dit hoofdstuk beschrijft het onderhavige proces en de verwerkingen van persoonsgegevens. De beschrijving van het proces en het inventariseren van de verwerkingen van persoonsgegevens zijn onderdeel geweest van de DPIA-workshop.

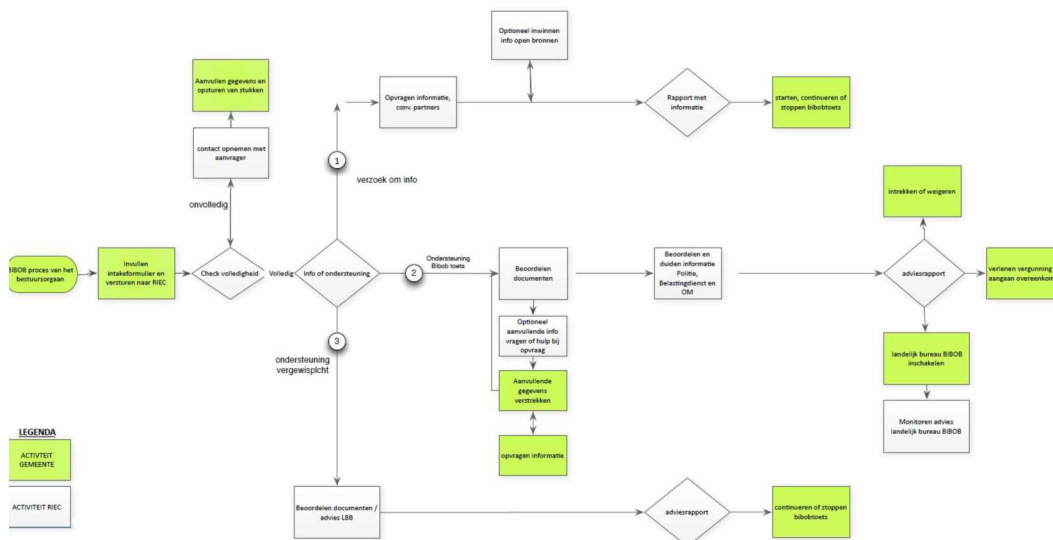
Systematische beschrijving van het proces

Het proces wordt door de volgende twee afbeeldingen schematisch weergegeven, waarbij beide afbeeldingen hetzelfde proces weergeven.

Figuur 1



Figuur 2



Een bestuursorgaan kan een Bibob onderzoek starten naar aanleiding van een aanvraag voor bijvoorbeeld het verlenen van een vergunning. Bestuursorganen kunnen hulp van het RIEC vragen bij het uitvoeren van een Bibob onderzoek. De ondersteuning in het Bibob proces die door het RIEC aan het bestuursorgaan wordt geleverd, is afhankelijk van de behoefte van het bestuursorgaan.

5.1.2.d en 5.2.1.i

In ieder geval dient er altijd een aanvraagformulier ingevuld door de aanvrager aanwezig te zijn. Een aanvraag kan zowel gegevens bevatten van de aanvrager als van derden. De aanvrager is de persoon die de initiële aanvraag heeft ingediend bij het bestuursorgaan. Over deze persoon of personen kan door het RIEC (namens het bestuursorgaan) of het bestuursorgaan zelf informatie bij convenantpartners worden opgevraagd. Derden zijn personen in het proces die niet zelf een aanvraag bij een bestuursorgaan hebben gedaan, maar die wel een rol spelen in het Bibob onderzoek.⁴ Gezamenlijk vormen de aanvrager en de derde(n) de betrokkenen binnen dit proces.

Vervolgens zijn er drie onderdelen in de ondersteuning bij het Bibob proces die het RIEC kan toepassen, waarvan het afhankelijk is van de behoefte van het bestuursorgaan welke van de stappen (of alle stappen) door het RIEC worden uitgevoerd. De stappen zijn hieronder beschreven:

1. *Ondersteuning Bibob toets*

Het RIEC kan het bestuursorgaan op aanvraag ondersteuning bieden bij het Bibob proces.

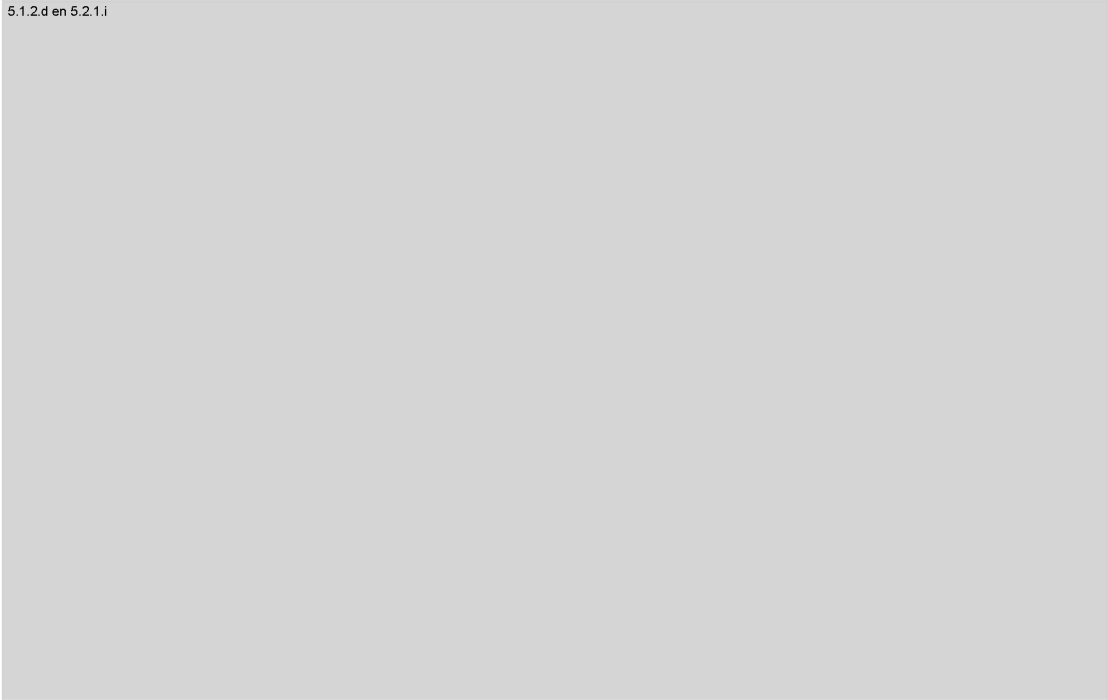
5.1.2.d en 5.2.1.i

² Een informatie verzoekformulier, zoals het hier bedoeld is, heeft niet met het recht op inzage (artikel 15 AVG) te maken.

³ Zo kan een medewerker van het RIEC signaleren dat het raadzaam is om een huurovereenkomst op te vragen en op deze manier de aanvraag aan te vullen.

⁴ Dit kan bijvoorbeeld een zakenrelatie zijn bij wie de betrokkene een lening heeft afgesloten.

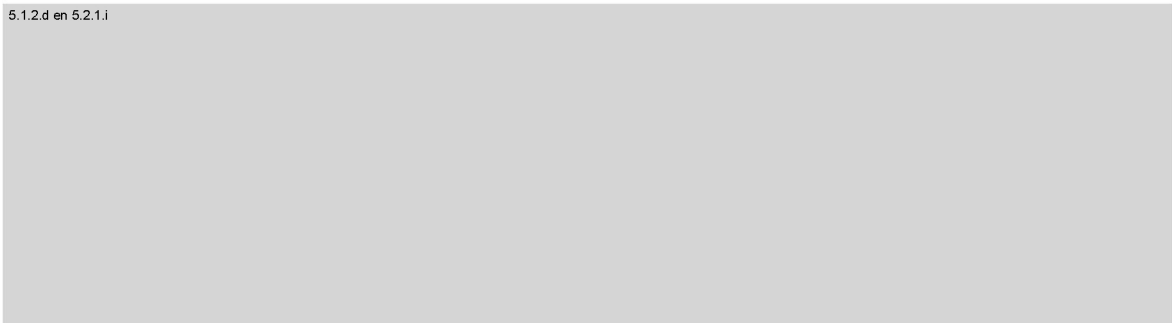
5.1.2.d en 5.2.1.i



De volgende stap bij de ondersteuning van de Bibob toets door het RIEC is het beoordelen van de aangeleverde documentatie op volledigheid en (juridische) juistheid. Wat betreft de juridische juistheid gaat het RIEC na of er inderdaad een grondslag aanwezig is voor de gegevens die zijn aangeleverd en daarmee ook of het dossier niet te veel informatie bevat. Als het verzoek om ondersteuning tevens een informatieverzoek bevat wordt deze gelijktijdig beoordeeld en uitgezet bij de convenantpartners (zie stap 2: informatieverzoek)

Het RIEC kan zelf ook informatie opvragen, zoals bij ‘half open bronnen’ indien er informatie ontbreekt. In principe zal eerst het bestuursorgaan gevraagd worden de gegevens aan te leveren, enkel bij uitzondering vraagt het RIEC deze gegevens op namens het bestuursorgaan. Hierbij kan gedacht worden aan de Kamer van Koophandel of het Kadaster, bijvoorbeeld om te controleren of de gegevens nog actueel zijn.

5.1.2.d en 5.2.1.i



Vervolgens kan het RIEC op verzoek van het bestuursorgaan een adviesrapport opstellen. In het adviesrapport verwijst het RIEC, indien van toepassing, naar het

eerder opgestelde verslag van bevindingen. Uit dit adviesrapport kunnen de volgende adviezen aan het bestuursorgaan volgen:

- Het zelf voortzetten van het Bibob proces met behulp van aanwijzingen van het RIEC;
- De gevraagde vergunning te verlenen/overeenkomst aan te gaan (eventueel met aanvullende voorwaarden);
- Er is sprake van een reguliere weigeringsgrond;
- De vergunning te weigeren of in te trekken dan wel de overeenkomst niet aan te gaan; of
- Het Landelijk Bureau Bibob (LBB) in te schakelen.

Bovendien bevat het adviesrapport een uitwerking van welke convenantpartijen persoonsgegevens over de betrokkene(n) hebben verstrekt, een samenvatting van de voor het dossier relevante persoonsgegevens en een duiding van de verstrekte informatie. Het advies wordt door de behandelend RIEC medewerker geregistreerd in

5.1.2.d en 5.2.1.i

2. Informatieverzoek

In deze stap vraagt het bestuursorgaan het RIEC om haar te ondersteunen bij het opvragen van informatie bij convenantpartners.⁵ Het uitgangspunt in deze stap is dat het bestuursorgaan zelf al relevante informatie heeft opgevraagd binnen de organisatie. Voor het opvragen van informatie bij de convenantpartners moet het bestuursorgaan te allen tijde de bijbehorende informatieverzoekformulier(en) invullen. Op grond van deze formulieren weten de convenantpartners over welke (rechts)personen ze informatie verstrekken en wat de juridische grondslag is.

5.1.2.d en 5.2.1.i

⁵ Let op: met informatieverzoek wordt hier niet bedoeld het informatieverzoek van betrokkene overeenkomstig de privacywet- en regelgeving.

5.1.2.d en 5.2.1.i

Het RIEC kan op verzoek van het bestuursorgaan informatie opvragen uit open bronnen en/of informatie opvragen bij de politie, de Belastingdienst en andere convenantpartners. Het RIEC kan in deze ondersteunende rol niet meer informatie opvragen dan het bestuursorgaan zelf zou kunnen opvragen.

5.1.2.d en 5.2.1.i

3. *Ondersteuning vergewisplicht*

Het bestuursorgaan dient zich van ervan te vergewissen⁶ dat het onderzoek van het LBB op zorgvuldige wijze heeft plaatsgevonden. Daarbij mag in beginsel van het advies worden uitgegaan, maar moet de overheidsinstantie wel onderzoeken of de feiten de conclusie kunnen dragen. Dat is bijvoorbeeld niet het geval als de feiten te weinig (directe) aanwijzingen voor de conclusie bieden of omdat ze in verschillende richtingen wijzen, onderling tegenstrijdig zijn of niet stroken met hetgeen overigens bekend is. Het RIEC kan het bestuursorgaan ondersteuning bieden bij dit onderzoek.

Een verzoek voor ondersteuning bij de vergewisplicht wordt telefonisch gedaan en/of via een e-mail aan het RIEC met daarin vermelding van het casenummer. Het uitwisselen van het LBB advies en eventueel bijbehorende documenten vindt plaats via RIEC-IS. Het verzoek bevat minimaal het advies van het LBB en kan daarnaast de gegevens bevatten die worden aangeleverd door het bestuursorgaan in het kader van een verzoek ondersteuning Bibob toets (zie stap 1: Ondersteuning Bibob toets).

5.1.2.d en 5.2.1.i

Het resultaat van deze stap is dat het bestuursorgaan de Bibob toets stopt of continueert.

Systematische beschrijving van de verwerking

Onderstaand een schematische weergave van de persoonsgegevens. Wat ontvang je (wat krijg je), wat verwerk je (wat doe je ermee) en wat verstrek je (wat geef je door).

⁶ Artikel 3:9 Algemene wet bestuursrecht (Awb).

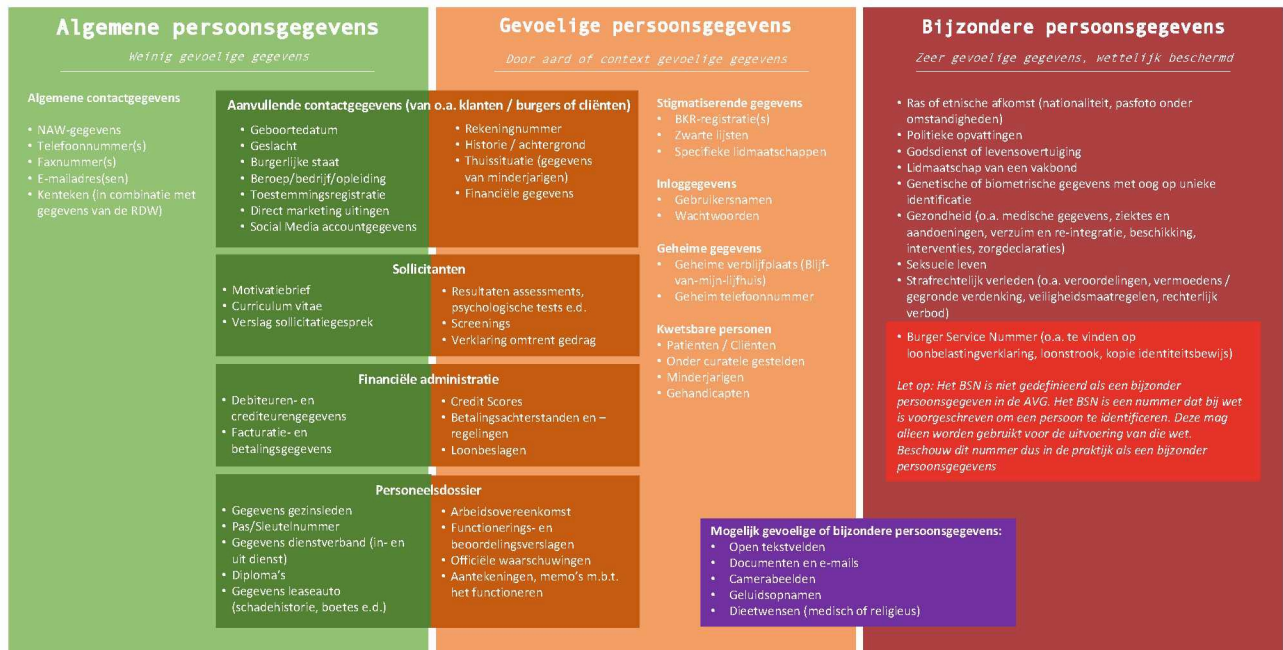
Wat krijg je	Van wie	Waar
Gegevens van betrokkenen en derden die worden aangeleverd door het bestuursorgaan in het kader van een verzoek ondersteuning Bibob toets (zie stap 1: Ondersteuning Bibob toets).	Bestuursorgaan	5.1.2.d en 5.2.1.i
LBB advies	Bestuursorgaan	
Strafrechtelijke en justitiële persoonsgegevens	Convenantpartner	
Financiële gegevens	Convenantpartner	
Casenummer	Dossier	

Wat doe je ermee	Middelen	Wie
Inzien aangeleverde gegevens	5.1.2.d en 5.2.1.i	Behandelend RIEC medewerker
Laten aanvullen door convenantpartners		Behandelend RIEC medewerker
Opstellen verslag/adviesrapport		Behandelend RIEC medewerker
Excel bestand met lopende zaken		Behandelend RIEC medewerker

Wat geef je door	Aan wie	Hoe
NAW gegevens (bij informatieaanvraag)	OM, politie, Belastingdienst	5.1.2.d en 5.2.1.i
Geboortedatum (bij informatieaanvraag)	OM, politie, Belastingdienst	
Gegevens onderneming: KVK uittreksel, ondernemersadres, vestigingsadres (bij informatieaanvraag)	OM, politie, Belastingdienst	
Verslag van bevindingen	Bestuursorgaan	
Adviesrapport	Bestuursorgaan	
Casenummer	Bestuursorgaan	

Persoonsgegevens

Wij hanteren de classificatie zoals weergegeven in onderstaande figuur om te bepalen welke persoonsgegevens worden verwerkt. Er wordt onderscheid gemaakt tussen weinig gevoelige gegevens (algemene persoonsgegevens), door de aard of context extra gevoelige gegevens (gevoelige persoonsgegevens) en zeer gevoelige gegevens die wettelijk extra beschermd zijn (bijzondere persoonsgegevens). Al naar gelang de situatie kunnen gegevens in verschillende categorie worden geplaatst.



Binnen de scope van deze DPIA worden de volgende categorieën van persoonsgegevens verwerkt van aanvragers of derden:

Algemeen	Gevoelig	Bijzonder
• NAW gegevens • Geboortedatum • Telecommunicatie- en internetgegevens en soortgelijke voor communicatie benodigde gegevens • Informatie over de organisatie en relatie persoon tot organisatie • KvK gegevens • Documenten (huurcontracten etc.) • Voertuiggegevens • Kadastrale gegevens • Gegevens die door het bestuursorgaan zijn verzameld met het oog op de toepassing van de Wet Bibob	• Financiële gegevens (inkomensgegevens) • Fiscale gegevens (waaronder ook vergrijpboetes en schulden⁷) • Gegevens van sociale media • Gegevens over eventuele huur van objecten (o.a. huurcontracten) • Gegevens opgevraagd bij convenantpartners	• Strafrechtelijke persoonsgegevens (waaronder politiegegevens (Wpg) en justitiële en strafvorderlijke gegevens (Wjsg)) • BSN • Gegevens betreffende de verblijfsstatus (mede omvattende gegevens omtrent visum of garantstelling) • Gegevens omtrent privaatrechtelijke en

⁷ Het gaat hierbij om bestuurlijke sanctioneringen en daarmee geen strafrechtelijke persoonsgegevens.

	• Handtekening aanvrager • Gegevens omtrent woonsituatie	bestuurlijke maatregelen of voornemens daartoe
--	---	--

4. Analyse privacy consequenties

Inleiding

Dit hoofdstuk beschrijft de resultaten uit de uitgevoerde DPIA per thema. Voor ieder thema geven we een korte toelichting en beschrijven wij de risico's, de impact van de risico's op de betrokkenen en het RIEC en de maatregelen die het RIEC kan treffen om de risico's tot een acceptabel niveau terug te brengen. Daarnaast worden ook de ethische aspecten die mogelijk spelen in dit hoofdstuk besproken.

4.1 Governance

Inleiding

Is helder wie de verantwoordelijke en de verwerker zijn en hoe wordt toegezien op een adequate bescherming van persoonsgegevens? Is er beleid gemaakt ten aanzien van privacy en wordt er intern gecontroleerd op naleving van dit beleid? Is duidelijk wie binnen de organisatie verantwoordelijk is voor privacy?

Feiten & analyse

Het RIEC is een samenwerkingsverband tussen convenantpartners. De convenantpartners zijn één of meer aangesloten partners bij de RIEC's en het LIEC. Dit volgt uit artikel 1.4 van het Convenant ten behoeve van Bestuurlijke en Geïntegreerde Aanpak Georganiseerde Criminaliteit, Bestrijding Handhavingssknelpunten en Bevordering Integriteitsbeoordelingen (hierna: convenant).

In het convenant zijn de samenwerkingsafspraken tussen de verschillende convenantpartners geregeld. Het convenant bevat afspraken die zijn gemaakt over onder meer de informatie-uitwisseling (artikel 5 van het convenant) en geheimhouding en beveiliging (artikel 6 van het convenant) van de gegevensverwerkingen.

Onder het convenant hangt het 'Privacyprotocol RIEC's-LIEC' (hierna: protocol). In het protocol staan onder meer de volgende zaken beschreven:

- Bevoegdheden en taken van de convenantpartners;
- Grondslagen van de verwerking per convenantpartner;
- Taken van de RIEC's en het LIEC;
- Werkwijze;
- In welke informatiesystemen informatie mag worden verwerkt;

- Welke persoonsgegevens worden verwerkt;
- Beveiliging; en
- Meldplicht datalekken.

De convenantpartners zijn afzonderlijke verwerkingsverantwoordelijke voor de persoonsgegevens die zij verstrekken aan het RIEC (artikel 11.1 van het protocol). De convenantpartners zijn conform artikel 26 AVG gezamenlijke verwerkingsverantwoordelijken voor de verwerking van persoonsgegevens die zij verwerken in de informatiesystemen van het RIEC in het kader van Bibob (artikel 11.2 van het protocol).

Onder het protocol vallen twee separate procedures: meldplicht datalekken en verzoeken rechten van betrokkenen. De procedures moeten door de RIEC's regionaal worden geïmplementeerd. De processen worden gecoördineerd door het hoofd RIEC (betrokken convenantpartner(s) informeren over datalek/AVG verzoek, plannen van een gezamenlijk overleg, zodat de betrokken bestuursorganen met elkaar in contact treden, etc.). Datalekken worden door het RIEC niet bij de Autoriteit Persoonsgegevens (AP) gemeld, maar door een convenantpartner wat als leidend bestuursorgaan is aangewezen. Wanneer het RIEC een datalek signaleert, geeft zij dit (eventueel met advies) door aan de betrokken convenantpartner(s).

Ieder RIEC heeft op grond van artikel 3.16 van het protocol een medewerker die belast is met de privacy advisering. De medewerkers van het RIEC zijn in dienst bij verschillende bestuursorganen. Binnen de scope van deze DPIA zijn de behandeld RIEC medewerkers, in het kader van het Bibob werkproces, in dienst bij/of ingehuurd via de gemeente Den Haag.

5.1.2.d en 5.2.1.i

Artikel 10.3 van het protocol benoemt bovendien specifiek welke persoonsgegevens er van betrokkenen mogen worden verwerkt.

5.1.2.d en 5.2.1.i

3

Risico's en maatregelen

Op basis van de analyse op het aspect *governance* zijn er geen risico's geïdentificeerd.

⁸ Op het moment van schrijven ligt de Wet gegevensverwerking door samenwerkingsverbanden ter behandeling bij de Eerste Kamer. In deze wet wordt mogelijk een clause opgenomen die dit verplicht.

4.2 Grondslag & Doelbinding

Inleiding

Het moet helder zijn wat het doel van de gegevensverzameling is, op het moment dat het RIEC deze verzamelt. Het doel moet ook in overeenstemming zijn met de normale werkzaamheden van het RIEC en onderbouwd zijn door één of meer wettelijke grondslagen.⁹

Feiten & analyse

Doel van de verwerking

Het algemene doel van de verwerking die het RIEC uitvoert in het kader van het Bibob proces is het bieden van ondersteuning aan de bestuursorganen die een aanvraag bij het RIEC indienen. Artikel 2.4 van het convenant benoemt dat de samenwerking tussen de convenantpartners onder meer als doel heeft de bevordering en ondersteuning van integriteitsbeoordelingen door het openbaar bestuur op grond van de Wet Bibob.

Wettelijke grondslag van de verwerking

De grondslag uit artikel 6 AVG die in het kader van dit proces van toepassing is, is artikel 6 lid 1 sub e AVG. De bestuursorganen vervullen een taak van algemeen belang op grond van de Wet Bibob. Artikel 28 lid 2 sub d jo. artikel 7a lid 6 Wet Bibob bepalen dat het bestuursorgaan bevoegd is om de gegevens die deze het in het kader van het eigen Bibob-onderzoek over betrokkene(n) heeft verzameld, te verstrekken aan een andere deelnemer van een regionaal samenwerkingsverband voor de aanpak van georganiseerde criminaliteit, voor zover deze gegevens noodzakelijk zijn voor het ondersteunen van het bestuursorgaan bij het toepassen van deze wet. De grondslag voor het ontvangen van de relevante persoonsgegevens van bestuursorganen is daarmee vastgelegd in de Wet Bibob. Artikel 7a lid 2 onderdeel c biedt bovendien de grondslag voor het verwerken van het Burgerservicenummer.

Daarnaast zijn op dit proces verschillende sectorale wetten van toepassing. Artikel 21 Wet politiegegevens (Wpg) jo. artikel 4:3 lid 1 sub l (L) van het Besluit politiegegevens (Bpg) bieden de grondslag voor het verstrekken van persoonsgegevens van strafrechtelijke aard door de politie aan de gemeente. De OM heeft een tipfunctie op grond van artikel 26 Wet Bibob. Deze artikelen vormen de uitzonderingsgrond voor de verwerking van strafrechtelijke persoonsgegevens op grond van artikel 10 AVG. Het RIEC geeft bij informatieverzoeken altijd aan op basis van welke grondslag gegevens worden opgevraagd. De verantwoordelijkheid voor het verstrekken van de juiste gegevens ligt bij de convenantpartners.

5.1.2.d en 5.2.1.i

⁹ De wettelijke grondslag is de rechtvaardiging om persoonsgegevens te mogen verwerken, zoals bedoeld in artikel 6 lid 1 e.v. van de Algemene Verordening Gegevensbescherming. De wettelijke grondslagen uit dit artikel zijn; toestemming, ter uitvoering van een overeenkomst, wettelijke plicht, vitale belang, taak van algemeen belang en het gerechtvaardigd belang.

Risico's en maatregelen

Op basis van de analyse op het aspect *grondslag en doelbinding* zijn geen risico's geïdentificeerd.

4.3 Juistheid

Inleiding

Is de kwaliteit van de gegevens gewaarborgd (actueel, juist en volledig)? Hoe worden gegevens over de personen verwerkt (handmatig of automatisch)? Vindt er controle op de datakwaliteit plaats en zo ja wanneer?

Feiten & Analyse

Het RIEC ontvangt de persoonsgegevens van het bestuursorgaan middels een aanvraag via RIEC-IS. De RIEC medewerker maakt hierbij een inschatting in welke mate de persoonsgegevens gevalideerd moeten worden. De medewerker doet in ieder geval altijd voor ieder van de processtappen een check op de volledigheid van de aangeleverde documentatie.

Ook maakt de RIEC medewerker een inschatting of er zaken zijn die opvallen aan het dossier. Op basis van deze inschatting kan een RIEC medewerker zelf nog een check uitvoeren. Wanneer sprake is van een verouderd KVK uittreksel is een nieuw uittreksel nodig om de informatie te valideren. In vrijwel alle gevallen zal eerst aan het bestuursorgaan worden voorgelegd om de actuele stukken aan te leveren. Als dit om een reden niet mogelijk is, heeft het RIEC een mogelijkheid om de gegevens op te vragen. Bij andere vragen of ontbrekende informatie neemt het RIEC contact op met het bestuursorgaan dat de aanvraag bij het RIEC heeft ingediend.

Risico's en maatregelen

Ten aanzien van het beginsel *Juistheid* zijn geen risico's geïdentificeerd.

4.4 Dataminimalisatie

Inleiding

Kan er met bijvoorbeeld minder persoonsgegevens, of op een andere manier worden gewerkt zonder de functionaliteit van het proces en systeem aan te tasten? Zijn er rapportages waarin tot individuen herleidbare informatie is opgenomen? Worden alleen die gegevens vastgelegd die absoluut noodzakelijk zijn voor het doel van de verwerking? Welke zijn dat niet?

Feiten & Analyse

In artikel 7a en artikel 7b Wet Bibob staat beschreven welke gegevens minimaal noodzakelijk zijn voor het eigen onderzoek van het bestuursorgaan. Het bestuursorgaan ontvangt deze gegevens van de betrokkene of kan deze uit openbare bronnen halen.

De persoonsgegevens die worden verwerkt in het kader van het Bibob proces, opgesomd in hoofdstuk 3 van deze rapportage, kunnen, afhankelijk van welke ondersteuning het RIEC biedt, noodzakelijk zijn voor het RIEC om te verwerken, teneinde het bestuursorgaan te ondersteunen bij de Bibob toets, een informatieverzoek en/of de vergewisplicht. Bij het verwerken van persoonsgegevens toetst de RIEC medewerker of de verwerking noodzakelijk is het voor het doel: ondersteunen van het bestuursorgaan.

Informatie over een betrokkene wordt in het Bibob proces van het RIEC stapsgewijs opgevraagd. Het is afhankelijk van de inschatting van de RIEC medewerker (op basis van professionele ervaring) of er, op basis van de door het bestuursorgaan aangeleverde informatie, nog aanvullende informatie moet worden opgevraagd. In de afweging van de RIEC medewerker worden het proportionaliteitsprincipe en het subsidiariteitsprincipe meegenomen. In plaats van het altijd opvragen van alle informatie die volgens de wet mag worden opgevraagd, wordt alleen extra informatie opgevraagd als de RIEC medewerker op basis van ervaring de inschatting maakt dat die informatie noodzakelijk is om een goed oordeel over de zaak te kunnen geven. Enkel de noodzakelijke gegevens worden hierdoor opgevraagd/verwerkt door het RIEC.

Het RIEC voert een check uit op de (juridische) juistheid van bepaalde informatie in een dossier (of een dossier informatie bevat die het op grond van de wet niet mag bevatten). Bevat een dossier te veel informatie, die het niet mag bevatten, dan koppelt het RIEC dit ook terug aan het bestuursorgaan.¹⁰ Het RIEC verwijdert de informatie daarna uit het betreffende dossier. Als het informatiedeling vanuit bijvoorbeeld de politie of het OM betreft is het uitgangspunt dat het RIEC deze informatie verifieert voordat het bestuursorgaan de informatie inziet. Doordat de gegevens die in de map zijn gezet, meteen inzichtelijk zijn voor het bestuursorgaan, is een tijdige verificatie niet altijd mogelijk.

5.1.2.d en 5.2.1.i

¹⁰ Er kan hier sprake zijn van een datalek door het bestuursorgaan.

5.1.2.d en 5.2.1.i



Risico's en maatregelen

Ten aanzien van het beginsel *dataminimalisatie* zijn de volgende risico's geïdentificeerd. Deze worden hieronder beschreven.

Risico: Kans op schending vertrouwelijkheid gegevens betrokkenen

Het risico bestaat dat de vertrouwelijkheid van de betreffende persoonsgegevens wordt geschonden door het vermelden van casenummers in het e-mailverkeer. Via de naam van de organisatie is het namelijk gemakkelijk te achterhalen wie hiervan de bestuurder/eigenaar is (bijvoorbeeld via het opvragen van een KvK uittreksel). Dit zorgt er bovendien voor dat er geen sprake meer is van een verwerking van gepseudonimiseerde persoonsgegevens via e-mail.

Maatregel

5.1.2.d en 5.2.1.i



5.1.2.d en 5.2.1.i



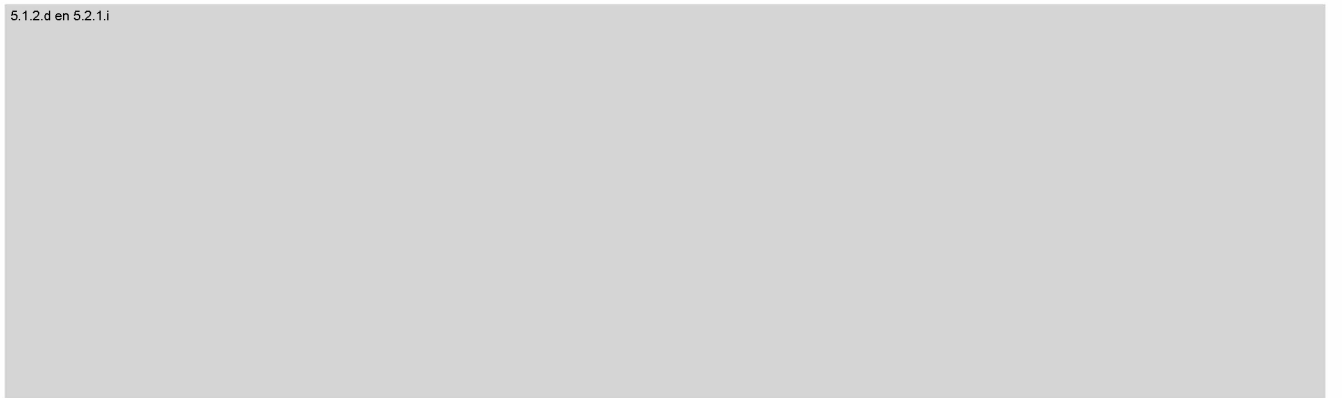
¹¹ Zo wordt bijvoorbeeld bijgehouden wat de status is van een informatieverzoek dat is uitgezet bij de convenantpartners.

RIEC Den Haag

Ons kenmerk

BD/

5.1.2.d en 5.2.1.i



4.5 Opslag

Inleiding

Welke bewaartermijnen zijn van toepassing? Hoe worden persoonsgegevens bewaard en worden persoonsgegevens die niet langer nodig zijn daadwerkelijk verwijderd? Worden op de middelen (desktop, pc, mobiele telefoon) zelf gegevens opgeslagen?

5.1.2.d en 5.2.1.i

Artikel 17 van het protocol gaat in op bewaartermijnen. Lid 2 benoemt dat persoonsgegevens gearcheveerd moeten worden zodra deze niet langer noodzakelijk zijn voor verwezenlijking van het doel van de verwerking en uiterlijk vijf jaar na de datum van de eerste verwerking. Lid 3 voegt hieraan toe dat de gearcheveerde gegevens gedurende een termijn van vijf jaar bewaard worden ten behoeve van verwerking met het oog op de afhandeling van klachten en de verantwoording van verrichtingen en vervolgens vernietigd. Het RIEC heeft nog geen gegevens vernietigd.

¹² Persoonsgegevens worden tegenwoordig niet meer per mail gedeeld. Dit gebeurde echter nog wel tot ongeveer 2020. Deze mappen bevatten daarom soms persoonsgegevens.

Op basis van dit artikel zijn nadere afspraken gemaakt over de bewaartermijnen. Indien na afronding van het adviesrapport de ondersteuning van het bestuursorgaan eindigt, zit de taak van het RIEC erop. Het is aan het bestuursorgaan, de politie, het OM en de Belastingdienst om de in dit kader door haar ingebrachte gegevens, conform haar eigen regelgeving, te bewaren voor zo lang als noodzakelijk. Deze ingebrachte gegevens moeten vervolgens bij het RIEC worden vernietigd.

5.1.2.d

Bestuursorganen hanteren eigen bewaartermijnen binnen het Bibob proces.

De opslag van persoonsgegevens vindt bovendien alleen plaats binnen de EER.

Risico's en maatregelen

Ten aanzien van het beginsel *opslag* zijn de volgende risico's geïdentificeerd. Deze worden hieronder beschreven.

Risico: Persoonsgegevens worden langer bewaard dan noodzakelijk

Door op dit moment geen gegevens definitief te vernietigen wordt er niet voldaan aan de verplichtingen uit zowel de AVG als het protocol. Er wordt derhalve niet voldaan aan het beginsel van opslagbeperking en het risico is hiermee dat gegevens (veel) langer worden bewaard dan noodzakelijk voor het doeleinde waarvoor zij verwerkt zijn.

Maatregel

Richt een procedure voor vernietiging in en bewaak bovendien dat de bewaartermijnen gehanteerd worden, bijvoorbeeld door periodieke controles uit te voeren op dossiers.

Vernietig de documenten die het RIEC ontvangt van andere convenantpartners zo snel mogelijk. Het RIEC verwerkt deze informatie in haar eigen documentatie (adviezen en rapporten), waardoor de noodzaak om de ontvangen documenten te bewaren verdwijnt.

Bepaal voor de eigen documentatie een passende bewaartermijn.

5.1.2.d en 5.2.1.i

5.1.2.d en 5.2.1.i

Risico: Informatie over casussen bevindt zich buiten RIEC-IS

In de communicatie via e-mail worden soms namen van de betreffende organisaties genoemd en er worden tijdelijk documenten op de netwerkschijf opgeslagen. Deze verwerkingen vinden plaats buiten RIEC-IS en de gegevens worden dus buiten de beheers- en gegevensbeschermingsmaatregelen, die op RIEC-IS van toepassing zijn, gedeeld.

5.1.2.d en 5.2.1.i

5.1.2.d en 5.2.1.i

Maatregel

Beperk de informatie over een dossier die buiten RIEC-IS wordt verwerkt. Zorg dat in de werkinstructie duidelijk wordt opgenomen dat gegevens enkel in RIEC-IS mogen worden opgeslagen en niet daar buiten (tenzij er nog aan een document wordt gewerkt) en breng dit onder de aandacht van de medewerkers. Ruim ook de netwerkschijf regelmatig op.

4.6 Bescherming

Inleiding

Persoonsgegevens moeten technisch en organisatorisch adequaat worden beschermd. Op welke wijze is de toegang tot gegevens afgeschermd? Is dit voldoende veilig in verhouding tot de gevoeligheid van de gegevens die verwerkt worden? Welke externe partijen hebben toegang tot de gegevens (leveranciers, samenwerkingspartners, dienstverleners) en hoe is de beveiliging daar geregeld?

5.1.2.d en 5.2.1.i

5.1.2.d

5.1.2.d

Iedere RIEC medewerker ondertekent een geheimhoudingsverklaring. De medewerkers van het RIEC die zich bezig houden met het Bibob proces proberen zo afgeschermd mogelijk te zitten, zodat een voorbijganger (niet zijnde een RIEC medewerker) niet direct kan zien waar de medewerkers aan werken.

5.1.2.d

5.1.2.d

Aanvragen/ondersteuningsvragen worden alleen uitgewisseld via 5.1.2.d. Wanneer het RIEC dit toch via e-mail ontvangt, wordt deze e-mail meteen verwijderd en wordt de verzender hierop aangesproken door het RIEC.

5.1.2.d

Risico's en maatregelen

Ten aanzien van het beginsel *bescherming* zijn de volgende risico's geïdentificeerd. Deze worden hieronder beschreven.

Risico: Integriteit onvoldoende gewaarborgd

De beheerders van de netwerkschijf met persoonsgegevens, in dienst van de gemeente Den Haag, zijn niet gescreend. Wel zijn zij in bezit van een VOG. Deze personen hebben via de netwerkschijf toegang tot (strafrechtelijke) persoonsgegevens van betrokkene(n). Wanneer de beheerders niet zijn gescreend brengt een mogelijk risico op onvoldoende waarborging van integriteit met zich mee. Wanneer personen gescreend zijn, is er meer zekerheid dat een persoon juist met persoonsgegevens zal omgaan.

Maatregel

Waarschijnlijk is er binnenkort per ministeriële regeling een uitbreiding van de VOG met VOG-P voor deze medewerkers mogelijk. Dit beperkt de kans op een onjuiste omgang met persoonsgegevens. Tot die tijd is het verstandig om bij de Gemeente Den Haag na te vragen welke beveiligingsmaatregelen er t.o.v. toegangsbescherming worden genomen en of dit voldoende is. Denk hierbij aan logging beheerderstaken, functiescheiding beheer netwerkschijf en beheer logging etc.

5.1.2.d en 5.2.1.i



5.1.2.d en 5.2.1.i



5.1.2.d en 5.2.1.i



5.1.2.d



4.7 Transparantie

Inleiding

Het RIEC is helder in de gegevens die zij verwerkt. De betrokkene moet goed kunnen begrijpen welke persoonsgegevens worden verwerkt (en waarom) en heeft het recht en de mogelijkheid om in te grijpen. De betrokkene heeft het recht op informatie, inzage, correctie en verwijdering.

Feiten & Analyse

De burger wordt door het bestuursorgaan niet in alle gevallen actief gewezen op de gegevensverwerkingen (delen van gegevens met het RIEC) die naar aanleiding van zijn aanvraag (kunnen) plaatsvinden. De verantwoordelijkheid voor de informatieplicht aan de burger ligt niet bij het RIEC, maar bij de individuele bestuursorganen.

Artikel 15.3 van het protocol gaat nader in op de rechten van betrokkenen. Daarnaast is er een werkproces “verzoeken rechten van betrokkenen”. Betrokkenen kunnen bij de convenantpartners een verzoek tot inzage, rectificatie of verwijdering indienen om met betrekking tot verwerkingsactiviteiten in het kader van de RIEC-samenwerking. Ook kan een betrokkene bezwaar maken tegen de verwerking. Het proces van beantwoording van verzoeken wordt gecoördineerd door het hoofd RIEC, maar de verantwoordelijkheid ligt bij de convenantpartner waar het verzoek wordt ingediend. Hierbij is het niet duidelijk of de verwerkingsverantwoordelijke (het bestuursorgaan) gehoor moet geven aan een inzageverzoek of dat de Wet Bibob hiervoor een uitzondering kent. Dit wordt daarom uitgezocht.

Risico's en maatregelen

Ten aanzien van het beginsel *transparantie* zijn de volgende risico's geïdentificeerd. Deze worden hieronder beschreven.

Risico (voor bestuursorgaan): Betrokkene is niet op de hoogte van gegevensverstrekking aan het RIEC

Doordat de betrokkene mogelijk niet in alle gevallen op de hoogte is van de verwerkingen van persoonsgegevens door het RIEC bestaat het risico dat er door het bestuursorgaan niet wordt voldaan aan het beginsel van transparantie (artikel 5 AVG) en de informatieplicht (artikel 12 e.v. AVG).

Maatregel

Een maatregel om dit risico te beperken is door in het aanvraagformulier op te nemen op welke wijze persoonsgegevens (mogelijk) verwerkt worden binnen het Bibob proces, waaronder verstrekking aan het RIEC/convenantpartners. Betrokkenen kunnen echter ook op andere wijze op de verwerking en hun rechten op grond van de AVG gewezen worden. Het is belangrijk dat de betrokkene weet waar en bij wie hij terecht kan voor vragen en de eventuele

uitoefening van zijn AVG-rechten, zoals het recht op inzage of verwijdering van gegevens. Het RIEC heeft een rol hierin om het bestuursorgaan hierop wijzen en ondersteuning te bieden om aan de informatieplicht te voldoen.

Risico (voor bestuursorgaan): Niet voldoende duidelijkheid over voldoen aan verzoeken van betrokkenen

Het RIEC draagt er zorg voor dat de ingewonnen informatie het gegeven advies kan dragen en dat in een latere fase het RIEC advies evt. bij de stukken ter inzage gelegd kan worden of ter beschikking gesteld kan worden indien de betrokkene een beroep doet op zijn inzagerecht krachtens de AVG of de Wet Bibob. Op dit moment is niet in alle gevallen duidelijk in hoeverre een bestuursorgaan moet voldoen aan verzoeken van betrokkenen, omdat het niet duidelijk is of de Wet Bibob een eventuele uitzondering biedt voor het voldoen aan verzoeken van betrokkenen. Hierdoor bestaat het risico dat er niet op een juiste wijze wordt voldaan aan verzoeken van betrokkenen door de bestuursorganen.

Maatregel

De verantwoordelijkheid voor het voldoen aan rechten van betrokkenen ligt bij het betreffende bestuursorgaan. De maatregel voor het RIEC in dit kader is om bestuursorganen te wijzen op de plicht om te voldoen aan de verzoeken van betrokkenen en de mogelijke uitzonderingen die de Wet Bibob hierop kan bieden. Indien er bij het bestuursorgaan geen onderlinge afspraken zijn gemaakt over de verzoeken van betrokkenen moet er een duidelijke procedure worden opgesteld en moet deze procedure ook worden vastgelegd.

4.8 Cultuur

Inleiding

Zijn medewerkers zich bewust van het belang van het beschermen van privacygevoelige gegevens? Gaat iedereen even zorgvuldig om met de gegevens, worden betrokkenen goed geïnformeerd over hoe men moet omgaan met die gegevens?

Feiten & analyse

Het RIEC besteedt op verschillende manieren aandacht aan privacy bewustwording binnen het Bibob proces. Zo is er een intensief inwerktraject voor alle medewerkers die ondersteuning (gaan) bieden bij de uitvoering van het Bibob proces. Dit inwerkproces omvat een introductie op de Wet Bibob, een presentatie over de werkzaamheden en een uitleg van het werkproces (inclusief instructie over het opslaan van de gegevens). Ook kijkt een ander behandeld RIEC medewerker de eerste keren met een beginnend RIEC medewerker mee (voor een dubbel check) als er bijvoorbeeld gegevens worden opgevraagd bij de politie, Belastingdienst of het OM.

In de documenten die het RIEC deelt met convenantpartners is een vertrouwelijkheidsclausule en een privacy disclaimer opgenomen om de convenantpartners te wijzen op het belang van de waarborging van privacy in het kader van de gegevens die uitgewisseld worden.

Wanneer er vergaderd wordt via Microsoft Teams worden dossiers alleen gecodeerd besproken. Hier vindt ook een zekere bewustwordingsactie naar bestuursorganen plaats door hen erop te wijzen wanneer zij niet gecodeerd een dossier bespreken.

Binnen het RIEC kan er in het algemeen gesproken worden van een grote aandacht voor integriteit. Dit komt bijvoorbeeld terug in het uitgebreide inwerktraject, de open cultuur waarin privacy issues besproken worden en de regelmatige trainingen die binnen het RIEC worden gegeven.

Risico's en maatregelen

Ten aanzien van het beginsel *Cultuur* zijn er geen risico's geïdentificeerd.

4.9 Ethische Aspecten

Inleiding

Zijn de belangen van de verwerkingsverantwoordelijke(n) in verhouding tot de belangen van de betrokkene(n)? Welke (publieke) waarden spelen een rol in dit proces? Hoe worden die gewogen?

Analyse

5.1.2.d en 5.2.1.i

Het Bibob proces vindt plaats ten behoeve van een bestuurlijke en geïntegreerde aanpak van georganiseerde criminaliteit, de bestrijding van handhavingsknelpunten en de bevordering van integriteitsbeoordelingen. Het proces heeft daarmee een maatschappelijke waarde om georganiseerde criminaliteit tegen te gaan en op die manier de samenleving te beschermen.

Bovendien geldt dat de mate waarin persoonsgegevens verwerkt worden binnen dit proces volledig volgt uit wet- en regelgeving. Zowel de Wet Bibob als het protocol en het convenant bieden duidelijke kaders welke persoonsgegevens wel en niet verstrekt en verwerkt mogen worden.

Risico's en maatregelen

Ten aanzien van de *Ethische aspecten* zijn er geen risico's geïdentificeerd.

5. Advies en accordering

In het risico overzicht dat als bijlage aan deze rapportage is toegevoegd wordt weergegeven welke privacy risico's de verwerking met zich meebrengt, welke beheersmaatregelen hiervoor nodig zijn en welke acties hieraan gekoppeld zijn. Dit overzicht wordt bewerkt zodra beheersmaatregelen worden uitgevoerd en risico's gemitigeerd, zo blijft de DPIA up to date ook na het uitvoeren van beheers acties.

Aanbevelingen voor vervolg

Wij adviseren om de hierboven genoemde risico's als volgt aan te pakken:

1. Benoem een business eigenaar van ieder risico in het risico overzicht en de bijbehorende maatregelen.
2. Geef de business eigenaar de opdracht de maatregelen in te voeren en daarmee het risico te mitigeren.
3. Geef periodiek een status update van de opvolging van deze aanbevelingen aan de FG en de Privacy Officer.

Advies FG

[GEBRUIK DEZE RUIMTE VOOR HET ADVIES VAN DE FG]

Naam: 5.1.2.e

Datum:

Accordering

Deze DPIA is opgeleverd aan:

Proceseigenaar	Functionaris Gegevensbescherming
Datum oplevering:	Datum oplevering:
Naam:	Naam: 5.1.2e
Voor akkoord:	Voor gezien:
Datum ondertekening:	Datum ondertekening:

Bijlage A

A1. Documentatie

De volgende documentatie is geraadpleegd.

Nr.	Documentnaam	Link
1	“Convenant ten behoeve van Bestuurlijke en Geïntegreerde Aanpak Georganiseerde Criminaliteit, Bestrijding Handhavingsknelpunten en Bevordering Integriteitsbeoordelingen”, versie september 2014, van het Landelijk Informatie en Expertise Centrum (LIEC).	https://www.riec.nl/maatregelen-en-documenten/documenten/convenanten/2014/09/01/convenant-tbv-bestuurlijke-en-geïntegreerde-aanpak-georganiseerde-criminaliteit
2	Privacyprotocol RIECs-LIEC	https://www.riec.nl/maatregelen-en-documenten/documenten/richtlijnen/2020/04/17/privacy-protocol-april-2020
3	Procesbeschrijving Bibob ondersteuning door bestuursorgaan	https://www.riec.nl/documenten/publicaties/2019/08/15/procesbeschrijving-bibob-ondersteuning-door-bestuursorgaan

A2. Geïnterviewden

De volgende personen hebben meegewerkt tijdens de DPIA sessie.

Datum	Geïnterviewden	Functie/Rol
18 augustus 2021	5.1.2.e	5.1.2.e
18 augustus 2021	5.1.2.e	5.1.2.e
18 augustus 2021	5.1.2.e	5.1.2.e

Betreft: advies DPIA RIEC BIBOB

Beste leden van de Stuurgroep RIEC-Den Haag,

Vorig jaar is de DPIA voor het werkproces Bibob bij het RIEC Den Haag ter advisering aan de FG's van de Belastingdienst, de Nationale Politie, de Gemeente Den Haag en het Openbaar Ministerie voorgelegd. Deze partijen zijn samen met de andere RIEC-partners gezamenlijke verwerkingsverantwoordelijken voor de verwerkingsactiviteiten die in RIEC-Den Haag verband plaatsvinden.

De FG's brengen individueel hun eigen organisatie en bestuurders op de hoogte met aandacht voor organisatiespecifieke omstandigheden. In deze brief treft u de belangrijkste organisatieoverstijgende bevindingen aan. Allereerst onze verontschuldigingen voor de vertraging van dit advies dat in totaliteit langer heeft geduurd dan u van ons mocht verwachten. Wij hebben onderling afspraken gemaakt om dit in de toekomst beter te stroomlijnen.

Samenvatting gezamenlijke bevindingen:

- In de DPIA is de noodzaak en evenredigheid voor het bestuursorgaan om het RIEC om ondersteuning te vragen nog onvoldoende aangetoond;
- De rechtmatigheid van het openbronnen onderzoek en van het delen van gegevens door de Belastingdienst is twijfelachtig;
- Onderdelen van de DPIA missen of zijn niet voldoende uitgewerkt, waaronder de uitwerking van de afspraken van de onderlinge samenwerking.

Advies:

Kort samengevat adviseren wij de stuurgroep om de rol van het RIEC in het Bibob-proces te heroverwegen en nadrukkelijk te bepalen wanneer de inzet van het RIEC en dus ook de RIEC-partners noodzakelijk is.

Hieronder worden bovenstaande punten uitgewerkt.

Noodzaak en evenredigheid

De inzet van het RIEC bij de toepassing van de Wet Bibob is al geruime tijd staande praktijk. Op de website www.riec.nl staat:

'Het RIEC kan het bestuur (vaak een gemeente) helpen met het opstellen van beleidsregels, de gemeente ondersteunen met de interpretatie van informatie en de gemeente van een advies voorzien. Bij gerede twijfel over de integriteit van de aanvrager kan de gemeente vervolgens advies vragen aan het Landelijk Bureau Bibob (LBB). Dit bureau beoordeelt hoe groot het risico op witwassen of criminele activiteiten is en stelt daarover een advies op. Zij hanteren daarbij een scherp beoordelingskader en kunnen breder onderzoek doen dan de gemeente of het RIEC en daarin een grotere kring van relevante (rechts)personen betrekken. De gemeente neemt als bevoegde instantie uiteindelijk eigenstandig het besluit tot weigering of intrekking.'

Volgens het Werkproces Bibob Ondersteuning Bestuursorgaan door het RIEC (versie 11 te vinden op de website www.riec.nl) (hierna Werkproces) kan de ondersteuning bestaan uit de volgende activiteiten:

- *Beleidsadvisering: het bestuursorgaan te laten delen in de expertise van het RIEC en deze desgevraagd van advies te dienen, bijvoorbeeld over het formuleren van het Bibob beleid of de toepassing van de wet Bibob. Bij beleidsadvisering worden geen persoonsgegevens uitgewisseld.*
- *Informatieuitvraag: het bestuursorgaan desgevraagd te assisteren bij het uitvragen c.q. opvragen van informatie bij andere convenantpartners die het bestuursorgaan nodig heeft in zijn Bibobonderzoek;*
- *Ondersteuning Bibobproces: het RIEC biedt desgevraagd ondersteuning bij de uitvoering van het Bibob onderzoek c.q. de Bibob toets van het bestuursorgaan;*
- *Signaalfunctie: naar aanleiding van door het RIEC verkregen informatie uit een Integrale Casus Analyse een bestuursorgaan te adviseren over de toepassing van de wet Bibob ter zake van een reeds eerder verstrekte vergunning.*

De Wet Bibob biedt in artikel 28 een bestuursorgaan de ruimte om indien noodzakelijk gegevens aan deelnemers aan het RIEC te verstrekken voor het ondersteunen van dit bestuursorgaan bij het toepassen van deze wet.

Uit de DPIA en nadere gesprekken komt naar voren dat het RIEC en de betreffende bestuursorganen niet nader hebben uitgewerkt wanneer de inzet van het RIEC noodzakelijk is. In praktijk komt erop neer dat de inzet van het RIEC Den Haag met name plaatsvindt wanneer sprake is van kennis- of capaciteitstekort bij het betreffende bestuursorgaan of wanneer bestuursorganen het lastig vinden om goede rechtstreekse ingangen bij anderen te vinden¹. De Bibob-specialist van het RIEC-Bureau verleent vooral assistentie in de vorm van expertise en het stroomlijnen van het proces. De betrokkenheid van de RIEC-partners beperkt zich tot het aanleveren van de gevraagde informatie. Er vindt geen integraal casusoverleg of iets vergelijkbaars plaats. Daarbij komt dat bestuursorganen, zeker sinds de recente wijziging van de Wet Bibob, waarin ook voor de Belastingdienst een speciale grondslag is gecreëerd, ook rechtstreeks informatie aan alle RIEC-partners kunnen vragen. Dat betekent dat er een minder ingrijpend alternatief voorhanden is.

Op basis van deze constatering komen wij als FG's tot de conclusie dat in de DPIA de noodzaak en evenredigheid voor het bestuursorgaan om het RIEC om ondersteuning te vragen nog onvoldoende is aangetoond.

Rechtmatigheid

Met betrekking tot de rechtmatigheid vallen twee zaken op. Ten eerste wordt op de website van het RIEC en in de DPIA de indruk gewekt dat door het RIEC zelfstandig nader (open) bronnenonderzoek of raadpleging van basisregistraties plaatsvindt. De DPIA toont echter niet aan wat hiervoor de rechtmatigheidsgrondslagen zouden zijn. Bovendien strookt deze werkwijze niet met het vastgestelde Privacyprotocol en Werkproces waarin niets over eigen bronnenonderzoek door het RIEC wordt vermeld². Desgevraagd is aangegeven dat bij het RIEC-Den Haag geen eigen bronnenonderzoek wordt verricht. De DPIA voor het RIEC Den Haag wordt op dit punt verduidelijkt.

¹ Dit volgt ook uit het Rapport 'De Wet Bibob en de toepassing hiervan in de gemeenten van de provincies Noord-Brabant en Zeeland' van 11 maart 2022 van Hogeschool Avans.

² In het wetsvoorstel Gegevensverwerking door Samenwerkingsverbanden is ook het uitgangspunt dat alleen gegevens afkomstig van samenwerkingspartners worden verwerkt.

Ten tweede valt op dat er gegevens van de Belastingdienst worden verwerkt terwijl de rechtmatigheid daarvan nog onvoldoende is aangetoond. Bovendien staat in het Werkproces het volgende vermeld:

'het RIEC kan in de ondersteunende rol niet meer informatie vragen dan het bestuursorgaan zelf zou kunnen vragen'

Dit betekent dat het RIEC Den Haag tot de recente wijziging van de Wet Bibob het RIEC niet conform het eigen werkproces heeft gehandeld. Met het oog op de rechtmatigheid is het van belang om na te gaan in hoeverre de huidige uitvoeringspraktijk waarbij (in de bijlage bij het Werkproces) concrete vragenlijsten worden gehanteerd in lijn is met het nieuwe artikel 7c van de Wet Bibob.

Overige aandachtspunten

Uit de DPIA komen nog enkele andere aandachtspunten naar voren. Ten eerste is er een betere beschrijving nodig van de categorieën personen en categorieën gegevens die worden verwerkt en wat de grondslag is om deze gegevens te verwerken. De DPIA bevat nu meer een beschrijving van de bronnen. Daarbij zou ook nadrukkelijk moeten worden vermeld welke gegevens als bijzondere persoonsgegevens, als strafrechtelijke persoonsgegevens (als bedoeld in artikel 10 van de AVG) of als unieke persoonsnummers (zoals BSN) moeten worden aangemerkt.

Ten tweede is onduidelijk in hoeverre relevante informatie uit eerder bij het RIEC uitgevoerde integrale casusanalyses wordt gebruikt.

Ten derde wordt in de DPIA niet vermeld hoe bij het RIEC Den Haag concreet invulling is gegeven aan de gezamenlijke verwerkingsverantwoordelijkheid. De afspraken van artikel 26 AVG zijn niet vermeld of bijgevoegd. Zo wordt niet vermeld welke afspraken over informatiebeveiliging zijn gemaakt of er een quick scan Informatiebeveiliging zoals bedoeld in de BIO (of vergelijkbare risico-analyse) is uitgevoerd en in hoeverre informatiebeveiligingsadviseurs van de

5.1.2.d en 5.2.1.i

5.1.2.d en 5.2.1.i

een punt van zorg. Zeker nu ook uit de DPIA naar voren komt dat het aan concreet beleid op het gebied van bewaren en vernietigen ontbreekt.

Deze aandachtspunten hebben grotendeels een landelijk karakter in die zin dat er in de ophanden zijnde 'blauwdruk DPIA RIEC' aandacht aan wordt besteed. Ons advies is om met uitzondering van de lokale benodigde maatregelen zoals op het gebied van informatiebeveiliging met het uitvoeren van deze aandachtspunten te wachten tot deze landelijk blauwdruk is vastgesteld en ter implementatie aan het RIEC Den Haag is aangeboden.

Hoe verder

Nu de noodzaak voor bestuursorganen om het RIEC bij hun Bibob-procedure te ondersteunen ons inziens onvoldoende is aangetoond is het de vraag hoe verder. Wij adviseren de stuurgroep om de rol van het RIEC in het Bibob-proces te herzien en nadrukkelijk te bepalen wanneer de inzet van het RIEC en dus ook de RIEC-partners noodzakelijk is.

Een mogelijke uitkomst zou kunnen zijn dat de ondersteuning door de Bibob-medewerker van het RIEC niet meer onder de gezamenlijke (verwerkings)verantwoordelijkheid plaatsvindt maar onder verantwoordelijkheid van het bevragende bestuursorgaan. Anders gezegd: de gemeente is dan zelf verantwoordelijk voor het uitvoeren van dit Bibob proces zonder dat het OM, de belastingdienst en de politie medeverwerkingsverantwoordelijk zijn.

Het inzetten van het RIEC is aangewezen wanneer er een noodzaak bestaat om een casus integraal met de RIEC-partners te bespreken. Bibob-ondersteuning komt in het wetsvoorstel Gegevensverwerking door Samenwerkingsverbanden niet als afzonderlijke activiteit van het RIEC terug. Er zal dus uiteengezet moeten worden wat maakt dat een Bibob casus integraal moet worden besproken om te onderbouwen dat het RIEC ingezet kan worden voor dit onderdeel.

Wij gaan er vanuit u hiermee voldoende te hebben geïnformeerd. Mochten er nog vragen zijn dan kan contact opgenomen worden met 5.1.2.e FG van de gemeente Den Haag.

Vriendelijke groet,

5.1.2.e FG Gemeente Den Haag

5.1.2.e FG Nationale Politie

5.1.2.e FG Openbaar Ministerie

Memo inzake reactie op advies FG's omtrent DPIA Bibob

Aan Stuurgroep RIEC
Datum 16 maart 2023
Betreft Agendapunt 6 - Reactie op advies FG's omtrent DPIA Bibob

U wordt gevraagd:

- Kennis te nemen van het advies van de functionaris gegevensbescherming van de Gemeente Den Haag, de Politie en het Openbaar Ministerie (hierna FG's) inzake de DPIA in het kader van het werkproces "Bibob Ondersteuning Bestuursorgaan door het RIEC" (hierna DPIA Bibob) en de reactie van het RIEC hierop.

De Stuurgroep RIEC wordt gevraagd in te stemmen met het voorstel van hoofd RIEC om als volgt op het advies te reageren:

- Ten aanzien van de informatie-uitvraag. Er zal in overleg met de politie worden gezien of dit kan worden voorgezet en of er dan aanvullende maatregelen nodig zijn. De informatie-uitvragen bij de belastingdienst zijn reeds voor uitkomen van het advies van de FG'en gestaakt omdat de belastingdienst een eigen proces heeft ingericht na wijziging van de wet Bibob.
- Ten aanzien van de adviesfunctie van het RIEC is in bijgaande notitie de algemene noodzaak nader onderbouwd. Daarnaast zal in vervolg bij elke ondersteuningsaanvraag door gemeenten bij het RIEC de noodzaak voor de ondersteuning worden onderbouwd. Dit wordt steekproefsgewijs gecontroleerd door de privacy-jurist van het RIEC.
- De overige aandachtspunten zijn in bijgaand memo geadresseerd.

Inleiding

Medio 2021 is er een Data Protection Impact Assessment (DPIA) uitgevoerd op het Bibob proces binnen het RIEC Den Haag. Deze DPIA is uitgevoerd door Verdonck, Klooster & Associates (VKA). De DPIA is ingezet om de privacyrisico's van het werkproces Bibob in kaart te brengen. De DPIA-bevindingen (privacyrisico's) zijn vastgelegd in een rapport. Dit rapport heeft voorzien van een reactie vanuit het RIEC voorgelegd in de stuurgroep RIEC van 8 december. Aanbevelingen die gedaan zijn in de DPIA zijn uitgevoerd. Inmiddels hebben de FG's van de gemeente Den Haag, Politie en OM de rapportage van bijgaand advies voorzien. Hieronder geven we per onderdeel van het advies een reactie.

Noodzaak en evenredigheid

De FG's concluderen dat de DPIA-rapportage dat de noodzaak en evenredigheid voor het bestuursorgaan om het RIEC om ondersteuning te vragen nog onvoldoende is aangetoond. Dit was inderdaad geen uitgebreid onderdeel van de DPIA. In bijgevoegd memo onderbouwen wij de noodzaak uitgebreider. Het is hierbij belangrijk om een onderscheid te maken tussen de informatie-uitvraag en de ondersteuning c.q. advisering in het Bibob proces.¹

¹ In de DPIA-rapportage wordt de informatieuitvraag omschreven als "informatieverzoek" en de ondersteuning Bibob proces als "ondersteuning Bibob toets".

Informatie-uitvraag

In het advies van de FG's komt naar voren dat de noodzaak en evenredigheid voor de informatieuitvraag niet kan worden aangetoond, des te meer nu het bestuursorgaan na wijziging van de wet Bibob (oktober 2022) de informatie ook rechtstreeks kan opvragen bij de Belastingdienst of Politie. Het RIEC-bureau heeft tot op heden de informatie-uitvragen uitgevoerd op verzoek van de Politie en Belastingdienst. Het uitvragen van informatie is als taak opgenomen in het landelijk vastgestelde werkproces voor de RIEC's. De rol die het RIEC uitvoerde voor de Belastingdienst was daarnaast opgenomen in een landelijke circulaire van het ministerie van Financiën. Sinds kort is hier een wijziging in opgetreden en per 1 maart 2023 zal het RIEC geen informatieverzoeken meer uitzetten bij de Belastingdienst. De aanleiding dat het RIEC-bureau voor het bestuursorgaan informatie uit ging vragen bij de eerdergenoemde RIEC-partners is gelegen in het feit dat bestuursorganen niet goed weten op basis van welke wettelijke grondslagen informatie mag worden opgevraagd. Daarnaast was voor de bestuursorganen ook niet altijd even duidelijk over welke personen informatie mag worden opgevraagd. Doordat een geheimhoudingsplicht rust op het Bibob dossier is de Politie niet in staat om te controleren of zij de informatie over de personen, genoemd in het informatieverzoek van het bestuursorgaan, mochten verstrekken. Het RIEC kan deze toets wel doen. Daarnaast verliep de verstrekking via onbeveiligde mail tussen het bestuursorgaan en de RIEC-partners. Door de informatieverzoeken via het RIEC te laten verlopen kan gebruik gemaakt worden van het beveiligde informatie-uitwisselingssysteem van het RIEC. In de praktijk is het dus wenselijk dat het RIEC-bureau ondersteunt om o.a. een rechtmatige gegevensdeling te borgen. In 2022 is door de Politie aangegeven dat zij deze werkwijze graag voortzetten. Inmiddels is de informatie-uitvraag bij de Belastingdienst aangepast. Naar aanleiding van het advies van de FG's zal met de Politie besproken worden of en hoe de werkwijze aangepast moet worden. De privacyfunctionaris van de Politie zal hierbij betrokken worden.

Ondersteuning Bibob proces

Met betrekking tot de ondersteuning van het Bibob proces, waarbij het RIEC desgevraagd ondersteuning biedt bij de uitvoering van het Bibob onderzoek c.q. de Bibob toets van het bestuursorgaan, is de noodzaak en evenredigheid voor het bestuursorgaan om het RIEC om ondersteuning te vragen onzes inziens aanwezig. De taak van de RIEC's staat omschreven in de wet Bibob (art 28) en is opgenomen in het RIEC-convenant. Daarbij is een landelijk werkproces afgesproken dat door alle RIEC's gevolgd wordt. De noodzaak voor uitvoering van deze taak door de RIEC's wordt onder meer onderbouwd door de wetgever. In de [memorie van toelichting](#) bij het conceptwetsvoorstel tot wijziging van de Wet Bibob naar aanleiding van de evaluatie van die wet, alsmede uitbreiding van de reikwijdte ervan en wijziging van enige andere wetten², wordt de ondersteunende rol van het RIEC omschreven. Uit de MvT blijkt onder andere dat de ondersteuning kan leiden tot een meer op criminogene branches toegespitste en een meer uniforme, zo lastenarm mogelijk, toepassing van de wet. Om te toetsen of de noodzaak aanwezig is, dient eveneens de behoeften van het bestuursorgaan in oogschouw te worden genomen. Zo zijn er bestuursorganen met onvoldoende kennis en kunde in huis. Deze bestuursorganen zullen eerder ondersteuning behoeven van het RIEC. Naar aanleiding van het advies van de FG's zal het bestuursorgaan in vervolg bij elke adviesaanvraag nader motiveren wat de

² Kamerstukken II 2010/11, 32676 nr. 3 (MvT).

noodzaak is voor de adviesaanvraag. De Bibob medewerker van het RIEC zal beoordelen of de noodzaak voldoende is gemotiveerd. Dit zal steekproefsgewijs door de privacy-jurist van het RIEC gecontroleerd worden. Voor de goede orde: het RIEC neemt geen taken van het bestuursorgaan over, wij bieden ondersteuning en het bestuursorgaan komt zelf tot besluitvorming.

Ten aanzien van de opmerking dat de Bibob taak van het RIEC niet in de concept Wet Gegevensverstrekking Samenwerkingsverbanden (verder WGS) is opgenomen geeft het ministerie van J&V aan dat dit niet nodig is de omdat de Wet Bibob als lex specialis boven de WGS gaat, wat een generieke wet is.

Rechtmatigheid

De punten in het advies onder het kopje “rechtmatigheid” zijn inmiddels opgelost. Door het RIEC-bureau wordt namelijk niet zelfstandig (open) bronnenonderzoek gedaan of het basisregister geraadpleegd. Blijkbaar staat dit nog wel op de website van het LIEC. Er is contact geweest met het LIEC om dit aan te passen.

Overige aandachtspunten

De FG's noemen nog een aantal overige aandachtspunten:

- Er is een betere beschrijving nodig van de categorieën personen en categorieën gegevens die worden verwerkt en wat deze grondslag is. Dit zal worden toegevoegd aan de DPIA-rapportage.
- Het is onduidelijk in hoeverre relevante informatie uit eerder bij het RIEC uitgevoerde integrale casusanalyses wordt gebruikt. Dit ziet op de signaalfunctie van het RIEC-bureau zoals omschreven in het werkproces ‘Bibob ondersteuning Bestuursorgaan door RIEC’. Uit het werkproces Integrale Casusanalyse kunnen feiten en omstandigheden naar voren komen die duiden op een mogelijk gevaar. Het RIEC geeft het bestuursorgaan dan een signaal met de aanbeveling ter zake van een beschikking of overeenkomst het Bibob proces te starten. Het signaal in het interventieadvies is het resultaat van het werkproces Integrale Casusanalyse. Het interventieadvies omvat het advies aan het bestuursorgaan om een interventie in te zetten: de Bibob toets. Om die reden wordt de beschrijving van dit proces in de DPIA buiten beschouwing gelaten en verwijzen wij naar het werkproces Integrale Casusanalyse.
- De overige aandachtspunten die worden genoemd door de FG's hebben ook onze aandacht. De DPIA en het advies van de FG's behorende bij deze DPIA is doorgestuurd naar het LIEC. De genoemde aandachtspunten hebben namelijk een landelijk karakter en worden ook benoemd in de ‘blauwdruk DPIA RIEC’. Het advies van de FG's om te wachten tot de landelijke blauwdruk is vastgesteld nemen we over. Aanvullend voeren we een overleg met de informatiebeveiligingsspecialisten van het LIEC en de gemeente Den Haag.
- De FG's geven aan bij ‘hoe verder’ dat het inzetten van het RIEC is aangewezen wanneer er een noodzaak bestaat om een casus integraal met de RIEC-partners te bespreken. Daar is geen sprake van als het gaat om het werkproces ‘Bibob ondersteuning Bestuursorgaan door RIEC’. Zoals reeds benoemd in deze notitie, is de taak van de RIEC's omschreven in de Wet Bibob (art. 28) en is opgenomen in het RIEC-convenant. Daarbij is een landelijk werkproces afgesproken dat door alle RIEC's gevolgd wordt. De noodzaak voor uitvoering van deze taak door de RIEC's wordt onder meer onderbouwd door de wetgever.



Inleiding Pre-scan DPIA (Data Protection Impact Assessment)

Versie: 3.4 definitief
Datum: 1 maart 2022
Regime: Becommentarieerde praktijk
Opdrachtgever: Privacy Adviseur Rijk en Directeur CIP

Versie 3.0 definitief van dit format Pre-scan DPIA is een samenvoeging van het format DPIA pre-scan, versie 1.1. d.d. 26 maart 2021 van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) en van het format Pre-scan PIA versie 2.0, d.d. oktober 2020 van het Centrum Informatiebeveiliging en Privacybescherming (CIP).

Organisaties kunnen het format Pre-scan DPIA organisatiespecifiek maken met gebruikmaking van de Creative Commons-licentie Naamsvermelding-GelijkDelen (CC BY SA). Zie hiervoor het onderstaande item Creative Commons.

Haal de beveiliging van het gewenste tabblad af (Excel 2016: Bestand/Werkmap beveiligen). Pas bijvoorbeeld het organisatielogo aan en maak voorbeelden organisatiespecifiek. Let goed op dat je geen formules kopieert of verwijdert, waardoor de uitkomst bij item 7. Resultaat Pre-scan DPIA of de melding 'Nog niet alle bovenstaande beoordelingscriteria zijn doorlopen' op het tabblad Pre-scan DPIA incorrect werken. Maak de kolommen D t/m H uit het tabblad Pre-scan DPIA zichtbaar. De betreffende formules worden getoond. Let ook op bij het kopiëren dat je geen toelichtingen onbedoeld kopieert.

Blokkeer bij voorkeur de vaste tekst in alle werkbladen (Excel 2016: rechtermuisknop, celeigenschappen, tabblad Bescherming), zodat deze tekst niet aangepast kan worden. Ook velden, waarin op basis van de geselecteerde teksten en antwoorden, automatisch teksten en uitkomsten verschijnen, blokkeer je. Invulvelden en selectievelden (tekst die wordt ingevuld) blokkeer je juist niet. Verberg de kolommen D T/m H.

Beveilig de Pre-scan DPIA na de modificatie, indien gewenst met een wachtwoord. Alleen invulvelden kunnen worden bewerkt en antwoorden kunnen worden geselecteerd. Naast het beveiligen van elk werkblad kan ook de werkmappenstructuur worden beveiligd.

Sla het bestand op als een Excel-sjabloon (.xltx), zodat het format intact blijft. Test de werking van de formules en controleer alle toelichtingen.

Disclaimer

Het CIP betracht zorgvuldigheid bij het samenstellen van zijn publicaties. Het kan voorkomen dat er toch sprake is van omissies, onjuistheden en/of gedateerdheid. Het is altijd de verantwoordelijkheid van de lezer zelf dit te beoordelen en desgewenst te corrigeren indien hij zich baseert op of gebruik maakt van een CIP-publicatie. Het CIP ontvangt graag correctieverzoeken en suggesties.

Considerans

CIP-producten steunen op kennis van professionals uit verschillende organisaties actief in het CIP-netwerk, zowel uit de overheid als de markt. Opmerkingen en aanvullingen kun je melden op cip-overheid.nl/contact.

Creative Commons



© Centrum Informatiebeveiliging en Privacybescherming. Het CIP heeft voor deze publicatie licentie Creative Commons Naamsvermelding-GelijkDelen 4.0 Internationaal (CC BY-SA 4.0) verleend. Voor meer informatie zie: <https://creativecommons.org/licenses/by-sa/4.0/deed.nl>.

Aanleiding

Je hebt een beeld gevormd van de beoogde verwerking. Je wilt inzicht krijgen of er hoge privacy-risico's zijn die de beoogde verwerking oplevert voor de betrokkenen. Hoe bepaal je of er sprake is van een verwerking met waarschijnlijk een hoog risico voor de betrokkenen? Om dit vast te kunnen stellen, zijn in het tabblad Pre-scan DPIA verschillende bronnen bijeengebracht die een handreiking bieden om eenduidig en gestructureerd te kunnen vaststellen of een verwerking waarschijnlijk een hoog risico inhoudt.

Voorafgaand aan het uitvoeren van een Pre-scan DPIA kan al duidelijk zijn dat het gaat om een beoogde verwerking met een hoog privacy-risico voor de betrokkenen. Het advies is om de Pre-scan DPIA in zijn geheel uit te voeren. Het geeft een overzicht van diverse hoog risico's. Wellicht ook risico's waar je in eerste instantie niet aan hebt gedacht.

Wat is een Pre-scan DPIA?

Het format Pre-scan DPIA is een gestandaardiseerde wijze om tot een afgewogen inschatting te komen. De uitkomst van de Pre-scan DPIA neemt de vraag weg, of de beoogde verwerking resulteert in een hoog privacy-risico voor de betrokkenen. Dus voor welke verwerkingen is het uitvoeren van een DPIA nodig.

Verder is de Pre-scan DPIA een verantwoordingsinstrument. Je maakt aantoonbaar dat je aan AVG-artikel 35 voldoet. Hiermee sluit je de cirkel van 'Tel me, Show me en Proof me'.

Met een DPIA wordt vervolgens onderzocht en vastgelegd wat de risico's zijn van de verwerking voor de privacy van de betrokkenen en welke beheersmaatregelen passend zijn voor deze risico's. Is een DPIA niet nodig, voer de overige privacy-taken uit, zoals het opnemen van de verwerking in het verwerkingsregister, beveiliging in het ontwerp meenemen (Privacy by Design) etc.

Uitgangspunten

De Pre-scan DPIA voer je uit indien:

- het gaat om persoonsgegevens;
- er sprake is van een geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens of het gaat om persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om in een bestand te worden opgenomen;
- je verwerkingsverantwoordelijke bent;
- het gaat om een beoogde verwerking (tenzij het gaat om achterstallig onderhoud);
- er een beeld is gevormd van de beoogde verwerking.

Instructie Pre-scan DPIA (Data Protection Impact Assessment)

Een privacy-professional faciliteert bij voorkeur de Pre-scan DPIA. Hij/zij heeft kennis van de privacy-begrippen en de privacy-processen. Zo wordt voorkomen dat er onjuiste en onvolledige inschattingen worden gemaakt, die in een later stadium negatief effect kunnen hebben op de betrokkenen of de eigen organisatie. De Pre-scan DPIA kan ook gefaciliteerd worden door een projectleider, lijnmanager, procesmanager of systeemeigenaar. In dat geval zorg dat bij de uitvoering van de Pre-scan DPIA een Privacy-professional actief betrokken is. Betrek bij voorkeur in deze fase al de Functionaris Gegevensbescherming (FG). De FG heeft een formele adviesrol als het gaat om een DPIA.

Geef bij elk beoordelingscriterium uit het tabblad Pre-scan DPIA aan of deze van toepassing is, ook al weet je dat de beoogde verwerking een hoog privacy-risico voor betrokkenen heeft. Mogelijk zijn er nog meer hoog risico's waar je in eerste instantie geen rekening mee hebt gehouden. Bij item 7. Het resultaat Pre-scan DPIA in het tabblad Pre-scan DPIA wordt pas na het doorlopen van alle beoordelingscriteria de definitieve uitkomst (of er wel of niet een hoog risico voor de betrokkenen is) getoond.

Ben je niet werkzaam voor de Rijksoverheid, beantwoord de vragen: 3. Ontwikkeling van beleid en regelgeving, 4. Groot politiek-bestuurlijk en maatschappelijk vraagstuk en 5. Grootschalig project met ICT-componenten met nee, tenzij je deze vragen wilt adopteren. Dit zijn verplichte beoordelingscriteria voor de Rijksoverheid.

Het invulformulier bevat toelichtingen en voorbeelden ter ondersteuning van het correct inschatten van beoordelingscriteria. De toelichtingen zijn herkenbaar aan de rode driehoek rechts bovenin een cel. Door met de muis over de cel te bewegen, komt de toelichting in beeld. Wil je informatie naar de herkomst van de informatie uit de toelichting, ga dan naar tabblad Bronvermelding.

Print de ingevulde Pre-scan DPIA (het gegevensbereik is ingesteld). Laat de Pre-scan DPIA ondertekenen door de verantwoordelijke(n) van de verwerking, bijvoorbeeld de Gegevens eigenaar. Stuur een kopie van de getekende Pre-scan DPIA naar de betrokkenen. Het origineel van de Pre-scan DPIA bewaart de verantwoordelijke van de verwerking.

Is er na ondertekening van de Pre-scan DPIA een wijziging in omstandigheden, doorloop de Pre-scan DPIA opnieuw. Denk bij wijziging in omstandigheden bijvoorbeeld aan:

- de intentie om een nieuwe technologie te gebruiken.
- de methode voor de verzameling van de persoonsgegevens zal veranderen.
- de omvang van de verzamelde persoonsgegevens verandert.
- een onderdeel van het verwerkingsproces wijzigt.
- de organisatie- of maatschappelijke context verandert.

Zijn er geen wijziging in omstandigheden? Herhaal dan de Pre-scan DPIA periodiek.

Pre-scan DPIA (Data Protection Impact Assessment)

Algemeen

Titel voorgenomen verwerking:
Toelichting op deze verwerking:

Informatiebeeld Buitengebied Het betreft een project vastgesteld onder de Stuurgroep onder de werktitel "Projectplan thema's ontwikkelingsstrategie Weerbaar Buitengebied" en wordt uitgevoerd onder het werkproces "Gebied/wijkscan en nulmeting" binnen enkele gebieden binnen deelnemende gemeenten met een groot buitengebied. Dit gebied is zeer lastig toezicht op te houden voor gemeenten. Er worden minimale gegevens van de KvK over bedrijvigheid, BAG over panden, WOZ-waarde en leegstandsgegevens van gemeenten verwerkt en geanalyseerd middels een beproefde handreiking uit regio Oost-Nederland. Het doel is om binnen de gemeenten postcodegebieden (postcode 6 niveau) aan te kunnen wijzen waar de score op vooraf geformuleerde indicatoren hoger is, hetgeen wijst op een mogelijke aanwezigheid van kwetsbaarheden voor (ondermijnende) criminaliteit. De gemeenten kunnen hun interventies, zoals communicatie of toezichtcapaciteit, daarmee effectiever inzetten. In het document "Methodiek" is de werkwijze en de noodzaak van de gegevenstypen onderbouwd. Er wordt niet tot personen herleidbaar verwerkt, wel tot onroerende zaken en bedrijven, maar dat wordt geaggregeerd tot postcode 6 niveau. De maatregelen die getroffen zijn betreffen: minimalisatie van regio's, de verwerking vindt plaats bij de Provincie intern, het delen van gegevens gaat via RIEC-IS, de gegevens worden direct na ontvangst geaggregeerd.
3 oktober 2023
Versie 0.5

Invuldatum Pre-scan DPIA:
Versie Pre-scan DPIA:
Status Pre-scan DPIA:

1. AP-lijst met hoog risico verwerkingen

Geef bij elke verwerking aan of dit wel of niet van toepassing is op de voorgenomen verwerking.

Score Ja op lijst hoog risico?

1.1 Heimelijk onderzoek

Grootschalige verwerkingen en/of stelselmatige monitoring van persoonsgegevens waarbij informatie wordt verzameld met onderzoek zonder de betrokkene daarvan vooraf op de hoogte te stellen.

Nee

0

0

Bij heimelijk controle door werkgevers om diefstal of fraude door werknemers te bestrijden. Ook incidentele gevallen vanwege de ongelijkwaardige machtsverhouding tussen de betrokkene (werknemer) en de verwerkingsverantwoordelijke (werkgever).

Nee

0

1.2 Zwarte lijsten

Verwerkingen waarbij persoonsgegevens over strafrechtelijke veroordelingen en strafbare feiten, gegevens over onrechtmatig of hinderlijk gedrag of gegevens over slecht betalingsgedrag door bedrijven of particulieren worden verwerkt en gedeeld met derden.

Nee

0

1.3 Fraudebestrijding

Grootschalige verwerkingen en/of stelselmatige monitoring van (bijzondere) persoonsgegevens voor fraudebestrijding.

Nee

0

1.4 Creditscores

Grootschalige gegevensverwerkingen en/of stelselmatige monitoring van persoonsgegevens die leiden tot of gebruik maken van inschattingen van de kredietwaardigheid van natuurlijke personen.

Nee

0

1.5 Financiële situatie

Grootschalige verwerkingen en/of stelselmatige monitoring van financiële gegevens waaruit de inkomens- of vermogenspositie of het bestedingspatroon van mensen valt af te leiden.

Nee

0

1.6 Genetische persoonsgegevens

Grootschalige verwerkingen en/of stelselmatige monitoring van genetische persoonsgegevens.

Nee

0

1.7 Gezondheidsgegevens

Grootschalige verwerkingen van gegevens over gezondheid waaronder ook grootschalige elektronische uitwisseling van gegevens over gezondheid, tenzij het gaat om individuele artsen en individuele zorgprofessionals.

Nee

0

1.8 Samenwerkingsverbanden

Het delen van persoonsgegevens in of door samenwerkingsverbanden waarin gemeenten of andere overheden met andere publieke of private partijen bijzondere persoonsgegevens of persoonsgegevens van gevoelige aard met elkaar uitwisselen.	Nee	0
1.9 Cameratoezicht		
Grootschalige verwerkingen en/of stelselmatige monitoring van openbaar toegankelijke ruimten met camera's, webcams of drones.	Nee	0
1.10 Flexibel cameratoezicht		
Grootschalig en/of stelselmatig gebruik van flexibel cameratoezicht.	Nee	0
1.11 Controle werknemers		
Grootschalige verwerkingen en/of stelselmatige monitoring van persoonsgegevens om activiteiten van werknemers te monitoren.	Nee	0
1.12 Locatiegegevens		
Grootschalige verwerkingen en/of stelselmatige monitoring van locatiegegevens van of herleidbaar tot natuurlijke personen.	Nee	0
1.13 Communicatiegegevens		
Grootschalige verwerkingen en/of stelselmatige monitoring van communicatiegegevens inclusief metadata herleidbaar tot natuurlijke personen, tenzij en voor zover dit noodzakelijk is ter bescherming van de integriteit en de veiligheid van het netwerk en de dienst van de betrokken aanbieder, of het randapparaat van de eindgebruiker.	Nee	0
1.14 Internet of things		
Grootschalige verwerkingen en/of stelselmatige monitoring van persoonsgegevens die worden gegenereerd door apparaten die verbonden zijn met internet en die via internet of anderszins gegevens kunnen versturen of uitwisselen.	Nee	0
1.15 Profileren		
Systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen gebaseerd op geautomatiseerde verwerking (profilering).	Nee	0
1.16 Observatie en beïnvloeding gedrag		
Grootschalige verwerkingen van persoonsgegevens waarbij op stelselmatige wijze via geautomatiseerde verwerking gedrag van natuurlijke personen geobserveerd of beïnvloed, dan wel gegevens die daarover worden verzameld en/of vastgelegd, inclusief gegevens die voor het doel online behavioural advertising worden verzameld.	Nee	0
1.17 Biometrische gegevens		
Grootschalige verwerkingen en/of stelselmatige monitoring van biometrische gegevens met als doel een natuurlijk persoon te identificeren. Enkel als de verwerking strikt noodzakelijk is voor authenticatie of beveiligingsdoeleinden.	Nee	0
2. EDPB-lijst met criteria		
Geef bij elk criterium aan of dit van toepassing is op de voorgenomen verwerking.		Score Ja op EDPB-lijst? 0,5
2.1 Mensen beoordelen met persoonskenmerken (evaluatie of scoretoekenning)		
Het gaat onder meer om profiling en het maken van prognoses, met name op basis van kenmerken als iemands beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren of interesses, betrouwbaarheid of gedrag, locatie of verplaatsingen.	Nee	0
2.2 Geautomatiseerde beslissingen		
Het gaat om beslissingen die voor de betrokkene rechtsgevolgen of vergelijkbare wezenlijke gevolgen hebben.	Nee	0
2.3 Stelselmatige en grootschalige monitoring		
Het gaat om monitoring van openbaar toegankelijke ruimten. Hierbij kunnen persoonsgegevens worden verzameld zonder dat betrokkenen weten wie hun gegevens verzamelt en wat daar vervolgens mee gebeurt. Bovendien kan het onmogelijk zijn voor mensen om zich in openbare ruimten aan deze gegevensverwerking te onttrekken.	Nee	0
2.4 Gevoelige gegevens of gegevens van zeer persoonlijke aard		
Het gaat om bijzondere categorieën van persoonsgegevens uit artikel 9 van de AVG. Ook strafrechtelijke gegevens vallen hieronder (artikel 10 van de AVG). Ook gaat het om gegevens die over het algemeen als privacygevoelig worden beschouwd.	Nee	0
2.5 Grootschalige gegevensverwerkingen		
Het gaat om grootschalige verwerkingen.	Nee	0
2.6 Gekoppelde datasets		
Het gaat om gegevensverzamelingen die aan elkaar gekoppeld of met elkaar gecombineerd zijn.	Ja	0
2.7 Gegevens over kwetsbare personen		
Bij het verwerken van dit type gegevens kan een DPIA nodig zijn omdat er sprake is van een ongelijke machtsverhouding tussen de betrokkene en de verantwoordelijke. Dit heeft als gevolg dat betrokkenen niet in vrijheid toestemming kunnen geven of weigeren voor het verwerken van hun gegevens.	Nee	0
2.8 Gebruik van nieuwe technologieën		
Het gaat om bij het gebruik van een nieuwe technologie.	Nee	0
2.9 Blokkering van een recht, dienst of contract		
Het gaat om gegevensverwerkingen die tot gevolg hebben dat betrokkenen: - een recht niet kunnen uitoefenen of; - een dienst niet kunnen gebruiken of; - een contract niet kunnen afsluiten.	Nee	0

Als slechts één van de criteria van de EDPB-lijst met Ja is beantwoord, kan er alsnog een hoog privacy risico zijn, waarbij een DPIA nodig is. Wordt de DPIA uitgevoerd? Kies ja of nee. Zo nee, onderbouw vervolgens hieronder waarom een DPIA niet nodig is.

0

Het betreft weinig en niet risicovolle gegevens van ondernemers die verwerkt worden en bij eerste verwerking worden geaggregeerd.

3. Ontwikkeling van beleid en regelgeving

Een PIA moet binnen de Rijksoverheid uitgevoerd worden bij de ontwikkeling van beleid en regelgeving als deze betrekking hebben op verwerkingen van persoonsgegevens of waaruit verwerkingen van persoonsgegevens voortvloeien. Is hiervan sprake?

Score Ja op EDPB-lijst?

1

0

4. Groot politiek-bestuurlijk en maatschappelijk vraagstuk

Een PIA moet binnen de Rijksoverheid uitgevoerd worden als de gegevensverwerking raakt aan een groot politiek-bestuurlijk en maatschappelijk vraagstuk. Is hiervan sprake?

0

5. Grootchalig project met ICT-component

Een PIA moet binnen de Rijksoverheid ook uitgevoerd worden bij projecten met een ICT-component van ten minste €5 miljoen. Is hiervan sprake?

0

6. Overige omstandigheden

Zijn er overige omstandigheden die niet onder één van de bovenstaande beoordelingscriteria vallen en een hoog privacy-risico voor de betrokkenen inhouden? Vermeld hieronder welke dit zijn.

0

0

7. Resultaat Pre-scan DPIA

Er is geen hoog risico voor de betrokkenen. Een DPIA is niet nodig.

8. Opmerkingen, besluiten en/of toelichting

Vermeld opmerkingen, genomen besluiten en/of een toelichting.

9. Contactgegevens

Noteer wie de formele contactpersoon en de contactpersoon in de praktijk voor de beoogde verwerking van persoonsgegevens is.

Naam formele contactpersoon:	5.1.2.e
Afdeling formele contactpersoon:	RIEC Den Haag
Functie/rol formele contactpersoon:	5.1.2.e
Telefoonnummer formele contactpersoon:	5.1.2.e
E-mailadres formele contactpersoon:	5.1.2.e @denhaag.nl
Naam contactpersoon:	5.1.2.e
Afdeling contactpersoon:	RIEC Den Haag
Functie/rol contactpersoon:	5.1.2.e
Telefoonnummer contactpersoon:	5.1.2.e
E-mailadres contactpersoon:	5.1.2.e @denhaag.nl

10. Ondertekening Pre-scan DPIA

Vul alle gegevens in en laat de Pre-scan DPIA ondertekenen door de eindverantwoordelijke(n) van de beoogde verwerking van persoonsgegevens.

Naam verantwoordelijke(n):	5.1.2.e
Directie/afdeling verantwoordelijke(n):	RIEC Den Haag
Functie verantwoordelijke(n):	5.1.2.e
Datum ondertekening:	
Handtekening:	

11. Distributie Pre-scan DPIA

Noteer alle ontvangers van de ingevulde en getekende Pre-scan DPIA.

Ontvangers:	5.1.2.e
-------------	---------

Bronvermelding

De onderstaande lijst bevat alle vermelde bronnen uit het format Pre-scan DPIA.

Inleiding Pre-scan DPIA

1. [Algemene verordening persoonsgegevens \(AVG\)](#)
2. [Wet politiegegevens \(Wpg\)](#)
3. [Wet justitiële en strafvorderlijke gegevens \(Wjsg\)](#)

AP-lijst met hoog risico verwerkingen

4. [Website AP, lijst van verwerkingen waarvoor een DPIA verplicht is](#)
5. [Besluit inzake lijst van verwerkingen van persoonsgegevens waarvoor een gegevensbeschermingseffectbeoordeling \(DPIA\) verplicht is, Autoriteit van Persoonsgegevens van 27 november 2019 \(Staatscourant nummer 64418\)](#)
6. [Zie voor een toelichting op het begrip stelselmatig de website van de AP, onder begrippen](#)
7. [Zie voor een toelichting op het begrip stelselmatig de Richtlijnen voor functionarissen voor gegevensbescherming \(Data Protection Officer, DPO\) van de WP29, goedgekeurd op 13 december 2016, laatstelijk herzien en goedgekeurd op 5 april 2017](#)
8. [Artikel 29 en 33 van de Uitvoeringswet Algemene verordening gegevensbescherming](#)
9. [Richtsnoeren inzake geautomatiseerde individuele besluitvorming en profilering voor de toepassing van Verordening \(EU\) 2016/679 van WP 29, vastgesteld op 3 oktober 2017 en gewijzigd en vastgesteld op 6 februari 2018.](#)

EDPB-lijst met criteria

10. [Richtsnoeren voor gegevensbeschermingseffectbeoordelingen en bepaling of een verwerking "waarschijnlijk een hoog risico inhoudt" in de zin van Verordening 2016/679 van de WP29, vastgesteld op 4 oktober 2017 en laatstelijk gewijzigd en vastgesteld op 4 oktober 2017](#)
11. [Website AP, EDPB-beoordelingscriteria of voorgenomen gegevensverwerking een hoog privacy-risico oplevert voor betrokkenen](#)
12. [Zie voor een toelichting op het begrip grootschalig, paragraaf 2.1.3 uit de Richtlijnen voor functionarissen voor gegevensbescherming \(Data Protection Officer, DPO\) van de WP29, goedgekeurd op 13 december 2016, laatstelijk herzien en goedgekeurd op 5 april 2017 \(officiële Nederlandse vertaling van Guidelines on Data Protection Officers \('DPOs'\)\)](#)
13. [Website AP, beantwoording vraag Wat ziet de AVG als een grootschalige verwerking van persoonsgegevens?](#)
14. [Handleiding GEB van de Belgische Gegevensbeschermingsautoriteit, versie 4.0, 21.04.2021](#)

Ontwikkeling van beleid en regelgeving

15. [Model DPIA Rijksdienst, versie 2.0 definitief 19 november 2021](#)
16. [Integraal afwegingskader voor wetgeving en beleid \(IAK\)](#)

Groot politiek-bestuurlijk en maatschappelijk vraagstuk

17. [Handboek Portfoliomanagement Rijk, versie 10.01 van 14 december 2020 \(alleen toegankelijk voor Rijksmedewerkers\)](#)

DPIA rapportage RIEC-liaison

Versiebeheer

Versie	Datum	Wijzigingen	Wie
0.9	29-07-21	Eerste concept opgeleverd	5.1.2.e
0.9	27-08-2021	Tweede concept opgeleverd	5.1.2.e
1.0	04-10-2021	Definitieve versie opgeleverd	5.1.2.e

Inhoudsopgave

1. Inleiding.....	3
<i>Aanleiding en onderwerp van de DPIA</i>	<i>3</i>
<i>Doelstelling.....</i>	<i>3</i>
<i>Scope</i>	<i>3</i>
<i>Opbouw van de analyse</i>	<i>4</i>
2. Managementsamenvatting	6
3. Beschrijving Verwerking	8
<i>Systematische beschrijving van het proces.....</i>	<i>8</i>
<i>Systematische beschrijving van de verwerking.....</i>	<i>11</i>
<i>Persoonsgegevens.....</i>	<i>12</i>
4. Analyse privacy consequenties	15
<i>Inleiding.....</i>	<i>15</i>
4.1 Governance.....	15
<i>Inleiding.....</i>	<i>15</i>
<i>Feiten & analyse.....</i>	<i>15</i>
<i>Risico's en maatregelen</i>	<i>16</i>
4.2 Grondslag & Doelbinding.....	18
<i>Inleiding.....</i>	<i>18</i>
<i>Feiten & analyse.....</i>	<i>18</i>
<i>Rechtmatigheid van de verwerking.....</i>	<i>19</i>
<i>Risico's en maatregelen</i>	<i>20</i>
4.3 Juistheid.....	21
<i>Inleiding.....</i>	<i>21</i>
<i>Feiten & Analyse.....</i>	<i>21</i>

Risico's en maatregelen	21
<i>4.4 Dataminimalisatie</i>	22
Inleiding.....	22
Feiten & Analyse.....	22
Risico's en maatregelen	23
<i>4.5 Opslag</i>	24
Inleiding.....	24
Feiten & Analyse.....	24
Risico's en maatregelen	25
<i>4.6 Bescherming</i>	26
Inleiding.....	26
Feiten & Analyse.....	26
Risico's en maatregelen	26
<i>4.7 Transparantie</i>	28
Inleiding.....	28
Feiten & Analyse.....	28
Risico's en maatregelen	29
<i>4.8 Cultuur</i>	30
Inleiding.....	30
Feiten & analyse.....	30
Risico's en maatregelen	30
5. Advies en accordering	32
Aanbevelingen voor vervolg	32
<i>Advies FG</i>	33
<i>Accordering</i>	34
Bijlage A	35
<i>A1. Documentatie</i>	35
<i>A2. Geïnterviewden</i>	35

1. Inleiding

Aanleiding en onderwerp van de DPIA

Vanuit het oogpunt van een zorgvuldige omgang met persoonsgegevens is de gemeente verplicht een DPIA uit te voeren voor verwerkingen die waarschijnlijk een verhoogd risico opleveren.

Voor het RIEC-liaison proces is vastgesteld dat een verhoogd risico bestaat, namelijk: er worden persoonsgegevens gedeeld met het RIEC (een samenwerkingsverband) waarin de gemeente met andere publieke en/of private partijen (bijzondere) persoonsgegevens of persoonsgegevens van gevoelige aard uitwisselt, zoals gegevens over BRP, betreffende vergunningen, betreffende subsidieaanvragen en verstrekkingen, gemeentelijke belastingen, bestuurlijke handhaving, bezwaarschriften, betreffende klachten- en meldingen openbare orde veiligheid en ruimtelijke ontwikkeling en vastgoed. De Autoriteit Persoonsgegevens verplicht het uitvoeren van een DPIA op gegevensverwerkingen in samenwerkingsverband.

Een DPIA is een middel om in kaart te brengen welke persoonsgegevens in een proces, systeem of organisatie verwerkt worden en wat hiervan de risico's voor betrokkenen zijn. Op 08-07-2021 en op 15-07-2021 is een DPIA-workshop gehouden om de benodigde informatie hiervoor op te halen. In Bijlage A is opgenomen wie aan deze bijeenkomst hebben deelgenomen. Dit rapport is het resultaat van deze DPIA.

Doelstelling

Deze DPIA rapportage schetst de eventuele privacy risico's van de onderhavige gegevensverwerking, en maatregelen die kunnen worden getroffen teneinde deze risico's te mitigeren.

In de DPIA wordt vooral gekeken naar de geplande maatregelen, waarborgen en mechanismen om de risico's te beperken, de persoonsgegevens te beschermen en aan te tonen dat aan de beginselen voor verwerking uit de AVG is voldaan. Deze DPIA is een momentopname. Bij nieuwe ontwikkelingen zoals wijzigingen in wetgeving, verandering van processen, inzet van nieuwe technologie e.d. moet de DPIA worden herhaald. Ook dienen uitgevoerde DPIA's periodiek te worden herijkt (iedere 3 jaar).

Scope

Deze DPIA wordt uitgevoerd ten aanzien van gegevensverwerkingen in het proces RIEC-liaison. De laatste DPIA op dit proces is in 2020 uitgevoerd. Doordat de afdeling ondermijning binnen de Directie Veiligheid een nieuw zaakstelsel (PGA-x) in gebruik neemt voor een drietal processen, onderdeel van het informatieknooppunt ondermijning (IKO), waaronder het RIEC-liaison-proces, wordt de reeds eerder uitgevoerde DPIA geactualiseerd.

Binnen de scope van dit proces valt het ontvangen van een quickscan- of informatieverzoek door het RIEC en beantwoording op basis van gegevens waar de gemeente over beschikt. Onderdeel van dit proces is ook het bevragen van voor het signaal relevante spoorhouders binnen de gemeente door de RIEC-liaison.

In het RIEC-casusoverleg wordt besloten welke interventies worden ingezet. De RIEC-liaison zorgt ervoor dat de gemeentelijke interventie intern wordt uitgezet, monitort hierop en koppelt terug in het RIEC-casusoverleg. Het uitzetten en monitoren van interventies is onderdeel van deze DPIA.

In deze DPIA wordt niet ingegaan op de gegevensverwerking in het RIEC en het gezamenlijke informatiesysteem RIEC-IS.

In sommige gevallen wordt in dit proces gebruik gemaakt van de reguliere voorzieningen van de Gemeente (netwerk, fysieke werkplek, inlogvoorziening). Waar het centrale proces van de Gemeente wordt gevolgd, zijn deze geen onderdeel van de DPIA. In dat soort gevallen wordt duidelijk vermeld dat deze buiten scope van deze DPIA blijven.

Het Bibob- en het gemeentesignalen proces worden behandeld in een afzonderlijke DPIA en zijn geen onderdeel van deze DPIA.

Opbouw van de analyse

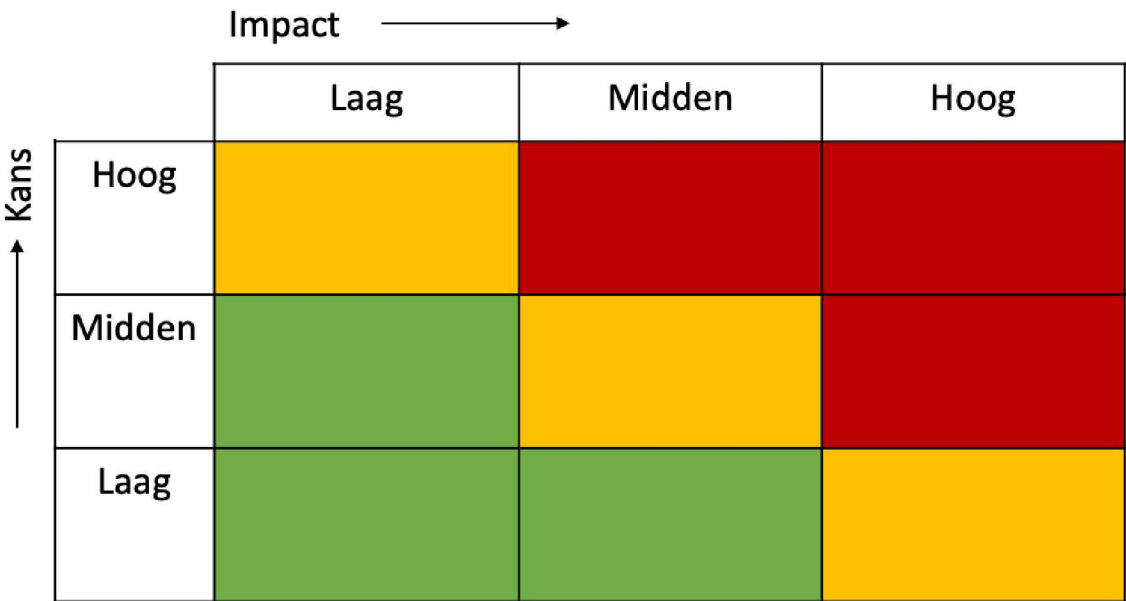
Dit document schetst de privacy risico's binnen bovengenoemde scope en de te nemen maatregelen die het betreffende risico kunnen mitigeren.

De uitvoering van deze DPIA verloopt via de zes beginselen waaraan elke verwerking moet voldoen. Deze zes beginselen zijn Juistheid, Data minimalisatie, Opslag, Bescherming, Transparantie en Grondslag & doelbinding. Daarnaast zijn ook de thema's 'Governance' en 'Privacycultuur' van belang.

Deze beginselen vormen de basis voor de uitvoering van deze analyse. Per thema worden eventuele risico's geanalyseerd en wordt de impact van deze risico's op de betrokkenen en de gemeente ingeschat. Daarnaast worden maatregelen die de eigenaar van de verwerking kan treffen om de risico's tot een acceptabel niveau terug te brengen beschreven. Hierbij wordt rekening gehouden met de haalbaarheid en maakbaarheid van deze maatregelen binnen de context van de gemeente. De eventuele acceptatie van risico's of restrisico's is de verantwoordelijkheid van de eigenaar van de verwerking.

Voor elk van de thema's zijn risico's geïnventariseerd die voor het onderhavige onderwerp relevant kunnen zijn voor de gegevensbescherming binnen de gemeente. De aanwezige deelnemers aan de workshop hebben tijdens het uitvoeren van de risicoanalyse de belangrijkste risico's benoemd en geclassificeerd volgens de onderstaande tabel.

Figuur 1



2. Managementsamenvatting

Wat zijn de belangrijkste (M-H) risico's die in de analyse zijn geconstateerd? Welke maatregelen zijn hierbij van toepassing.

Beginnel	Risico	Classificatie (L-M-H)	Maatregel (mogelijk)
Governance	Er zijn geen goede inhoudelijke afspraken gemaakt over de passende omgang met (persoons-)gegevens met 5.1.2.f 5.1.2.f waardoor er onvoldoende waarborgen zijn dat zorgvuldig met gegevens wordt omgegaan	M	Er moet zo snel mogelijk en uiterlijk voor de ingebruikname van PGA-x een overeenkomst met 5.1.2.f worden gesloten.
Governance	Medewerkers herkennen datalekken niet	M	Organiseer een specifieke datalektraining voor iedere medewerker, inclusief spoorhouders, in dit proces (of directie breed).
Governance	Te weinig fte's beschikbaar voor privacy ondersteuning	H	Draag zorg voor een vaste privacy officer die de medewerkers structurele ondersteuning kan bieden.
Governance	Verwerking niet opgenomen in het register van verwerkingsactiviteiten waardoor niet wordt voldaan aan verantwoordingsplicht	L	Voeg de verwerking toe aan het register van verwerkingsactiviteiten.
Grondslag & doelbinding	Spoorhouders weten niet altijd of ze gegevens mogen delen met de RIEC-liaison, hierdoor bestaat het risico dat er meer informatie gedeeld wordt dan noodzakelijk.	L	Zorg dat kaders voor de gegevensuitwisseling bekend zijn bij de spoorhouders (of ondersteunende privacy officers). Daarnaast moet de RIEC-liaison alle irrelevante gegevens afkomstig van spoorhouders verwijderen of anonimiseren, voordat de gegevens worden gedeeld met het RIEC.
Dataminimalisatie	Spoorhouders bewaren onnodig informatie over subject/object/signaal	M	Spreek af met de spoorhouders dat zij de informatie uit het signaal over subject/object direct verwijderen na het beantwoorden van de vragen in de QuickScan of informatieverzoekfase. Indien mogelijk wordt afgesproken dat

			de spoorhouders geen informatie over het signaal lokaal opslaan.
Datamini- malisatie	De gemeente ontvangt signalen die niet passen in de thematiek van het RIEC convenant	H	De gemeente dient het signaal direct terug te koppelen aan het RIEC. Zorg er voor dat het signaal niet wordt geregistreerd in PGAX en verwijder het direct uit eventuele opslaglocaties. Als het signaal is geregistreerd in PGAX en de liaison komt er pas na verrijking achter dat het signaal niet past in de thematiek van het convenant, dan wordt het signaal afgesloten. Idealiter wordt het signaal verwijderd of geanonimiseerd, zodat het signaal niet meer wordt gemonitord of getoond.
Opslag	Gegevens worden langer dan noodzakelijk is bewaard	M	Stel intern de bewaartermijn vast voor gegevens die worden verwerkt in het RIEC-liaison proces. Sluit aan bij de best practice voor het hanteren van bewaartermijnen voor dit soort signalen. Onderbouw de keuze voor de bewaartermijn, zodat hierop gestuurd kan worden. Toets de bewaartermijnen periodiek. Dit kan bijvoorbeeld jaarlijks.
Trans- parantie	Betrokkene worden niet goed geïnformeerd	H	Pas de privacyverklaring aan
Trans- parantie	Medewerkers weten niet hoe ze moeten voldoen aan de rechten van betrokkenen	H	Maak een werkinstructie voor de rechten van betrokkenen en deel deze met de RIEC-liaison
Cultuur	Er is te weinig aandacht voor privacy geweest waardoor medewerkers onvoldoende getraind zijn in het herkennen van privacy risico's in dit proces	M	Maak medewerkers meer bewust van privacy risico's

3. Beschrijving Verwerking

Dit hoofdstuk beschrijft het onderhavige proces en de verwerkingen van persoonsgegevens. De beschrijving van het proces en het inventariseren van de verwerkingen van persoonsgegevens zijn onderdeel geweest van de DPIA-workshop.

Systematische beschrijving van het proces

Start proces

Het RIEC-liaison proces vangt aan door het ontvangen van een signaal vanuit het RIEC. Dit signaal wordt ontvangen door de RIEC-liaison per e-mail. In de e-mail staat dat een notificatie klaar staat in het RIEC-IS systeem, met een hyperlink naar het systeem. Dit systeem is geen onderdeel van deze DPIA. De RIEC-liaison logt via multi-factor authenticatie (MFA) in om de melding te bekijken.

Het signaal

De RIEC-liaison bekijkt het signaal in het RIEC-IS. Het signaal is vastgelegd in een Word document of pdf-file. Hierin staat in ieder geval:

- Een korte samenvatting van de casuïstiek;
- Binnen welk landelijk of regionaal thema uit het RIEC-LIEC Convenant het signaal valt. Bij uitzondering kan het voorkomen dat een casus aan de RIEC-liaison wordt verstuurd die niet binnen de vastgelegde thema's valt. De casus wordt dan niet in behandeling genomen en afgesloten. De casus verdwijnt uit de werkvoorraad. Er vindt een terugkoppeling plaats aan het RIEC.
- Persoonsgegevens van de betrokkene(n) in de casus. Dit kunnen naam, achternaam, geboortedatum, telefoonnummer of BSN zijn.

Registratie in PGA-x

Het document waarin het signaal staat wordt uit het RIEC-IS gedownload door de RIEC-liaison en opgeslagen op de G-schijf in een daarvoor bestemde en afgeschermd map. Daarna wordt het document geüpload in PGA-x.

Dossier wordt aangemaakt in PGA-x

In PGA-x wordt automatisch een dossier aangemaakt. PGA-x maakt een uniek dossiernummer aan. De dossiernaam die door het RIEC wordt gehanteerd, wordt handmatig aan het dossier toegevoegd.

Signaal wordt verrijkt met persoonsgegevens

Het signaal wordt door de RIEC-liaison verrijkt met aanvullende persoonsgegevens.

De RIEC-liaison kan de gegevens van in het signaal vermelde natuurlijke-/rechtspersonen controleren/valideren op basis van BRP, BAG, KvK en BRK. Deze systemen zijn via HaalCentraal gekoppeld aan PGAx. Alle raadplegingen worden gelogd. De RIEC-liaison bepaalt zelf welke aanvullende gegevens noodzakelijk zijn op te nemen in het dossier in PGAx.

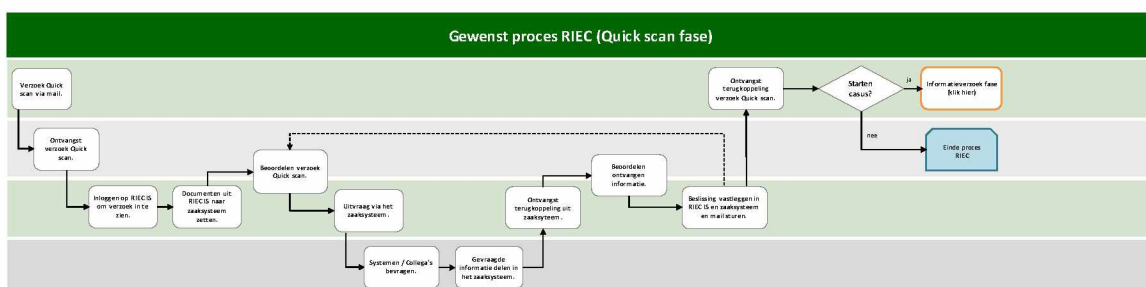
Één van de voorbeelden waarin de RIEC-liaison moet bepalen of aanvullende gegevens noodzakelijk zijn voor het dossier werd uitgelegd in de workshop aan de hand van de volgende casus:

De RIEC-liaison kan de verblijfplaats van de betrokkene controleren. Bijvoorbeeld om te zien hoeveel personen er op een adres woonachtig zijn. Eventuele huisgenoten die staan ingeschreven op dit adres kunnen door de koppeling met bovenstaande bronnen in PGAX worden getoond. Het is aan de RIEC-liaison om te bepalen of deze personen relevant zijn voor het onderzoek. Dit kan hij doen door een vinkje aan te klikken in het systeem. De personen die een vinkje hebben gekregen worden daarna geüpload in het dossier.

De lijst met personen die PGA-x toont, wordt niet opgeslagen in het systeem, behalve als de RIEC-liaison de namen aanklikt en toevoegt aan het dossier.

Alle handelingen in PGA-x worden gelogd. Rapportages van de logs kunnen beschikbaar worden gesteld aan de gemeente. Er is nog geen key-user functioneel beheer aangesteld, maar dit wordt waarschijnlijk in samenwerking met het Zorg- en Veiligheidshuis geregeld.

Quickscan fase



Op basis van het originele signaal wordt een Quickscan aangemaakt. In de Quickscan wordt het volgende door de RIEC-liaison vermeld:

- Namen en adressen van natuurlijke -en rechtspersonen;
- Casusomschrijving;
- Thema(s) RIEC-LIEC Convenant (Georganiseerde hennepcultuur, mensenhandel en smokkel, criminele motorbendes, misbruik en fraude binnen de vastgoedsector en witwassen en daaraan gerelateerde vormen van financieel-economische criminaliteit).

De Quickscan wordt, via PGA-x, verstuurd naar 'spoorhouders' bij de verschillende diensten van de gemeente Den Haag. Deze spoorhouders zijn de contactpersonen binnen andere diensten van de RIEC-liaison. Spoorhouders hebben toegang tot achterliggende bronsystemen binnen hun eigen domein. In de Quickscan worden drie vragen aan de spoorhouder gesteld:

1. Ben je bekend en heb je informatie van het subject?
2. Heb je interventiemogelijkheden?
3. Heb je belang bij het oppakken van de casus?

Via PGA-x wordt een notificatiemail naar de spoorhouders verstuurd met de melding dat er bericht klaarstaat in PGA-x. De spoorhouders beantwoorden de drie vragen met 'ja' of 'nee'. Er worden (nog) geen persoonsgegevens gedeeld door de spoorhouders met de RIEC-liaison.

De RIEC-liaison geeft een terugkoppeling aan het RIEC. In de terugkoppeling staat of de gemeente wel/geen belang heeft bij de casus. Er wordt geen terugkoppeling gedaan op afdeling/dienstniveau. De terugkoppeling vindt plaats via het RIEC-IS of per e-mail aan de accounthouder binnen het RIEC.

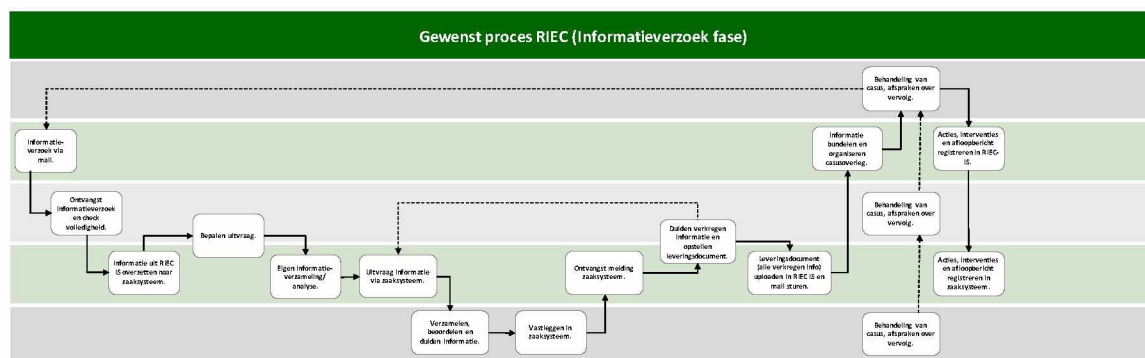
Beshuitvorming RIEC

De Ondernijningstafel in het RIEC besluit (formeel) of er voldoende partijen belang hebben bij de casus voor opvolging daarvan. In de praktijk is dit ook vaak de accountmanager. Er moeten in de regel minimaal twee partijen deelnemen. De casus wordt dan een formele RIEC-casus.

Als er onvoldoende partijen belang hebben bij deelname, zijn er voor de gemeente Den Haag twee alternatieven:

1. De status van het dossier veranderd naar 'gesloten' en wordt een jaar bewaard in PGA-x.
2. De RIEC-casus wordt gerouteerd naar het Informatieknooppunt Ondernijning (IKO) als 'gemeentesignaal'. Het proces 'gemeentesignalen' wordt vervolgens gevolgd. Dit proces valt buiten scope van deze DPIA.

Informatiefase



Als de casus wordt behandeld in het RIEC volgt een (nieuw) informatieverzoek. De RIEC-liaison zet dit verzoek uit bij de deelnemende diensten van de gemeente. Dit zijn de diensten die in de Quicksan fase hebben aangegeven informatie te hebben over het subject of de onderneming en belang te hebben bij de casus.

Het informatieverzoek wordt uitgezet via PGA-x. De spoorhouders ontvangen een notificatiemail en kunnen via een hyperlink inloggen in PGA-x waar het informatieverzoek klaarstaat. De spoorhouders leveren gegevens uit de betreffende bronsystemen voor zover deze noodzakelijk zijn voor de aanpak van het signaal.

Voldoen aan informatieverzoek

De RIEC-liaison genereert alle ontvangen gegevens, indien mogelijk, in één document. Niet noodzakelijke gegevens worden door de RIEC-liaison verwijderd. Dit document wordt gedownload op de G-schijf en daarna geüpload op PGA-x. De eindversie van het document wordt geüpload en gedeeld met het RIEC via het RIEC-IS.

Casusoverleg RIEC (valt buiten scope)

Na de informatiefase vindt er een casusoverleg plaats in het RIEC. Dit valt buiten de scope van deze DPIA.

Het casusoverleg heeft twee mogelijke uitkomsten:

1. Er worden verdiepingsvragen gesteld;
2. De gemeente wordt verzocht bepaalde interventie(s) uit te voeren. De RIEC-liaison zorgt ervoor dat de interventie(s) bij de verantwoordelijke afdeling(en) worden uitgezet.

De acties uit het casusoverleg worden gedeeld met de bij de casus betrokken RIEC-partners.

Verdiepingsvragen;

Er kunnen verdiepingsvragen worden gesteld door partners in het RIEC gedurende het verloop van de casus. Deze vragen worden gesteld via het RIEC-IS. De RIEC-liaison ontvangt hiervan een notificatiemail en zet de vragen uit bij de betreffende diensten.

Gemeentelijke interventies

Als de gemeente de mogelijkheid heeft om te interveniëren, dan volgt er een actie voor de dienst(en). De actie wordt gedeeld via het RIEC-IS. De RIEC-liaison registreert de actie tot interventie in PGA-x.

De RIEC-liaison monitort deze interventies. PGA-x geeft een herinnering op de dag dat er een interventie plaatsvindt door een dienst. Ook geeft het systeem twee weken voor de interventiedatum een herinnering. Indien noodzakelijk (r)appelleert de RIEC-liaison de dienst(en) met een interventie als deze nog niet is uitgevoerd.

Interventies die uitgevoerd worden door (niet gemeentelijke) partners worden niet vastgelegd in PGAx.

De uitkomst van de interventies wordt via het RIEC-IS gedeeld met de deelnemende partners in het RIEC.

De status van het dossier in PGA-x blijft op actief staan tot het RIEC de casus heeft afgesloten. Als de RIEC-liaison een melding krijgt via het RIEC-IS dat de casus is gesloten, dan zal de RIEC-liaison deze ook in PGA-x afsluiten.

Systematische beschrijving van de verwerking

Onderstaand een schematische weergave van de persoonsgegevens. Wat ontvang je (wat krijg je), wat verwerk je (wat doe je ermee) en wat verstrek je (wat geef je door).

Wat krijg je	Van wie	Hoe
<i>Signaal:</i> - <i>Casusbeschrijving</i> - <i>Convenant thematiek</i> - <i>Subjectgegevens:</i> - o <i>NAW gegevens</i> - o <i>Geboortedatum</i> - o <i>BSN</i> - o <i>Onroerend goed</i> - o <i>Telefoonnummer</i> - <i>Gegevens over rechtspersoon:</i> - o <i>KvK-nummer</i> - o <i>Adresgegevens</i> - o <i>Handelsnaam</i> - o <i>Rechtsvorm</i> - o <i>DGA</i> - o <i>Nevenvestigingen (en andere adresgegevens)</i> - o <i>Telefoonnummer</i> - <i>Locaties (bijvoorbeeld gebouwen van subject)</i>	<i>Natuurlijke personen, rechtspersonen</i>	<i>RIEC-IS systeem</i>

Wat doe je ermee	Middelen	Wie
<i>Verrijking in bronsystemen</i>	<i>KvK, kadaster, BRP</i>	<i>RIEC-liaison</i>
<i>Quicksan verzoek</i>	PGA-x	Spoorhouders
<i>Informatieverzoek</i>	PGA-x	Spoorhouders

Wat geef je door	Aan wie	Hoe
Reactie op de quickscan	RIEC	RIEC-IS
Reactie op het informatieverzoek (dit is vrij breed). Informatie vanuit verschillende directies, vaak gevoelige gegevens.	RIEC	RIEC-IS
Resultaten van de interventies	RIEC	RIEC-IS

Persoonsgegevens

Wij hanteren de classificatie zoals weergegeven in onderstaande figuur om te bepalen welke persoonsgegevens worden verwerkt. Er wordt onderscheid gemaakt tussen weinig gevoelige gegevens (algemene persoonsgegevens), door de aard of context extra gevoelige gegevens (gevoelige persoonsgegevens) en zeer gevoelige gegevens die wettelijk extra beschermd zijn (bijzondere persoonsgegevens). Al naar gelang de situatie kunnen gegevens in verschillende categorie worden geplaatst.



Binnen de scope van deze DPIA worden de volgende categorieën van persoonsgegevens verwerkt:

	Algemeen	Gevoelig	Bijzonder
Vaste velden	• geen	• geen	• geen
Open/ Ongestructureerde velden	<i>Subjectgegevens:</i> • NAW gegevens • Geboortedatum • Onroerend goed • Telefoonnummer <i>Gegevens over rechtspersoon:</i> • KvK-nummer • Adresgegevens • Handelsnaam • Rechtsvorm • DGA	• <i>Casusbeschrijving</i>	- BSN

Gemeente Den Haag

Ons kenmerk

BD/

	• <i>Nevenvestigingen (en andere adresgegevens)</i> <i>Locaties (bijvoorbeeld gebouwen van subject)</i>		
--	--	--	--

4. Analyse privacy consequenties

Inleiding

Dit hoofdstuk beschrijft de resultaten uit de uitgevoerde DPIA per thema. Voor ieder thema geven we een korte toelichting en beschrijven wij de risico's, de impact van de risico's op de betrokkenen en de gemeente en de maatregelen die de gemeente kan treffen om de risico's tot een acceptabel niveau terug te brengen. Daarnaast worden ook de ethische aspecten die mogelijk spelen in dit hoofdstuk besproken.

4.1 Governance

Inleiding

Is helder wie de verantwoordelijke en de verwerker zijn en hoe wordt toegezien op een adequate bescherming van persoonsgegevens? Is er beleid gemaakt ten aanzien van privacy en wordt er intern gecontroleerd op naleving van dit beleid? Is duidelijk wie binnen de organisatie verantwoordelijk is voor privacy?

Feiten & analyse

De gemeente Den Haag is een samenwerkingspartner in het Regionaal Informatie en Expertise Centrum Haaglanden (RIEC). De gemeente wordt binnen het RIEC vertegenwoordigd door de RIEC-liaison. De RIEC-liaison (werkzaam binnen de IKO-infodesk) vertegenwoordigt de gemeente Den Haag in het RIEC.

De gemeente Den Haag wordt aangemerkt als verwerkingsverantwoordelijke voor de persoonsgegevens die zij verwerken in de uitoefening van hun publiekrechtelijke taken en bevoegdheden.

De deelnemers aan het RIEC zijn ieder zelfstandig verwerkingsverantwoordelijk voor de persoonsgegevens die zij verwerken in de uitoefening van hun publiekrechtelijke taken en bevoegdheden. Hieronder wordt mede verstaan de verstrekking van persoonsgegevens aan partners (in het samenwerkingsverband) en het ontvangen van persoonsgegevens. Partijen zijn echter gezamenlijk verwerkingsverantwoordelijk voor de gegevensverwerking in gezamenlijke informatiesystemen, zoals het RIEC-IS. Dit is echter geen onderdeel van de scope van deze DPIA. Samenwerking in het RIEC vindt plaats op basis van de afspraken die tussen de samenwerkingspartners zijn gemaakt in het RIEC-LIEC Convenant en bijbehorend Privacy Protocol.

Binnenkort wordt het zaaksysteem PGA-x in gebruik genomen. De leverancier van dit zaaksysteem is ^{5.1.2.f} [redacted], ^{5.1.2.f} [redacted] treedt op als verwerker voor de directie Veiligheid van de gemeente Den Haag. Er is nog geen verwerkersovereenkomst gesloten waarin afspraken zijn gemaakt over de kaders van de gegevensverwerking. ^{5.1.2.f} [redacted] maakt gebruik van een subverwerker: ^{5.1.2.f} [redacted]

Er is een gemeentebreed privacybeleid aanwezig. De ontwikkeling van dit beleid is pril en staat nog in de kinderschoenen volgens de privacy officer van BSD. Het beleid bevat

voornamelijk algemene privacy-uitgangspunten. De rollen en verantwoordelijkheden zijn nog niet beschreven in het beleid. Het gemeentebrede privacy beleid is geen onderdeel van deze DPIA. Wij hebben daarom geen kennis genomen van dit document. Het is belangrijk dat hier op centraler niveau binnen de gemeente aandacht aan wordt besteed.

Er is een gemeentebreed datalekprotocol aanwezig. Er zijn ook afspraken gemaakt over de meldplicht datalekken in het privacyprotocol RIEC-LIEC. De RIEC-liaison is tevens gehouden aan het nakomen van deze afspraken. De RIEC-liaison heeft in het kader van dit proces nog geen datalekken meegemaakt. Medewerkers hebben geen training gehad waarin is stilgestaan bij beveiligingsincidenten en datalekken. Tijdens de workshop werd aangegeven dat meer bewustwording over dit thema wenselijk is.

Er is een privacy officer aangesteld binnen BSD. De privacy officer vervult echter slechts een tijdelijke rol en heeft weinig beschikbare FTE, aldus de privacy officer. Er is daardoor weinig mogelijkheid om vragen te stellen over privacy en gegevensbescherming. De gemeente heeft ook een FG aangesteld om toezicht te houden op de naleving van de AVG en gerelateerde wetgeving.

De gemeente houdt een register van verwerkingsactiviteiten bij (in iNavigator) waarin alle gemeentelijke processen zijn opgenomen. Het RIEC-liaison proces is niet opgenomen.

Risico's en maatregelen

Op basis van de analyse op het aspect *governance* zijn de volgende risico's geïdentificeerd.

Risico: Er zijn geen goede inhoudelijke afspraken gemaakt over de passende omgang met (persoons-)gegevens met 5.1.2.f 5.1.2.f waardoor er onvoldoende waarborgen zijn dat zorgvuldig met gegevens wordt omgegaan

Er is momenteel nog geen verwerkersovereenkomst afgesloten met de leverancier van PGA-x, 5.1.2.f. Zowel de gemeente als de leverancier zijn echter verplicht om de (voorgenomen) verwerking te regelen in (bijvoorbeeld) een verwerkersovereenkomst. Contractuele afspraken omtrent de verwerking van persoonsgegevens ontbreken. De gemeente kan daardoor niet aantonen dat de verwerking in overeenstemming met de AVG wordt uitgevoerd.

Maatregel

Er moet zo snel mogelijk en uiterlijk voor de ingebruikname van PGA-x een overeenkomst met 5.1.2.f worden gesloten. Lukt dit niet? Zorg dan dat alle onderstaande afspraken op een andere manier worden geborgd. In de verwerkersovereenkomst moet in ieder geval het volgende worden vastgelegd: algemene beschrijving, instructies, geheimhoudingsplicht, beveiliging, subverwerkers, privacy rechten, gegevens verwijderen en audits. Zorg er daarnaast voor dat er een mechanisme wordt gevonden waarbij structureel en periodiek wordt gestuurd op de nakoming en effectiviteit van deze maatregel.

Risico: Medewerkers herkennen datalekken niet

In de workshop wordt aangegeven dat medewerkers geen datalek hebben ontdekt en gemeld. Medewerkers hebben geen training gehad waarin is stilgestaan bij beveiligingsincidenten en datalekken. Daardoor kunnen medewerkers datalekken niet direct herkennen. Indien datalekken niet worden herkend, kunnen ze ook niet worden opgelost en afgehandeld. Dit zorgt voor een blijvend risico op datalekken.

Maatregel

Organiseer een specifieke datalektraining voor iedere medewerker, inclusief spoorhouders, in dit proces (of directie breed). Zorg ervoor dat in deze training wordt stilgestaan bij het herkennen en melden van beveiligingsincidenten en datalekken. Maak hierbij gebruik van het gemeentebrede datalekprotocol.

Risico: Onvoldoende fte's beschikbaar voor privacy officer directie Veiligheid waardoor aandachtspunten en issues niet tijdig worden opgepakt

De verantwoordelijke privacy officer heeft momenteel onvoldoende fte ter beschikking om de medewerkers bij dit proces structureel van privacy advies te voorzien. Hier is echter wel behoefte aan binnen de directie. Hierdoor ontstaat het risico dat er te weinig kennis en capaciteit is om de privacyaspecten binnen dit proces te bewaken, waardoor aandachtspunten en issues niet tijdig de aandacht krijgen of niet juist worden aangepakt.

Maatregel

Er moet structureel meer fte beschikbaar worden gesteld voor de privacy officer van de directie Veiligheid, zodat medewerkers in dit proces gevraagd en ongevraagd advies krijgen over de toepassing van privacywetgeving in dit proces. Afhankelijk van het takenpakket wordt geadviseerd om minimaal 0.6 fte beschikbaar te stellen voor de privacy officer van de directie Veiligheid. Het is belangrijk dat het verantwoordelijke managementniveau binnen de gemeente wordt geïnformeerd over deze noodzaak.

Risico: Verwerking niet opgenomen in het register van verwerkingsactiviteiten waardoor niet wordt voldaan aan verantwoordingsplicht

De verwerking is niet opgenomen in het gemeentebrede register van verwerkingsactiviteiten. De vastlegging en beschrijving van doel en grondslag voor de verwerkingsactiviteit ontbreekt daarom. De AVG verplicht de gemeente om een register van verwerkingsactiviteiten bij te houden. Dit is noodzakelijk om aantoonbaar te maken dat een verwerking aan de eisen uit de AVG voldoet. Het bijhouden van een register draagt daarom bij aan het waarborgen van de privacy van betrokkenen. Het is tevens noodzakelijk in het kader van de verantwoordingsplicht van de gemeente.

Maatregel

Voeg deze verwerking toe aan het register van verwerkingsactiviteiten in iNavigator. De privacy officer kan hierover adviseren. Het is bijvoorbeeld belangrijk dat er een duidelijke beschrijving van de grondslag en het doel van de verwerkingsactiviteit wordt vastgelegd (en goedgekeurd door het juiste managementniveau).

4.2 Grondslag & Doelbinding

Inleiding

Het moet helder zijn wat het doel van de gegevensverzameling is, op het moment dat de gemeente deze verzamelt. Het doel moet ook in overeenstemming zijn met de normale werkzaamheden van de gemeente en onderbouwd zijn door één of meer wettelijke grondslagen.¹

Feiten & analyse

De gemeenten heeft diverse, uiteenlopende publiekrechtelijke taken en bevoegdheden die van belang zijn voor de in het convenant gestelde doelstellingen ten behoeve van de samenwerking binnen het RIEC.

De grondslag en het doel van de verwerking van persoonsgegevens in dit proces is vastgelegd en beschreven in het Convenant en bijbehorend privacyprotocol RIEC-LIEC (zie hieronder). De grondslag en doelbinding is binnen de gemeente nog niet vastgelegd en beschreven in het register van verwerkingsactiviteiten (zie risico onder governance).

De grondslag is artikel 6 lid 1 sub d AVG. 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 (de gemeente) is opgedragen. De rechtsgrondslag moet dan zijn vastgelegd in het Unierecht of nationaal recht. Artikel 172 Gemeentewet belast de burgemeester met de handhaving van de openbare orde onder gewone omstandigheden. Dit is van direct belang voor de aanpak van ondermijning, bijvoorbeeld doordat de burgemeester de bevoegdheid heeft om een pand te doen sluiten bij verstoring van de openbare orde of drugshandel. Daarnaast zijn er bevoegdheden in de handhaving van de openbare orde en veiligheid die niet specifiek aan de burgemeester, maar bij andere organen van de gemeente zijn belegd.

De wettelijke basis voor het handhavend optreden van de gemeente kan ook (verder) zijn uitgewerkt in specifieke wet- en regelgeving, zoals bijvoorbeeld de drank- en horecawet. Daarnaast bevat deze specifieke wet- en regelgeving (in veel gevallen) ook specifieke artikelen over de te nemen bestuurlijke maatregelen (vergunningen intrekken, uitkeringen terugvorderen, panden sluiten, personen weren).

De gemeentelijke bevoegdheden in specifieke wetgeving concretiseren daarom de meer algemene openbare orde bevoegdheid van de burgemeester in de Gemeentewet. Daarmee bieden zij ook een (mogelijke) grondslag voor de verwerking van persoonsgegevens ten behoeve van de aanpak van ondermijning.

De gemeente zal de grondslag ook (intern) moeten onderbouwen en vastleggen (zie risico onder Governance).

¹ De wettelijke grondslag is de rechtvaardiging om persoonsgegevens te mogen verwerken, zoals bedoeld in artikel 6 lid 1 e.v. van de Algemene Verordening Gegevensbescherming. De wettelijke grondslagen uit dit artikel zijn; toestemming, ter uitvoering van een overeenkomst, wettelijke plicht, vitale belang, taak van algemeen belang en het gerechtvaardigd belang.

De samenwerking tussen de convenantpartners en tussen de daartoe opgerichte samenwerkingsverbanden RIEC's en het LIEC heeft als doel gezamenlijk invulling te geven aan:

- Een bestuurlijke en geïntegreerde aanpak van de georganiseerde criminaliteit door naast het strafrechtelijk laten vervolgen van individuele daders en het ontmantelen van criminele samenwerkingsverbanden ook bestuursrechtelijke interventies en fiscale handhaving aan te wenden om de georganiseerde criminaliteit te bestrijden
- De identificering van gelegenheidsstructuren binnen die economische sectoren en publieke voorzieningen die vatbaar zijn voor beïnvloeding door de georganiseerde criminaliteit opdat, middels het treffen van maatregelen ter bescherming, wordt voorkomen dat criminelen of criminele organisaties bewust of onbewust worden gefaciliteerd door de overheid en daardoor de democratische rechtstaat wordt ondermijnd.

De focus binnen de aanpak van ondermijnende criminaliteit door de RIEC's en het LIEC ligt momenteel op de volgende landelijke thema's:

- Georganiseerde hennepcultuur;
- Mensenhandel en -smokkel;
- Criminele motorbendes;
- Misbruik en fraude binnen de vastgoedsector;
- Witwassen en daaraan gerelateerde vormen van financieel-economische criminaliteit.

Naast deze landelijke thema's maakt elk RIEC regionale handhavingsschakelpunten inzichtelijk en organiseert de aanpak hiervan.

Persoonsgegevens die worden verwerkt in dit proces worden ook voor andere doeleinden gebruikt. Deze zijn:

- Het maken van rapportages in PGA-x. Er kunnen twee soorten rapportages beschikbaar worden gesteld.
 - Een fast-report tool op persoonsniveau of geaggregeerd niveau. Deze rapportages kunnen alleen bekeken worden door geautoriseerde gebruikers. Deze rapportage kan geëxporteerd worden. Deze exportfunctie wordt gelogd.
 - Er kunnen gegevens beschikbaar gesteld worden voor Index-rapportages aan de gemeente Den Haag. Voor deze functie heeft de gemeente Den Haag niet gekozen.
- Andere IKO-processen: een signaal kan als trigger dienen voor het Bibob en/of gemeentesignalen proces. Relevante informatie wordt gedeeld met behandelaar. Het is onbekend of de overdracht binnen PGA-x plaats kan vinden.

Rechtmatigheid van de verwerking

Op basis van de analyse valt te stellen dat de verwerking rechtmatig is. De gemeente moet de grondslag intern nog wel beschrijven, vastleggen en laten goedkeuren door de juiste managementniveaus in afstemming met de Gemeenteraad.

Risico's en maatregelen

Op basis van de analyse op het aspect *grondslag en doelbinding* zijn de volgende aandachtspunten en risico geïdentificeerd.

Aandachtspunten:

- De processen Bibob, RIEC-liaison en gemeentesignalen kennen overlap. Tevens kunnen persoonsgegevens voor het ene proces ook van belang zijn voor het andere proces. Schets kaders voor de uitwisseling van gegevens tussen deze processen. Leg vast op welke wijze PGA-x dit wel/niet kan faciliteren.
- De fast-report tool maakt rapportages op persoonsniveau mogelijk. Dit is niet wenselijk of noodzakelijk. Maak alleen rapportages op geaggregeerd niveau.

Risico: Spoorhouders weten niet altijd of ze gegevens mogen delen met de RIEC-liaison, hierdoor bestaat het risico dat er meer informatie gedeeld wordt dan noodzakelijk.

Spoorhouders weten niet altijd of en wanneer ze gegevens mogen delen met de RIEC-liaison. De kaders hiervoor zijn beschreven in het Handboek Privacy IKO Infodesk en zijn verder uitgewerkt in het *“Werkproces integrale casusaanpak door het Regionaal Informatie en Expertise Centrum (RIEC)”*. Deze kaders zijn (nog) niet voldoende bekend (bij de spoorhouders). Daarnaast is er geen privacy officer die hierbij kan ondersteunen. Hierdoor kunnen er al snel geen of juist te veel gegevens beschikbaar worden gesteld aan de RIEC-liaison. Uit de workshop is gebleken dat dit vaak plaatsvindt.

Maatregel:

Zorg dat bovenstaande kaders voor de gegevensuitwisseling bekend zijn bij de spoorhouders (of ondersteunende privacy officers). Daarnaast moet de RIEC-liaison alle irrelevante gegevens afkomstig van spoorhouders verwijderen of anonimiseren, voordat de gegevens worden gedeeld met het RIEC.

5.1.2.f heeft tijdens de workshop aangegeven dat er een e-learning ontwikkeld kan worden voor gebruikers van PGA-x over privacy en gegevensbescherming in het kader van ondermijning. Geadviseerd wordt gebruik te maken van deze optie.

4.3 Juistheid

Inleiding

Is de kwaliteit van de gegevens gewaarborgd (actueel, juist en volledig)? Hoe worden gegevens over de personen verwerkt (handmatig of automatisch?) Vindt er controle op de datakwaliteit plaats en zo ja wanneer?

Feiten & Analyse

De RIEC-liaison verifieert de gegevens in het ontvangen signaal. PGA-x ontsluit de BRP, KvK en het BRK.

De gegevens van de rechtspersoon worden gecontroleerd in het Handelsregister van de KvK. Informatie over de rechtspersonen wordt automatisch opgehaald op basis van het KVK-nummer uit het handelsregister. De identiteit van de betrokkene wordt gecontroleerd in het BRP. De RIEC-liaison valideert deze gegevens. In deze DPIA wordt uitgegaan van de juistheid van de bronsystemen.

In het signaaldocument afkomstig van het RIEC staan vrije tekstvelden. Dit is foutgevoelig en daardoor zijn de gegevens in sommige gevallen onjuist. Bovenstaande verificatie is daarom essentieel. Indien verkeerde informatie is doorgegeven, door bijvoorbeeld typefouten of verhuizingen, dan worden de gegevens gecorrigeerd. Aanpassingen worden handmatig in het systeem verwerkt. De bron wordt nooit aangepast.

De RIEC-liaison verrijkt het signaal ook met aanvullende gegevens uit bovenstaande bronnen. Dit kan gaan om rechtspersonen waaraan subjecten uit het signaal aan verbonden zijn, maar niet vermeld zijn in het signaalformulier. Dit geldt ook voor locatiegegevens.

Het komt regelmatig voor dat casus een lange doorlooptijd heeft. De RIEC-liaison verifieert de gegevens daarom altijd in bovenstaande bronnen als er een actie wordt uitgevoerd op een casus. Dit voorkomt dat gegevens over de betrokkene onjuist zijn: een betrokkene kan immers verhuisd zijn of een onderneming inmiddels failliet. Verificatie vindt, om dezelfde reden, ook plaats voordat een interventie wordt uitgevoerd.

Er worden geen dossiers gemigreerd naar PGA-x. Hierin wordt begonnen met een schone lei. Er is daarom geen migratiestrategie nodig voor dit proces.

Risico's en maatregelen

Ten aanzien van het beginsel *Juistheid* is het volgende aandachtspunt geïdentificeerd:

Aandachtspunt: de RIEC-liaison beoordeelt op basis van zijn professionele afweging of andere subjecten worden meegenomen in het onderzoek. Er zijn geen werkinstructies of richtlijnen gemaakt die vuistregels bieden. Werkinstructies of richtlijnen komen de consistentie in het proces ten goede en helpen ook nieuwe werknemers bij het maken van deze afweging.

4.4 Dataminimalisatie

Inleiding

Kan er met bijvoorbeeld minder persoonsgegevens, of op een andere manier worden gewerkt zonder de functionaliteit van het proces en systeem aan te tasten? Zijn er rapportages waarin tot individuen herleidbare informatie is opgenomen? Worden alleen die gegevens vastgelegd die absoluut noodzakelijk zijn voor het doel van de verwerking? Welke zijn dat niet?

Feiten & Analyse

In dit proces worden persoonsgegevens over natuurlijke personen (subjecten) en rechtspersonen (objecten) verwerkt, evenals locatiegegevens. Locatiegegevens kunnen bijvoorbeeld nevenvestigingen, andere adressen of andere gebouwen van de betrokkene zijn die relevant blijken voor het onderzoek.

Het informatieverzoek vanuit het RIEC is uiteengezet in twee fases; de Quickscanfase en de Informatieverzoekfase. In de Quickscanfase wordt nog niet alle gemeentelijke informatie uit de beschikbare bronnen gedeeld met het RIEC. Voor het signaal relevante spoorhouders worden door de RIEC-Liaison benaderd via PGA-x met de volgende vragen:

- Is er informatie aanwezig binnen de gemeente betreffende het signaal?
- Is er belang bij de gemeente om deel te nemen aan het casusoverleg?
- Zijn er voor de gemeente interventiemogelijkheden inzake het signaal?

De spoorhouder beantwoordt deze vragen in PGA-x alleen met ja/nee. PGA-x staat geen andere antwoorden toe. De spoorhouder verstrekt in deze fase dus nog geen persoonsgegevens uit de bronsystemen aan de RIEC-liaison. Op basis van de antwoorden van de spoorhouders beslist de RIEC-liaison of deelname aan de RIEC-casus relevant is voor de gemeente. Deze informatie wordt gedeeld met (de accounthouder van) het RIEC.

Als er voldoende partners in het RIEC willen deelnemen aan de casus, start de Informatieverzoekfase. De RIEC-liaison ontvangt via het RIEC-IS het informatieverzoek. De RIEC-liaison verzoekt de spoorhouders die hebben aangegeven belang bij de RIEC-casus te hebben, om aanvullende informatie via PGA-x. De spoorhouders ontvangen aanvullende informatie uit het signaalformulier ter toelichting op het signaal subjecten (personen en/of bedrijven), objecten (panden en adressen), korte beschrijving verdenking en eventueel informatie uit open bronnen). In de Quickscanfase wordt deze informatie nog niet gedeeld met de spoorhouders door de RIEC-liaison. De RIEC-liaison beoordeelt in deze fase welke aanvullende informatie gedeeld wordt met de spoorhouder(s) en legt, ter verantwoording, een (korte) motivering hiervoor vast in het dossier.

Het vraagstuk noodzakelijkheid, proportionaliteit, subsidiariteit en doelbinding wordt voor ieder informatieverzoek beoordeeld door de RIEC-liaison wanneer spoorhouders gegevens aanleveren via PGA-x. De RIEC-liaison beoordeelt of irrelevante gegevens verwijderd dienen te worden. Irrelevante gegevens worden in een mapje gestopt en binnen een jaar verwijderd. Tijdens de workshop werd aangegeven dat het moeilijk is om irrelevante gegevens, als onderdeel van een groter geheel, te verwijderen (zie risico onder grondslag &

doelbinding. Als de gegevens niet kunnen worden verwijderd volgt advies om te anonimiseren).

De gemeente ontvangt soms een signaal vanuit het RIEC die niet aansluit op de thematiek in het RIEC convenant. Dit signaal wordt afgesloten en daarmee verwijderd uit de werkvoorraad. De RIEC-liaison geeft een terugkoppeling aan het RIEC. In de praktijk is dit nog niet voorgekomen.

De RIEC-liaison zorgt ervoor dat alleen de noodzakelijke gegevens worden gedeeld met de bij de casus betrokken spoorhouders en RIEC-partners.

Risico's en maatregelen

Ten aanzien van het beginsel *dataminimalisatie* is het volgende risico geïdentificeerd. Deze worden hieronder beschreven.

Risico: Spoorhouders bewaren onnodig informatie over subject/object/signaal

Bij een casus betrokken spoorhouders ontvangen vertrouwelijke informatie over subject/object. De informatie wordt uitgewisseld via PGA-x. Het is niet bekend of spoorhouders deze informatie ook lokaal bewaren. Dit vergroot namelijk het risico op datalekken en zorgt er mogelijk voor dat de persoonsgegevens langer worden bewaard dan toegestaan is.

Maatregel:

Spreek af met de spoorhouders dat zij de informatie uit het signaal over subject/object direct verwijderen na het beantwoorden van de vragen in de QuickScan of informatieverzoekfase. Indien mogelijk wordt afgesproken dat de spoorhouders geen informatie over het signaal lokaal opslaan.

Risico: De gemeente ontvangt signalen die niet passen in de thematiek van het RIEC convenant

Signalen zijn onrechtmatig door het RIEC verstrekt als deze niet in de landelijke of regionale thema's van het RIEC convenant en bijbehorend Privacyprotocol vallen.

Maatregel:

De gemeente dient het signaal direct terug te koppelen aan het RIEC. Zorg er voor dat het signaal niet wordt geregistreerd in PGAx en verwijder het direct uit eventuele overige opslaglocaties (zoals de G:schijf). Als het signaal is geregistreerd in PGAx en de liaison komt er pas na verrijking achter dat het signaal niet past in de thematiek van het convenant, dan wordt het signaal afgesloten. Ook dan moet het signaal worden verwijderd of geanonimiseerd, zodat het signaal niet meer (herleidbaar) wordt gemonitord of getoond.

4.5 Opslag

Inleiding

Welke bewaartermijnen zijn van toepassing? Hoe worden persoonsgegevens bewaard en worden persoonsgegevens die niet langer nodig zijn daadwerkelijk verwijderd? Worden op de middelen (desktop, pc, mobiele telefoon) zelf gegevens opgeslagen?

Feiten & Analyse

De gegevens in het RIEC-liaison proces worden op meerder plekken opgeslagen:

RIEC-IS: Het RIEC-IS systeem is het gezamenlijke informatiesysteem van partners in het RIEC en valt buiten de scope van deze DPIA.

PGA-x: De gegevens die door de RIEC-liaison worden verzameld n.a.v. een QuickScan of informatieverzoek, worden opgeslagen in PGA-x.

G:schijf: De G:schijf binnen de gemeente wordt gebruikt als tijdelijke opslaglocatie. De leverancier onderzoekt of PGA-x kan voorzien in een standaard download- en upload locatie op de G:schijf. Dit is ten tijde van deze DPIA nog niet het geval.

De server van PGA-x staat in Rotterdam. De gegevens in PGA-x worden binnen de EER verwerkt.

De bewaartermijn voor persoonsgegevens in dit proces is nog niet vastgesteld door de gemeente Den Haag. De gemeente sluit aan bij de bewaartermijn die wordt gehanteerd voor persoonsgegevens die worden verwerkt door het RIEC in het kader van een casus.

- Indien het Quicksan verzoek niet leidt tot een casus, wordt de casus voor maximaal een jaar bewaard in PGA-x.
- Indien het wel een RIEC-casus wordt, wordt het maximaal vijf jaar bewaard (deze bewaartermijn is van toepassing op het RIEC. Dit staat in artikel 17 van het Privacy Protocol RIEC's LIEC).
- Als het signaal doorgezet wordt naar het gemeentesignalenproces, worden de bewaartermijnen van dit proces gevolgd.

Deze bewaartermijnen zijn nog niet als instructie gegeven aan ^{5.1.2.f} voor implementatie van PGA-x.

De back-up worden volgens ^{5.1.2.f} bewaard conform de afspraken in de verwerkersovereenkomst. Zoals vastgesteld onder het thema 'Governance' moet de verwerkersovereenkomst nog worden gesloten. Er zijn dus nog geen afspraken over het back-up beleid bekend bij ^{5.1.2.f}

Nadat de bewaartermijn is verstreken wordt het dossier in PGA-x op een archiveringslijst (recordlijst) gezet. Deze recordlijst kan worden geëxporteerd naar het gemeentelijk archief, zodat te allen tijde duidelijk wordt wat er is vernietigd. Het is onduidelijk of deze verplichting

in de archiefwet staat. De metadata van verwijderde dossiers is, na vernietiging, nog steeds beschikbaar in de vorm van rapportages.

Inactieve dossiers met daarin gegevens die niet langer worden gebruikt, worden niet verwijderd uit de lijst met actieve dossiers. Deze dossiers blijven zichtbaar op het dashboard en zijn toegankelijk voor geautoriseerde.

De gemeente heeft nog geen autorisatiematrix of ander toegangsbeleid gedeeld met 5.1.2.f. Er zijn daarom nog geen rechten bekend. Toegang is gebaseerd op need-to-know. 5.1.2.f checkt eenmaal per drie maanden bij eigenaren van een dossier of de lijst met beheerders nog actueel is.

Risico's en maatregelen

Ten aanzien van het beginsel *opslag* is/zijn de volgende aandachtspunten en risico geïdentificeerd. Deze worden hieronder beschreven.

Aandachtspunten:

- Ga na of de recordlijst (verplicht) naar het gemeentelijk archief geëxporteerd dient te worden. Ga na of de exportlijst verplicht gearchiveerd dient te worden.
- Ga na of de G:schijf kan worden voorzien van een bewaartermijn. Verwijder afgesloten of inactieve dossiers van de lijst met actieve dossiers. Richt hiervoor een aparte lijst in met beperkte toegang.
- Leg de wettelijke of vanuit de bedrijfsvoering gehanteerde bewaartermijnen en het back-up beleid zo snel mogelijk vast in een verwerkersovereenkomst met 5.1.2.f

Risico: gegevens worden langer dan noodzakelijk is bewaard

De gemeente heeft intern geen bewaartermijn(en) vastgesteld voor het RIEC-liaison proces. De gemeente hanteert dezelfde bewaartermijnen als het RIEC. Gegevens die door de RIEC-liaison worden verzameld in het kader van een QuickScan die niet leidt tot een RIEC-casus worden één jaar bewaard. Overige gegevens worden vijf jaar bewaard. De bewaartermijnen zijn daarentegen niet onderbouwd voor dit proces. De noodzaak is daardoor niet (voldoende) aangetoond. De gegevens kunnen geraadpleegd worden in het RIEC-IS en/of zijn te herleiden uit verschillende bronbestanden. Gegevens worden daarom mogelijk langer dan noodzakelijk bewaard. Dit maakt een inbreuk op de rechten en vrijheden van betrokkenen. De impact van een datalek neemt hierdoor bijvoorbeeld aanzienlijk toe.

Maatregel:

Stel intern de bewaartermijn vast voor gegevens die worden verwerkt in het RIEC-liaison proces. Sluit aan bij de best practice voor het hanteren van bewaartermijnen voor dit soort signalen. Onderbouw de keuze voor de bewaartermijn, zodat hierop gestuurd kan worden. Toets de bewaartermijnen periodiek. Dit kan bijvoorbeeld jaarlijks.

4.6 Bescherming

Inleiding

Persoonsgegevens moeten technisch en organisatorisch adequaat worden beschermd. Op welke wijze is de toegang tot gegevens afgeschermd? Is dit voldoende veilig in verhouding tot de gevoeligheid van de gegevens die verwerkt worden? Welke externe partijen hebben toegang tot de gegevens (leveranciers, samenwerkingspartners, dienstverleners) en hoe is de beveiliging daar geregeld?

Feiten & Analyse

De medewerkers maken gebruik van een afgeschermd G:schijf. De G:schijf is alleen toegankelijk voor de medewerkers van het team ondermijning. 5.1.2.f
5.1.2.i

5.1.2.f is ISO 27001 en NEN 7510 gecertificeerd. Er vindt jaarlijks een externe audit plaats. Daarnaast vinden maandelijks tot jaarlijks interne audits (afhankelijk van het onderwerp) plaats. Tweemaal per jaar vindt een code review plaats en wordt een pentest uitgevoerd. De ISO heeft de effectiviteit van de door 5.1.2.f getroffen maatregelen beoordeeld op basis van vooraf bepaalde informatiebeveiligingseisen. De getroffen maatregelen zijn volgens de ISO in lijn met de gestelde eisen.

5.1.2.f maakt gebruik van een subverwerker: 5.1.2.f s ISO 27001 en NEN 7510 gecertificeerd. Ze beschikken tevens over een ISAE 3402 type II verklaring en SOC2 Assurance rapport. Scope is onbekend.

De gemeente heeft nog geen autorisatiematrix of ander toegangsbeleid gedeeld met 5.1.2.f Er zijn daarom nog geen rechten bekend. Toegang is gebaseerd op need-to-know. 5.1.2.f checkt eenmaal per drie maanden bij eigenaren van een dossier of de lijst met beheerders nog actueel is.

Medewerkers kunnen inloggen in PGA-x via Single Sign On (SSO). Medewerkers loggen in op het netwerk via mulfi-factor authentication (MFA).

Er is nog geen key-user functioneel beheer aangesteld, maar dit wordt waarschijnlijk in samenwerking met het Zorg- en Veiligheidshuis geregeld.

Risico's en maatregelen

Ten aanzien van het beginsel *bescherming* zijn de volgende aandachtspunten geïdentificeerd. Deze worden hieronder beschreven.

Aandachtspunten:

- De gemeente heeft nog geen autorisatiematrix opgesteld waarin het toegangsbeheer voor PGA-x wordt geregeld. Maak een autorisatiematrix gebaseerd op role based access. Laat deze autorisatiematrix toetsen door de Information Security Officer.

- Het functioneel beheer van PGA-x is nog niet belegd. Zorg ervoor dat het functioneel beheer duidelijk belegd wordt. Mocht het functioneel beheer belegd worden bij ^{5.1.2.f} zorg dan voor duidelijke afspraken over de omgang met persoonsgegevens. De medewerker(s) die als functioneel beheerder te werk gaan zullen aan een geheimhoudingsverklaring gebonden moeten worden.
- ^{5.1.2.i}
- Leg de informatiebeveiligingseisen vast in de verwerkersovereenkomst.

4.7 Transparantie

Inleiding

De gemeente is helder in de gegevens die zij verwerkt. De betrokkene moet goed kunnen begrijpen welke persoonsgegevens worden verwerkt (en waarom) en heeft het recht en de mogelijkheid om in te grijpen. De betrokkene heeft het recht op informatie, inzage, correctie en verwijdering.

Feiten & Analyse

De RIEC-liaison verzamelt gegevens uit openbare bronnen en uit gemeentelijke bronsystemen via spoorhouders van diensten binnen de gemeente over een subject/object n.a.v. een QuickScan of informatieverzoek en deelt de gegevens met het RIEC. De betrokkene wordt hierover niet geïnformeerd.

De betrokkene wordt momenteel niet geïnformeerd over het RIEC proces of de deelname van de gemeente Den Haag daaraan. Wel is er een pagina "Haags veiligheidsbeleid" waar de 3 sporen aanpak wordt beschreven².

In aanvulling hierop wordt in artikel 15 lid 2 van het Privacy Protocol het volgende gelezen over de algemene informatievoorziening aan betrokkene(n). 'In het belang van de algemene transparantie over de geïntegreerde aanpak van de georganiseerde criminaliteit worden het Convenant, Privacyprotocol en de werkprocessen van de RIEC's gepubliceerd op de websites van alle RIEC's en alle convenantpartijen'.

Op de website van het RIEC staan de werkwijzen van het RIEC uitvoerig toegelicht.

In dit proces moet onderscheid worden gemaakt tussen een generieke informatieverstrekking en een specifieke informatieverstrekking. De generieke informatieverstrekking hoort thuis in de privacyverklaring en/of bijbehorende pagina's van de gemeente Den Haag. De specifieke informatieverstrekking vindt plaats op onderstaande wijze en wordt gecoördineerd vanuit het RIEC.

Indien tot interventie wordt besloten, vindt de mededeling/verstrekking van informatie plaats tegelijk met de feitelijke uitvoering van de interventie.

Indien wordt besloten het onderzoek aan te houden of van een interventie af te zien, vindt de mededeling/verstrekking plaats binnen een termijn van één maand. Deze mededeling/verstrekking kan, gelet op artikel 41 UAVG, op een later moment plaatsvinden of achterwege blijven, voor zover dit noodzakelijk is in het belang van onder meer de voorkoming, het onderzoek, de opsporing en vervolging van strafbare feiten, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid.

De gemeente heeft (nog) geen AVG verzoeken ontvangen van betrokkenen over RIEC casuïstiek. Betrokkenen bij een RIEC-casus kunnen bij de gemeente een verzoek indienen in

² <https://www.denhaag.nl/nl/in-de-stad/veiligheid/haags-veiligheidsbeleid.htm>

het kader van een verwerkingsactiviteit in een RIEC-casus. Beantwoording van deze verzoeken wordt gecoördineerd door het RIEC overeenkomstig het bepaalde in artikel 15.3 van het Privacyprotocol RIEC-LIEC. De medewerkers van de gemeente Den Haag zijn niet op de hoogte van dit proces. Als er een verzoek binnenkomt, zouden zij advies vragen bij een collega.

Risico's en maatregelen

Ten aanzien van het beginsel *transparantie* zijn de volgende risico's geïdentificeerd. Deze worden hieronder beschreven.

Risico: Betrokkenen worden onvoldoende geïnformeerd over de gegevensverwerking en/of de rechten die zij kunnen uitoefenen op grond van de AVG.

Betrokkenen worden onvoldoende geïnformeerd over de verwerkingsactiviteit door de gemeente Den Haag in het RIEC-liaison proces en de deelname aan de casusaanpak in het RIEC. Betrokkenen zijn zich daardoor niet bewust van de rechten die zij kunnen uitoefenen (inzage, rectificatie, bezwaar etc.).

Maatregel

Neem in de privacyverklaring van de gemeente Den Haag een onderdeel op over het RIEC-liaison proces en/of verwijs naar de pagina over het Haags Veiligheidsbeleid. In het kader van transparantie naar betrokkenen zou dit een logisch plek zijn om bijvoorbeeld onder punt 3 “integrale aanpak van ondermijning”, toe te voegen: “De gemeente werkt samen met andere partijen in het RIEC. Voor meer informatie zie www.riec.nl.”

Risico: Medewerkers weten niet hoe ze moeten voldoen aan de rechten van betrokkenen

In het privacyprotocol RIEC-LIEC staat een werkinstructie over de uitvoering van de rechten van betrokkenen. Deze werkinstructie is niet bekend bij de medewerkers. Als er een verzoek wordt ontvangen door de medewerkers, vragen zij om hulp bij een collega. Een aangewezen persoon hiervoor is de privacy officer.

Maatregel:

Informeer medewerkers over de werkwijze bij het ontvangen van een AVG-verzoek. Zorg ervoor dat de medewerkers makkelijk toegang hebben tot de procedure doordat deze beschikbaar is. Daarnaast is het belangrijk dat medewerkers met vragen over het behandelen van een AVG-verzoek terecht kunnen bij de privacy officer. Het is essentieel dat deze rol structureel wordt ingevuld.

4.8 Cultuur

Inleiding

Zijn medewerkers zich bewust van het belang van het beschermen van privacygevoelige gegevens? Gaat iedereen even zorgvuldig om met de gegevens, worden betrokkenen goed geïnformeerd over hoe men moet omgaan met die gegevens?

Feiten & analyse

Privacy wordt een steeds belangrijker thema binnen de directie Veiligheid. Dit blijkt bijvoorbeeld uit het volgende:

De afdeling Ondermijning heeft vorig jaar een het 'Handboek Privacy IKO-infodesk' laten opstellen door een extern adviesbureau. Dit handboek beschrijft de werkprocessen voor het Bibob, RIEC-liaison en gemeentesignalen proces vanuit privacy perspectief.

De afdeling Ondermijning heeft een externe privacy expert ingehuurd om te adviseren over de implementatie van de werkprocessen in PGA-x.

Op dit moment wordt nog te weinig gedaan om de bewustwording van medewerkers op het gebied van privacy te vergroten. Zo is er al ruime tijd geen bewustwordingsactiviteit, zoals een training of e-learning, georganiseerd voor medewerkers. Tijdens de workshop is duidelijk aangegeven dat medewerkers hier behoefte aan hebben. Medewerkers zijn bereid zich te verdiepen in dit thema en erkennen de relevantie daarvan in het licht van de aard van de verwerkingsactiviteit.

Er is geen formeel clean-desk beleid aanwezig. In de workshop wordt aangegeven dat medewerkers hun laptop niet altijd vergrendelen. Tevens blijven veel documenten op bureaus liggen en worden de deuren niet altijd op slot gedaan.

PGA-x biedt een privacy module aan voor de gemeente Den Haag. Het is nog onbekend of deze door de gemeente Den Haag geïmplementeerd wordt.

Risico's en maatregelen

Op basis van de analyse op het aspect *cultuur* zijn de volgende risico's geïdentificeerd. Deze worden hieronder beschreven.

Risico: Er is te weinig aandacht voor privacy geweest waardoor medewerkers onvoldoende getraind zijn in het herkennen van privacy risico's

Medewerkers zijn lange tijd niet getraind in privacy bewustwording. Hierdoor zijn zij onvoldoende ervaren om privacy risico's en/of datalekken te herkennen. Ook weten medewerkers niet altijd hoe ze hiermee om moeten gaan.

Maatregel

Vergroot het privacybewustzijn van de medewerkers. Dit kan bijvoorbeeld door e-learning, klassikale trainingen, posters, gadgets en het organiseren van een informatieve lunch. Zorg er idealiter voor dat deze trainingen zijn afgestemd op praktische situaties gericht op de ondermijningspraktijk. Het is ook belangrijk dat

medewerkers bij een privacy officer terecht kunnen met privacy gerelateerde vraagstukken (zie governance). Implementeer de privacy module in PGA-x en zorg ervoor dat medewerkers deze uitvoeren, voordat zij aan de slag gaan met het systeem.

5. Advies en accordering

In het risico overzicht dat als bijlage aan deze rapportage is toegevoegd wordt weergegeven welke privacy risico's de verwerking met zich meebrengt, welke beheersmaatregelen hiervoor nodig zijn en welke acties hieraan gekoppeld zijn. Dit overzicht wordt bewerkt zodra beheersmaatregelen worden uitgevoerd en risico's gemitigeerd, zo blijft de DPIA up to date ook na het uitvoeren van beheers acties.

Aanbevelingen voor vervolg

Wij adviseren om de hierboven genoemde risico's als volgt aan te pakken:

1. Benoem een business eigenaar van ieder risico in het risico overzicht en de bijbehorende maatregelen.
2. Geef de business eigenaar de opdracht de maatregelen in te voeren en daarmee het risico te mitigeren.
3. Geef elke 2 maanden een status update van de opvolging van deze aanbevelingen aan de FG en de Privacy Officer.

De huidige analyse is uitgevoerd voordat alle inhoudelijke gesprekken met de leverancier over implementatiekeuzes zijn gevoerd. Wij doen daarom een aanbeveling om een verdiepende analyse uit te voeren op de volgende onderwerpen nadat alle implementatiekeuzes zijn gemaakt:

- Beveiliging en opslag

Advies FG

[GEBRUIK DEZE RUIMTE VOOR HET ADVIES VAN DE FG]

Naam: 5.1.2.e

Datum: [DATUM]

Accordering

Deze DPIA is opgeleverd aan:

[PROCESEIGENAAR FUNCTIE]	Functionaris Gegevensbescherming
Datum oplevering: [DATUM]	Datum oplevering: [DATUM]
Naam: 5.1.2.e	Naam: 5.1.2.e
Voor akkoord: [HANDTEKENING PROCESEIGENAAR]	Voor gezien: [HANDTEKENING FG]
Datum ondertekening: [DATUM]	Datum ondertekening: [DATUM]

Tekent voor gezien:

(Algemeen) Directeur [DIENST]
Datum oplevering: [DATUM]
Naam: 5.1.2.e
Tekent voor gezien: [HANDTEKENING DIRECTEUR]
Datum ondertekening: [DATUM]

Bijlage A

A1. Documentatie

De volgende documentatie is geraadpleegd.

Nr.	Documentnaam	Link
1	DPIA RIEC proces gemeente Den Haag	
2	Convenant ten behoeve van Bestuurlijke en Geïntegreerde Aanpak Georganiseerde Criminaliteit, Bestrijding Handhavingsknelpunten en Bevordering Integriteitsbeoordelingen	Convenant ten behoeve van Bestuurlijke en Geïntegreerde Aanpak Georganiseerde Criminaliteit, Bestrijding Handhavingsknelpunten en Bevordering Integriteitsbeoordelingen Convenant RIEC-LIEC Informatie- en Expertisecentrum
3	Handboek Privacy IKO Infodesk - final2	
4	Informatiebeveiligingseisen externe dienstverlening PGA-x	

A2. Geïnterviewden

De volgende personen hebben meegewerkt tijdens de DPIA sessie.

Datum	Geïnterviewden	Functie/Rol
08-07-2021	5.1.2.e	5.1.2.e
08-07-2021	5.1.2.e	
08-07-2021	5.1.2.e	
08-07-2021	5.1.2.e	
08-07-2021	5.1.2.e	
08-07-2021	5.1.2.e	