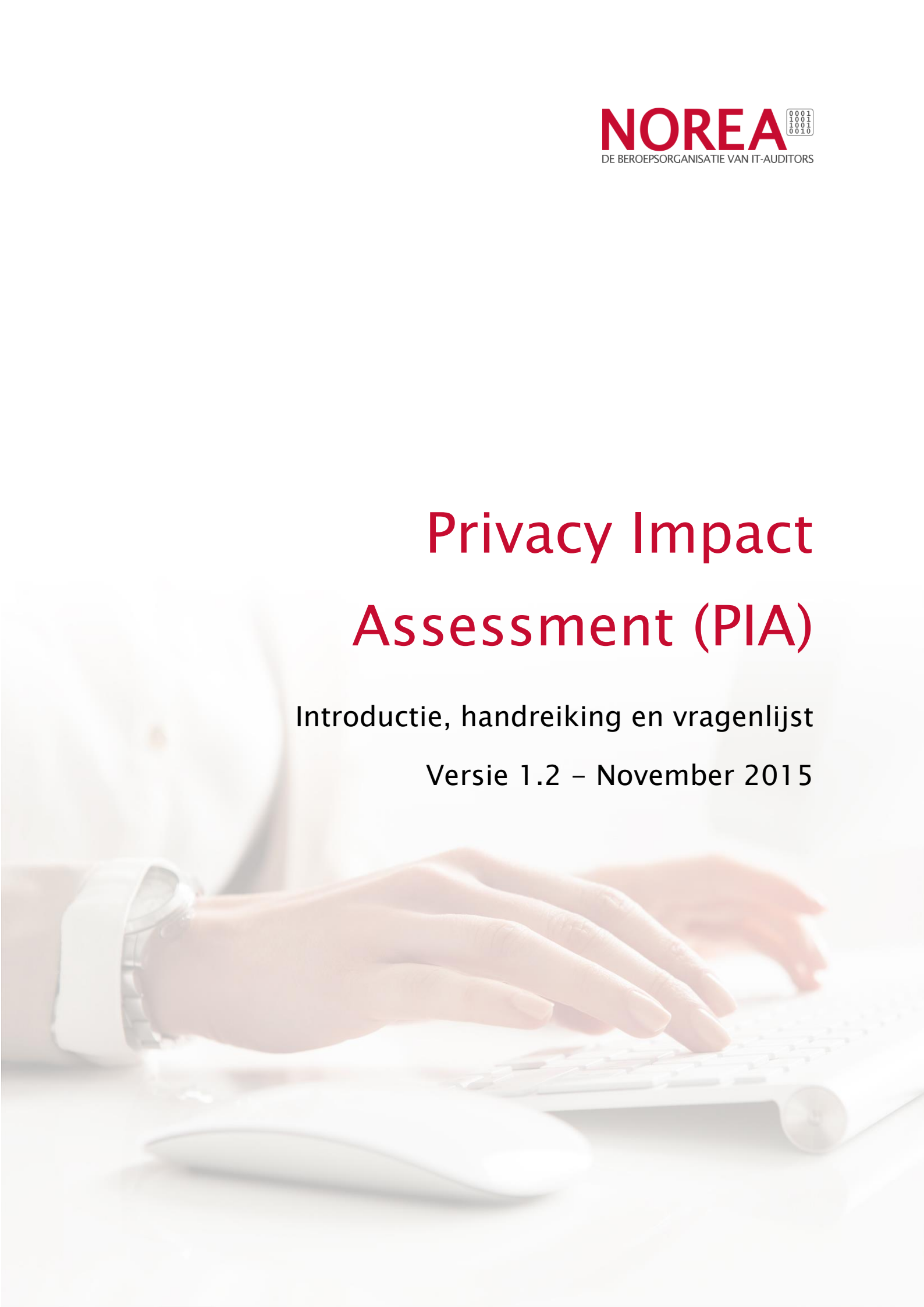
NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Privacy Impact Assessment (PIA)

Introductie, handreiking en vragenlijst

Versie 1.2 – November 2015



Over deze handreiking Privacy Impact Assessment (PIA)

Beheer

Voor vragen en opmerkingen kunt u zich wenden tot:
NOREA
Postbus 7984, 1008 AD Amsterdam
telefoon: 020-3010380
e-mail: norea@norea.nl

Meer informatie kunt u vinden op:
www.norea.nl
www.privacy-audit-proof.nl

De PIA zal worden geëvalueerd en in de toekomst verder worden verbeterd. Het is de bedoeling om de PIA op basis van ervaring en evaluatie als NOREA-handreiking (conform artikel 15 Reglement Beroepsbeoefening) vast te stellen. Dit document heeft tot dat moment de formele status van studierapport (conform artikel 18 Reglement Beroepsbeoefening).

Deelnemers

De volgende organisaties hebben mede een bijdrage geleverd aan de ontwikkeling van deze PIA:

- Auditdienst Rijk (ADR)
- Autoriteit persoonsgegevens
  (voorheen: College bescherming persoonsgegevens / Cbp)
- PBLQ/HEC
- PwC

Namens de NOREA Kennisgroep Privacy,

drs. Erik König EMITA en Wolter Karssenberg RE, CIPP/E, CIPM

Versiebeheer		
Versie	**Datum**	**Wijziging**
1.0	Mei 2013	Publicatie eerste versie
1.1	Juni 2015	Reacties en suggesties verwerkt
1.2	November 2015	Toevoegen meldplicht datalekken

Inhoud

Voorwoord

Privacybescherming staat in toenemende mate in de belangstelling. Voor een groeiend aantal bedrijven is het zorgvuldig omgaan met persoonsgegevens een onderwerp waarmee zij zich in positieve zin willen onderscheiden van concurrerende bedrijven. Zij zien privacy-bescherming als 'unique selling point'. Ook voor de Rijksoverheid, de lagere overheden en de overige publieke sector (zoals onderwijs- en zorginstellingen) is het van belang om zorgvuldig om te gaan met persoonsgegevens. In het belang van de burger, maar ook in het belang van een goede en integere dienstverlening. In het regeerakkoord (PvdA/VVD-2012) is vastgelegd dat de uitvoering van een Privacy Impact Assessment een vanzelfsprekende maatregel is bij de bouw van systemen en het aanleggen van databestanden.

Voor het meewegen van privacybelangen in de besluitvorming over de ontwikkeling van producten, diensten of wetgeving is het van groot belang dat dit in een vroegtijdig stadium gebeurt. Als de risico's voor inbreuken op de privacy pas worden onderkend als de ontwikkeling van het product, dienst of wetsvoorstel al in een vergevorderd stadium verkeert, is de kans immers groot dat noodzakelijke aanpassingen zeer tijdrovend en kostbaar zijn. Om organisaties een instrument te bieden om privacyrisico's in een vroeg stadium op een gestructureerde en heldere manier in beeld te kunnen brengen, is deze methode voor Privacy Impact Assessment (PIA) door NOREA, de beroepsorganisatie van IT-auditors, gepubliceerd.

Een PIA stimuleert organisaties om proactief na te denken over vragen als: *Wat is de impact van het beoogde project op de privacy van de betrokkenen? Wat zijn de risico's voor de betrokkenen en voor de organisatie? Is een aanpak die minder gevolgen heeft voor de privacy ook mogelijk, gegeven de doelstellingen van het project?* Na het uitvoeren van een PIA kan de 'verantwoordelijke' gerichte opdrachten geven aan degene die het product of de dienst verder ontwikkelt opdat maatwerk kan worden geleverd en wordt voorkomen dat in een later stadium kostbare aanpassingen nodig zijn.

Als indiener van de 'Motie Franken[1]' spreekt het voor zich dat ik deze publicatie van harte in uw belangstelling aanbeveel,

prof. mr. Hans Franken,
voormalig Lid Eerste Kamer der Staten Generaal

[1] Deze PIA sluit nadrukkelijk aan bij de steeds sterker wordende politieke druk op het uitvoeren van PIA's voor verwerkingen die bijzondere privacy risico's inhouden. Zo is in 2011 in de Eerste Kamer een motie van het lid Franken (CDA) aangenomen die de regering verzoekt om bij wetsvoorstellen, waarbij van een beperking op het grondrecht van de bescherming van de persoonlijke levenssfeer sprake is, o.a. een PIA in de afweging en besluitvorming te betrekken en daarvan in de memorie van toelichting bij het betreffende wetsvoorstel verslag te doen (http://www.eerstekamer.nl/motie/motie_franken_cda_c_s_over). Via een aangenomen motie riep de Tweede Kamer de regering op om tot directe uitvoering van de motie Franken over te gaan (https://zoek.officielebekendmakingen.nl/kst-32761-8-n1.html). Voorts is in de concept EU privacy verordening (http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf) opgenomen dat een "data protection impact assessment" ("privacyeffectbeoordeling") verplicht is bij verwerkingen die naar hun aard, reikwijdte of doeleinden bijzondere privacyrisico's inhouden.

Leeswijzer

Deze PIA bestaat uit de volgende delen:

Deel 1: Introductie: over het instrument PIA

Dit deel gaat in op de achtergrond en het belang van de PIA. U[2] 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?*

Deel 2: Handreiking voor het PIA proces

Dit deel bevat een handreiking voor het effectief en efficiënt uitvoeren van een PIA. 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?*

Deel 3: PIA-vragenlijst

Na het doorlopen van de PIA-vragenlijst heeft u antwoorden op vragen als *Wat zijn de privacy risico's van de verwerking van persoonsgegevens voor de betrokkenen én voor mijn organisatie?*

Deel 4: Bijlagen

Een verklaring van de gebruikte begrippen en de succes- en faalfactoren voor het uitvoeren van een PIA vindt u in de bijlagen.

[2] Met "u" wordt in dit document in het algemeen zowel de binnen de organisatie eindverantwoordelijke voor de verwerking van persoonsgegevens als de projectleider van de uitvoering van de PIA aangesproken.

1 Introductie: Over het instrument PIA

Dit deel gaat in 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[3]. Er zijn verschillende vormen van privacy, zo wordt bijvoorbeeld onderscheid gemaakt naar relationele, lichamelijke, territoriale, communicatieve, medische en informationele privacy[4]. Deze dimensies geven invulling aan de persoonlijke levenssfeer. Eerbiediging van de persoonlijke levenssfeer is als grondrecht vastgelegd in artikel 10 van de Grondwet.

In de PIA, zoals in dit document uitgewerkt, heeft privacy betrekking op de informationele privacy. De vastlegging en verwerking van persoonsgegevens valt onder de informationele privacy. De bescherming van persoonsgegevens kan omschreven worden als het recht op eerlijke, veilige en betrouwbare informatieverwerking.

Leidend in het denken en praten over bescherming van persoonsgegevens zijn de privacy-principes van de OECD/OESO[5]. Deze principes bieden houvast voor het op een goede manier verwerken van persoonsgegevens. Momenteel regelt Europese Richtlijn 95/46/EG[6] de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens in de Europese Unie. In Nederland is deze Richtlijn geïmplementeerd in de Wet bescherming persoonsgegevens (Wbp)[7].

Door snelle technologische ontwikkelingen zijn nieuwe uitdagingen voor de bescherming van persoonsgegevens ontstaan. Persoonsgegevens in de Europese Unie worden op gefragmenteerde wijze beschermd, er is sprake is van rechtsonzekerheid en in brede lagen van de bevolking bestaat het beeld dat met name onlineactiviteit aanzienlijke risico's inhoudt. Om die reden wordt gewerkt aan een Algemene Verordening Gegevens-bescherming (AVG)[8]. Naar

[3] The right to privacy, Warren and Brandeis, Harvard Law Review, 15 december 1890. http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html

[4] Privacyregulering in theorie en praktijk, Recht en Praktijk, deel 75, prof. mr. J.M.A. Berkvens, prof. mr. C. Prins, 2002

[5] Organisation for Economic Cooperation and Development/Organisatie voor Economische Samenwerking en Ontwikkeling. http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

[6] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:nl:HTML

[7] http://wetten.overheid.nl/BWBR0011468/

[8] Voorstel voor een verordening van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (algemene verordening gegevensbescherming), 25 januari 2012. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:NL:PDF

huidige verwachting zal de AVG in 2018 in werking treden. De AVG zal consequenties hebben die tot heroverweging van de beheersmaatregelen met betrekking tot privacybescherming leiden. In de NOREA-publicatie over de nieuwe Europese verordening worden de kernelementen van deze verordening beschreven[9].

1.2 Beschrijving van het instrument PIA

1.2.1 Wat is een PIA?

De afkorting PIA staat voor Privacy Impact Assessment.

Een PIA legt in de eerste plaats de privacyrisico's bloot van nieuwe (projecten en initiatieven) of bestaande verwerkingen van persoonsgegevens en draagt bij aan het vermijden of verminderen van deze privacyrisico's.

Op basis van deze PIA wordt op systematische wijze inzichtelijk gemaakt hoe groot de kans is dat de privacy van de betrokken personen van wie gegevens worden verwerkt wordt geschaad, waar deze risico's zich voordoen en welke gevolgen daaraan voor hen verbonden zijn.

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; en
- 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.

Vanaf 1 september 2013 is het uitvoeren van een PIA binnen de Rijksdienst verplicht bij ontwikkeling van nieuwe wetgeving en beleid waarmee de bouw van nieuwe ICT-systemen of de aanleg van grote databestanden wordt voorzien[10]. De PIA is (vooralsnog) geen verplicht instrument voor het bedrijfsleven. In de AVG zullen ook voor het bedrijfsleven verplichtingen voor het uitvoeren van een PIA worden opgenomen. Naar ons inzicht is de PIA een onmisbaar hulpmiddel voor organisaties om de privacy impact in te schatten of te evalueren.

Het verdient aanbeveling de PIA onderdeel te laten uitmaken van de privacy strategie en het kwaliteitssysteem van een organisatie alsmede van de kwaliteitsbeheersing van projecten waardoor verwerking van persoonsgegevens tot stand komt.

---

[9] Het Europees privacyrecht in beweging (IT-Recht, februari 2013 NOREA/Kluwer en Duthler Associates)

[10] Op basis van het Toetsmodel Privacy Impact Assessent Rijksdienst, 21 juni 2013. http://www.rijksoverheid.nl/documenten-en-publicaties/publicaties/2013/06/24/toetsmodel-privacy-impact-assessment-pia-rijksdienst.html

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

1.2.2 Wat levert een PIA op?

De PIA kent een aantal 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 privacyrisico'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.

1.2.3 Voor wie is het instrument PIA bedoeld?

De PIA kan gebruikt worden door alle typen organisaties.

Binnen deze doelgroep is de PIA bedoeld voor opdrachtgevers en opdrachtnemers van projecten en andere belanghebbenden. In het algemeen kan worden gezegd dat het zinvol is een PIA uit te voeren bij een nieuw project of grote wijziging van een bestaand systeem of proces waarbij persoonsgegevens worden verwerkt. De PIA kan uiteraard ook op bestaande verwerkingen van persoonsgegevens worden toegepast, indien dat nog niet eerder is geschiedt.

1.2.4 Wanneer voert u een PIA uit?

Een PIA kan het beste gestart worden in een zeer vroeg stadium van een project. Vervolgens kan de verdere uitwerking van de PIA aansluiten bij de verdere uitwerking van het project. Op die manier helpt de PIA u om het privacybelang structureel mee te nemen in het project. Daarmee wordt de PIA een belangrijk onderdeel van het ontwerp proces.

Ook aanpassingen of wijzigingen van bestaande verwerkingen van persoonsgegevens 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.

U kunt door structureel PIA's uit te voeren bij projecten die te maken hebben met de verwerking van persoonsgegevens, of op reeds bestaande verwerkingen, op gestructureerde wijze inzicht krijgen in het totale risicoprofiel van uw organisatie.

1.2.5 Hoeveel tijd kost het om een PIA uit te voeren?

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 uiterst complexe projecten kan dit oplopen tot tientallen dagen. Dit is een substantiële investering, maar daarmee kunnen zeer omvangrijke schade-posten worden voorkomen of beperkt.

De belangrijkste factoren van invloed zijn:

1. het aantal belanghebbenden bij het project en de mate waarin deze vragen of twijfels hebben over de consequenties voor privacy;
2. de impact en het belang van het project op de organisatie en de samenleving;
3. de (technische en organisatorische) complexiteit van de verwerking.

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

1.2.6 Andere privacy instrumenten

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

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

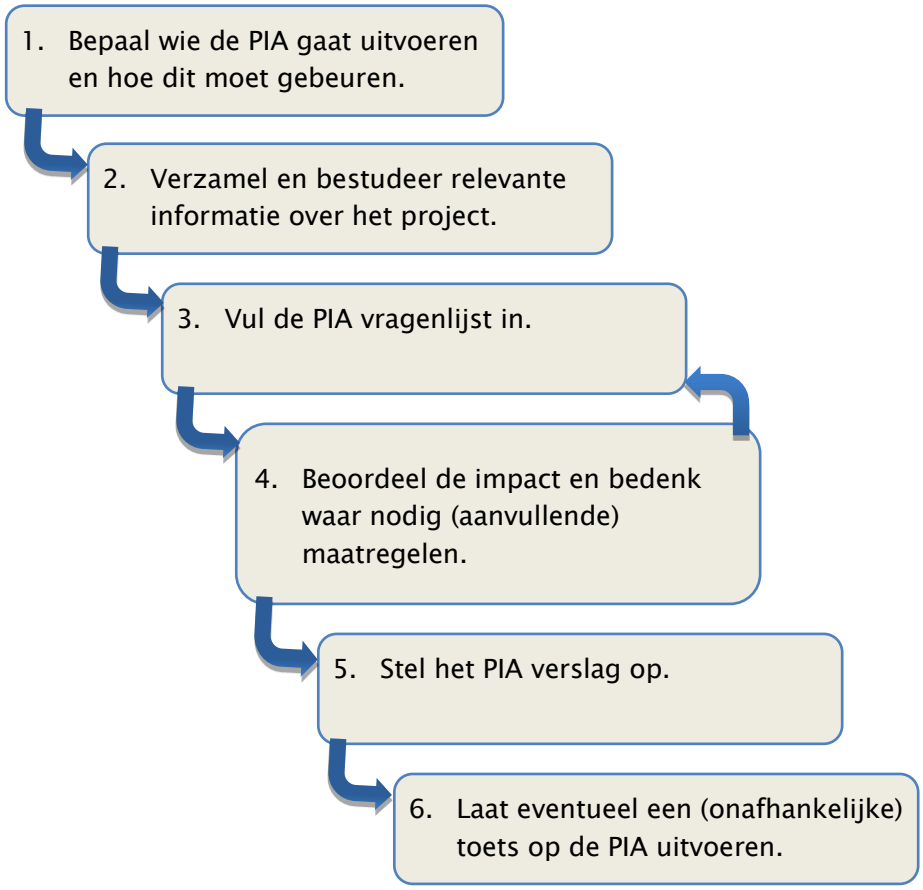
Deze PIA is geen nalevingsinstrument, maar een risicoanalyse-instrument waarmee privacy-risico's kunnen worden geïdentificeerd en gelokaliseerd. Ook in deze PIA wordt het uitvoeren van zo'n compliance check in veel gevallen aangeraden.

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?*

2.1 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.

2.1.1 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. Privacy behoeft een multidisciplinaire insteek. De resultaten van de PIA worden daardoor beter, doordat 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 B 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 C, door te nemen en te bepalen hoe hiermee omgegaan wordt.

De antwoorden op bovenstaande vragen worden samengevat in een plan van aanpak zodat hier geen verwarring over kan ontstaan.

2.1.2 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.
- Van wie de gegevens worden verzameld.
- Het type gegevens (o.a. de gevoeligheid) dat gebruikt gaat worden.
- De wijze waarop deze gegevens verzameld en verwerkt gaan worden.
- 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).
- 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.

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:

1. De organisatie die het project uitvoert en (indien dit niet dezelfde is) de opdrachtgever.
2. Overige organisaties betrokken bij het project.
3. Organisaties en individuen die belang hebben bij het project en de uitkomsten ervan (zoals leveranciers en afnemers).
4. Organisaties en individuen die worden geraakt door het project en de uitkomsten ervan (burgers, klanten, belangenverenigingen).
5. 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:

1. Eerdere PIA's en informatie over gelijkwaardige projecten.
2. Beschrijving van de gebruikte technologie en zijn gebruikswijzen (vooral relevant bij het gebruik van nieuwe technologie of het gebruik van bekende technologie op een nieuwe manier).
3. Factsheets, whitepapers, rapporten en artikelen van onderzoeksorganisaties, samenwerkingsverbanden tussen bedrijven/ beroepsgroepen en aanbieders van technologie.
4. Consultaties met beroepsverenigingen.
5. Consultaties met private organisaties die de organisaties en individuen die worden geraakt door het project en de uitkomsten ervan representeren of daaraan advies geven.
6. Relevante wetgevingsdocumentatie en jurisprudentie.
7. Onderzoeken, richtsnoeren en andere publicaties van toezichthouders.

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.

2.1.3 Vul de PIA vragenlijst in

De vragenlijst is opgenomen in hoofdstuk 3.

Het is niet 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. De vragenlijst bestaat uit zeven risicogebieden die elke met een aantal vragen worden behandeld.

Risicogebieden die samenhangen met de omgeving waarin u opereert:

1. Het type project.
2. De gegevens die u wilt gebruiken.
3. De partijen die betrokken zijn bij de uitvoering van het project.

Risicogebieden die samenhangen met een bepaalde fase van de verwerking:

4. Het verzamelen van de gegevens.
5. Het gebruik van de gegevens.
6. Het bewaren en vernietigen van de gegevens.
7. De beveiliging van de gegevens.

De risico's met betrekking tot de privacy principes volgen uit de beantwoording van de vragen (op basis van de verwijstabel zoals opgenomen in bijlage I):

- Dataminimalisatie.
- Gegevenskwaliteit.
- Doelbinding en verenigbaarheid van verdere verwerking.
- Limitering van het gebruik van gegevens.
- Beveiliging van gegevens.
- Transparantie.
- Rechten van betrokkenen.
- Verantwoordelijkheid en verantwoording.

2.1.4 Beoordeel de impact en bedenk waar nodig (aanvullende) maatregelen

Op 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.

2.1.4.1 Impactbepaling

Bij het beoordelen van de impact zijn er twee zaken waar u rekening mee moet houden, namelijk 'impact op de betrokkene' en 'impact op de 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 A Begrippen).
- Risico op en gevolgen van identiteitsdiefstal / -fraude (waarbij anderen (opzettelijk) verplichtingen aangaan 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 E).

Uitgangspunt in deze PIA is dat indien de privacy van de betrokkenen op een van deze gebieden wordt geschaad en/of niet aan wetgeving wordt voldaan, 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.
- Sancties door toezichthouders worden opgelegd, zoals boetes.

Impact op de organisatie
De impact (zoals reputatieschade, maar ook materiële financiële schade als gevolg van compliance issues, 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 en de (voorbeeld)functie van de organisatie.

2.1.4.2 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 of en op welke wijze de risico's vermeden of verkleind kunnen en/of moeten 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.

Indien u hebt geïdentificeerd dat aanvullende maatregelen nodig zijn om de risico's van de gegevensverwerking te rechtvaardigen zult u deze met de verantwoordelijken voor het project moeten bespreken. Daarmee doorloopt u stap 3 nogmaals.

U herhaalt deze stappen zo vaak als nodig, totdat de risico's acceptabel zijn en het ontwerp gerealiseerd kan worden dan wel dat het project wordt stopgezet.

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 of verminderd 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 privacy principe kunnen ook maatregelen getroffen worden die het risico verminderen. Hieronder zijn per privacy principe enkele voorbeelden opgenomen[11]:

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 de 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 privacy beleid, gedragscode of het laten certificeren van de verwerking.
7. **Rechten van betrokkenen**
   Betrokkenen zeggenschap geven over zijn gegevens door de invoer van een 'self service' bijvoorbeeld via een beveiligd internet portal.
8. **Verantwoordelijkheid en Verantwoording**
   Invoeren van periodieke externe controle.

2.1.5 Stel het PIA-rapport op

De resultaten van de PIA worden vastgelegd in een rapport. Een voorbeeld indeling voor een rapport is opgenomen in bijlage D. Op basis van het rapport kan de gebruiker van de resultaten van de PIA eventueel noodzakelijke beslissingen nemen.

[11] 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/volwassenheids-niveau) 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.

De risicogebieden waar de privacy van de betrokkene mogelijk wordt geschaad volgen uit de ingevulde PIA. Vervolgens wordt in het rapport ruimte geboden om de impact op de betrokkenen en op de organisatie zelf in te vullen. Daarnaast worden de belangen van zowel de betrokkenen als de organisatie beschreven. Vervolgens worden de belangen in relatie tot de impact gewogen en de rechtvaardiging van de gegevensverwerking beschreven.

Ook wordt ruimte opgenomen voor een advies over de eventuele noodzakelijke maatregelen om de rechtvaardiging van de gegevensverwerking te borgen. De overwegingen die ten grondslag liggen aan de antwoorden op de vragenlijst zijn een belangrijk onderdeel van het rapport en de aanbevelingen hier in.

Het rapport 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 rapport op onderdelen geactualiseerd kan worden. Het verdient aanbeveling aan het eind van het project een definitieve versie van de PIA vast te stellen die gebaseerd is op de productionele eigenschappen daarvan.

2.1.6 Laat eventueel een (onafhankelijke) review uitvoeren

Tot slot kan het raadzaam zijn dat u het rapport (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. De IT-auditor kan/zal door middel van zijn audit-team de juiste expertise waarborgen.

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 nader onderzoek noodzakelijk of wenselijk is. Onderstaande verwijzingen kunnen u mogelijk op weg helpen bij uw verdere inspanningen:

- U wilt meer informatie over het vermijden van privacy risico's door het toepassen van oplossingen in de technologie. Zie 'Privacy by Design' en 'Privacy Enhancing Technologies'[12] (PET).
- 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' [12] en diverse andere publicaties, waaronder informatiebladen van de Autoriteit persoonsgegevens.
- U wilt het Burgerservicenummer verwerken. Zie de 'Handreiking BSN voor gebruikers'[13].
- U wilt weten of wordt voldaan aan de eisen van de Wbp. Zie de Zelfevaluatie [14] dan wel het Raamwerk Privacy Audit [15].
- U wilt weten hoe u de persoonsgegevens moet beveiligen. Zie de best practices en standaarden op het gebied van informatiebeveiliging (zoals ISO27001/27002 [19, 20]).

[12] https://privacybydesign.ca/

[13] http://www.rijksdienstvooridentiteitsgegevens.nl/BSN/Informatiebank/Procedures/Handreikingen

3 PIA vragenlijst

Na het doorlopen van het vierde deel heeft u antwoorden op vragen als Wat zijn de privacyrisico's van de verwerking van persoonsgegevens voor de betrokkenen en voor mijn organisatie? Waar liggen deze risico's? Dit vierde deel bevat hiertoe informatie en een vragenlijst op basis waarvan een aantal privacy relevante aspecten van het project (waaronder de voorgenomen handelingen met persoonsgegevens en de gegevensstromen) én de privacy impact van een project inzichtelijk worden.

Onderstaande vragen helpen u bij het in kaart brengen van de privacyrisico's (gedefinieerd als een verhoogde kans dat een risico gelopen wordt) die gepaard gaan met het project.

De vragenlijst bestaat uit 7 onderdelen die achtereenvolgens ingaan op:

1. Het type project.
2. De gegevens die u wilt gebruiken.
3. De partijen die betrokken zijn bij de uitvoering van het project.
4. Verzamelen van gegevens.
5. Gebruik van gegevens.
6. Bewaren en vernietigen van gegevens.
7. Beveiligen van gegevens.

Alle vragen kunt u met ja of nee beantwoorden. Bij de vragen is een toelichting gegeven. Soms is dit 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.

Het is niet 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.

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.

#	Vraag	Extra informatie	Ja	Nee
1	Het type project			
1.1	Is er sprake van het verwerken[14] van persoonsgegevens[15]?		Ga verder.	U kunt stoppen.
1.2	Is het duidelijk wie verantwoordelijk[16] 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.	Ga verder.	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.
1.3	Verwerkt uw organisatie de persoonsgegevens in opdracht en onder verantwoordelijkheid van een andere organisatie? Ofwel: Treedt uw organisatie op als bewerker[17]?	Deze vragenlijst is bedoeld voor organisaties die persoonsgegevens verwerken in de rol van verantwoordelijke[18]. Deze vragenlijst is niet bedoeld voor organisaties die persoonsgegevens verwerken in de rol van bewerker.	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 in het project) inzichtelijk te maken.	Bepaal wie (bedrijfsonderdeel, persoon) binnen uw organisatie de verantwoordelijke is.

[14] Verwerking van persoonsgegevens: 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, alsmede het afschermen, uitwissen of vernietigen van gegevens.

[15] Persoonsgegevens: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.

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

[17] Bewerker: degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen.
Voor aanvullende informatie over de interpretatie van de begrippen verantwoordelijke (controller) en bewerker (processor) wordt verwezen naar de opinie van de *Art. 29 Data Protection Working Party* (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf).

[18] Verantwoordelijke: de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. Zie ook de Handleiding voor verwerkers van persoonsgegevens (http://www.rijksoverheid.nl/documenten-en-publicaties/brochures/2006/07/13/handleiding-wet-bescherming-persoonsgegevens.html)

#	Vraag	Extra informatie	Ja	Nee
1.4	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 moet worden gezorgd dat de risico's worden beheerst (bijvoorbeeld door deze PIA periodiek uit te voeren)	Ga verder.	Het risico bestaat dat de maatregelen in de toekomst niet meer worden gevolgd of niet meer passen bij de situatie.
1.5	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 management; Is er iemand verantwoordelijk voor het realiseren van het doel? **Realistisch**; of de doelstelling haalbaar is. **Tijdgebonden**; wanneer (in de tijd) het doel bereikt moet zijn.	Ga verder.	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).
1.6	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.	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.	Ga verder.
b.	Gebruik van technologie die bij het publiek vragen of weerstand op kan roepen?	Bijvoorbeeld biometrie, RFID, behavioural targeting (profilering).		Ga verder.
c.	De invoering van bestaande technologie in een nieuwe context?	Zoals cameratoezicht of drugscontrole op de werkvloer.		Ga verder.
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 of koppelen van verschillende overheidsregistraties, invoering van nieuwe vormen van identificatie of vervanging van een systeem waarin persoonsgegevens worden opgeslagen.		Ga verder.

#	Vraag	Extra informatie	Ja	Nee
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.	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.	Ga verder.
f.	Het verzamelen van meer of andere persoonsgegevens dan voorheen of een nieuwe manier van verzamelen.	Bijvoorbeeld gegevensverrijking door enquêtes en klantonderzoeken of benadering van klanten of burgers op basis van beschikbare gegevens voor nieuwe producten of diensten.		Ga verder.
g.	Gebruik van al verzamelde gegevens voor een nieuw doel of een nieuwe manier van gebruiken.	Bijvoorbeeld het samenvoegen van interne databases om klantprofielen op te stellen.		Ga verder.
1.7	Heeft u op alle bovenstaande (a t/m g) nee geantwoord?		U kunt stoppen. De (mogelijke) privacy-risico's van uw verwerking zijn laag. Het verder uitvoeren van deze PIA heeft daarmee weinig toegevoegde waarde. Let op! U dient wel aan de eisen van de Wbp te voldoen. Dit kan door middel van een compliance check worden vastgesteld.	Ga verder.
1.8	Is er (naast de Wbp) veel wet- en regel-geving 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.	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.	Ga verder.

#	Vraag	Extra informatie	Ja	Nee
1.9	Zijn er veel maatschappelijke belanghebbenden?	Houd bij de beantwoording rekening met: 1. Medewerkers, afnemers, leveranciers, belangengroeperingen, burgers, klanten toezichthouders. 2. Welke beroepsgroepen betrokken zijn bij de verwerking.	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.	Ga verder.
1.10	Zijn er bij veel partijen betrokken de uitvoering van het project?	Houd bij de beantwoording rekening met: 1. Aannemers en dienstverleners. 2. Hardware en software leveranciers. 3. IT Service providers.	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 inschatten.	Ga verder.
1.11	Is er een geschillenregeling of een partij waar de betrokkene terecht kan bij vragen of klachten?		Ga verder.	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 een geschillenregeling.

#	Vraag	Extra informatie	Ja	Nee
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: 1. Is per data-element vastgesteld wat de toegevoegde waarde is en waarom dit noodzakelijk is? 2. Kan volstaan worden met het gebruik van alleen een ja/nee in plaats van het volledige gegeven? 3. Kan volstaan worden met het verschil tussen 2 waarden in plaats van beide waarden afzonderlijk? 4. Kan gebruikgemaakt worden van andere wiskundige methodieken (bijvoorbeeld voor het bepalen van afwijkingen)?	Ga verder.	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 service niveaus kunnen worden verhoogd. • U zult minder gegevens hoeven te onderhouden en updaten en de kans op fouten wordt verkleind. Bovendien loopt 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 gepseudonimiseerde gegevens worden bereikt (terwijl daar op dit moment geen gebruik van wordt gemaakt)?	Door pseudonimisering, 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 anonimisering worden alle direct en uniek identificerende gegevens verwijderd.	U loopt een verhoogd risico door het gebruiken van persoonsgegevens. Door het gebruik van geanonimiseerde en/of gepseudonimiseerde gegevens valt u niet meer onder het regime van de Wbp. U verwerkt immers geen persoonsgegevens meer. Door de gegevens te anonimiseren of te pseudonimiseren 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.	Ga verder.
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.	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 personeelsvolg-systeem is instemming van de OR nodig.	Ga verder.
2.4	Is sprake van het verwerken van:			

#	Vraag	Extra informatie	Ja	Nee
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.	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).	Ga verder.
b.	Uniek identificerende gegevens?	Bijvoorbeeld biometrische gegevens, vingerafdrukken, DNA-profielen.	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).	Ga verder.
c.	Wettelijk voorgeschreven persoonsnummers.	Bijvoorbeeld het burgerservicenummer (BSN).	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).	Ga verder.
d.	Andere gegevens dan hiervoor beschreven waarvoor geldt dat sprake is van een (gepercipieerde) verhoogde gevoeligheid?	Bijvoorbeeld creditcardinformatie, financiële informatie, erfrechtelijke aspecten, arbeidsprestaties of gegevens waarvoor een geheimhoudingsplicht geldt?	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.	Ga verder.

#	Vraag	Extra informatie	Ja	Nee
2.4.1	Bij een van bovenstaande Ja: kan het doel met andere gegevens worden bereikt die een verminderd risico op misbruik met zich mee brengen?		U loopt een verhoogd risico. Het risico bestaat dat betrokkenen minder snel willen meewerken, of het 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).	Ga verder.
2.5	Verwerkt u gegevens over 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).	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.	Ga verder.
2.6	Hebben de gegevens betrekking op de gehele of grote delen van de bevolking?		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).	Ga verder.

#	Vraag	Extra informatie	Ja	Nee
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 de 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.	U loopt een verhoogd risico. Zorg voor een duidelijke beschrijving van de taken en verantwoordelijkheden met betrekking tot de gegevens waarbij onder andere wordt beschreven: • De beveiliging van gegevens. • Afhandeling van fouten. • Terugmelden van fouten. • Afstemming van beveiligingsbeleid. • Controle. Zorg voor een duidelijke gegevensbeschrijving.	Ga verder.
3.2	Zijn er (na afronding van het project) bij het verzamelen en verder verwerken van de gegevens meerdere *externe* partijen betrokken?	Houd bij de beantwoording rekening met: 1. Voor en door wie het project wordt uitgevoerd. 2. Welke partijen gebruikmaken van de gegevens. 3. Of andere partijen worden ingeschakeld voor het bereiken van het doel (wordt de verwerking van gegevens geoutsourced). 4. Of de gegevens worden verkocht. 5. Welke personen buiten de organisatie toegang hebben tot de gegevens.	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. • Terugmelding van fouten. • Controle. Zorg ook voor een duidelijke gegevens-beschrijving. Leg afspraken contractueel vast.	Ga verder.

#	Vraag	Extra informatie	Ja	Nee
3.3	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 bescher-ming 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: https://cbpweb.nl/nl/onderwerpen/internationaal-gegevensverkeer/doorgifte-naar-derde-landen 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.	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.	Ga verder.

#	Vraag	Extra informatie	Ja	Nee
3.4	Is de verstrekking van de gegevens aan derde partijen in lijn met het doel waarvoor de gegevens oorspronkelijk zijn verzameld?	Houd bij de beantwoording rekening met: 1. Wat het/de doel(en) is/zijn voor het gebruik van de gegevens. 2. Welke gegevens aan welke partijen worden verstrekt voor welk doel. 3. Of de verstrekking aan de andere partijen een 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 gepseudonimiseerd zijn).	Ga verder.	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 heeft mogelijk een compliance risico (Zie art. 9 lid 1 en 2 Wbp).
3.5	Worden de gegevens verkocht aan derde partijen?	De Wbp stelt voorwaarden aan het gebruik van gegevens voor commerciële of charitatieve doelen, zoals het recht van verzet.	U loopt een compliance risico. Het gebruik van gegevens van commerciële doelen stelt extra eisen (zie art. 41 lid 3 Wbp).	Ga verder.
4	Verzamelen van gegevens			
4.1	Kan de manier waarop de gegevens worden verzameld worden opgevat als privacy gevoelig?	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 of tracking door cookies of GPS?	U wordt geadviseerd na te gaan of de gegevens op een andere manier kunnen worden verzameld.	Ga verder.

#	Vraag	Extra informatie	Ja	Nee
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.	Ga verder.	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: 1. U vraagt toestemming. 2. De gegevens zijn noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene een partij is. 3. De gegevens zijn nodig voor het volgen van een wettelijke verplichting. 4. De betrokkene heeft er een vitaal belang bij dat u de gegevens verzamelt. 5. De gegevens zijn nodig voor de goede vervulling van een publiekrechtelijke taak. 6. U heeft een gerechtvaardigd belang bij de verwerking.	Ga verder	Voor het verwerken van persoonsgegevens is een grondslag noodzakelijk. Indien deze ontbreekt, loopt u compliance risico (art. 8 Wbp).
4.4	Is duidelijk of u de gegevens verzamelt op basis van opt-in (verzameling uitsluitend als de betrokkene daarvoor toestemming heeft gegeven) of op basis van opt-out (verzameling tenzij de betrokkene daartegen bezwaar heeft gemaakt)?	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)	Ga verder	U loopt een verhoogd risico. Indien de betrokkene verrast wordt door de verwerking zonder toestemming bestaat het risico dat deze bezwaar maakt.

#	Vraag	Extra informatie	Ja	Nee
4.4.1	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.	Ga verder.	U loopt een verhoogd risico. Indien u niet kunt voldoen aan verzoeken van betrokkenen om de verwerking van gegevens te stoppen of omdat u deze mogelijkheid niet aanbiedt kan dit leiden tot irritatie van betrokkenen of kostbare aanpassingen in systemen. U wordt geadviseerd de betrokkenen de mogelijkheid te bieden de toestemming in te trekken en dit systeemtechnisch mogelijk te maken.
4.4.2	Is de impact van het intrekken van de toestemming groot voor de betrokkene?	Bijvoorbeeld omdat de dienstverlening aan de betrokkene stopgezet wordt terwijl deze daarvan afhankelijk is.	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).	Ga verder.
4.5	Meldt u de betrokkene dat de gegevens worden verzameld?	Houd bij de beantwoording rekening met: 1. Waar de gegevens vandaan komen (van de betrokkene, een interne 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) de gegevens aan andere partijen worden verstrekt. 9. Hoe lang de gegevens worden bewaard.	Ga verder met vraag 4.5.2	Ga verder met vraag 4.5.1.

#	Vraag	Extra informatie	Ja	Nee
4.5.1	Bij Nee: kunnen de betrokkenen op de hoogte zijn van het verzamelen van de gegevens?		Ga verder met vraag 4.6.	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). Ga verder met vraag 4.6.
4.5.2	Bij Ja (op vraag 4.5): meldt u de betrokkene waarom de gegevens worden verzameld (wat u er mee gaat doen)?		Ga verder.	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).
4.5.3	Bij Ja: (op vraag 4.5): meldt u de betrokkene aan wie de gegevens worden verstrekt (daar waar dit geen wettelijke verplichting is)?		Ga verder.	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.

#	Vraag	Extra informatie	Ja	Nee
4.6	Zou de betrokkene kunnen worden verrast door de verwerking (op het moment dat hij daarover wordt geïnformeerd)?	Houd bij de beantwoording rekening met: 1. De mate waarin de betrokkene wordt geïnformeerd. 2. Hoe de 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 de gegevens vandaan komen, van de betrokkene, een interne afdeling, een andere partij, uit eigen waarneming, et cetera. 6. Wat het doel is / de 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) de gegevens aan andere partijen worden verstrekt. 9. Hoe lang de gegevens worden bewaard.	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 kunnen worden verzameld of dat de doelen van verder gebruik in lijn zijn met het doel van verzamelen.	Ga verder.

#	Vraag	Extra informatie	Ja	Nee
5	Gebruik van gegevens			
5.1	Is het gebruik van de gegevens verenigbaar (in lijn) met het doel van het verzamelen?	Houd bij de beantwoording rekening met: 1. Wat het verzameldoel is. 2. Waarvoor de gegevens worden gebruikt. 3. Welke gegevens worden verzameld. 4. Of deze gegevens bijzondere gegevens betreffen. 5. Waar de 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.	Ga verder.	Het gebruik van 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?		Ga verder met vraag 5.2.1.	Ga verder met vraag 5.3.
5.2.1	Past het doel van dit bedrijfsproces bij het oorspronkelijke doel van verzamelen?		Ga verder.	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).

#	Vraag	Extra informatie	Ja	Nee
5.3	Is de kwaliteit van de gegevens gewaarborgd, dat wil zeggen: zijn de gegevens actueel, juist en volledig?	Houd bij de beantwoording rekening met: 1. Of de gegevens worden gecontroleerd, op welke wijze en op welke aspecten de controle plaatsvindt. 2. Of de gegevens kunnen worden gecorrigeerd. 3. Welke personen toegang hebben tot de gegevens voor correctie, verwijderen et cetera van de gegevens. 4. Welke afdelingen toegang hebben tot de gegevens. 5. Hoe vaak de gegevens worden geüpdatet. 6. Wat de 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.	Ga verder.	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).
5.4	Worden op basis van de gegevens beslissingen genomen over de betrokkenen?		Ga verder met vraag 5.4.1.	Ga verder met vraag 5.5.

#	Vraag	Extra informatie	Ja	Nee
5.4.1	Bij Ja: leveren de gegevens een volledig en actueel beeld van de betrokkenen op?	Houd bij de beantwoording rekening met: 1. Wat het doel is van het verzamelen van de gegevens. 2. Welke gegevens (data elementen) worden verzameld. 3. Of de gegevens worden gecontroleerd (frequentie en aspecten). 4. Of de gegevens gecorrigeerd kunnen worden. 5. Hoe vaak de gegevens worden geüpdatet. 6. De wijze waarop de gegevens op betrouwbaarheid (actualiteit, volledigheid, juistheid) en relevantie (voor het doel) worden gecheckt. 7. Wat de gevolgen zijn van het gebruiken van onjuiste gegevens. 8. Of de gegevens gebruikt worden om profielen op te stellen. 9. Of de profielen op individueel niveau opgeslagen worden. 10. Welke profielen worden gebruikt.	Ga verder.	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.
5.5	Is sprake van koppeling, verrijking of vergelijking van gegevens uit verschillende bronnen?		U loopt een verhoogd risico dat de gegevens gebruikt worden of in de toekomst gebruikt gaan worden voor andere doeleinden dan waar zij oorspronkelijk voor zijn 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.	Ga verder.

#	Vraag	Extra informatie	Ja	Nee
5.6	Worden de gegevens breed verspreid binnen de organisatie?	Houd bij de 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.	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: • De beveiliging van gegevens. • Afhandeling van fouten. • Terugmelding van fouten. • Afstemming van begeleidingsbeleid. • Controle. Zorg voor een duidelijke gegevensbeschrijving.	Ga verder.

#	Vraag	Extra informatie	Ja	Nee
5.7	Worden de gegevens verspreid buiten de organisatie?	Houd bij de 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 (bv. papier, CD-ROM, geheugenstick, email, internet). 4. De maatregelen om ander gebruik te voorkomen.	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. • Terugmelding van fouten. • Controle. Zorg ook voor een duidelijke gegevens-beschrijving. Leg afspraken contractueel vast.	Ga verder met vraag 5.8.

#	Vraag	Extra informatie	Ja	Nee
5.7.1	Is het doorgeven van de gegevens aan partijen buiten de organisatie in lijn met de verwachtingen van het individu?	Houd bij de 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 de betrokkenen toestemming geven om de gegevens te verzamelen. 5. Wat het doel is / de doelen 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.	Ga verder.	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 compliance risico (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.	Ga verder met vraag 5.8.1.	Ga verder met vraag 5.9.

#	Vraag	Extra informatie	Ja	Nee
5.8.1	Indien profielen worden opgesteld, kan het profiel tot uitsluiting of stigmatisering leiden?	Houd bij de 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 gebruikt. 4. Of een automatische beslissing gebaseerd wordt op de gegevens. 5. Wat de logica achter deze beslissing is. 6. Partijen aan wie de gegevens worden verstrekt.	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 profilering – duidelijk is: • Op basis waarvan deze profielen 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.	Ga verder.
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 de eigen gegevens door middel van een informatiesysteem (waarbij wel moet vast staan dat gegevens alleen ingezien kunnen worden door personen die dat mogen).	Ga verder.	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).	Ga verder.	U loopt een verhoogd risico. Het bieden van een mogelijkheid tot correctie verbetert de gegevenskwaliteit. Als correcties niet doorgevoerd (kunnen) worden, verslechtert de gegevenskwaliteit en zijn de gegevens uiteindelijk (mogelijk) niet meer geschikt. U loopt hiermee ook een compliance risico (zie art. 36 Wbp).

#	Vraag	Extra informatie	Ja	Nee
5.11	Kunnen de betrokkenen hun gegevens verwijderen of daarom vragen?	Hierbij kan gedacht worden aan een reactie op verzoeken of het geven van verwijderingsmogelijkheden in de eigen gegevens door middel van een informatie-systeem (waarbij wel moet vast staan dat gegevens alleen verwijderd kunnen worden door personen die dat mogen).	Ga verder.	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 een bewaartermijn voor de gegevens vastgesteld?	Houdt hierbij rekening met het doel waarvoor de gegevens zijn verzameld en vervolgens worden verwerkt en bedrijfs-richtlijnen en wettelijk vastgestelde bewaartermijnen zoals bijvoorbeeld in de Archiefwet en belastingwetgeving.	Ga verder.	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 te 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.

#	Vraag	Extra informatie	Ja	Nee
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.	Ga verder met 6.2.1.	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 te 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. Ga verder met vraag 7.1.

#	Vraag	Extra informatie	Ja	Nee
6.2.1	Zo ja (op vraag 6.2), worden de gegevens na verstrijken van de bewaartermijn op zo'n manier vernietigd of verwijderd dat ze niet meer te benaderen en te gebruiken zijn?	Houd bij de beantwoording rekening met: 1. Of regelgeving of beleid bestaat voor de vernietiging van gegevens (bijvoorbeeld de Archiefwet). 2. Waar (welke locatie) de gegevens worden bewaard. 3. Op welk medium (papier, CD, harde schijf) de gegevens worden bewaard. 4. Of deze locatie / dit medium zijn afgeschermd voor gebruik (bijvoorbeeld het archief). 5. Welke andere redenen bestaan om de gegevens te bewaren zoals bedrijfs-historische, wettelijke, juridische redenen.	Ga verder.	Het zo kort mogelijk bewaren van gegevens heeft een aantal voordelen. • De benodigde opslag en rekencapaciteit van uw computer systemen is lager, waardoor prestaties, hersteltijden en service niveaus 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 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.
7	Beveiliging			
7.1	Is sprake van intern geformuleerd beleid over het beveiligen van informatie?	Houd bij de beantwoording rekening met: 1. Of iemand verantwoordelijk is voor dit beleid. 2. Of wordt aangesloten bij algemene beveiligingsstandaarden. 3. Of rekening wordt gehouden met het bijzondere of gevoelige karakter van gegevens. 4. Of het beveiligingsbeleid wordt getoetst.	Ga verder.	Beveiligingsbeleid is noodzakelijk voor het maken van keuzes en het effectief en efficiënt nemen van maatregelen die de gegevens beveiligen. Ga verder met vraag 8.1.
7.2	Zo ja (op vraag 7.1), is duidelijk met welke maatregelen er voor wordt gezorgd 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).	Ga verder.	U wordt geadviseerd een informatiebeveiligingsplan op te stellen met daarin maatregelen die voor een passende bescherming van de gegevens zorgen. Ga verder met vraag 8.1.

#	Vraag	Extra informatie	Ja	Nee
7.3	Zo ja, is bij het vaststellen van de maatregelen rekening gehouden met de Richtsnoeren Beveiliging van persoonsgegevens[19] die de Autoriteit persoonsgegevens heeft gepubliceerd?	De Richtsnoeren Beveiliging van persoonsgegevens leggen uit hoe de Autoriteit persoonsgegevens bij het onderzoeken en beoordelen van beveiliging van persoonsgegevens in individuele gevallen de beveiligingsnormen uit de Wbp toepast. In de Richtsnoeren wordt verwezen naar en aangesloten bij algemeen geaccepteerde beveiligingsstandaarden, zoals bijvoorbeeld ISO/IEC 27001/27002 en NEN 7510.	Ga verder.	U wordt geadviseerd om alsnog te toetsen of en zo ja in welke mate de beveiliging van de persoonsgegevens is geborgd in lijn met de eisen van de Richtsnoeren en met relevante beveiligingsstandaarden.
8	Meldplicht datalekken			
8.1	Zijn maatregelen getroffen om datalekken indien noodzakelijk te melden aan de Autoriteit persoonsgegevens en aan de getroffen personen van wie de gegevens zijn gelekt?	In de Wbp is een meldplicht opgenomen voor datalekken. Deze meldplicht houdt in dat bedrijven, overheden en andere organisaties die persoonsgegevens verwerken datalekken onder bepaalde voorwaarden moeten melden aan de Autoriteit persoonsgegevens en in bepaalde gevallen ook aan de betrokkene. De betrokkene is degene van wie persoonsgegevens zijn gelekt.	Ga verder.	Maatregelen zijn noodzakelijk om gestructureerd en adequaat invulling te geven aan de wettelijke meldplicht van datalekken. U wordt geadviseerd alsnog maatregelen te treffen. Einde vragenlijst.

[19] Richtsnoeren Beveiliging van persoonsgegevens, Autoriteit persoonsgegevens, februari 2013. https://cbpweb.nl/sites/default/files/downloads/rs/rs_2013_richtsnoeren-beveiliging-persoonsgegevens.pdf

#	Vraag	Extra informatie	Ja	Nee
8.2	Zo ja, is bij het vaststellen van de maatregelen rekening gehouden met de Richtsnoeren die de Autoriteit persoonsgegevens over de meldplicht datalekken heeft gepubliceerd[20]?	Organisaties tot wie de meldplicht datalekken zich richt moeten zelf een beredeneerde afweging maken of een concreet datalek (inclusief datalekken bij bewerkers) dat hen ter kennis komt onder het bereik van de wettelijke meldplicht valt. Doel van de richtsnoeren is om hen daarbij te ondersteunen. Deze richtsnoeren dienen tevens als uitgangspunt voor de Autoriteit persoonsgegevens bij het toepassen van handhavende maatregelen.	Einde vragenlijst.	U wordt geadviseerd om alsnog te toetsen of en zo ja in welke mate de meldplicht van datalekken is geborgd in lijn met de eisen van de Richtsnoeren. Einde vragenlijst.

[20] De meldplicht datalekken in de Wet bescherming persoonsgegevens, Autoriteit persoonsgegevens, december 2015.

A 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.

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. Verantwoordelijkheid en Verantwoording

1. **Collection Limitation Principle (limitering 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 fulfilment 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 (verantwoordelijkheid en 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 in Nederland voor vier grondwettelijke 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 het voorgaande lid zijn voorafgaande legitimatie en mededeling van het doel van het binnentreden vereist, behoudens bij de 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 privacy risico 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, alsmede het afschermen, uitwissen of vernietigen van gegevens.

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

B Mogelijke betrokkenen bij het uitvoeren van een 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/initiatiefnemers en investeerders 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 data-eigenaren.
- **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, document- en archiefbeheer en dergelijke)? Kennen we de risico's en beheersen we deze afdoende? Verantwoordelijk voor de uitvoering van het initiatief zijn veelal de directie/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 rekening gehouden met alle belanghebbenden?
- **Meedenkers / Experts:** Krijgt het onderwerp privacy en hieraan gerelateerde onderwerpen (beveiliging, document- en 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, product-ontwikkelaars 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 met name 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 Compliance Officer, de Privacy Officer en de Functionaris voor de 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.

C Wat zijn succes- en faalfactoren in het uitvoeringsproces van een PIA?

C.1 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 privacy impact dan wel privacyrisico's wijzigen) geactualiseerd (het 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 het 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.

C.2 Faalfactoren

Negatief geformuleerd zijn 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 voortdurend 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.

D PIA-rapport

Dit deel bevat een index voor een rapport en geeft u antwoord op de vraag *Welke elementen kunnen in een rapport aan de orde komen*? Ook hier geldt weer dat geen enkel rapport er hetzelfde uit zal zien. Er wordt dan ook niet een template opgelegd, maar een voorbeeld geschetst. Het voorbeeld kan worden gebruikt om de resultaten van de PIA terug te koppelen. Het rapport 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 het rapport 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 de 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.
- De weging van de impact en de risico's voor de betrokkenen en de organisatie, verbijzonderd naar de verschillende geïdentificeerde risicogebieden en de belangen voor de betrokkenen en de organisatie.
- Antwoord op de vraag: is er reden om af te zien van de gegevensverwerking, is de gegevensverwerking te rechtvaardigen? (go/no go).
- Aandachtspunten voor degene die het systeem/beleid/enzovoorts verder gaat ontwikkelen. Beschrijving van oplossingsrichtingen (bestaande uit mogelijke privacy maatregelen en compliance mechanismen).
- Naam functionaris die verantwoordelijk is voor het beheer en de evaluatie van de PIA.

In het rapport 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 al degenen die in het onderzoek zijn geraadpleegd hebben recht op het rapport.

E Waarden (persoonlijke 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 de zelfde 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).

F 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 VIP's:

- 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:

- Gevangenbewaarders
- Behandelaars in een TBS kliniek
- Medewerkers van de veiligheidsdiensten
- Geheimagenten

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

G Referentiemateriaal

PIA instrumenten

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 http://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, http://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, http://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, http://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, Office of the Privacy Commissioner for Personal Data, http://www.pcpd.org.hk/english/publications/files/eprivacy_booklet.pdf.

6. *Privacy impact assessment handbook*, New Zealand, April 2008, Privacy Commissioner, http://www.privacy.org.nz/privacy-impact-assessment-handbook/?highlight=privacy%20impact%20assessment.

7. *Conducting privacy impact assessments*, code of practice, United Kingdom, Februari 2014, Information Commissioner's Office, https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf.

8. *Privacy impact assessment – the Privacy Office official guidance*, United States, Juni 2010, The Privacy Office, https://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_guidance_june2010.pdf.

9. *E-Government Act Section 208 implementation guidance*, United States, September 2003, Office of Management and Budget, http://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.

Overige instrumenten en modellen

11. *Privacy Communicatie Model*, Ministerie van Economische Zaken, 2010, http://www.ecp-epn.nl/sites/default/files/privacymodel_0.pdf
12. *Handleiding voor verwerkers van persoonsgegevens*, Ministerie van Justitie, Den Haag, april 2002, http://www.rijksoverheid.nl/documenten-en-publicaties/brochures/2006/07/13/handleiding-wet-bescherming-persoonsgegevens.html
13. Quickscan bescherming persoonsgegevens, Autoriteit persoonsgegevens
14. *Wbp Zelfevaluatie*, Samenwerkingsverband Audit Aanpak/Werkgroep Zelfevaluatie, april 2001
15. *Raamwerk Privacy Audit, Samenwerkingsverband Audit Aanpak/Werkgroep Privacy Audit*, april 2001, https://www.privacy-audit-proof.nl/readfile.aspx?ContentID=41152&ObjectID=383730&Type=1&File=0000022882_Raamwerk_Privacyaudit.pdf
16. *Contouren voor Compliance, Handreiking bij het Raamwerk Privacy Audit, samengesteld en* gepubliceerd door de Autoriteit persoonsgegevens in samenwerking met Koninklijk Nederlands Instituut van Registeraccountants (NIVRA) en de Nederlandse Orde van Register EDP-Auditors (NOREA), 24 mei 2005, https://www.privacy-audit-proof.nl/readfile.aspx?ContentID=41152&ObjectID=383730&Type=1&File=0000022883_handreiking_rpa.pdf
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, Part I ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/DPP/CWA15499-02-2006-Feb.pdf, Part II ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/DPP/CWA15499-01-2006-Feb.pdf
18. *Self-Assessment Framework for Managers (EU Directive EC95/46)*, CWA 16112:2010, april 2010, ftp://ftp.cen.eu/CEN/Sectors/List/ICT/CWAs/CWA16112.pdf
19. NEN-ISO/IEC 27001, Informatietechnologie - Beveiligingstechnieken - Managementsystemen voor informatiebeveiliging - Eisen (ISO/IEC 27001:2013).
20. NEN-ISO/IEC 27002, Informatietechnologie - Beveiligingstechnieken - Code voor informatiebeveiliging (ISO/IEC 27002:2013).
21. Richtsnoeren beveiliging van persoonsgegevens (Autoriteit persoonsgegevens, februari 2013).

I Relatie tussen vragen en privacy principes

Deze tabel geeft inzicht in de relatie tussen vragen, onderwerpen en privacy principes. Hij is bedoeld om 'onder water' te faciliteren dat nadat de vragenlijst is ingevuld, inzicht bestaat 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'.

#	Vraag	1. limitering van het verzamelen van gegevens	2. Gegevenskwaliteit	3. Doelbinding	4. Limitering van het gebruik van gegevens	5. Beveiliging	6. Transparantie	7. Rechten van betrokkenen	8. Verantwoordelijkheid en Verantwoording
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?						x	x	x
1.3	Verwerkt uw organisatie de persoonsgegevens in opdracht en onder verantwoordelijkheid van een andere organisatie? Ofwel: Treedt uw organisatie op als bewerker?						x	x	x
1.4	Is het duidelijk wie na afloop van het project verantwoordelijk is voor het in stand houden en evalueren van de getroffen maatregelen?								x
1.5	Is het doel van de verwerking van persoonsgegevens binnen het project voldoende SMART omschreven?	x		x	x				
1.6	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.	De invoering van bestaande technologie in nieuwe context?	x	x	x	x	x	x	x	
d.	(Andere) grote verschuivingen in de werkwijze van de organisatie, de manier waarop persoonsgegevens worden verwerkt en/of de technologie die daarbij gebruikt wordt?	x	x	x	x	x	x	x	
e.	Gebruik van al verzamelde gegevens voor een nieuw doel of een nieuwe manier van gebruiken.	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		

g.	Gebruik van al verzamelde gegevens voor een nieuw doel of een nieuwe manier van gebruiken.	x	x	x	x		x	x	
1.7	Heeft u op alle bovenstaande vragen (a t/m j) nee geantwoord?								
1.8	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	x	x
1.9	Zijn er veel maatschappelijke belanghebbenden?						x	x	x
1.10	Zijn er veel partijen betrokken bij de uitvoering van het project?				x	x	x		x
1.11	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 gepseudonimiseerde 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 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

3.3	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
3.4	Is de verstrekking van de gegevens aan derde partijen in lijn met het doel waarvoor de gegevens oorspronkelijk zijn verzameld?		x	x	x				
3.5	Worden de gegevens verkocht aan derde partijen?				x		x	x	
4	Verzamelen van gegevens								
4.1	Kan de manier waarop de gegevens worden verzameld worden opgevat als privacy gevoelig?	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	
4.4	Is duidelijk of u de gegevens verzamelt op basis van toestemming (opt-in) of op basis van een andere grondslag (opt-out)	x			x		x	x	
4.4.1	Indien u toestemming aan de betrokkene vraagt (opt-in) kunnen de betrokkenen de toestemming op een later tijdstip intrekken (opt-out)?	x			x				
4.4.2	Is de impact van het intrekken van de toestemming groot voor het individu?	x			x				
4.5	Vertelt u tegen de betrokkene dat de gegevens worden verzameld?						x	x	
4.5.1	Bij Nee: Kunnen de betrokkenen op de hoogte zijn van het verzamelen van de gegevens?	x		x			x	x	
4.5.2	Bij Ja (op vraag 4.4): Vertelt u tegen de betrokkene waarom de gegevens worden verzameld (wat u er mee gaat doen)?	x		x			x	x	
4.5.3	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		
4.6	Zou de betrokkene kunnen worden verrast door de verwerking (op het moment dat hij daarover wordt geïnformeerd)?			x			x	x	
5	Gebruik van de 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?		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			
6.2.1	Zo ja, worden de gegevens na verstrijken van de bewaartermijn op zo'n 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 aan de gestelde eisen in het beveiligingsbeleid voldaan gaat worden?					x			
7.3	Zo ja, is bij het vaststellen van de maatregelen in voldoende mate rekening gehouden met de Richtsnoeren Beveiliging van persoonsgegevens die de Autoriteit persoonsgegevens heeft gepubliceerd alsmede met algemeen geaccepteerde beveiligingsstandaarden?					x			x
8	**Meldplicht datalekken**								
8.1	Zijn maatregelen getroffen om datalekken te melden aan de Autoriteit persoonsgegevens en aan de getroffen personen van wie de gegevens zijn gelekt?					x	x		x
8.2	Zo ja, is bij het vaststellen van de maatregelen in voldoende mate rekening gehouden met de Richtsnoeren die de Autoriteit persoonsgegevens over de meldplicht datalekken heeft gepubliceerd					x	x		x