INFORMATIE
BEVEILIGINGS
DIENST

TOELICHTING PIA

Een van de producten van de operationele variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN **IN OPDRACHT VAN**
VERENIGING VAN NEDERLANDSE GEMEENTEN

INFORMATIE
BEVEILIGINGS
DIENST

Colofon

Naam document
Toelichting PIA

Versienummer
1.0

Versiedatum
Maart 2014

Versiebeheer
Het beheer van dit document berust bij de Informatiebeveiligingsdienst voor gemeenten (IBD).

Rechten en vrijwaring
KING is zich bewust van haar verantwoordelijkheid een zo betrouwbaar mogelijke uitgave te verzorgen. Niettemin kan KING geen aansprakelijkheid aanvaarden voor eventueel in deze uitgave voorkomende onjuistheden, onvolledigheden of nalatigheden. KING aanvaardt ook geen aansprakelijkheid voor enig gebruik van voorliggende uitgave of schade ontstaan door de inhoud van de uitgave of door de toepassing ervan.

Met dank aan
De expertgroep en de reviewgemeenten die hebben bijgedragen aan het vervaardigen van dit product en de gemeente Amsterdam voor het aanleveren van hun PIA methode.

In samenwerking met
De producten van de operationele variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) worden vervaardigd in samenwerking met:

TASKFORCE

INFORMATIE
BEVEILIGINGS
DIENST

Voorwoord

De IBD is een gezamenlijk initiatief van de Vereniging van Nederlandse Gemeenten (VNG) en het Kwaliteitsinstituut Nederlandse Gemeenten (KING) en actief sinds 1 januari 2013. Aanleiding voor de oprichting van de IBD vormen enerzijds de leerpunten uit een aantal grote incidenten op informatiebeveiligingsvlak en anderzijds de visie Digitale Overheid 2017.
De IBD is er voor alle gemeenten en richt zich op bewustwording en concrete ondersteuning om gemeenten te helpen hun informatiebeveiliging naar een hoger plan te tillen.

De IBD heeft drie doelen:

1. het preventief en structureel ondersteunen van gemeenten bij het opbouwen en onderhouden van bewustzijn als het gaat om informatiebeveiliging.
2. het leveren van integrale coördinatie en concrete ondersteuning op gemeente specifieke aspecten in geval van incidenten en crisissituaties op het vlak van informatiebeveiliging.
3. het bieden van gerichte projectmatige ondersteuning op deelgebieden om informatiebeveiliging in de praktijk van alle dag naar een hoger plan te tillen. De ondersteuning die de IBD biedt bij het ICT-Beveiligingsassessment DigiD is een voorbeeld van een dergelijk project.

Hoe realiseert de IBD haar doelen?

Om invulling te kunnen geven aan haar doelen is door de IBD op basis van de Baseline Informatiebeveiliging Rijksdienst (BIR) een vertaalslag gemaakt naar een baseline voor de gemeentelijke markt. Deze Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) betreft twee varianten, een Strategische- én een Tactische Baseline. Beide varianten van de BIG zijn beschikbaar voor alle gemeenten op de community van de IBD, zodat door iedere gemeente tot implementatie van de BIG kan worden overgegaan. Bestuur en management hebben met deze baseline een instrument in handen waarmee zij in staat zijn om te meten of de organisatie ‘in control’ is op het gebied van informatiebeveiliging. Om de implementatie van de Strategische en Tactische Baseline te ondersteunen, zijn door de IBD in samenwerking met de Taskforce Bestuur en Informatieveiligheid Dienstverlening producten ontwikkeld op operationeel niveau. Dit heeft een productenportfolio opgeleverd, genaamd de Operationele Baseline Nederlandse Gemeenten. Onderhavig product is onderdeel van het productenportfolio.
Naast een productenportfolio, heeft de IBD voor gemeenten ook een dienstenportfolio ontwikkeld. Voor een volledig overzicht van het producten- en dienstenportfolio, kunt u terecht op de website van de IBD.

De gemeente is zelf verantwoordelijk voor het opstellen en/of uitvoeren en/of handhaven van de regels. Hierbij geldt:

- Er is wetgeving waar altijd aan voldaan moet worden, zoals niet uitputtend: GBA, SUWI, BAG, PUN en WBP, maar ook de archiefwet.
- Er is een gemeenschappelijk normenkader als basis: de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).
- De gemeente stelt dit normenkader vast, waarbij er ruimte is in de naleving van dat kader voor afweging en prioritering op basis van het ‘pas toe of leg uit’ principe.

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

Leeswijzer

Dit product maakt onderdeel uit van de operationele variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

Doel
Dit document is de toelichting bij het Privacy Impact Assessment (PIA) instrument ter ondersteuning bij het uitvoeren van de PIA.

Doelgroep
Dit document is van belang voor het management van de gemeente, de systeemeigenaren, de ICT-afdeling en de CISO.

Relatie met overige producten

- Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)
  - Strategische variant van de Baseline Informatiebeveiliging voor Gemeenten
  - Tactische variant van de Baseline Informatiebeveiliging voor Gemeenten
- Informatiebeveiligingsbeleid van de gemeente
- Verkorte Risicoanalyse / Baselinetoets

Maatregelen tactische variant Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)

10.8.5.1	Er zijn richtlijnen met betrekking tot het bepalen van de risico's die het gebruik van gemeentelijke informatie in kantoorapplicaties met zich meebrengen en richtlijnen voor de bepaling van de beveiliging van deze informatie binnen deze kantoorapplicaties. Hierin is minimaal aandacht besteed aan de toegang tot de interne informatievoorziening, toegankelijkheid van agenda's, afscherming van documenten, privacy, beschikbaarheid, back-up en in voorkomend geval Cloud-diensten.
15.1.4.1	De bescherming van gegevens en privacy behoort te worden bewerkstelligd in overeenstemming met relevante wetgeving, voorschriften en indien van toepassing contractuele bepalingen.

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

INFORMATIE
BEVEILIGINGS
DIENST

Inhoudsopgave

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

1 Over het instrument PIA

In dit eerste deel wordt ingegaan op de achtergrond en het belang van de PIA. U krijgt antwoord op vragen als: Wat is een PIA? Wat is het belang van een PIA? Wat levert het uitvoeren van een PIA op? Hoe verhoudt de PIA zich tot andere privacy instrumenten?

1.1 Wat is privacy?

Privacy is een veel omvattend begrip. Kortweg wordt privacy ook wel omschreven als 'het recht om met rust te worden gelaten'. Het begrip privacy bevat onderdelen (dimensies) waarmee invulling aan de persoonlijke levenssfeer kan worden gegeven. Voorbeelden van deze dimensies van privacy zijn het eigen lichaam, de eigen woning, het familie- en gezinsleven, vertrouwelijke communicatie en persoonsgegevens. De bescherming van deze dimensies zijn grondrechten.
Daarnaast hanteert men ook informationele zelfbeschikking: burgers dienen (behoudens wettelijke uitzonderingen) zelf controle te hebben over wat er met hun gegevens gebeurd.

In deze PIA, die is overgenomen van NOREA en de gemeente Amsterdam, heeft privacy vooral betrekking op de bescherming van persoonsgegevens. De bescherming van persoonsgegevens kan omschreven worden als het recht op transparante, eerlijke, veilige en betrouwbare informatieverwerking.

Leidend in het denken en praten over bescherming van persoonsgegevens zijn de privacy principes van de OECD/OESO[1]. Deze principes bieden houvast voor het op een goede manier verwerken van persoonsgegevens. Momenteel regelt de EU Richtlijn 95/46/EG de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens. In Nederland is deze Richtlijn geïmplementeerd in de Wet bescherming persoonsgegevens (Wbp)[2]. Naar verwachting zal in 2014 de nieuwe EU-privacy verordening in werking treden. U dient er rekening mee te houden dat de nieuwe verordening consequenties kan hebben die tot heroverweging van de beheersmaatregelen met betrekking tot privacy kunnen leiden.
In de NOREA-publicatie over de nieuwe Europese verordening worden de kernelementen van deze verordening beschreven[3].

1.2 Beschrijving van het instrument PIA

Wat is een PIA?

PIA staat voor Privacy Impact Assessment.
De PIA legt in de eerste plaats de risico's bloot van projecten die te maken hebben met privacy, en dragen bij aan het vermijden of verminderen van deze privacy risico's.
Op basis van de antwoorden van de PIA wordt op systematische wijze inzichtelijk gemaakt of er een kans is dat de privacy van de betrokkene wordt geschaad, hoe hoog deze is en op welke gebieden dit is.

[1] Organisation for Economic Cooperation and Development/Organisatie voor Economische Samenwerking en Ontwikkeling
[2] http://wetten.overheid.nl/BWBR0011468/
[3] Het Europees privacyrecht in beweging (IT-Recht, februari 2013 NOREA/Kluwer en Duthler Associates)

De PIA doet dit door op gestructureerde wijze:

- De mogelijk (negatieve) gevolgen van het gebruik van persoonsgegevens voor de betrokken personen en organisaties in kaart te brengen.
- De risico's voor de betrokken personen en organisaties zo veel mogelijk te lokaliseren.

Op basis van de uitkomsten van de PIA kunt u gericht acties ondernemen om deze risico's te verminderen.

De PIA is een verplicht instrument en een onmisbaar hulpmiddel voor organisaties om de privacy impact van hun projecten te evalueren.

Door het gebruik van de PIA kan bescherming van persoonsgegevens op een gestructureerde manier onderdeel uitmaken van de belangenafweging en besluitvorming over een project.

Wat levert een PIA op?

De PIA kent een aantal belangrijke doelen. Het belangrijkste doel is:

1. Het voorkomen van kostbare aanpassingen in processen, herontwerp van systemen of stopzetten van een project door vroegtijdig inzicht in de belangrijkste privacy risico's.

Daarnaast kunnen nog de volgende doelen worden onderscheiden:

2. Het verminderen van de gevolgen van toezicht en handhaving.
3. Het verbeteren van de kwaliteit van gegevens.
4. Het verbeteren van de dienstverlening.
5. Het verbeteren van de besluitvorming.
6. Het verhogen van het privacy bewustzijn binnen een organisatie.
7. Het verbeteren van de haalbaarheid van een project.
8. Het verstevigen van het vertrouwen van de klanten, werknemers of burgers in de wijze waarop persoonsgegevens worden verwerkt en privacy wordt gerespecteerd.
9. Het verbeteren van de communicatie over privacy en de bescherming van persoonsgegevens.
10. Inzicht in, of ontdekken van, schaduw registraties waar mogelijk verplicht gebruik van basisregistraties van toepassing hoort te zijn.

Voor wie is het instrument PIA bedoeld?

De PIA kan gebruikt worden door alle typen organisaties. In het algemeen kan worden gezegd dat het noodzakelijk is een PIA uit te voeren bij een nieuw project of grote wijziging van een bestaand systeem of proces, waarbij persoonsgegevens worden verwerkt. Binnen deze doelgroep is de PIA bedoeld voor opdrachtgevers en opdrachtnemers van projecten en andere belanghebbenden. De personen die de PIA kunnen uitvoeren staan in bijlage 2.

Wanneer wordt een PIA uitgevoerd?

Een PIA kan het beste in de definitiefase van een project uitgevoerd worden, als vervolg op de Baselinetoets of de verkorte Risicoanalyse. Immers, als u de PIA in een te vroeg stadium uitvoert, heeft u nog geen zicht op de feitelijke gegevensstromen en datasets. De PIA kan ook worden uitgevoerd bij een bestaand systeem als men twijfelt of er wel voldoende privacy maatregelen gedefinieerd en genomen zijn.

Ook aanpassingen of wijzigingen van bestaande systemen of projecten rechtvaardigen een PIA. Op die manier kunt u voorkomen dat later kostbare aanpassingen nodig zijn om alsnog de noodzakelijke beheersmaatregelen met betrekking tot privacy te implementeren. Ook wanneer de omstandigheden van een project tijdens de looptijd veranderen, is het raadzaam de PIA te herhalen en/of te evalueren bij de afsluiting van een project.

Hoeveel tijd kost het om een PIA uit te voeren?

Er zijn verschillende factoren van invloed op de tijd die het kost om een PIA uit te voeren.

De belangrijkste zijn:
- Het aantal belanghebbenden bij het project en de mate waarin deze vragen of twijfels hebben over de consequenties voor privacy.
- De impact en het belang van het project op de organisatie en de samenleving.
- De (technische en organisatorische) complexiteit van de verwerking.

De hoeveelheid tijd en doorlooptijd die het uitvoeren van een PIA kost, zal per PIA verschillen en hangt van veel factoren af. Het uitvoeren van de gehele PIA voor een eenvoudige gegevensverwerking zal enkele dagdelen kosten, dit is inclusief het verzamelen van gegevens en het uitvoeren van een controle. Bij complexere projecten kan dit oplopen tot tientallen dagen. Dit lijkt een substantiële investering maar daarmee kan een zeer omvangrijke schadepost worden voorkomen of beperkt.

Bij het opstellen van deze PIA is ernaar gestreefd de benodigde tijd zoveel mogelijk te beperken.

Andere privacy instrumenten

Naast de PIA bestaan diverse andere privacy-instrumenten om (al dan niet zelfstandig) te kijken naar privacyaspecten (zie bijlage 7 Referentiemateriaal). Veel van deze instrumenten zijn op naleving gericht.

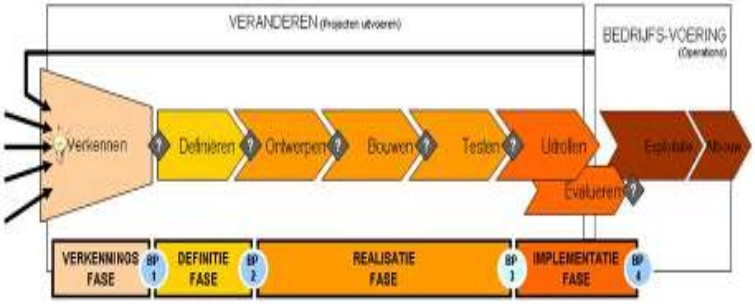
Het naleven van wet- en regelgeving wordt ook wel ‘compliance’ genoemd. Om voor uw organisatie na te gaan of u voldoet aan de Wet bescherming persoonsgegevens (Wbp) kunt u een compliance check laten uitvoeren. Daarmee kunt u aantonen dat u volgens wet- en regelgeving handelt.

Deze PIA is geen nalevingsinstrument, maar een risicoanalyse-instrument waarmee privacyrisico’s kunnen worden geïdentificeerd en gelokaliseerd. Ook in deze PIA wordt het uitvoeren van een dergelijke compliance check in veel gevallen aangeraden.

1.3 PIA in PPM (Project Portfolio Management)

De PIA wordt (indien nodig) uitgevoerd in de defintiefase van een informatievoorziening (IV) project.

Informatiebeveiliging en Privacy in IV-Projecten



Verkennin g

Definitie

Realisatief ase

Verkorte Risicoanalyse Informatiebeveiliging en Privacy

+ 28

- 28

Uitgebreide Risicoanalyse en/of Privacy Impactanalyse

Maatregelen Baseline

Maatregelen Baseline +

Ontwerpen
Functioneel Ontwerp
Technisch Ontwerp
Beheer en

Inkoop
Programma van

Contracten
Leveranciers
Convenant gebruikers
SLA

Privacy
Functionaris gegevensbescherming
Transparantiedocume nt

Projectaudits

Testen
Testplan
Pentest
Functioneel
Technisch

Werkinstructies
Gebruikers
Functioneel beheer
Technisch/applicati e beheer

2 Handreiking voor het PIA-proces

Dit deel bevat een handreiking voor het effectief en efficiënt uitvoeren van een PIA. Afhankelijk van de omstandigheden waarin de PIA wordt uitgevoerd kan op het onderstaande stappenplan worden gevarieerd. U krijgt antwoorden op vragen als: Uit welke stappen bestaat het PIA-proces? Wie kan ik betrekken bij de PIA? Wat zijn succes- en faalfactoren?

Wat zijn de stappen in een PIA proces?
De uitvoering van een PIA kan bestaan uit de volgende stappen:

Deze stappen worden hierna kort toegelicht.

2.1 Bepaal wie de PIA gaat uitvoeren en hoe dit moet gebeuren

De vragenlijst kan worden ingevuld door één persoon of door een team. Het heeft de voorkeur om de PIA door een team uit te laten voeren. De resultaten van de PIA worden daardoor beter omdat de verschillende deelnemers ieder vanuit hun eigen invalshoek het project kunnen bekijken. Indien dit om praktische redenen niet mogelijk is, kan ervoor gekozen worden om de PIA door één persoon uit te laten voeren en te laten reviewen door een tweede persoon. In bijlage 2 is een overzicht opgenomen van de personen die betrokken kunnen worden bij een PIA.

Voordat begonnen wordt met het uitvoeren van de PIA is het belangrijk vast te stellen wat u wilt bereiken, wie wat met de resultaten gaat doen en op welke manier de resultaten gebruikt gaan worden. Hierbij is het goed om de belangrijkste succes- en faalfactoren, zoals opgenomen in bijlage 3, door te nemen en te bepalen hoe hiermee omgegaan wordt.

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

2.2 Verzamel en bestudeer relevante informatie

Om de PIA-vragenlijst zo goed mogelijk in te kunnen vullen, is informatie nodig over:

- Het project en de maatschappelijke context hiervan.
- Wie de belanghebbenden zijn en welke eisen en wensen zij hebben.
- Het type gegevens (o.a. de gevoeligheid/bijzonderheid) dat gebruikt gaat worden.
- De wijze waarop deze gegevens verzameld en verwerkt gaan worden (de bron?)
- De verschillende systemen die gebruikt gaan worden om de gegevens te verzamelen, op te slaan en te versturen.
- De manier waarop de gegevens tussen de verschillende systemen worden uitgewisseld.
- Waar de gegevens voor worden gebruikt (het doel of doelen)/noodzakelijkheid.
- De reikwijdte van de verdere verwerking van de gegevens.
- Of op basis van de gegevens persoonsprofielen worden gegenereerd.
- De bedrijfsprocessen die dit doel ondersteunen of realiseren.
- De proceseigenaar / wie er verantwoordelijk voor is.
- Wie de beheerder is.
- Welke wettelijke grondslag er is.

Deze informatie kunt u op verschillende manieren verkrijgen, bijvoorbeeld:

- Opvragen en nazoeken van documentatie over het project.
- Interviews of workshops met belanghebbenden.

Het heeft de voorkeur dat u alle benodigde informatie voorafgaand aan het invullen van de vragenlijst verzamelt. Dit heeft twee voordelen:

- Bij de beantwoording van de vragen wordt een volledig beeld meegenomen in de overwegingen.
- U vermijdt dat u meerdere keren terug moet naar dezelfde personen om aanvullende informatie te vragen.

Voor het bepalen van de belanghebbenden kunt u gebruik maken van een zogenaamde stakeholderanalyse indien deze voor het project al uitgevoerd is. Indien deze niet is uitgevoerd kunt u denken aan de volgende partijen:

- De organisatie die het project uitvoert en (indien dit niet dezelfde is) de opdrachtgever.
- Overige organisaties betrokken bij het project.
- Organisaties en individuen die belang hebben bij het project en de uitkomsten ervan. (zoals leveranciers en afnemers).
- Organisaties en individuen die worden geraakt door het project en de uitkomsten ervan. (burgers, klanten, belangenverenigingen).
- Organisaties die de middelen/technologie en diensten leveren om het project mogelijk te maken.

Tijdens interviews of workshops met de belanghebbenden over de wensen en eisen met betrekking tot privacy- en (informatie)beveiliging zijn de belangrijkste vragen: ‘Wat zijn ieders belangen, eisen en/of wensen ten aanzien van (de uitkomst van) het project en welke invloed kunnen zij op het project uitoefenen?’.

Bij het verzamelen van documentatie kunt u aan de volgende documenten denken:

- Eerdere PIA’s en informatie over gelijkwaardige projecten.

- Beschrijving van de gebruikte technologie en zijn gebruikswijze (vooral relevant bij het gebruik van nieuwe technologie of het gebruik van bekende technologie op een nieuwe manier).
- Factsheets, white papers, rapporten en artikelen van onderzoekscentra, samenwerkingsverbanden tussen bedrijven / beroepsgroepen en aanbieders van technologie.
- Consultaties met organisaties die worden geraakt door het project.
- Relevante wetgevingsdocumentatie en jurisprudentie.

Ook moet u rekening houden met de volgorde van de uit te voeren activiteiten. Interviews zullen meer informatie opleveren op het moment dat alle documentatie doorgenomen is, omdat het dan mogelijk is om specifiekere vragen te stellen. Tegelijkertijd is de volgorde van interviews belangrijk voor de informatie en/of documentatie die verkregen wordt. Consultaties kunnen bijvoorbeeld het beste gehouden worden op het moment dat al (redelijk) concreet is welk resultaat het project dient te hebben.

2.3 Vul de PIA-vragenlijst in

Het is noodzakelijk dat u alle vragen beantwoordt. Niet alle vragen zijn voor elk project relevant. In dat geval is het advies om bij de antwoorden op de vragenlijst een toelichting op te nemen waarom een vraag niet relevant is, zodat dit duidelijk is voor de gebruiker van de resultaten. Het is echter aan te raden om alle relevante vragen te beantwoorden.

De risicogebieden die in de vragenlijst worden gebruikt zijn:

- Risicogebieden in relatie tot:
  - Het type project.
  - De gegevens die u wilt gebruiken.
  - De partijen die betrokken zijn bij de uitvoering van het project.

  -Een bepaalde fase van de verwerking:- Het verzamelen van de gegevens.
  - Het gebruik van de gegevens.
  - Het bewaren en vernietigen van de gegevens.
  - De beveiliging van de gegevens.
- De risicogebieden met betrekking tot de privacy principes:
  - Dataminimalisatie.
  - Gegevenskwaliteit.
  - Doelbinding en verenigbaarheid van verdere verwerking.
  - Limitering van gebruik van gegevens.
  - Beveiliging van gegevens.
  - Transparantie.
  - Rechten van betrokkenen.

  -Verantwoording.

Schat de impact in en bedenk (aanvullende) maatregelenOp basis van het overzicht van de risicogebieden waar de privacy van de betrokkene mogelijk wordt geschaad kunt u een inschatting maken hoe groot de impact is binnen uw project en op uw organisatie. Vervolgens kunnen maatregelen genomen worden om de risico's te verkleinen. Deze twee stappen worden hieronder beschreven.

Impactbepaling
Bij het beoordelen van de impact zijn er twee zaken waar u rekening mee moet houden, namelijk 'impact op betrokkene' en 'impact op organisatie'.

Impact op de betrokkene
Een hogere 'impact op betrokkene' betekent dat de gegevens zelf en/of de context waarin deze gegevens worden gebruikt een verhoogd risico vormen voor de persoonlijke levenssfeer van degene op wie de persoonsgegevens betrekking hebben.

Bij het beantwoorden van de vraag wat de impact op de betrokkene is, moet aandacht besteed worden aan:

- De van toepassing zijnde privacy dimensie(s) (zie bijlage 1 Begrippen).
- Risico op en gevolgen van identiteitsdiefstal / -fraude. Diefstal van identiteit (waarbij anderen (opzettelijk) verplichtingen aan gaan uit naam van de betrokkene zonder medeweten van de betrokkene).
- Risico op en gevolgen van mogelijke (overige) privacy inbreuken welke een bedreiging vormen voor iemands vrijheid, financiën, relaties of gezondheid (zie ook overzicht van waarden / persoonlijke belangen in bijlage 5).

Uitgangspunt in deze PIA is dat indien de privacy van de betrokkenen op een van deze gebieden wordt geschaad, de impact op de organisatie ook groter wordt en daarmee het risico groter wordt dat:

- De organisatie kostbare aanpassingen in processen of systemen moet doorvoeren of het project vroegtijdig moet stopzetten.
- Het vertrouwen van klanten, werknemers of burgers wordt geschaad.
- Negatieve publiciteit over het niet waarborgen van de privacy ontstaat.
- De organisatie wordt onderworpen aan toezicht en handhaving.
- De gegevenskwaliteit onvoldoende is voor de dienstverlening.
- De besluitvorming wordt gebaseerd op onvoldoende betrouwbare informatie.
- Maatregelen getroffen moeten worden om de gegevens te beveiligen.

Impact op de organisatie
De impact (zoals reputatieschade, maar ook materiële financiële schade als gevolg van compliance problemen, klachten en incidenten) die bovenstaande bedreigingen op uw organisatie hebben moet u zelf vaststellen. Deze wordt onder andere beïnvloed door de branche waarin u zich begeeft, het belang dat uw klanten aan privacy hechten, de maatschappelijke aandacht.

Maatregelen nemen om risico's te verkleinen of weg te nemen
Op basis van de inschatting van de impact op de betrokkenen of de organisatie, moet worden nagegaan op welke wijze de risico's vermeden of verkleind kunnen worden. U wordt geadviseerd na te gaan of de negatieve privacy impact op de betrokkene noodzakelijk is en kan worden gerechtvaardigd. De belangen van de doelen van het project, het belang van de organisatie en het belang van het individu moeten hierbij worden afgewogen.

Het vermijden of verminderen van risico's houdt overigens niet altijd in dat de projectdoelen moeten worden bijgesteld. Naarmate de inschatting van de impact hoger wordt, is het raadzamer om maatregelen te treffen om de risico's weg te nemen of te verminderen. In de vragenlijst zijn diverse suggesties opgenomen over de manier waarop dit kan. Deze suggesties zijn niet uitputtend en uiteraard hangt de maatregel sterk af van de omgeving. Hieronder worden nog enkele voorbeelden gegeven van de manieren waarop risico's vermeden kunnen worden:

Vermijden van risico's
Het vermijden van de risico's kan door helemaal geen persoonsgegevens te verwerken. Het doel kan bijvoorbeeld toch bereikt worden door:

- Opslag van gegevens bij het individu in plaats van binnen de organisatie.
- Het gebruik van anonieme gegevens, of pseudoniemen.
- Het toepassen van mathematische methodes, zonder de onderliggende gegevens op te vragen en te registreren.

Verminderen van risico's
Afhankelijk van het risico en het privacyprincipe kunnen ook maatregelen getroffen worden die het risico verminderen. Hieronder zijn per privacyprincipe enkele voorbeelden opgenomen[4].

1 Limitering van het verzamelen van gegevens:
Het verminderen van de hoeveelheid gegevens, door de gegevens niet op te slaan of niet te bewaren.
2 Gegevenskwaliteit:
Introduceren van geautomatiseerde controles op gegevens.
3 Doelbinding:
De doelen voor het verzamelen en verenigbaarheid van verdere verwerking nader specificeren en hierover communiceren.
4 Limitering van gebruik van gegevens:
Het beperken van de mogelijkheid om grote hoeveelheden gegevens in een keer binnen en buiten de organisatie te verspreiden door gefragmenteerde opslag, in plaats van concentreren van alle gegevens in één database.
5 Beveiliging van gegevens:
Het toepassen van encryptie en logische toegangsbeveiliging.
6 Transparantie:
Het opstellen van een privacybeleid, gedragscode of het laten certificeren van de verwerking.
7 Rechten van betrokkenen:

[4] Diverse bronnen bestaan waaruit maatregelen kunnen worden ontleend. (zie bijlage G). Op basis van deze normstelsels kunnen organisaties, al dan niet in samenwerking met een privacydeskundige verkennen in hoeverre de te treffen beheersmaatregelen al dan niet reeds getroffen zijn. Het in kaart brengen van de eisen waar precies aan moet worden voldaan, het definiëren van het te behalen ambitieniveau/volwassenheidsniveau van de organisatie, welke beheersmaatregelen de organisatie zou moeten treffen (passend bij de ambitie/volwassenheidsniveau) alsmede het in kaart brengen van de mate waarin de organisatie de te treffen maatregelen ook daadwerkelijk reeds heeft getroffen/geïmplementeerd, maakt geen onderdeel uit van de PIA.

Betrokkenen zeggenschap geven over zijn gegevens door de invoer van een 'self service' bijvoorbeeld via een beveiligd internet portal.

8 Verantwoording:
Invoeren van periodiek externe controle.

2.4 Stel het PIA verslag op

De resultaten van de PIA worden vastgelegd in een verslag. Een voorbeeld voor een PIA-verslag is opgenomen in bijlage 4. Op basis van dit verslag kan de gebruiker van de resultaten van de PIA eventueel noodzakelijke beslissingen nemen.

De risicogebieden waar de privacy van de betrokkene mogelijk wordt geschaad volgen uit de ingevulde PIA. Vervolgens wordt in de rapportage ruimte geboden om de impact op de betrokkenen en op de organisatie zelf in te vullen. Ook is ruimte opgenomen voor een advies hoe hiermee dient te worden omgegaan. De overwegingen die ten grondslag liggen aan de antwoorden op de vragenlijst zijn een belangrijk onderdeel van het PIA-verslag.

Het PIA-verslag kan een dynamisch document zijn. Hiermee wordt bedoeld dat in geval van wijzigingen in het project de PIA (deels) opnieuw doorlopen kan worden en waar nodig het verslag op onderdelen geactualiseerd kan worden. Het verdient aanbeveling om aan het einde van het project een definitieve versie van de PIA vast te stellen, die gebaseerd is op de productionele eigenschappen daarvan.

2.5 Laat eventueel een (onafhankelijke) review uitvoeren

Tot slot kan het raadzaam zijn dat u de PIA-rapportage (en de onderliggende ingevulde PIA-vragenlijst) laat reviewen. Een review kan zowel intern als extern uitgevoerd worden.

Bij een interne review kan dit bijvoorbeeld uitgevoerd worden door personen die niet aan de uitvoering van de PIA deel hebben genomen (dit is zeker aan te raden als het PIA-team niet breed opgezet is). Maar ook kunt u denken aan personen van een ander project of personen uit de organisatie die verder van het project af staan.

Een externe review kan uitgevoerd worden door specifieke deskundigen.
Hierbij kan bijvoorbeeld een onafhankelijke beoordeling plaatsvinden op:

1. Interpretatie en inschatting van de risico's.
2. Juridische interpretatie van de vragen en antwoorden.
3. Praktische en inhoudelijke juistheid, haalbaarheid en volledigheid van voorgestelde maatregelen. De benodigde expertise hangt uiteraard af van het doel van de review.

Na het invullen van de vragenlijst kan ook blijken dat u eigenlijk iets anders (of nog meer) wilt weten. Onderstaande verwijzingen kunnen u mogelijk op weg helpen bij uw verdere inspanningen:

- U wilt meer informatie over het vermijden van privacyrisico's door het toepassen van oplossingen in de technologie. Zie 'Privacy by Design' en 'Privacy Enhancing Technologies'(PET) [6].
- U wilt meer informatie hebben over één of meerdere regels van de Wbp en de praktische interpretatie daarvan. Zie de 'Handleiding voor verwerkers – Ministerie van Justitie' [16] en diverse andere publicaties, waaronder informatiebladen van het CBP.

- U wilt het burgerservicenummer (BSN) verwerken. Zie de ‘Handleiding voor gebruikers van het Burgerservicenummer’, zie website www.burgerservicenummer.nl.
- U wilt weten of wordt voldaan aan de eisen van de Wbp. Zie de ‘Zelfevaluatie’ [11] dan wel het ‘Raamwerk Privacy Audit’ [12].
- U wilt weten hoe u de persoonsgegevens moet beveiligen. Zie de best practices en standaarden op het gebied van informatiebeveiliging (zoals ISO27001/27002 [18]).

Bijlage 1 Begrippen

In de PIA wordt een aantal begrippen gebruikt dat in deze PIA een specifieke betekenis heeft. De belangrijkste begrippen worden toegelicht:

Betrokkene:
Degene op wie een persoonsgegeven betrekking heeft.

Bewerker:
Degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen.

Bijzondere Persoonsgegevens:
Persoonsgegevens betreffende ras, politieke gezindheid, gezondheid, seksuele leven, alsmede persoonsgegevens betreffende het lidmaatschap van een vakvereniging. Daarnaast ook strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag. Zie ook art. 16 tot en met 23 in de Wet bescherming persoonsgegevens (Wbp).

Compliance:
Voldoen aan wet- en regelgeving.

Compliance check:
Beoordeling of voldaan wordt aan wet- en regelgeving.

OECD Data Protection Principles:
1. Limitering van het verzamelen van gegevens
2. Gegevenskwaliteit
3. Doelbinding
4. Limitering van het gebruik van gegevens
5. Beveiliging van gegevens
6. Transparantie
7. Rechten van betrokkenen
8. Verantwoording

1 Collection Limitation Principle (beperking van het verzamelen van gegevens): There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
2 Data Quality Principle (gegevenskwaliteit): Personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
3 Purpose Specification Principle (doelbinding): The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
4 Use Limitation Principle (limitering van het gebruik van gegevens): Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in principle 3, except:

a) with the consent of the data subject; or
b) by the authority of law.

5 Security Safeguards Principle (beveiliging van gegevens): Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

6 Openness Principle (transparantie): There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

7 Individual Participation Principle (rechten van betrokkenen): An individual should have the right:
a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him;
c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and
d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

8 Accountability Principle (verantwoording): A data controller should be accountable for complying with measures which give effect to the principles stated above.

Persoonsgegevens:
Elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.

Privacy dimensies:
Het begrip privacy wordt voor vier situaties gebruikt:

1. Lichamelijke privacy, Grondwet artikel 11:
   Ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op onaantastbaarheid van zijn lichaam.
2. Ruimtelijke privacy, Grondwet artikel 12:
   1. Het binnentreden in een woning tegen de wil van de bewoner is alleen geoorloofd in de gevallen bij of krachtens de wet bepaald, door hen die daartoe bij of krachtens de wet zijn aangewezen.
   2. Voor het binnentreden overeenkomstig voorgaand lid zijn voorafgaande legitimatie en mededeling van het doel van binnentreden vereist, behoudens bij wet gestelde uitzonderingen.
   3. Aan de bewoner wordt een schriftelijk verslag van het binnentreden verstrekt.
3. Relationele privacy, Grondwet artikel 13:
   1. Het briefgeheim is onschendbaar, behalve, in de gevallen bij de wet bepaald, op last van de rechter.
   2. Het telefoon- en telegraafgeheim is onschendbaar, behalve, in de gevallen bij de wet bepaald, door of met machtiging van hen die daartoe bij de wet zijn aangewezen.
4. Informationele privacy, Grondwet artikel 10:
   1. Ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op eerbiediging van zijn persoonlijke levenssfeer.
   2. De wet stelt regels ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens.

3. De wet stelt regels inzake de aanspraken van personen op kennisneming van over hen vastgelegde gegevens en van het gebruik dat daarvan wordt gemaakt, alsmede op verbetering van zodanige gegevens.

Privacy risico:
Het risico dat gepaard gaat met een bedreiging. Het privacyrisico is de kans van optreden van een bedreiging dat de privacy van een betrokkene wordt geschonden maal de impact die de bedreiging heeft op de betrokkene en de organisatie.

Project:
Het begrip 'project' wordt gebruikt om het (mogelijke) object van de PIA aan te duiden. Dit object kan een activiteit of functie zijn die met behulp van de PIA wordt geanalyseerd. Het gaat om projecten waarbij (veelal) de verwerking van persoonsgegevens aan de orde is. Het project kan bijvoorbeeld een initiatief, review, systeem, database, programma, applicatie, dienst dan wel wets- of beleidsvoorstel zijn.

Stakeholder:
Een persoon of organisatie die invloed ondervindt (positief of negatief) of zelf invloed kan uitoefenen op een specifieke organisatie, een overheidsbesluit, een nieuw product of een project.

Stakeholderanalyse:
Een analyse van de personen of organisaties die door het project geraakt worden, de mate waarin deze geraakt worden (positief of negatief) en de mate waarin deze invloed kunnen uitoefenen (op de uitvoering, het resultaat of de acceptatie) van het project.

Verwerken:
Elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, evenals het afschermen, uitwissen of vernietigen van gegevens.

Verantwoordelijke:
De natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.

Bijlage 2 Betrokkenen PIA

Indien de PIA door een team wordt uitgevoerd kan sprake zijn van verschillende rollen, al dan niet verdeeld over verschillende deelnemers. Hierna is een aantal rollen opgenomen. De rollen illustreren welke partijen betrokken kunnen zijn bij het uitvoeren van de PIA en welke type vragen zij met de uitvoering van de PIA wensen te beantwoorden:

- **Opdrachtgevers van het project:**

Is het initiatief/project haalbaar vanuit de optiek van privacybescherming en de daarmee samenhangende risico's? Doen we, gegeven de risico's, een verantwoorde investering? Dit zijn bijvoorbeeld aandeelhouders, producteigenaren,
proceseigenaren, systeemeigenaren en dataeigenaren.

- **Opdrachtnemer/verantwoordelijke uitvoering van het project:**

Houden we ook voldoende rekening met de niet-functionele eisen en wensen, in dit geval het onderwerp privacybescherming en hieraan gerelateerde onderwerpen (beveiliging, documenten archiefbeheer en dergelijke)? Kennen we de risico's en beheersen we deze afdoende? Verantwoordelijk voor de uitvoering van het initiatief zijn veelal de directie/ het management en indien aangesteld de projectleiding.

- **Opdrachtnemer/verantwoordelijke uitvoering van de PIA:**

Wordt de PIA op een gedegen wijze uitgevoerd? Worden de juiste experts ingezet? Wordt er rekening gehouden met alle belanghebbenden?

- **Meedenkers / experts:**

Krijgt het onderwerp privacy en hieraan gerelateerde onderwerpen (beveiliging, documenten archiefbeheer en dergelijke) juiste/voldoende aandacht? Is helder wat een en ander concreet betekent voor de praktijk van de uitvoering? Meedenkers zijn te splitsen in drie 'competentiegroepen':

1. Personen die de organisatie en/of het project goed kennen.

2. Experts die deskundig zijn op het onderwerp:
   - Techniek
   - Informatiebeveiliging
   - Privacy
   - Juridische aspecten
   - Organisatorische aspecten
   - Andere aandachtsgebieden die voor het project van belang zijn

3. Uitvoerders:
   De resultaten van de PIA moeten leiden tot concrete instructies c.q. randvoorwaarden voor de uitvoerders. Deze uitvoerders zijn bijvoorbeeld de systeemontwikkelaars (waaronder ICT-dienstverleners), architecten, productontwikkelaars en beleidsmakers. Zij moeten precies weten binnen welke kaders zij hun werk kunnen doen. Om dit te kunnen weten, is het gewenst dat zij meedenken.

- **Meekijkers/beoordelaars (PIA-assessor):**

Wordt op adequate wijze rekening gehouden met de impact van het project op betrokkenen en met de risico's voor de betrokkenen, voor de eigen organisatie en de belanghebbenden? Meekijkers vervullen voornamelijk een Quality Assurance rol tijdens het traject en beoordelaars vervullen meer een controlerende rol aan het einde van (bepaalde fases in) het project. Deze rollen kunnen worden vervuld door professionele privacy assessors (privacy-adviseurs en privacy-auditors), maar mogelijk ook de CISO, een informatiemanager, de CIO of de functionaris gegevensbescherming.

Overigens zullen niet alle personen continu bij de PIA-activiteiten betrokken zijn. De samenstelling van het PIA-team en de betrokken expertises kunnen gedurende de verschillende fasen van het project wijzigen. Zo zullen aanvankelijk de juridische experts meer betrokken zijn en pas later bijvoorbeeld beveiligingsspecialisten en uitvoerders (waaronder architecten).

De personen kunnen uit de eigen organisatie komen, dan wel van daarbuiten.

Bijlage 3 Succes en faalfactoren

Succesfactoren

Hierna zijn een aantal factoren opgenomen die bij kunnen dragen aan een succesvolle uitvoering van de PIA:

- PIA is een integraal onderdeel van de risicomanagementstrategie en/of PIA heeft een plek in de projectmethodiek, de PIA is geïntegreerd in processen (de PIA is geen ad hoc/toevallige activiteit en geen add on).
- PIA wordt zo vroeg mogelijk in het project opgestart en uitgevoerd (in plaats van 'als mosterd na de maaltijd').
- Tijdens de PIA worden de relevante interne en externe belanghebbenden betrokken (in plaats van alleen de PIA-teamleden).
- PIA's zijn toekomstgericht om er zo aan bij te dragen dat privacyrisico's worden geïdentificeerd voordat systemen in gebruik worden genomen en programma's worden geïmplementeerd.
- De PIA wordt gedurende het project (in ieder geval als de privacyimpact dan wel privacyrisico's wijzigen) geactualiseerd (het PIA-rapport is dus een dynamisch document in plaats van een statisch document).
- PIA wordt bij voorkeur uitgevoerd door een team waarin verschillende expertises en vaardigheden aanwezig zijn (in plaats van door één persoon).
- PIA's zijn voorts meer effectief:
  - Als deze onderdeel uitmaken van een systeem van motivering, sancties en toetsing.
  - Als deze deel uitmaken van de project aanpak/methodiek of Quality Assurance proces.
  - Als de individuen die de PIA uitvoeren beschikken over kennis van het project/programma, dan wel toegang hebben tot privacy relevante expertise (privacy wetgeving, informatiebeveiliging, records management en andere functionele expertise waar relevant).
  - Als ook externen die door het initiatief worden geraakt worden betrokken (gehoord, geconsulteerd).
  - Als er een (formeel dan wel informeel) proces is van externe/onafhankelijke toetsing.

Faalfactoren

Negatief geformuleerd zijn naast de succesfactoren tevens de faalfactoren. Hier komen drie specifieke aandachtspunten bij, namelijk:

- PIA wordt gezien als een doel op zich. PIA's zijn alleen zinvol als deze worden beschouwd als een middel dat de potentie heeft om een voorstel/initiatief te veranderen als dat nodig is om privacyrisico's te vermijden of verminderen. Als deze worden uitgevoerd als een voorgeschreven oefening met het doel om te voldoen aan een interne verplichting of een bureaucratische eis, dan worden deze beschouwd als een manier om te legitimeren in plaats van een risicoanalyse en gaat de toegevoegde waarde verloren.
- PIA wordt gezien als het noodzakelijke middel om privacy compliance tot stand te brengen. Het uitvoeren van een PIA is weliswaar een goede manier om de privacyrisico's in kaart te brengen, privacy compliance komt echter pas tot stand als de aanbevelingen uit een PIA worden opgevolgd en er een volledige implementatie heeft plaatsgevonden van de noodzakelijke maatregelen om aan de privacywet- en regelgeving te voldoen.
- Te veel fixatie op de uitkomst. Het uitvoeren van een goede PIA is geen 'rechttoe rechtaan' proces. Het proces waarin het rapport tot stand komt is minstens zo belangrijk als het

resultaat ervan. Als het proces te snel of onzorgvuldig wordt uitgevoerd, bestaat het gevaar dat relevante privacyrisico's en daarmee samenhangende oplossingsrichtingen niet goed worden doordacht.

Bijlage 4 PIA rapportage

Dit deel bevat een index voor een rapportage en geeft u antwoord op de vraag: 'Welke elementen kunnen in een PIA-rapportage aan de orde komen?' Ook hier geldt weer dat geen enkele rapportage er hetzelfde uit zal zien. Er wordt dan ook geen template opgelegd maar enkele aspecten genoemd, die mogelijk relevant zijn bij de terugkoppeling van de bevindingen en resultaten van de PIA.
De rapportage kan worden gebruikt ten behoeve van:

A Discussie/gespreksfacilitatie
B Belangenafweging
C Advisering over aandachtspunten voor verdere ontwikkeling dan wel te nemen maatregelen
D Faciliteren van besluitvorming

In de rapportage zal in elk geval aan de orde moeten komen:

- Een korte beschrijving van de uitgevoerde PIA (door wie uitgevoerd, wanneer, met welk doel, en, door wie eventueel gevalideerd en/of gecontroleerd).
- Een korte beschrijving van het project, waaronder een beschrijving van het gegevensmodel en gegevensstroom (data flow analysis / gegevensstroomanalyse).
- Een beschrijving van de impact die naar voren is gekomen en de risico's voor de betrokkenen en de organisatie.
- Antwoord op de vraag: 'Is er reden om af te zien van de gegevensverwerking?' (go/no go).
- Aandachtspunten voor degene die het systeem/beleid/enzovoorts verder gaat ontwikkelen.
- Beschrijving van oplossingsrichtingen (bestaande uit mogelijke privacymaatregelen en compliance mechanismen).
- Naam functionaris die verantwoordelijk is voor het beheer en de evaluatie van de PIA.

In de rapportage is ruimte voor de opdrachtgever om de uitkomsten en bevindingen van de PIA te becommentariëren, en eventueel te accorderen. De verspreiding van de PIA moet in het rapport expliciet worden benoemd. Minimaal alle personen die in het onderzoek zijn geraadpleegd hebben recht op de rapportage.

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

Bijlage 5 Waarden (belangen) die mogelijk in het geding zijn

De impact die een inbreuk van de privacy van de betrokkene kan hebben wordt mede bepaald door de mate waarin de volgende waarden (persoonlijke belangen) in het geding zijn:

- Verlies aan zelfstandigheid (bijvoorbeeld de mogelijkheid om bepaalde handelingen niet meer uit te voeren).
- Vrij blijven van stigmatisering (bijvoorbeeld de wijze waarop betrokkene behandeld wordt op basis van bepaalde kenmerken).
- Gelijkheid (bijvoorbeeld het op dezelfde wijze benaderen van betrokkenen).
- Bewegingsvrijheid (bijvoorbeeld het beperken van de toegang tot bepaalde etablissementen of ruimtes).
- Vrij blijven van manipulatie (bijvoorbeeld, door het beïnvloeden van het gedrag op basis van een (afwijkend) levenspatroon).
- Integriteit (bijvoorbeeld door het aanbieden van geschenken).
- Ongestoord leven (bijvoorbeeld door het (onaangenaam) afbreken van rust en stilte).
- Eigenwaarde (bijvoorbeeld door afbreuk aan persoonlijkheid).
- Autonomie (bijvoorbeeld door beperking van de vrijheid om de eigen regels te volgen).

Bijlage 6 Categorieën van speciale (groepen) personen

Categorieën van mensen van wie de fysieke veiligheid extra bescherming vereist:

- Mensen die dreiging van geweld ondervinden:
  - Slachtoffers van huiselijk geweld
  - Deelnemers aan een getuigen beschermingsprogramma
  - Personen die zich proberen te onttrekken van criminele organisaties of netwerken
  - Personen die controversiële functies bekleden
- Beroemdheden, notabelen en Vips:
  - Politici
  - Sportlieden
  - Artiesten
  - Mensen die op andere wijze in de belangstelling staan, zoals winnaars van de lotto
- Mensen die een beroep hebben in de beveiliging:
  - BOA’s
  - Gevangenbewaarders
  - Behandelaars in een TBS-kliniek
  - Medewerkers van veiligheidsdiensten
  - Politie en Defensie

Mensen van wie de fysieke veiligheid niet direct in gevaar is maar die kwetsbaar worden geacht of die het moeilijk vinden om controle over hun gegevens te kunnen hebben, zoals:

- Kinderen
- Verstandelijk gehandicapten
- Lichamelijk gehandicapten
- Ernstig zieken zoals comapatiënten
- Psychiatrisch patiënten
- Dak- en thuislozen
- Ex-gedetineerden
- Vluchtelingen

Bijlage 7 Referentiemateriaal

[1] Privacy impact assessment guide, Australia, August 2006, Australian Government, Office of the Privacy Commissioner, http://www.privacy.gov.au/publications/pia06/index.html. [1B] Checklist Identifying privacy issues early, Privacy NSW Privacy Essentials No 3 April 2004 www.lawlink.nsw.gov.au/lawlink/privacynsw/ll_pnsw.nsf/vwFiles/privacyessentials_03_2005.pdf/$file/privacyessentials_03_2005.pdf

[2] Privacy impact assessment guidelines: a framework to manage privacy risks, Canada, August 2002, Treasury Board of Canada Secretariat, www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paipg-pefrld1_e.asp.

[3] Audit report of the Privacy Commissioner of Canada – assessing the privacy impacts of programs, plans, and policies, Canada, October 2007, Office of the Privacy Commissioner, www.privcom.gc.ca/information/pub/ar-vr/pia_200710_e.asp.

[4] Privacy impact assessment policy, Canada, May 2002, Treasury Board of Canada Secretariat, www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paip-pefr_e.asp.

[5] E-privacy: a policy approach to building trust and confidence in e-business, Hong Kong, 2001, Officeof the Privacy Commissioner for Personal Data, www.pcpd.org.hk/english/publications/eprivacy_9.html.

[6] Privacy impact assessment handbook, New Zealand, April 2008, Privacy Commissioner, www.privacy.org.nz/privacy-impact-assessment-handbook/?highlight=privacy%20impact%20assessment. [7] Privacy impact assessment handbook, United Kingdom, December 2007, Information Commissioner's Office, www.ico.gov.uk/upload/documents/pia_handbook_html/html/1-intro.html.

[8] Privacy impact assessment the Privacy Office official guidance, United States, May 2007, The Privacy Office, www.dhs.gov/xinfoshare/publications/gc_1209396374339.shtm.

[9] E-Government Act Section 208 implementation guidance, United States, September 2003, Office of Management and Budget, www.whitehouse.gov/omb/memoranda/m03-22.html.

[10] Privacy Impact Assessments: International Study of their Application and Effects, United Kingdom, October 2007, Linden Consulting Inc for Information Commissioner's Office.

[11] Privacy Communicatie Model, Ministerie van Economische Zaken, 2010. www.ecp.nl/privacyvierkant

[12] Handleiding voor verwerkers van persoonsgegevens, Ministerie van Justitie, Den Haag, april 2001.

[13] Quickscan bescherming persoonsgegevens, College bescherming persoonsgegevens www.cbpweb.nl/downloads_audit/quickscan.pdf

[14] Wbp Zelfevaluatie, Samenwerkingsverband Audit Aanpak/Werkgroep Zelfevaluatie, april 2001.

[15] Raamwerk Privacy Audit, Samenwerkingsverband Audit Aanpak/Werkgroep Privacy Audit, april 2001.

[16] Contouren voor Compliance, Handreiking bij het Raamwerk Privacy Audit, samengesteld en gepubliceerd door het College bescherming persoonsgegevens (CBP) in samenwerking met Koninklijk Nederlands Instituut van Registeraccountants (NIVRA) en de Nederlandse Orde van Register EDP-Auditors (NOREA), 24 mei 2005.

[17] Personal Data Protection Audit Framework (EU Directive EC95/46) Part I: Baseline Framework CWA 15499-1 & Part II: Checklists, questionnaires and templates for users of the framework CWA 15499-2, February 2006.

[18] (Verwacht) Self-Assessment Framework for Managers (EU Directive EC95/46), CWA 16112, maart 2010. ftp://ftp.cen.eu/CEN/Sectors/List/ICT/CWAs/CWA16112.pdf

[19] De Wet bescherming persoonsgegevens en de richtsnoeren beveiliging van persoonsgegevens (CBP 2013)

[20] PIA aanpak van de gemeente Amsterdam

Bijlage 8 Relatie tussen vragen en privacy principes

Deze tabel geeft inzicht in de relatie tussen vragen, onderwerpen en privacy dimensies. Deze is bedoeld om 'onder water' te faciliteren dat nadat de vragenlijst is ingevuld, inzicht bestaat in welke onderwerpen en/of principes aandacht behoeven. Op basis hiervan kan de vragenlijst ook per dimensie gesorteerd worden, zodat bijvoorbeeld inzicht ontstaat in de risico's rondom 'gegevenskwaliteit'

		1 Beperking van het verzamelen van gegevens	2 Gegevenskwaliteit	3 Doelbinding	4 Beperking van het gebruik van gegevens	5 Beveiliging	6 Transparantie	7 Rechten van betrokkenen	8 Verantwoording
1	**Type project**								
1.1	Is sprake van het verwerken van persoonsgegevens?						**X**	**X**	**X**
1.2	Is het duidelijk wie verantwoordelijk is voor de verwerking van de gegevens?						**X**	**X**	**X**
1.2.1	Verwerkt uw organisatie de persoonsgegevens in opdracht en onder verantwoordelijkheid van een andere organisatie? Ofwel: Treedt uw organisatie op als bewerker?						**X**	**X**	**X**
1.3	Is het duidelijk wie na afloop van het project verantwoordelijk is voor het in stand houden en evalueren van de getroffen maatregelen?								**X**
1.4	Is het doel van de verwerking van persoonsgegevens binnen het project voldoende SMART omschreven?	**X**		**X**	**X**				
1.5	Is er sprake van:								
a	Gebruik van nieuwe technologie?	**X**	**X**	**X**	**X**	**X**	**X**	**X**	
b	Gebruik van technologie die bij het publiek vragen of weerstand op kan roepen?	**X**	**X**	**X**	**X**	**X**	**X**	**X**	
c	Invoering bestaande technologie in nieuwe context?	**X**	**X**	**X**	**X**	**X**	**X**	**X**	
d	(Andere) grote verschuivingen in	**X**	**X**	**X**	**X**	**X**	**X**	**X**	

	de werkwijze van de organisatie, de manier waarop persoonsgegevens worden verwerkt en/of de technologie die daarbij gebruikt wordt?								
e	Een nieuwe verwerking van persoonsgegevens	**X**	**X**	**X**	**X**				
f	Het verzamelen van meer of andere persoonsgegevens dan voorheen of een nieuwe manier van verzamelen.	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**
g	Gebruik van al verzamelde gegevens voor een nieuw doel of een nieuwe manier van gebruiken.			**X**			**X**		
1.6	Hebt u op alle bovenstaande vragen (a t/m j) nee geantwoord?								
1.7	Is er (naast de Wbp) veel wet- en regelgeving ten aanzien van persoonsgegevens waar het project mee te maken heeft?	**X**	**X**	**X**	**X**	**X**	**X**		
1.8	Zijn er veel maatschappelijke belanghebbenden?						**X**	**X**	**X**
1.9	Zijn er veel partijen betrokken bij de uitvoering van het project?				**X**	**X**	**X**		**X**
1.10	Is er een geschillenregeling of een partij waar de betrokkene terecht kan bij vragen of klachten?							**X**	**X**
2	**Gegevens**								
2.1	Zijn alle gegevens nodig om het doel te bereiken (worden er zo min mogelijk gegevens verzameld)?	**X**	**X**						
2.2	Kan het doel met geanonimiseerde of pseudo-anonieme gegevens worden bereikt (terwijl daar op dit moment geen gebruik van wordt gemaakt)?				**X**	**X**			
2.3	Kunnen de gegevens gebruikt worden om het gedrag, de aanwezigheid of prestaties van mensen in kaart te brengen en/of te beoordelen (ook al is dit niet het doel)?		**X**	**X**		**X**	**X**		
2.4	Is er sprake van het verwerken van:								
a	Bijzondere persoonsgegevens?	**X**	**X**		**X**	**X**	**X**	**X**	
b	Uniek identificerende gegevens?				**X**	**X**			
c	Wettelijk voorgeschreven persoonsnummers?			**X**	**X**				

d	Andere gegevens dan hiervoor beschreven waarvoor geldt dat sprake is van een verhoogde gevoeligheid?		X		X	X	X	X	
2.4.1	Bij een van bovenstaande Ja: Kan het doel met minder ingrijpende (andere) gegevens worden bereikt?	X	X	X					
2.5	Verwerkt u gegevens over kwetsbare groepen of personen?	X	X		X	X	X	X	
2.6	Hebben de gegevens betrekking op de gehele of grote delen van de bevolking?	X		X		X	X		
3	**Andere partijen**								
3.1	Zijn er (na afronding van het project) bij het verzamelen en verder verwerken van de gegevens meerdere interne partijen betrokken?		X			X	X	X	X
3.2	Zijn er (na afronding van het project) bij het verzamelen en verder verwerken van de gegevens meerdere externe partijen betrokken?		X			X	X	X	X
3.2.1	Zijn er partijen betrokken (in het project of bij de verwerking) die zich niet aan een met Nederland vergelijkbare privacywetgeving hoeven te houden?					X	X	X	X
3.2.2	Is de verstrekking van de gegevens aan derde partijen in lijn met het doel waarvoor de gegevens oorspronkelijk zijn verzameld?		X	X	X				
3.2.3	Worden de gegevens verkocht aan de derde partijen?				X		X	X	
4	**Verzamelen van gegevens**								
4.1	Kan de manier waarop de gegevens worden verzameld worden opgevat als privacygevoelig?	X		X			X		
4.2	Is het doel van het verzamelen van de gegevens publiekelijk bekend of kan het publiekelijk bekend gemaakt worden?			X			X		
4.3	Verzamelt u de gegevens op basis van een van de wettelijke grondslagen?	X		X	X		X	X	
4.3.1	Is duidelijk of u de gegevens	X			X		X	X	

	verzamelt op basis van toestemming (opt-in) of op basis van een andere grondslag (opt-out)								
4.3.2	Indien u toestemming aan de betrokkene vraagt (opt-in) kunnen de betrokkenen de toestemming op een later tijdstip intrekken (opt-out)?	**X**			**X**				
4.3.3	Is de impact van het intrekken van de toestemming groot voor de betrokkene?	**X**			**X**	**X**			
4.4	Vertelt u tegen de betrokkene dat de gegevens worden verzameld?						**X**	**X**	
4.4.1	Bij Nee: Kunnen de betrokkenen o p de hoogte zijn van het verzamelen van de gegevens?	**X**		**X**			**X**	**X**	
4.4.2	Bij Ja (op vraag 4.4): Vertelt u teg en de betrokkene waarom de gegevens worden verzameld (wat u er mee gaat doen)?	**X**		**X**			**X**	**X**	
4.4.3	Bij Ja: (op vraag 4.4): Vertelt u tegen de betrokkene aan wie de gegevens worden verstrekt (daar waar dit geen wettelijke verplichting is)?				**X**	**X**	**X**		
4.5	Zou de betrokkene kunnen worden verrast door de verwerking (op het moment dat hij daarover wordt geïnformeerd)?			**X**			**X**	**X**	
5	**Gebruik van gegevens**								
5.1	Is het gebruik van de gegevens verenigbaar (in lijn) met het doel van het verzamelen?	**X**		**X**	**X**				
5.2	Worden de gegevens gebruikt voor andere bedrijfsprocessen of -doelen dan waar ze oorspronkelijk voor verzameld zijn?	**X**		**X**	**X**	**X**	**X**		
5.2.1	Past het doel van dit bedrijfsproces bij het oorspronkelijke doel van verzamelen?	**X**		**X**	**X**	**X**	**X**		
5.3	Is de kwaliteit van de gegevens gewaarborgd, dat wil zeggen: zijn de gegevens actueel, juist en volledig?		**X**	**X**				**X**	
5.4	Worden op basis van de gegevens beslissingen genomen over de betrokkenen?		**X**			**X**	**X**	**X**	

5.4.1	Bij Ja: Leveren de gegevens een volledig en actueel beeld van de betrokkenen op?		X			X	X	X	
5.5	Is sprake van koppeling, verrijking of vergelijking van gegevens uit verschillende bronnen?	X	X		X	X			
5.6	Worden de gegevens breed verspreid binnen de organisatie?	1.	X	X	X				
5.7	Worden de gegevens breed verspreid buiten de organisatie?			X	X				
5.7.1	Is het doorgeven van de gegevens aan partijen buiten de organisatie in lijn met de verwachtingen van het individu?	X					X		
5.8	Stelt uw organisatie profielen op van de betrokkenen, al dan niet geanonimiseerd?			X	X			X	
5.8.1	Indien profielen worden opgesteld, kan het profiel tot uitsluiting of stigmatisering leiden?	X	X			X			
5.9	Kunnen de betrokkenen hun gegevens inzien of daarom vragen?						X	X	
5.10	Kunnen de betrokkenen hun gegevens corrigeren of daarom vragen (verbeteren, aanvullen)?		X				X	X	
5.11	Kunnen de betrokkenen hun gegevens verwijderen of daarom vragen?		X				X	X	
6	**Bewaren en vernietigen**								
6.1	Is een bewaartermijn voor de gegevens vastgesteld?			X	X	X			
6.2	Kunnen de gegevens na afloop van de bewaartermijn fysiek worden verwijderd (uit een bestand) of vernietigd (papier)?			X	X	X			
6.3	Zo ja, worden de gegevens na vers trijken van de bewaartermijn op een dusdanige manier vernietigd of verwijderd dat ze niet meer te benaderen en te gebruiken zijn?	X	X	X	X				
7	**Beveiliging**								
7.1	Is sprake van intern geformuleerd beleid over het beveiligen van informatie?					X			
7.2	Zo ja, is duidelijk op welke wijze het project er voor zorg draagt dat					X			

	aan de gestelde eisen in het beveiligingsbeleid voldaan gaat worden?								

INFORMATIE BEVEILIGINGS DIENST

**INFORMATIEBEVEILIGINGSDIENST
V00R GEMEENTEN (IBD)**

**NASSAULAAN 12
2514 JS DEN HAAG**

**POSTBUS 30435
2500 GK DEN HAAG**

**HELPDESK 070 373 80 11
ALGEMEEN 070 373 80 08
FAX 070 363 56 82**

**INFO@IBDGEMEENTEN.NL
WWW.IBDGEMEENTEN.NL**

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN **IN OPDRACHT VAN**
VERENIGING VAN NEDERLANDSE GEMEENTEN