INFORMATIE
BEVEILIGINGS
DIENST

VRAGENLIJST 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
Vragenlijst PIA

Versienummer
1.0

Versiedatum
April 2014

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

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

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

TASKFORCE

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

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 vragenlijst die gebruikt kan worden 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
- PIA-verslag
- PIA-uitleg

Maatregelen tactische variant Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)

Maatregel 10.8.5.1	Er zijn richtlijnen met betrekking tot het bepalen van de risico's die het gebruik van gemeentelijk 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.
Maatregel15.1.4.1	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

Inhoudsopgave

1 PIA-vragenlijst

De vragenlijst bestaat uit 7 onderdelen die achtereenvolgens ingaan op:

- Het type project.
- De gegevens die u wilt gebruiken.
- De partijen die betrokken zijn bij de uitvoering van het project.
- Verzamelen van gegevens.
- Gebruik van gegevens.
- Bewaren en vernietigen van gegevens.
- Beveiligen van gegevens.

Alle vragen kunt u met ja of nee beantwoorden. Bij de vragen is een toelichting gegeven. Soms is dit een specifieke uitleg van de vraag, meestal wordt aangegeven met welke factoren rekening gehouden moet worden bij de beantwoording van de vraag. Uiteraard hangen de factoren waarmee u rekening moet houden af van het project en kunnen deze per project variëren. De genoemde factoren zijn daarmee ook niet uitputtend maar slechts richtinggevend.

Nadat u de vragenlijst heeft ingevuld krijgt u een overzicht van de mogelijke risico's van het project per onderwerp / stap in de verwerking. Deze zijn eveneens uitgesplitst naar privacy principe.

Deze vragenlijst maakt integraal deel uit van de projectdocumentatie en dient als vervolg op de verkorte risicoanalyse te worden uitgevoerd in de definitiefase van een systeem en te worden verzonden aan de functionaris gegevensbescherming of de CISO binnen de gemeente.

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN
VERENIGING VAN NEDERLANDSE GEMEENTEN

INFORMATIE
BEVEILIGINGS
DIENST

Privacy Impact Analyse Vragenlijst

<Gemeente / Dienst / Afdeling>
<projectnaam>

Datum:
Projectnummer:
Projectleider:
Opdrachtgever:
Versie:
Auteur:
Functie:

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN
VERENIGING VAN NEDERLANDSE GEMEENTEN

Versiebeheer

Versies

Versie	Datum	Auteur	Samenvatting van de wijzigingen
0.1			
0.X			

Goedkeuring

Versie	Datum	Naam
		CISO
		Informatiemanager

Ter informatie aan

Versie	Datum	Naam
		Functionaris gegevensbescherming gemeente

1	**Type project**			
1.1	Is sprake van het verwerken van persoonsgegevens?			
1.2	Is het duidelijk wie verantwoordelijk is voor de verwerking van de gegevens?	Houd bij de beantwoording rekening met: 1. Voor en door wie het project wordt uitgevoerd. 2. Of er iemand formeel verantwoordelijk is voor de verwerking van de gegevens. 3. Of er een intern contactpersoon is.	JA/NEE	Als nee: U loopt een verhoogd risico. Het risico bestaat dat niet duidelijk is wie de maatregelen die getroffen moeten worden om risico's af te dekken moet nemen en dat daardoor de risico's niet worden afgedekt. Bovendien loopt u een compliance risico omdat er diverse wettelijke verplichtingen op de verantwoordelijke rusten en het risico bestaat dat niet alle wettelijke verplichtingen worden nagekomen.
1.2.1	Verwerkt uw organisatie de persoonsgegevens in opdracht en onder verantwoordelijkheid van een andere organisatie? Ofwel: Treedt uw organisatie op als bewerker?	Deze vragenlijst is bedoeld voor organisaties die persoonsgegevens verwerken in de rol van verantwoordelijke 11. Deze vragenlijst is niet bedoeld voor organisaties die persoonsgegevens verwerken in de rol van bewerker.	JA/NEE	Als ja: U kunt stoppen. Uiteraard kunt u deze PIA wel gebruiken om beter inzicht te krijgen in de risico's van het project en daarmee uw eigen risico (in de rol van bewerker of als betrokkene) inzichtelijk te maken Als nee: Bepaal wie (bedrijfsonderdeel, persoon) binnen uw organisatie de verantwoordelijke is.
1.3	Is het duidelijk wie na afloop van het project verantwoordelijk is voor het in stand houden en evalueren van de getroffen maatregelen?	Uiteraard moeten ook in de toekomst de getroffen maatregelen in stand gehouden worden en worden gezorgd dat de risico's worden beheerst (bijvoorbeeld door deze PIA periodiek uit te voeren)	JA/NEE	Als nee: Het risico bestaat dat de maatregelen in de toekomst niet meer worden gevolgd of niet meer passen bij de situatie
1.4	Is het doel van de verwerking van persoonsgegevens binnen het project voldoende SMART omschreven?	SMART staat voor: Specifiek; de doelstelling moet eenduidig zijn. Meetbaar; onder welke (meetbare /observeerbare) voorwaarden of vorm is het doel bereikt. Acceptabel; of deze acceptabel genoeg is voor de doelgroep en/of het management; is er iemand verantwoordelijk voor het realiseren van het doel?	JA/NEE	Als nee: Een SMART omschreven doelstelling is essentieel voor het maken van keuzes voor het inrichten van een kwalitatief goede gegevensverwerking. Bovendien loopt uw organisatie compliance risico's als het doel niet voldoende precies is omschreven.(zie Art. 7 Wbp)

		Realistisch; of de doelstelling haalbaar is. Tijdgebonden; wanneer (in de tijd) het doel bereikt moet zijn.		
1.5	Is er sprake van:			
a	Gebruik van nieuwe technologie?	Bijvoorbeeld intelligente transportsystemen, locatie of volgsystemen op basis van GPS, mobiele technologie, gezichtsherkenning in samenhang met cameratoezicht.	JA/NEE	Als ja: U loopt verhoogde risico's, de impact van uw project op de betrokkenen en de wijze waarop deze gaan reageren is moeilijk in te schatten. Dit kan leiden tot verhoogde kans op imagoschade, verstoring van de bedrijfscontinuïteit, en acties door handhavers en toezichthouders.
b	Gebruik van technologie die bij het publiek vragen of weerstand op kan roepen?	Bijvoorbeeld biometrie, RFID, behavioural targeting (profilering).		
c	Invoering bestaande technologie in nieuwe context?	Zoals cameratoezicht of drugscontrole op de werkvloer.		
d	(Andere) grote verschuivingen in de werkwijze van de organisatie, de manier waarop persoonsgegevens worden verwerkt en/of de technologie die daarbij gebruikt wordt?	Bijvoorbeeld het samenvoegen koppelen van verschillende overheidsregistraties, invoering van nieuwe vormen van identificatie of vervanging van systeem waarin persoonsgegevens worden opgeslagen		
e	Een nieuwe verwerking van persoonsgegevens	Het gebruik van gegevens voor andere bedrijfsprocessen dan waarvoor ze zijn verzameld, of bredere verspreiding van de gegevens binnen of buiten de organisatie.	JA/NEE	Als ja: Uw risicoprofiel verandert. U wordt geadviseerd een compliance check uit te voeren. Dergelijke projecten vragen om een goede beoordeling van de consequenties op het gebied van privacy.
f	Het verzamelen van meer of andere persoonsgegevens dan voorheen of een nieuwe manier van verzamelen.	Bijvoorbeeld gegevensverrijking door enquêtes en klantonderzoek of benadering van klanten/burgers op basis van beschikbare gegevens voor nieuwe producten of diensten.		
g	Gebruik van al verzamelde gegevens	Bijvoorbeeld het samenvoegen van interne		

	voor een nieuw doel of een nieuwe manier van gebruiken.	databases om klantprofielen op te stellen.		
1.6	Hebt u op alle bovenstaande vragen (a t/m j) nee geantwoord?		JA/NEE	Als ja: U kunt stoppen. De (mogelijke) privacyrisico's van uw verwerking zijn laag. Verder uitvoeren van deze PIA heeft daarmee weinig toegevoegde waarde. Let op! U dient wel aan de eisen van de Wbp te voldoen.
1.7	Is er (naast de Wbp) veel wet- en regelgeving ten aanzien van persoonsgegevens waar het project mee te maken heeft?	Houd bij de beantwoording rekening met: 1. Sectorale wetgeving 2. Gedragscodes 3. Algemene maatregelen van bestuur 4. Jurisprudentie 5. Internationale aspecten	JA/NEE	Als ja: U loopt een verhoogd risico. Hoe meer wet- en regelgeving hoe hoger het risico dat u hieraan niet voldoet. Een grote hoeveelheid wet- en regelgeving duidt tevens op het maatschappelijk belang dat wordt gehecht aan het onderwerp. U wordt geadviseerd de van toepassing zijnde wet- en regelgeving in kaart te brengen en de (privacy) consequenties inzichtelijk te maken.
1.8	Zijn er veel maatschappelijke belanghebbenden?	Houd bij beantwoording rekening met: 1. Medewerkers, afnemers, leveranciers, belangengroeperingen, burgers, klanten toezichthouders 2. Welke beroepsgroepen betrokken zijn bij de verwerking	JA/NEE	Als ja: U loopt een verhoogd risico. De wijze waarop maatschappelijke belanghebbenden reageren varieert waardoor het project kan vertragen. U wordt geadviseerd een plan te maken waarin u aangeeft op welke manier de verschillende belanghebbenden bij het project worden betrokken of over het project worden geïnformeerd.
1.9	Zijn er veel partijen betrokken bij de uitvoering van het project?	Houd bij beantwoording rekening met: 1. Aannemers en dienstverleners 2. Hard en software leveranciers 3. ICT-serviceproviders	JA/NEE	Als ja: U loopt een verhoogd risico. Het risico bestaat dat niet alle partijen zorgvuldig met gegevens omgaan die tijdens het project worden verzameld. Ook bestaat het risico dat de partijen de risico's en de inspanning die nodig is om deze te verminderen anders schatten. U moet in ieder geval oog hebben voor een bewerkersovereenkomst met die partijen!
1.10	Is er een geschillenregeling of een partij waar de betrokkene terecht kan bij vragen of klachten?		JA/NEE	Als nee: U loopt een verhoogd risico. Een (onafhankelijke) partij waarbij geschillen kunnen worden beslecht draagt bij aan verbetering van de voorlichting, het imago en een evenwichtige belangenbehartiging. U wordt geadviseerd een contactpunt voor vragen en klachten aan te wijzen en waar mogelijk aan te sluiten bij

				geschillenregeling
2	**De gegevens**			
2.1	Zijn alle gegevens nodig om het doel te bereiken (worden er zo min mogelijk gegevens verzameld)?	Houd bij de beantwoording rekening met: - Is per data-element vastgesteld wat de toegevoegde waarde is en waarom dit noodzakelijk is? - Kan volstaan worden met het gebruik van alleen ja/nee in plaats van het volledige gegeven? - Kan volstaan worden met het verschil tussen twee waarden in plaats van beide waarden afzonderlijk? - Kan gebruikgemaakt worden van andere wiskundige methodieken (bijvoorbeeld voor het bepalen van afwijkingen)?	JA/NEE	Als nee: Het verwerken van zo min mogelijk gegevens heeft een aantal voordelen: - De benodigde opslag en rekencapaciteit van uw computer systemen is lager, waardoor prestaties, hersteltijden en serviceniveaus kunnen worden verhoogd. - U zult minder gegevens te hoeven onderhouden en updaten en de kans op fouten wordt verkleind. Bovendien loop uw organisatie compliance risico's als u te veel gegevens voor het doel verzamelt. (zie Art 9, lid 1 en 2 Wbp).
2.2	Kan het doel met geanonimiseerde of pseudo-anonieme gegevens worden bereikt (terwijl daar op dit moment geen gebruik van wordt gemaakt)?	Door gegevens pseudo-anoniem te maken, worden de direct identificerende gegevens van de betrokkene op een eenduidige wijze vervangen, waardoor in de toekomst bepaalde partijen nog steeds gegevens kunnen toevoegen, maar de uniek identificerende gegevens niet meer teruggehaald kunnen worden. Door anonimiseren worden alle direct, uniek identificerende gegevens verwijderd.	JA/NEE	Als ja: U loopt een verhoogd risico door het gebruiken van persoonsgegevens. Door het gebruik van geanonimiseerde en/ of pseudo-anonieme gegevens valt u niet meer onder het regime van de Wbp. U verwerkt immers geen persoonsgegevens meer. Door gegevens te anonimiseren of pseudo-anoniem te maken kunt u het nemen van verdere maatregelen ter bescherming van de privacy van de betrokkenen minimaliseren. U wordt geadviseerd periodiek na te gaan of de gegevens niet indirect herleidbaar zijn.
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)?	Denk hierbij bijvoorbeeld ook aan geolocatie, personeelsvolgsystemen, beslisondersteuning bij het als dan niet aanbieden van producten of diensten.	JA/NEE	Als ja: U loopt een verhoogd risico. Het risico bestaat dat de betrokkenen of de algemene opinie dit als een potentiële bedreiging voor hun privacy zien. Ook als de gegevens niet voor dit doel worden gebruikt bestaat het risico dat dit (in de toekomst) wel gebeurt. Voor de invoering van een personeelvolgsysteem is instemming van de OR nodig.
2.4	Is sprake van het verwerken van:			

a	Bijzondere persoonsgegevens?	De Wbp (artikel 16) noemt zogenaamde bijzondere persoonsgegevens: persoonsgegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, persoonsgegevens betreffende het lidmaatschap van een vakvereniging, strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag.	JA/NEE	Als ja: Het werken met dit type gegevens brengt een verhoogd risico van misbruik met zich mee die (potentieel grote) impact op de betrokkene heeft en vraagt daarmee om betere beveiliging. Het verwerken van deze gegevens is alleen toegestaan onder bepaalde wettelijke voorwaarden (art. 16 e.v. Wbp).
b	Uniek identificerende gegevens?	Bijvoorbeeld biometrische gegevens, vingerafdrukken, DNA-profielen.	JA/NEE	Als ja: Het werken met dit type gegevens brengt een verhoogd risico van misbruik met zich mee die (potentieel grote) impact op de betrokkene heeft en vraagt daarmee om betere beveiliging. Het verwerken van deze gegevens is alleen toegestaan onder bepaalde wettelijke voorwaarden (zie ook art. 21 lid 4 Wbp).
c	Wettelijk voorgeschreven persoonsnummers?	Bijvoorbeeld het Burgerservicenummer (BSN).	JA/NEE	Als ja: Het verwerken van een uniek bij wet voorgeschreven persoonsnummer zoals het BSN is verboden (art. 24 lid 1 Wbp). U mag dit nummer alleen verwerken als u daarvoor een wettelijke basis heeft. Voor overheidsorganisaties is deze wettelijke basis neergelegd in de Wet algemene bepalingen Burgerservicenummer (Wabb)
d	Andere gegevens dan hiervoor beschreven waarvoor geldt dat sprake is van een verhoogde gevoeligheid?	Bijvoorbeeld creditcardinformatie, financiële informatie, erfrechtelijke aspecten, arbeidsprestaties of gegevens waarvoor een geheimhoudingsplicht geldt?	JA/NEE	Als ja: Het werken met dit type gegevens brengt een verhoogd risico van misbruik met zich mee die (potentieel grote) impact op de betrokkene heeft en vraagt daarmee om betere beveiliging.
2.4	Bij een van bovenstaande Ja: Kan het doel met minder		JA/NEE	Als ja: U loopt een verhoogd risico. Het risico bestaat dat betrokkenen minder snel willen meewerken, of het

	ingrijpende (andere) gegevens worden bereikt?			vertrouwen in de organisatie vermindert. U wordt geadviseerd andere minder ingrijpende gegevens te gebruiken. Bovendien loopt uw organisatie compliance risico's als dit het geval is (zie art. 11 lid 1 Wbp).
2.5	Verwerkt u gegevens ove r kwetsbare groepen of personen?	Bijvoorbeeld minderjarige personen, verstandelijk gehandicapten, gedetineerden, onder toezicht gestelden, mensen van wie de fysieke veiligheid in gevaar is (zie bijlage F).	JA/NEE	Als ja: U loopt een verhoogd risico. Indien deze gegevens worden misbruikt heeft dit negatieve beeldvorming in de publieke opinie over de organisatie tot gevolg. U wordt geadviseerd maatregelen te treffen op een hoger beveiligingsniveau (zie art 13 Wbp) en betrokkenen de mogelijkheid te bieden zich aan de verwerking te onttrekken.
2.6	Hebben de gegevens betrekking op de gehele of grote delen van de bevolking?		JA/NEE	Als ja: U loopt een verhoogd risico. De kans op misbruik van de gegevens wordt groter naarmate u meer gegevens verwerkt. U wordt geadviseerd maatregelen te treffen op een hoger beveiligingsniveau (zie art 13 Wbp).
3	**Betrokken partijen**			
3.1	Zijn er (na afronding van het project) bij het verzamelen en verder verwerken van de gegevens meerdere interne partijen betrokken?	Houd bij beantwoording rekening met: 1. Afdelingen die gebruikmaken van de gegevens. 2. Afdelingen die de gegevens verzamelen. 3. De personen die toegang hebben tot de gegevens.	JA/NEE	Als ja: U loopt een verhoogd risico. Zorg voor duidelijke beschrijving van taken en verantwoordelijkheden met betrekking tot de gegevens waarbij onder andere wordt beschreven: - Beveiliging van gegevens - Afhandeling van fouten - Terugmelden van fouten - Afstemming van het beveiligingsbeleid - Controle Zorg voor een duidelijke gegevensbeschrijving.
3.2	Zijn er (na afronding van het project) bij het verzamelen en verder verwerken van de gegevens meerdere externe partijen betrokken?	Houd bij beantwoording rekening met: 1. Voor en door wie het project wordt uitgevoerd. 2.Welke partijen gebruikmak en van de gegevens. 3. Of andere partijen worden ingeschakeld voor het bereiken van het doel (wordt de verwerking van gegevens geoutsourcet). 4. Of de gegevens worden verkocht. 5. Welke personen buiten de	JA/NEE	Als ja: U loopt een verhoogd risico. Hoe meer partijen betrokken zijn, hoe groter de kans op verlies van gegevens, onduidelijkheden in verantwoordelijkheden, het gebruik van de gegevens voor andere doelen en de kans op fouten. Zorg voor een duidelijke beschrijving van de taken en verantwoordelijkheden met betrekking tot de gegevens waarbij onder andere wordt beschreven: - De beveiliging van gegevens en de afstemming daarvan tussen de partijen - De gegevenskwaliteit

		organisatie toegang hebben tot de gegevens.		- Afhandeling van fouten - Terugmelden van fouten - Controle Zorg ook voor een duidelijke gegevensbeschrijving. Leg afspraken contractueel vast.
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?	Voor gegevens die worden verwerkt buiten de Europese Economische Ruimte (EER) moet een adequaat niveau van bescherming geboden worden. Alle landen binnen de EER dienen te voldoen aan de Europese gegevensbeschermingsrichtlijn. De Europese Commissie neemt een beslissing over het passend zijn van het geboden beschermingsniveau voor landen buiten de EER. Een lijst van deze landen kan gevonden worden op internet: www.cbpweb.nl/Pages/int_lijst.aspx Houd bij het beantwoorden van deze vraag rekening met: 1. Of de gegevens van het grondgebied komen waar ze worden opgeslagen. 2. Of de gegevens aan partijen worden verstrekt die niet op het grondgebied zijn gevestigd waar de gegevens worden verzameld.	JA/NEE	Als ja: U wordt geadviseerd na te gaan in hoeverre een adequaat beschermingsniveau wordt geboden door het betreffende land of de betreffende organisatie. Maak schriftelijke afspraken over hoe dit beschermingsniveau gehandhaafd kan worden.
3.2.2	Is de verstrekking van de gegevens aan derde partijen in lijn met het doel waarvoor de gegevens oorspronkelijk zijn verzameld?	Houd bij beantwoording rekening met: 1. Wat het doel is/zijn voor het gebruik van de gegevens. 2. Welke gegevens aan wie worden verstrekt voor welk doel. 3. Of de verstrekking aan andere partijen een	JA/NEE	Als nee: Indien gegevens verstrekt worden aan andere partijen zonder dat deze gegevens daarvoor verzameld zijn bestaat het risico dat deze gegevens niet geschikt zijn voor het doel en dat betrokkenen worden geschaad door de verdere verspreiding van de gegevens. U hebt mogelijk een compliance risico (Zie art. 9 lid 1 en 2 Wbp).

		wettelijke verplichting is. 4. Of de gegevens verkocht worden aan andere partijen. 5. Of andere partijen ingeschakeld worden voor het bereiken van het doel (outsourcing). 6. Hoe vaak (frequentie) worden de gegevens aan andere partijen verstrekt (eenmalig, periodieke update, continue). 7. Op welke wijze gegevens worden verstrekt aan andere partijen. 8. Of wordt vastgelegd aan welke partijen gegevens worden verstrekt. 9. Of de andere partij soortgelijke gegevens ontvangt op basis waarvan te herleiden valt op wie de gegevens betrekking hebben (indien deze geanonimiseerd of pseudo-anoniem gemaakt zijn).		
3.2.3	Worden de gegevens verkocht aan de derde partijen?	De Wbp stelt voorwaarden aan het gebruik van gegevens voor commerciële of charitatieve doelen, zoals recht van verzet.	JA/NEE	Als nee: U loopt een compliance risico. Het gebruik van gegevens van commerciële doelen stelt extra eisen. Zie art. 41 lid 3 Wbp).
4	**Verzamelen van gegevens**			
4.1	Kan de manier waarop de gegevens worden verzameld worden opgevat als privacygevoelig?	Bijvoorbeeld omdat intieme of gevoelige informatie wordt gevraagd in een publiek gebied waar anderen dit kunnen horen, of omdat gebruik gemaakt wordt van (camera)observatie, tracking door cookies of GPS?	JA/NEE	Als ja: U wordt geadviseerd na te gaan of de gegevens op een andere manier kunnen worden verzameld.
4.2	Is het doel van het verzamelen van de gegevens publiekelijk bekend of kan het publiekelijk bekend gemaakt worden?	Houd bij de beantwoording rekening met of de betrokkene redelijkerwijs op de hoogte kan zijn van de verwerking van de gegevens.	JA/NEE	Als nee: De verwerking van gegevens zonder dat dit publiekelijk bekend is of gemaakt kan worden brengt een hoog risico voor de betrokken met zich mee. U wordt geadviseerd een belangenafweging te maken of het doel van de verwerking opweegt tegen de

				risico's voor de betrokkenen
4.3	Verzamelt u de gegevens op basis van een van de wettelijke grondslagen?	De Wbp kent een beperkt aantal grondslagen op basis waarvan gegevens mogen worden verwerkt: - U vraagt toestemming. - De gegevens zijn noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene een partij is. - De gegevens zijn nodig voor het volgen van een wettelijke verplichting. - De betrokkene heeft er een vitaal belang bij dat u de gegevens verzamelt. - De gegevens zijn nodig voor de goede vervulling van een publiekrechtelijke taak. - U hebt een gerechtvaardigd belang bij de verwerking.	JA/NEE	Als nee: Voor het verwerken van persoonsgegevens is een grondslag noodzakelijk. Indien deze ontbreekt, loopt u compliance risico (art. 8 Wbp).
4.3.1	Is duidelijk of u de gegevens verzamelt op basis van toestemming (opt-in) of op basis van een andere grondslag (opt-out)	Bij het verwerken van de gegevens moet duidelijk zijn of de betrokkene toestemming moet geven (opt-in) of dat niet hoeft, maar later bezwaar kan maken (opt-out).	JA/NEE	Als nee: U loopt een verhoogd risico. Indien de betrokkene verrast wordt door de verwerking zonder toestemming bestaat het risico dat deze bezwaar maakt.
4.3.2	Indien u toestemming aan de betrokkene vraagt (opt-in) kunnen de betrokkenen de toestemming op een later tijdstip intrekken (opt-out)?	Deze toestemming moet een vrije, specifieke en op informatie berustende wilsuiting zijn.	JA/NEE	Als nee: U loopt een verhoogd risico. Indien u niet kunt voldoen aan verzoeken van betrokkenen om verwerking van gegevens te stoppen of omdat u deze mogelijkheid niet aanbiedt kan dit leiden tot irritatie of kostbare aanpassingen in systemen. U wordt geadviseerd betrokkenen de mogelijkheid te bieden de toestemming in te trekken en dit systeem technisch mogelijk te maken.
4.3.3	Is de impact van het intrekken van de toestemming groot voor de betrokkene?	Bijvoorbeeld omdat dienstverlening aan betrokkene stopgezet wordt terwijl deze daarvan afhankelijk is.	JA/NEE	Als nee: U loopt een verhoogd risico. Indien de impact van het intrekken van de toestemming groot is, is er waarschijnlijk geen sprake van een vrije wilsuiting. U loopt daarmee een compliance risico (art. 8 Wbp).

4.4	Vertelt u tegen de betrokkene dat de gegevens worden verzameld?	Houd bij de beantwoording rekening met: 1. Waar de gegevens vandaan komen (van de betrokkene, een in terne afdeling, een andere partij, uit eigen waarneming, et cetera). 2. Op welke wijze de gegevens worden verzameld. 3. De mogelijkheid dat de betrokkene redelijkerwijs op de hoogte kan zijn van de verwerking van de gegevens. 4. De mate waarin de betrokkene wordt geïnformeerd. 5. De gebruikte technologie. 6. Wat het doel is/ doelen zijn voor het gebruik. 7. Of de gegevens of uitkomsten van gegevensbewerking intern binnen het bedrijf verspreid worden. 8. Op welke wijze (mondeling, schriftelijk, automatisch, elektronisch, waarneming, papier) wor den de gegevens aan andere partijen verstrekt. 9. Hoe lang de gegevens worden bewaard.	JA/NEE	Als ja: Ga verder met vraag 4.4.2. Als nee: Ga verder met vraag 4.4.1.
4.4.1	Bij Nee: Kunnen de betro kkenen op de hoogte zijn van het verzamelen van de gegevens?		JA/NEE	Als nee: Het verstrekken van informatie over welke gegevens worden verzameld draagt bij aan de transparantie en wekt vertrouwen bij de betrokkenen. Bovendien loopt u een compliance risico indien de informatie niet wordt verstrekt (zie art 33 e.v. Wbp).
4.4.2	Bij Ja (op vraag 4.4): Ve rtelt u tegen de betrokke ne waarom de gegevens worden verzameld (wat u er mee gaat doen)?		JA/NEE	Als nee: Het verstrekken van informatie over wat u met de verzamelde gegevens gaat doen draagt bij aan de transparantie en wekt vertrouwen bij de betrokkenen. Bovendien loopt u een compliance risico indien de informatie niet wordt verstrekt (zie art. 33 e.v.

				Wbp).
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)?		JA/NEE	Als nee: U wordt geadviseerd (per verstrekking) vast te leggen aan wie gegevens worden verstrekt. Eveneens wordt u geadviseerd om op het moment dat de gegevens worden verzameld, de betrokkenen te vertellen aan welke partijen de gegevens verstrekt zullen worden. Als laatste wordt u geadviseerd om, als betrokkenen daarom vraagt, hem te vertellen welke informatie wanneer aan wie is verstrekt.
4.5	Zou de betrokkene kunnen worden verrast door de verwerking (op het moment dat hij daarover wordt geïnformeerd)?	Houd bij beantwoording rekening met: 1. De mate waarin de betrokkene wordt geïnformeerd. 2. Hoe gegevens worden verzameld (langs welke weg). 3. De gebruikte technologie. 4. De mogelijkheid dat de betrokkene redelijkerwijs op de hoogte kan zijn van de verwerking van de gegevens. 5. Waar gegevens vandaan komen, van de betrokkene, een interne afdeling, een andere partij, uit eigen waarneming, et cetera. 6. Wat het doel is / doelen zijn voor het gebruik. 7. Of gegevens/uitkomsten van gegevensbewerking intern binnen het bedrijf verspreid worden. 8. Op welke wijze (mondeling, schriftelijk, automatisch, elektronisch, waarneming, papier) worden de gegevens aan andere partijen verstrekt. 9. Hoe lang de gegevens worden bewaard.	JA/NEE	Als ja: U loopt een verhoogd risico. Indien betrokkenen worden verrast door de gegevens verwerking bijvoorbeeld omdat meer gegevens worden verzameld dan op het eerste gezicht noodzakelijk is, of omdat het verdere gebruik niet in lijn is met het doel van verzamelen bestaat het risico dat de betrokkene de gegevens niet wil verstrekken of bezwaar maakt tegen het gebruik. U wordt geadviseerd na te gaan of de gegevens via een andere weg kunnen worden verzameld, of minder gegevens worden verzameld of dat de doelen van verder gebruik in lijn zijn met het doel van verzamelen.
5	**Gebruik van gegevens**			
5.1	Is het gebruik van de	Houd bij beantwoording	JA/NEE	Als nee: Het gebruik van de gegevens

	gegevens verenigbaar (in lijn) met het doel van het verzamelen?	rekening met: 1. Wat het verzameldoel is. 2. Waarvoor de gegevens worden gebruikt. 3. Welke gegevens worden v erzameld. 4. Of deze gegevens bijzondere gegevens betreffen. 5. Waar gegevens vandaan komen, van de betrokkene, een interne afdeling, een andere partij, uit eigen waarneming, et cetera. 6. Hoe vaak (frequentie) de gegevens worden verzameld (eenmalig, regelmatig of voortdurend). 7. Op welke wijze (mondeling, schriftelijk, automatisch, elektronisch, waarneming, papier) de gegevens worden verzameld en verspreid. 8. Welke afdelingen/personen en andere partijen toegang hebben tot de gegevens.		moet in overeenstemming met het doel van de verwerking zijn. Indien dit niet het geval is bestaat het risico dat de gegevens niet geschikt zijn voor het doel omdat bijvoorbeeld de kwaliteit niet goed is. U loopt een compliance risico indien u hier niet aan voldoet (zie art. 9 lid 1 en 2 Wbp).
5.2	Worden de gegevens gebruikt voor andere bedrijfsprocessen of doelen dan waar ze oorspronkelijk voor verzameld zijn?			
5.2.1	Past het doel van dit bedrijfsproces bij het oorspronkelijke doel van verzamelen?		JA/NEE	Als nee: Het gebruik van de gegevens dient in overeenstemming met het doel van de verwerking te zijn. U loopt een compliance risico indien u hier niet aan voldoet (zie art. 9 lid 1 en 2 Wbp).
5.3	Is de kwaliteit van de gegevens gewaarborgd, dat wil zeggen: zijn de gegevens actueel, juist en volledig?	Houd bij beantwoording rekening met: 1. Of gegevens worden gecontroleerd, op welke wijze en op welke aspecten controle plaatsvindt. 2. Of de gegevens kunnen worden gecorrigeerd. 3. Welke personen toegang hebben tot gegevens voor correctie, verwijderen et cetera. van de gegevens. 4. Welke afdelingen toegang hebben tot de gegevens.	JA/NEE	Als nee: U loopt een verhoogd risico. Het is van belang dat de verwerkte gegevens juist zijn om ervoor te zorgen dat geen verkeerde conclusies worden getroffen of verkeerde acties worden ondernomen. U loopt hiermee ook een compliance risico (zie art. 11 lid 2 Wbp).

		5. Hoe vaak de gegevens worden geüpdatet. 6. Wat gevolgen zijn van het gebruiken van onjuiste gegevens. 7. Of maatregelen getroffen worden om ander gebruik dan het beoogde te voorkomen. 8. Of kwaliteitswaarborgen worden verstrekt bij verstrekking van de gegevens. 9. Wat er gebeurt als (delen van) de gegevens niet aan de andere partijen worden verstrekt.		
5.4	Worden op basis van de gegevens beslissingen genomen over de betrokkenen?		JA/NEE	Als ja: Ga verder met vraag 5.4.1 Als nee: Ga verder met vraag 5.5
5.4.1	Bij Ja: Leveren de gegevens een volledig en actueel beeld van de betrokkenen op?	Houd bij beantwoording rekening met: 1. Wat het doel is van verzamelen van de gegevens. 2. Welke gegevens (data elementen) worden verzameld. 3. Of gegevens worden gecontroleerd (frequentie en aspecten). 4. Of de gegevens gecorrigeerd kunnen worden. 5. Hoe vaak de gegevens worden geüpdatet. 6. Wijze waarop gegevens op betrouwbaarheid (actualiteit vol ledigheid, juistheid) en relevantie (voor het doel) worden gecheckt. 7. Wat gevolgen zijn van het gebruiken van onjuiste gegevens. 8. Of de gegevens gebruikt worden om profielen op te stellen. 9. Of de profielen op	JA/NEE	Als nee: Er bestaat een verhoogd risico dat er foutieve beslissingen genomen worden op basis van de gegevens waardoor schade voor betrokkenen of de organisatie kan ontstaan als gegevens onjuist, verouderd of onvolledig zijn.

		individueel niveau opgeslagen worden. 10.Welke profielen worden gebruikt.		
5.5	Is sprake van koppeling, verrijking of vergelijking van gegevens uit verschillende bronnen?		JA/NEE	Als ja: U loopt een verhoogd risico dat de gegevens gebruikt worden of in de toekomst gebruikt gaan worden voor andere doeleinden dan oorspronkelijk voor verzameld (function creep). U wordt geadviseerd maatregelen te treffen om deze zogenaamde function creep te voorkomen of onmogelijk te maken, bijvoorbeeld door het hanteren van strikte bewaartermijnen.
5.6	Worden de gegevens breed verspreid binnen de organisatie?	Houd bij beantwoording rekening met: 1. Welke afdelingen toegang hebben tot de gegevens. 2. Welke personen toegang hebben tot de gegevens. 3. De doelen en het gebruik van de gegevens.	JA/NEE	Als ja: U loopt een verhoogd risico. Het verspreiden van gegevens binnen de organisatie verhoogt het risico dat de gegevens voor zaken gebruikt worden waar ze niet voor bedoeld zijn of in handen komen van mensen die hier niet voor geautoriseerd zijn. Zorg voor een duidelijke beschrijving van de taken en verantwoordelijkheden met betrekking tot de gegevens waarbij onder andere wordt beschreven: - Beveiliging van gegevens - Afhandeling van fouten - Terugmelden van fouten - Afstemming van begeleidingsbeleid - Controle Zorg voor een duidelijke gegevensbeschrijving.
5.7	Worden de gegevens breed verspreid buiten de organisatie?	Houd bij beantwoording rekening met: 1. Welke organisaties en personen toegang tot de gegevens hebben. 2. Hoe vaak (frequentie) de gegevens worden verstrekt. 3. Het medium dat gebruikt wordt voor verspreiding (papier, CD, internet). 4. De maatregelen om ander gebruik te voorkomen.	JA/NEE	Als ja: U loopt een verhoogd risico. Hoe meer partijen betrokken zijn, hoe groter de kans op verlies van gegevens, onduidelijkheden in verantwoordelijkheden, het gebruik van de gegevens voor andere doelen en de kans op fouten. Zorg voor een duidelijke beschrijving van de taken en verantwoordelijkheden met betrekking tot de gegevens waarbij onder andere wordt beschreven: - De beveiliging van gegevens en de afstemming daarvan tussen de partijen - De gegevenskwaliteit - Afhandeling van fouten - Terugmelden van fouten

				- Controle Zorg ook voor een duidelijke gegevensbeschrijving. Leg afspraken contractueel vast.
5.7.1	Is het doorgeven van de gegevens aan partijen buiten de organisatie in lijn met de verwachtingen van het individu?	Houd bij beantwoording rekening met: 1.Voor en door wie het project wordt uitgevoerd. 2.Wat voor technologie wordt gebruikt. 3.Of de betrokkene redelijkerwijs op de hoogte kan zijn van de verwerking van de gegevens. 4.Of betrokkenen toestemming geven om gegevens te verzamelen. 5.Wat het doel/de doelen is/zijn voor het gebruik. 6.Of alle gegevens noodzakelijk zijn voor het doel. 7.Welke personen toegang hebben tot de gegevens. 8.Andere partijen die ook gebruikmaken van de gegevens. 9.Welke gegevens (data elementen) aan andere partijen worden verstrekt. 10.Hoelang de gegevens bewaard worden nadat ze voor het (primaire) doel zijn gebruikt.	JA/NEE	Als nee: U loopt een verhoogd risico. Bij verstrekking van gegevens buiten de organisatie is het van belang dat de betrokkene hiervan op de hoogte is en dat maatregelen zijn getroffen om de gegevens te beschermen. U loopt ook een risico compliance (zie art. 34 lid 1 onder b Wbp).
5.8	Stelt uw organisatie profielen op van de betrokkenen, al dan niet geanonimiseerd?	Denk hierbij aan profielen op basis van het gebruik van diensten, de afname van producten of bepaalde combinaties van eigenschappen.	JA/NEE	Als ja: Ga verder met vraag 5.8.1 Als nee: Ga verder met vraag 5.9
5.8.1	Indien profielen worden opgesteld, kan het profiel tot uitsluiting of stigmatisering leiden?	Houd bij beantwoording rekening met: 1.Of de profielen op individueel niveau opgeslagen worden. 2.Op basis van welke gegevens de profielen worden opgesteld. 3.Welke profielen worden	JA/NEE	Als ja: U loopt een verhoogd risico. Het nemen van beslissingen op basis van een bepaalde profilering kan uitgelegd worden als discriminatie van bepaalde bevolkings-, leeftijds- of andere groepen. Zorg ervoor dat indien u toch gebruik maakt van profileringen duidelijk is: - Op basis waarvan deze profielen

		gebruikt. 4. Of een automatische beslissing gebaseerd wordt op gegevens. 5. Wat de logica achter deze beslissing is. 6 Partijen aan wie de gegevens worden verstrekt.		worden opgesteld. - Welke beslissingen op welke wijze worden genomen op basis van de profielen. - Of uit profielen gevoelige informatie is af te leiden. Zorg er ook voor dat indien nodig betrokkenen geïnformeerd worden over deze profilering en mogelijke beslissingen.
5.9	Kunnen de betrokkenen hun gegevens inzien of daarom vragen?	Hierbij kan gedacht worden aan reactie op verzoeken of het geven van inzage in eigen gegevens doormiddel van een informatiesysteem (waarbij wel moet vast staan dat gegevens alleen ingezien kunnen worden door personen die dat mogen).	JA/NEE	Als nee: U loopt een verhoogd risico. Betrokkenen hebben het recht om hun gegevens in te zien. Hierbij is het van belang dat u zelf ook een helder overzicht heeft van de gegevens die worden verwerkt en waar deze zich binnen de organisatie bevinden. U loopt ook een compliance risico aangezien het verplicht is betrokkenen (op verzoek, eventueel tegen een redelijke vergoeding) inzage te geven (zie art.35 e.v. Wbp).
5.10	Kunnen de betrokkenen hun gegevens corrigeren of daarom vragen (verbeteren, aanvullen)?	Hierbij kan gedacht worden aan het vragen van een reactie op opgestuurde overzichten of het geven van (eigen) correctiemogelijkheden in de eigen gegevens door middel van een informatiesysteem (waarbij de betrokkene wel op een toereikende wijze geïdentificeerd dient te worden).	JA/NEE	Als nee: U loopt een verhoogd risico. Het bieden van een mogelijkheid tot correctie verbetert de gegevenskwaliteit. Als correcties niet doorgevoerd (kunnen) worden, verslechterd de gegevenskwaliteit en zijn de gegevens uiteindelijk (mogelijk) niet meer geschikt. U loopt hiermee ook een compliance risico (zie art. 36 Wbp).
5.11	Kunnen de betrokkenen hun gegevens verwijderen of daarom vragen?	Hierbij kan gedacht worden aan een reactie op verzoeken of het geven van eigen verwijderingsmogelijkheden in de eigen gegevens door middel van een informatiesysteem (waarbij wel moet vast staan dat gegevens alleen verwijderd kunnen worden door personen die dat mogen).	JA/NEE	Als nee: U loopt een verhoogd risico. Betrokkenen hebben het recht om te verzoeken om verwijdering van gegevens. Als er geen zwaarwegende redenen zijn om dit niet te doen, dient dit ook uitgevoerd te worden. In andere gevallen heeft de betrokkene het recht meegedeeld te worden om welke reden (deels) niet aan het verzoek wordt voldaan. U loopt hiermee een compliance risico (zie art. 36 Wbp).
6	**Bewaren en vernietigen**			
6.1	Is er een bewaartermijn	Houdt hierbij rekening met	JA/NEE	Als nee: U loopt een verhoogd risico.

	voor de gegevens vastgesteld?	het doel waarvoor de gegevens zijn verzameld en vervolgens worden verwerkt, en bedrijfsrichtlijnen en wettelijk vastgestelde bewaartermijnen bijvoorbeeld in de archiefwet, belastingwet.		Indien gegevens oneindig bewaard worden wordt het risico dat deze gebruikt worden door ongeautoriseerde personen hoger. Eveneens brengt het kosten met zich mee om de gegevens te bewaren (en onderhouden). U loopt hiermee ook een compliance risico (zie art. 10 Wbp). U dient gegevens slechts zo lang te bewaren als nodig is voor het voldoen aan de doelstellingen. U kunt gegevens na deze periode wel geanonimiseerd bewaren.
6.2	Kunnen de gegevens na afloop van de bewaartermijn fysiek worden verwijderd (uit een bestand) of vernietigd (papier)?	Het is niet voldoende om gegevens aan te merken als 'verlopen'; na het aflopen van de bewaartermijn dienen deze daadwerkelijk verwijderd te worden. Houd bij de beantwoording van de vraag rekening met: 1. Of het mogelijk is (delen van) de gegevens te vernietigen of te verwijderen. 2. Indien de gegevens worden vernietigd of verwijderd, of dit ongedaan kan worden gemaakt. 3. Of de gegevens anoniem kunnen worden gemaakt om ze te bewaren.	JA/NEE	Als nee: U loopt een verhoogd risico. Indien gegevens oneindig bewaard worden wordt het risico dat deze gebruikt worden door ongeautoriseerde personen hoger. Eveneens brengt het kosten met zich mee om de gegevens te bewaren (en onderhouden). Daarnaast is het wenselijk (en in veel gevallen verplicht) gegevens op verzoek van de betrokkene te verwijderen. U loopt hiermee een compliance risico. U dient gegevens slechts zo lang te bewaren als nodig is voor het voldoen aan de doelstellingen (zie art. 10 Wbp en art. 36 Wbp). U wordt geadviseerd de gegevens nadat ze niet meer nodig zijn te vernietigen (als een wettelijke verplichting om ze te bewaren dit niet in de weg staat) of indien dit niet mogelijk is te anonimiseren.
6.3	Zo ja, worden de gegeve ns na verstrijken van de bewaartermijn op een dusdanige manier vernietigd of verwijderd dat ze niet meer te benaderen en te gebruiken zijn?	Houd bij beantwoording rekening met: 1. Of regelgeving of beleid bestaat voor vernietiging van gegevens (bijvoorbeeld archiefwet). 2. Waar (welke locatie) gegevens worden bewaard. 3. Op welk medium (papier, CD, harde schijf) gegevens worden bewaard. 4. Of deze locatie/medium zijn afgeschermd voor gebruik (bijvoorbeeld het archief). 5. Welke andere redenen	JA/NEE	Als nee: Het zo kort mogelijk bewaren van gegevens heeft een aantal voordelen. - De benodigde opslag en rekencapaciteit van uw computer systemen is lager, waardoor prestaties, herstel tijden en serviceniveaus kunnen worden verhoogd. - U zult minder gegevens hoeven te onderhouden en updaten en de kans op fouten wordt verkleind. Eveneens bestaat het risico dat de gegevens worden gebruikt voor andere doelen dan oorspronkelijk verzameld en opgeslagen. Uw organisatie loopt

		bestaan om de gegevens te bewaren zoals bedrijfshistorische, wettelijke, juridische redenen.		daarnaast compliance risico's als u te veel gegevens voor het doel bewaart (zie art. 11 lid 1 Wbp). U wordt geadviseerd per gegevensdrager te bepalen op welke wijze de gegevens hierop vernietigd moeten worden. Zie hiervoor de procedure 'Veilige afvoer van ICT-middelen' van de IBD welke begin april 2014 uitkomt.
7	**Beveiliging**			
7.1	Is duidelijk op welke wijze het project er voor zorg draagt dat aan de gestelde eisen in het beveiligingsbeleid voldaan gaat worden?	Denk hierbij aan welke maatregelen getroffen worden om te voldoen aan het beschreven beleid (een informatiebeveiligingsplan).	JA/NEE	Als nee: U wordt geadviseerd tijdens het project een informatiebeveiligingsplan op te stellen met daarin beveiligingsmaatregelen / maatregelen die voor een passende bescherming van de gegevens zorgen.

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