Radboud Universiteit

Master's Thesis

Over het NOREA Privacy Impact Assessment

Master Informatiekunde
Radboud Universiteit Nijmegen
dinsdag 10 maart 2015

Joep Kockelkorn
s4255968

Begeleider: dr. J.E.W. Smetsers
Tweede beoordelaar: prof. dr. E. Barendsen

SAMENVATTING

Door de onthullingen van Edward Snowden en datalekken bij bekende organisaties als Adobe heeft privacy de afgelopen jaren veel media-aandacht gekregen. Wellicht staat privacy ook in de schijnwerpers omdat de huidige informatie-economie een paradox oplevert. Door gemakzucht of onwetendheid geven we toestemming om onze persoonsgegevens af te staan terwijl we de gebruiksvoorwaarden niet lezen of begrijpen. Tegelijkertijd vinden we onze privacy toch belangrijk. Om de technische ontwikkelingen bij te benen wordt er op Europees niveau aan de nieuwe Algemene Verordening Gegevensbescherming (AVG) gewerkt. Hierin wordt het relatief nieuwe concept Privacy by Design (PbD) aangekondigd. PbD impliceert dat men in het gehele ontwikkelingsproces van informatiesystemen rekening moet houden met privacy, van het vroege ontwerp tot de gerealiseerde productieomgeving. Dit manifesteert zich o.a. in het inbouwen van Privacy Enhancing Technologies (PET's); dat zijn technieken die de privacy van mensen bevorderen.

Een manier om de onderliggende principes van PbD (het *wat*) te vertalen naar toepasbare PET's is door een Privacy Impact Assessment (PIA) toe te passen (het *hoe*). Een PIA biedt een proces om in een vroege fase of voor de start van een project de impact op de privacy in te schatten en te verkleinen. Een dergelijk impact assessment wordt waarschijnlijk in de nieuwe Europese wet in bepaalde gevallen verplicht. In Nederland zijn er momenteel twee standaarden gepubliceerd om een PIA uit te voeren. In deze thesis is onderzoek gedaan naar de in 2013 gepubliceerde PIA standaard van NOREA (de IT-auditors beroepsgroep).

In het onderzoek is nagegaan in hoeverre de NOREA PIA geschikt is om privacyrequirements vast te stellen. Hiervoor zijn drie facetten van de PIA onderzocht: 1. hoe deze zich verhoudt tot de andere Nederlandse PIA, 2. welke inzichten over het NOREA PIA proces de uitvoering van een PIA bij een organisatie (Nigella IT) oplevert, en 3. in hoeverre de privacyrisico-identificerende vragenlijst valide is wat betreft compliance met de Wet bescherming persoonsgegevens (Wbp). Uit het onderzoek kan geconcludeerd worden dat de NOREA PIA in Nederland momenteel de beste standaard is om privacyrequirements vast te stellen door middel van een Privacy Impact Assessment, maar er niet voor zorgt dat alle juridische eisen van de Wbp worden meegenomen. Ook biedt de NOREA PIA documentatie geen stap-voor-stap omschrijving om privacyrisico's in maatregelen te vertalen en is de kwaliteit van de resulterende privacyrequirements dus zeer afhankelijk van de expertise van de uitvoerder(s).

VOORWOORD

Deze thesis is het resultaat van mijn afstudeeronderzoek om de Master Informatiekunde aan de Radboud Universiteit af te sluiten. Ik wil hierbij iedereen bedanken die het mij mogelijk heeft gemaakt om mijn thesis te schrijven.

Zonder mijn begeleider Sjaak Smetsers en de hulp van Erik Barendsen zouden mijn ideeën zich nooit hebben geuit in de thesis. Daarnaast wil ik het leuke bedrijf Nigella IT bedanken voor de kans om een PIA uit te voeren en de mogelijkheid om op locatie in Bocholtz mijn thesis te schrijven. De collega's wil ik bedanken voor de medewerking en daarnaast voor alle gezelligheid. Uiteraard wil ik ook mijn vriendin en ouders bedanken voor alle ondersteuning tijdens mijn studie in Nijmegen.

Veel plezier bij het lezen van mijn thesis.

Joep Kockelkorn
Bocholtz, maart '15

Inhoud

1 INLEIDING

1.1 AANLEIDING

Privacy is in Europa een fundamenteel grondrecht. Zonder privacy zou de samenleving volgens velen niet werken. Privacy staat echter over de hele wereld in de negatieve schijnwerpers vanwege grote datalekken, overheden die ons bespioneren en misschien vooral omdat we zelf toestemming geven omdat Facebook anders niet werkt. De privacywetgeving in Europa dateert alweer uit 1995 en is nodig toe aan actualisering. Enerzijds laten de technische mogelijkheden van dit digitale tijdperk de wet voelen als een dinosaurus. Dezelfde technische mogelijkheden kunnen anderzijds gebruikt worden om onze privacy preventief te beschermen voor het te laat is en de wetgeving gehandhaafd moet worden.

Technische maatregelen die onze privacy zullen bevorderen worden Privacy Enhancing Technologies (PET's) genoemd. Het meenemen van privacy in het gehele ontwikkelingsproces van informatiesystemen van het vroege ontwerp tot de gerealiseerde productieomgeving, wordt Privacy by Design (PbD) genoemd. Het vertalen van abstracte privacy-principes naar (non)functionele requirements en de integratie hiervan in het gehele ontwikkelingsproces ging in 2010 echter nog niet probleemloos (Shapiro, 2010). Daarnaast loopt PbD of 'privacy engineering' tegen het probleem aan dat privacy per definitie moeilijk te engineeren is (Gürses, 2014). Privacy is namelijk een **sociaal** probleem dat men met **techniek** probeert op te lossen. Het is onmogelijk om onze maatschappij te ontwerpen, maar onze ontworpen systemen beïnvloeden wel onze maatschappij. Dus we moeten het toch proberen.

Concepten van de aankomende Europese Algemene Verordening Gegevensbescherming (AVG) tonen aan dat privacybescherming toch stappen maakt. Privacy by Design is onderdeel geworden van de AVG en in bepaalde gevallen wordt het verplicht om een zogenaamd impact assessment uit te voeren. Een dergelijk Privacy Impact Assessment (PIA) biedt een proces om de PbD gedachte te verwerkelijken (Kroener & Wright, 2014). Een PIA identificeert op systematische wijze privacyrisico's en biedt vervolgens handvatten om deze risico's te beperken of weg te nemen. Tegenwoordig zijn er dus oplossingen die het probleem van 2010, waarin PbD nog een vaag concept wordt genoemd, proberen aan te pakken.

In rap tempo worden standaarden/modellen om een PIA uit te voeren over heel de wereld gepubliceerd. Maar wat is de stand van zaken in Nederland? In Nederland zijn momenteel twee standaarden gepubliceerd waarmee een PIA uitgevoerd kan worden: Het Toetsmodel PIA van de Rijksdienst en de PIA van de NOREA beroepsgroep voor IT-auditors. De focus van deze thesis is gelegd op de NOREA PIA. Er is ingezoomd op een aantal facetten van deze PIA.

1.2 HET ONDERZOEK

Een PIA identificeert op systematische wijze privacyrisico's. Vervolgens worden handvatten geboden om organisatorische of technische maatregelen te bedenken die de geïdentificeerde risico's beperken of wegnemen. De technische maatregelen worden vaak in de vorm van requirements neergezet.

De NOREA PIA standaard is in 2013 gepubliceerd door de NOREA: een beroepsgroep van IT-auditors. Een van de doelen van de NOREA is het bevorderen van de ontwikkeling van het vakgebied. De publicatie van de NOREA PIA draagt bij aan die ontwikkeling door in Nederland als eerste een PIA standaard voor het bedrijfsleven te bieden. De NOREA is daarmee in Nederland samen met de Rijksdienst een pionier op het gebied van PIA's. De NOREA PIA is vanwege het vooroplopende karakter nog geen beproefde methode en vraagt om een kritische blik. Dit duidt de NOREA zelf ook aan: *"Dit PIA instrument zal worden geëvalueerd en in de toekomst verder worden verbeterd. Het is bedoeld om op basis van ervaring en evaluatie als NOREA-handreiking (…) te worden vastgesteld. Tot zolang heeft het document de formele status van studierapport (…)"*. De bovenliggende vraag die wordt beantwoordt in deze thesis is daarom de volgende:

Hoofdvraag

Hoe geschikt is de NOREA PIA om privacyrequirements vast te stellen?

Om deze vraag te beantwoorden is een aantal facetten van de NOREA PIA onderzocht. Aangezien er in Nederland twee PIA standaarden zijn gepubliceerd was het voor de hand liggend om de NOREA PIA met de ander (het Toetsmodel PIA Rijksoverheid) te vergelijken. Daarnaast diende voorafgaand aan het onderzoek van deze thesis de mogelijkheid zich voor om een PIA uit te voeren (casestudy) bij Nigella IT, een IT organisatie in Bocholtz. Omdat in de NOREA PIA expliciet wordt vermeld dat de vragenlijst niet gebruikt kan worden als compliance check, is ten slotte onderzoek gedaan naar de mate waarin hij wél nagaat of er compliance is. Met andere woorden: de validiteit van de vragenlijst is onderzocht. Bovenstaande heeft geleid tot de volgende onderzoeksvragen:

Deelvragen

1. *Hoe verhoudt de NOREA PIA zich tot de andere Nederlandse PIA, het Toetsmodel PIA van de Rijksdienst?*
2. *Welke inzichten over het NOREA PIA proces levert de uitvoering van de PIA bij Nigella IT op?*
3. *In hoeverre trekt de vragenlijst van de NOREA PIA de juiste conclusie wat betreft compliance met de Wbp?*

1.3 AANPAK

De vergelijking van de NOREA PIA met het Toetsmodel PIA Rijksoverheid is gedaan op basis van criteria die zijn ontleend aan een rapport waarin acht PIA's uit zes verschillende landen worden vergeleken (Wright, Finn, & Rodrigues, 2013). Naast de criteria uit dat rapport is ook de leesbaarheid onderzocht m.b.v. een online tool. Om antwoord te geven op de eerste onderzoeksvraag is gekeken tot op welke hoogte de twee Nederlandse PIA's voldoen aan bovengenoemde criteria.

Om de tweede onderzoeksvraag te beantwoorden is de uitvoering van de NOREA PIA bij Nigella IT geëvalueerd. De uitvoering van de PIA is gedaan zoals beschreven in de NOREA PIA documentatie door middel van deskresearch en ad-hoc interviews. De focus van de evaluatie is gelegd op het proces, niet op de inhoudelijke resultaten van de uitgevoerde PIA. Tijdens de evaluatie van het proces is per fase gekeken tegen welke problemen men is aangelopen en welke aandachtspunten zijn opgevallen die in een andere situatie tot problemen zouden kunnen leiden.

Om de derde onderzoeksvraag te beantwoorden is de validiteit van de vragenlijst van de NOREA PIA in drie stappen onderzocht. De Wbp is vertaald naar een stroomschema zodat snel en overzichtelijk te zien is welk artikel van de Wbp onder welke voorwaarden van toepassing is. Vervolgens is aan de hand van dat stroomschema de vragenlijst van de NOREA PIA geanalyseerd om te beoordelen in hoeverre de Wet bescherming persoonsgegevens in de vragen wordt behandeld. Vervolgens zijn alle paden van de vragenlijst doorgelopen om te beoordelen of de vragenlijst de juiste conclusies trekt wat betreft compliance.

1.4 LEESWIJZER

De scriptie is als volgt opgebouwd. In hoofdstuk 2 wordt alle relevante theorie uiteengezet die benodigd is om deze thesis te kunnen lezen.

In hoofdstuk 3 wordt de vergelijking tussen de twee Nederlandse PIA's beschreven. Met die beschrijving wordt de **eerste onderzoeksvraag** beantwoord.

In hoofdstuk 4 wordt toegelicht welke inzichten de uitvoering van de NOREA PIA bij Nigella IT heeft opgebracht. Daarmee wordt de **tweede onderzoeksvraag** beantwoord.

Hoofdstuk 5 omschrijft validiteitsanalyse van de vragenlijst van de NOREA PIA. Aan de hand van die analyse wordt de **derde onderzoeksvraag** beantwoord.

Hoofdstuk 6 beschrijft de conclusie van de thesis. Met de antwoorden op de onderzoeksvragen wordt getracht de hoofdvraag te beantwoorden.

In hoofdstuk 7 wordt het onderzoek uitvoerig besproken en worden aanbevelingen gedaan voor eventueel vervolgonderzoek.

In voetnoten wordt verwezen naar algemene bronnen. In de tekst wordt geparafraseerd uit wetenschappelijke bronnen die uitvoerig zijn beschreven in de bibliografie.

2 THEORETISCH KADER

In dit hoofdstuk worden alle concepten uiteengezet die in de thesis gebruikt worden. Allereerst wordt het concept privacy toegelicht aan de hand van twee definities uit de literatuur. Vervolgens wordt onderbouwd hoe onze privacy in de samenleving wordt bedreigd. Hoe deze bedreiging weerstand wordt geboden wordt daarna belicht. Enerzijds wordt belicht hoe privacywetgeving onze privacy probeert te beschermen, anderzijds wordt belicht hoe privacy kan worden beschermd door technologie in onze systemen te ontwerpen en te bouwen. In de laatste paragraaf wordt het Privacy Impact Assessment verduidelijkt, wat centraal staat in deze thesis.

2.1 PRIVACY

2.1.1 SOORTEN PRIVACY

Om misverstanden te voorkomen wordt voor deze thesis het begrip privacy gedefinieerd. Dit wordt gedaan aan de hand van de definitie van Clarke en de definitie van Finn en anderen. Finn en anderen bouwen voort op de definitie van Clarke om deze te actualiseren.

De eerste definitie is de werkbare definitie van Roger Clarke (Clarke, 2006): *"Privacy is the interest that individuals have in sustaining a 'personal space', free from interference by other people and organisations"*. Deze wordt gedetailleerd uiteengezet in vier soorten privacy:

- **Privacy of the person** is 'fysieke privacy'.
  Deze vorm van privacy kan volgens Clarke worden gerelateerd aan bijvoorbeeld vrijheid van marteling en het recht op medische behandeling. Duidelijker gerelateerd zijn bloedtransfusie zonder toestemming of het verplicht moeten afstaan van biometrische gegevens zoals vingerafdrukken.

- **Privacy of personal behaviour** is 'privacy van persoonlijk gedrag'.
  Deze vorm heeft te maken met iemands gedrag, bijvoorbeeld systematisch in de gaten gehouden worden door een journalist of overheid. Dit verschilt met iemand die jou kort bekijkt als je de supermarkt inloopt. Ook de behoefte aan privacy op het toilet is een voorbeeld, aangezien niemand jouw gedrag daar kan waarnemen (hopelijk).

- **Privacy of personal communications** is 'privacy van persoonlijke communicatie'.
  Denk aan het gebruik van een alias in e-mailverkeer of het op afstand opnemen van persoonlijke gesprekken met audioapparatuur. Een recenter voorbeeld is het gebruik van end-to-end versleuteling door Whatsapp, waardoor niemand buiten de verstuurder en ontvanger het bericht kunnen lezen en aftappen dus geen zin heeft.

- **Privacy of personal data** is 'data/informatie privacy'.
  Data die iets zegt over jou als persoon (persoonsgegevens) wil je standaard niet toegankelijk maken voor anderen, vooral als deze data wordt beheerd door een ander.

Clarke schrijft dat privacy in de volksmond een combinatie is van de laatste twee soorten, **privacy of personal communications** en **privacy of personal data**. Ook wel genoemd: privacy in de informationele sfeer. Vooral deze vorm van privacy is zeer gedetailleerd uitgewerkt in de wetgeving. Clarke geeft in 2006 al aan dat er een sociale behoefte is om die uitwerking van

informationele privacy in wetgeving weer breder te trekken zodat ook de eerste twee vormen van privacy weer onder de aandacht komen.

Vanwege recente technologische ontwikkelingen zijn de vier soorten van Clarke niet meer adequaat om potentiële privacy issues te benoemen. Een voorbeeld van een dergelijke technologische ontwikkeling is: 'Whole Body Imaging' (WBI). Deze techniek maakt het mogelijk om een scan te maken van het gehele lichaam van een persoon. Die afbeelding onthult gevoelige details over de **privacy of the person** en **privacy of personal behaviour**. Echter is het niet direct het lichaam waarvan dit wordt afgeleid, maar een afbeelding van het lichaam. **Privacy of personal data** zal dus ook afbeeldingen (**image**) moeten omvatten om actueel te blijven. Daarom breidden Finn en anderen (Finn, Wright, & Friedewald, 2013) de definitie uit naar de volgende zeven soorten privacy:

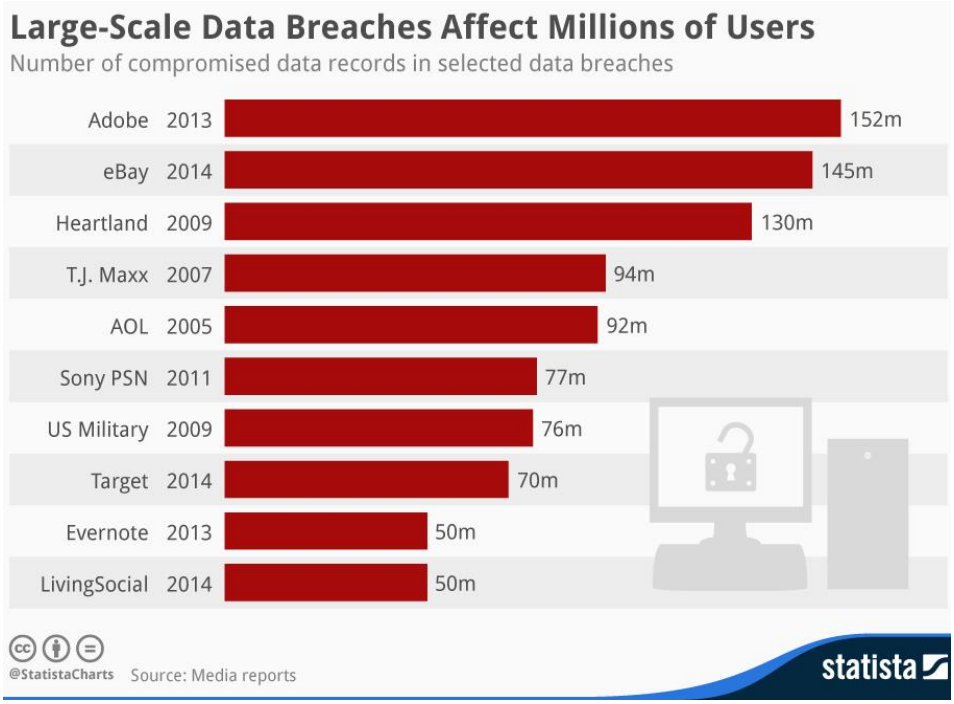
- **Privacy of the person** komt vrijwel overeen met de definitie van Clarke. Zij omschrijven het als het recht om lichaamsfunctionaliteit en lichaamseigenschappen privé te houden.
- **Privacy of behaviour and action** is een uitbreiding van de tweede soort privacy die Clarke omschrijft. Zij breiden 'privacy of behaviour' uit met *action* vanwege het feit dat niet alleen gedrag (seksuele voorkeur, politieke activiteit) maar ook de acties die daarmee te maken hebben van belang zijn.
- **Privacy of communication** komt overeen met de derde soort privacy die Clarke noemt.
- **Privacy of data and image** is een uitbreiding van de vierde soort privacy die Clarke noemt. Ze breiden de definitie uit met afbeeldingen aangezien afbeeldingen van een persoon ook iets zeggen over die persoon.
- **Privacy of thoughts and feelings** heeft te maken met de gedachten en gevoelens van mensen. Technologie zou er in de toekomst bijvoorbeeld voor kunnen zorgen dat bepaalde gevoelens en gedachten die niet worden vertaald in gedrag onthuld worden.
- **Privacy of location and space** gaat over het wel of niet onthullen van de locatie waarop of de ruimte waarin iemand zich kan bevinden. Deze vorm van privacy is steeds belangrijker geworden door de opkomst van technieken als GPS en Google Street View.
- **Privacy of association (group privacy)** heeft te maken met het recht om je te associëren met wie je wilt. Enerzijds kun je je wel of niet voegen bij politieke groeperingen maar anderzijds is het onmogelijk om je etnische afkomst te veranderen. Het is een stap verwijderd van bijvoorbeeld het recht op vrijheid van religie of van het recht op vrijheid van vereniging.

Privacy heeft tegenwoordig (vergeleken met 2006) in de volksmond alweer een andere betekenis, mede door onthullingen van Edward Snowden en bijvoorbeeld de iCloud hack van 2014. Naast **privacy of personal communications** en **privacy of personal data (and image)** worden nu ook **privacy of location and space**, **privacy of association** en **privacy of behaviour and action** geheel of gedeeltelijk bedoeld wanneer in de media over privacy wordt gesproken. De verschillende soorten privacy overlappen steeds meer met elkaar, omdat persoonsgegevens (data & image) details kunnen onthullen over de andere soorten privacy.

2.1.2 PRIVACY WORDT BEDREIGD

De onthullingen van Edward Snowden zijn het ultieme voorbeeld van de manier waarop onze privacy wordt bedreigd. Volgens een artikel van the Guardian[1] wordt ongelooflijk veel data over ons verzameld door de Amerikaanse National Security Agency (NSA). Volgens dezelfde krant is de NSA onderdeel van de 'Five Eyes' inlichtingendiensten-samenwerking tussen Australië, Canada, Nieuw-Zeeland en het Verenigd Koningrijk[2]. Het nut van die inbreuk op onze privacy is echter moeilijk te bewijzen waardoor het vertrouwen van de gewone burger ongetwijfeld is geschaad. Er is gebleken dat meer inlichtingendiensten naast de NSA (ook in Europa[3]) zich bezighouden met massatoezicht, soms zonder duidelijke democratische achterban.

Buiten de praktijken die onze overheden in hun geheime agenda erop nahouden zijn er nog andere activiteiten die onze privacy bedreigen. In onderstaande afbeelding zijn meerdere grote datalekken weergegeven die zijn veroorzaakt door hackers. Die data kunnen gevoelige persoonsgegevens zijn waarmee kwaadwillenden inbreuk op jouw privacy kunnen maken.



FIGUUR 1: RECENTE DATALEKKEN[4]

Tegen de privacy ophef wordt wel eens het argument gebruikt: "Ik heb toch niets te verbergen?". Deze gedachtegang is verkeerd, iedereen heeft wel iets te verbergen. Denk bijvoorbeeld aan creditcardgegevens die gebruikt kunnen worden om fraude te plegen. In 2014 was in de V.S. de grootste angst van burgers: gestolen creditcardgegevens bij een winkel waar je net iets hebt gekocht[5]. De angst dat je computer of smartphone gehackt wordt komt op de tweede plaats.

---

[1] Edward Snowden and the NSA files – timeline d.d. 21 augustus 2013
[2] Snowden spyware revelations: unmask the five-eyed monster d.d. 26 november 2013
[3] GCHQ and European spy agencies worked together on mass surveillance d.d. 1 november 2013
[4] Large-Scale Data Breaches Affect Millions of Users d.d. 6 augustus 2014
[5] Hacking Tops List of Crimes Americans Worry About Most d.d. 27 oktober 2014

Onze privacy wordt ook steeds meer bedreigd door de opkomst van de informatie-gedreven economie. Door gebruik te maken van een 'gratis' dienst als Facebook worden onze persoonsgegevens verkocht aan advertentiebedrijven. Adverteerders kunnen dan vervolgens gerichte reclame aanbieden op Facebook. Elk activiteit die je op Facebook uitvoert heeft dus invloed op je privacy. Daarnaast kan Facebook veel meer weten dan jij hen geeft. Het is namelijk gebleken dat op basis van alle 'likes' van een persoon redelijk accurate voorspellingen gedaan kunnen worden van bepaalde attributen als seksuele geaardheid, politieke gezindheid of etnische afkomst (Kosinski, Stillwell, & Graepel, 2013).

Tegenwoordig leidt deze constructie tot een paradox. Enerzijds klagen we dat Facebook steeds meer aan de haal gaat met onze privacy terwijl we daar zelf toestemming voor geven door akkoord te gaan met de gebruikersvoorwaarden. Maar wie leest daadwerkelijk de gebruiksvoorwaarden en permissies die getoond worden bij het installeren van een nieuwe app? Er is onderzocht hoeveel mensen bewust aandacht besteden aan de permissies die een app toont als je hem gaat installeren (Felt et al., 2012). Daaruit is gebleken dat 83% geen aandacht besteed aan de permissies en maar 3% begrijpt wat er met de permissies bedoeld wordt. Men kiest dus vaak onbewust ervoor om een deel van hun privacy op te geven.

Toch zijn er de afgelopen jaren ook goede ontwikkelingen geweest op het gebied van privacy bijvoorbeeld de plotselinge opkomst van Snapchat. De belofte dat communicatie alleen tijdelijk bewaard wordt, bleek niet te worden nagekomen. Maar de massale omarming van het idee om communicatie maar tijdelijk op te slaan is een stap voorwaarts (Landau, 2014). Daarnaast zijn sinds de onthullingen van Snowden maatregelen genomen om de inbreuk op onze privacy te verkleinen zoals de introductie van het Europese 'recht om te vergeten worden'. Dit recht zorgt ervoor dat mensen zoekmachines kunnen verzoeken om irrelevante informatie te vergeten. Wat datalekken betreft is er ook positief nieuws: het is gebleken dat 90% van de datalekken van de eerste helft van 2014 voorkomen had kunnen worden[6]. Slechts 40% van die lekken waren veroorzaakt door externe hackers.

Het gebruik van techniek is niet altijd afdoende om privacy te beschermen, non-technische maatregelen zijn net zo belangrijk. Er dient vastgelegd te zijn wat er mag en wanneer de privacy van een persoon wordt aangetast. Vandaar dat privacy enerzijds beschermd wordt in wetgeving. Het opleggen van sancties en straffen gebeurt echter pas nadat de privacy van een persoon is aangetast: reactief, wanneer het te laat is. Anderzijds kunnen preventief op eigen initiatief technologische maatregelen genomen worden om je privacy te waarborgen zoals de Blackphone[7] of het gebruik van encryptie. Voor overheden en het bedrijfsleven is het belangrijk dat zij ook preventieve maatregelen nemen om hun klanten privacy-vriendelijke producten/diensten aan te bieden. Hoe privacy in ICT wordt verwerkt en beschermd wordt uitgelegd in paragraaf 2.3. In het volgende hoofdstuk wordt uitgelegd hoe privacy reactief en preventief wordt beschermd in wetgeving.

[6] Over 90% of Data Breaches in 2014 Could Have Been Prevented d.d. 21 januari 2015
[7] https://blackphone.ch/phone/ d.d. 2014

2.2 WETGEVING

Om te voorkomen dat de privacy van een persoon wordt geschaad zal tegen inbreuk moeten worden opgetreden. Om het begrip privacy werkbaar te maken zal ergens opgeschreven moeten worden waar de grenzen liggen en wat de sancties zijn bij een overtreding. Daarom wordt privacy gereguleerd in het wettenstelsel.

Sinds 1970 zijn er pogingen gedaan om principes op te stellen voor een wereldwijde/supranationale interpretatie van privacy in het bijzonder gegevensbescherming. De twee meest toonaangevende zijn de *Fair Information Practice Principles (FIPP's)* uit 1973 van de United States Federal State Commission en de *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* uit 1980 (herzien in 2013[8]). De tweede (OECD richtlijn) wordt kort toegelicht in de volgende paragraaf. Deze dient als basis voor de huidige Europese gegevensbescherming wetgeving.

2.2.1 OECD RICHTLIJN

De Organisatie voor Economische Samenwerking en Ontwikkeling (Engelse afkorting: OECD) bespreekt, bestudeert, en coördineert sociaal en economisch beleid. Het is van oorsprong een Europese organisatie, maar bestaat tegenwoordig ook uit niet-Europese landen, in totaal 34. Een van haar doelen is het verbeteren van de internationale samenwerking tussen autoriteiten op het gebied van gegevensbescherming. Haar oorspronkelijke richtlijn heeft als fundament gediend voor de actuele Europese richtlijn voor gegevensbescherming[9]. De volgende principes vormen de kern van de herziende OECD richtlijn:

1. Collection Limitation Principle:
Persoonsgegevens zullen gelimiteerd verzameld moeten worden, op gepaste wijze voor een gerechtvaardigd doel, en waar mogelijk met toestemming of wetenschap van de betreffende persoon.

2. Data Quality Principle:
Persoonsgegevens moeten relevant zijn voor de doelen waar ze voor verzameld zijn, en voor zover nodig voor die doelen, dienen ze nauwkeurig, compleet en actueel te zijn.

3. Purpose Specification Principle:
De doelen waarvoor de persoonsgegevens worden verzameld dienen niet later vastgesteld te worden dan het verzamelmoment, en verder gebruik zal gelimiteerd zijn tot volbrenging van die doelen of doelen die niet in strijd zijn met de oorspronkelijke doelen. Iedere keer als het doel van verwerking wijzigt, dient het te worden vastgelegd.

[8] OECD work on privacy d.d. juli 2013
[9] Richtlijn 95/46/EG d.d. 24 oktober 1995

4. Use Limitation Principle:
Persoonsgegevens worden niet onthuld of bekend gemaakt voor andere doelen dan die vastgesteld bij principe 3, behalve: met toestemming van de betreffende persoon, of door bevoegdheid van de wet.

5. Security Safeguards Principle:
Persoonsgegevens moeten worden beschermd door passende beveiligingsmaatregelen tegen risico's zoals verlies, onbevoegde toegang, misbruik, wijziging of onthulling/bekendmaking van gegevens.

6. Openness Principle:
Er dient algemeen beleid te zijn over ontwikkelingen, de praktijk en beleidsstukken betreffende persoonsgegevens. Middelen dienen beschikbaar te zijn om het bestaan, de oorsprong, de doelen, het gebruik van persoonsgegevens te achterhalen, evenals de identiteit en gebruikelijke verblijfplaats van de gegevensbeheerder.

7. Individual Participation Principle:
Een individu moet het recht hebben:

a) om van een gegevensbeheerder of op een andere manier, bevestiging te ontvangen of er persoonsgegevens betreffende hem worden verwerkt;
b) om persoonsgegevens betreffende hem, binnen een redelijke tijd, eventueel tegen niet-buitensporige vergoeding, op een redelijke manier, op gemakkelijk begrijpelijke wijze in te zien;
c) om een reden voor afwijzing van het aangevraagde onder punt a) en b), en om een dergelijke afwijzing in twijfel te trekken;
d) om persoonsgegevens betreffende hem in twijfel te trekken, en als deze niet kloppen, om de gegevens te laten verwijderen, rectificeren, aanvullen of wijzigen.

8. Accountability Principle:
Een gegevensbeheerder is verantwoordelijk om bovenstaande principes en de maatregelen die daar uitvoering aan geven, na te leven.

2.2.2 EUROPESE WETGEVING

Op de hierboven omschreven principes is de eerder genoemde Europese gegevensbescherming richtlijn gebaseerd[10]. Alle Europese landen hebben deze richtlijn verwerkt in hun nationale wetgeving. In bredere zin is privacy een fundamenteel recht dat is opgenomen in het Europees Verdrag voor de rechten van de Mens (EVRM), artikel 8. In Europese landen die deelnemen aan dit verdrag is dit fundamentele recht verwerkt in de nationale wetgeving.

Op Europees niveau is nieuwe wetgeving over gegevensbescherming in aantocht: de Algemene Verordening Gegevensbescherming (Data Protection Regulation). Waarschijnlijk wordt deze pas in 2016 aangenomen en hoeven lidstaten pas vanaf 2018 eraan te voldoen. De belangrijkste veranderingen zijn:

- Verhoogde boetes (tot maximaal 1.000.000 of 5% van de wereldwijze jaaromzet)
- Verplicht aanstellen van een Functionaris voor de Gegevensbescherming

[10] Richtlijn 95/46/EG d.d. 24 oktober 1995

- Meldplicht datalekken
- Documentatieplicht (ter vervanging van de meldplicht bij het CBP)
- Bewerkers van persoonsgegevens krijgen meer verantwoordelijkheid
- Invulling van het eerder genoemde 'recht om te vergeten worden'
- Gegevensuitwisseling met andere landen wordt strenger
- In veel gevallen moet een *"Data Protection Impact Assessment"* uitgevoerd worden
- Bij een nieuwe of veranderde gegevensverwerking moet aandacht besteed worden aan *"Privacy by Design"* en *"Privacy by Default"*

Over de laatste twee punten wordt meer uitleg gegeven in paragraaf 2.3.2. Hoe de huidige gegevensbescherming richtlijn is geïmplementeerd in de Nederlandse wetgeving wordt in de volgende paragraaf omschreven.

2.2.3 Nederlandse privacy wetgeving

In onderstaande tabel is gedeeltelijk weergegeven hoe de Europese wetgeving is vertaald in het Nederlandse rechtssysteem.

Europese Unie wetgeving	Overeenkomende Nederlandse wet
Artikel 8 over privacy van het Europese Verdrag voor de Rechten van de Mens (EVRM)	Artikel 10 t/m 13 van de Grondwet
Richtlijn 95/46/EC	Wet bescherming persoonsgegevens
Conventie ETS no. 108	Wet bescherming persoonsgegevens
Richtlijn 2009/136/EC, over cookies	Telecommunicatiewet
e-Privacy Richtlijn, 2002/58/EC	Telecommunicatiewet

2.2.4 Operationaliseren van wetgeving

De hierboven genoemde wetten omschrijven gedeeltelijk hoe er in Nederland met persoonsgegevens omgegaan moet worden. De eisen die gesteld worden aan gegevensverwerkingen zijn zelden heel concreet en specifiek omschreven. Meestal zijn deze zo omschreven dat ze op meerdere situaties van toepassing zijn en in de toekomst ook nog doeltreffend zijn. Wat het betekent om te voldoen aan de wet (compliance) is meestal verre van duidelijk en is voor een organisatie een kwestie van afwegingen en beslissingen maken. Als er sprake is van een datalek van persoonsgegevens kan de privacy van een persoon worden aangetast maar of daadwerkelijk de wet wordt overtreden is vaak niet kristalhelder. Vandaar dat een zorgvuldige beoordeling van een autoriteit benodigd is (bijvoorbeeld een rechtbank) waarbij alle omstandigheden, wetten en andere wetsuitspraken tegen elkaar worden afgewogen.

Om deze balanceeruitdaging in de praktijk iets gemakkelijker te maken heeft de Nederlandse autoriteit van gegevensbescherming, het College Bescherming Persoonsgegevens (CBP), richtsnoeren gepubliceerd[11]. Een van de richtsnoeren is gericht op gegevensbeveiliging. De richtsnoeren geven het CBP enerzijds houvast wanneer een gegevensverwerking op compliance beoordeeld dient te worden. Anderzijds kunnen organisaties de richtsnoeren gebruiken om de wetgeving te concretiseren om te beslissen welke maatregelen zij dienen te nemen.

[11] Richtsnoeren van het CBP d.d. 2007-2013

De sancties en boetes die in privacy wetgeving zijn verwerkt zijn reactieve maatregelen. Ze treden in werking ná overtreding van de wet. De eisen die wetgeving stelt aan een gegevensverwerking zijn preventieve maatregelen. Ze zijn dwingend opgesteld zodat de betreffende organisatie/persoon zich houdt aan de wet. Een voorbeeld van een preventieve maatregel is het zich moeten schikken naar de richtsnoeren van het CBP.

In het meest recente richtsnoer[12] wordt verwezen naar het concept *privacy by design*, dat betekent dat *"de bescherming van persoonsgegevens en de borging van de rechten van de betrokkenen vanaf het allereerste begin in de informatiesystemen wordt ingebouwd"*. Het principe valt buiten de scope van het richtsnoer terwijl het in deze thesis centraal staat. Privacy by Design wordt in het volgende hoofdstuk uitgelegd.

2.3 Privacy door technologie

Een taak van de overheid is het beschermen van de privacy van haar burgers door naast de reactieve sancties en boetes ook preventieve maatregelen af te dwingen in wetgeving. Vanwege het feit dat iedereen altijd met elkaar verbonden wilt zijn via het internet en sociale media en het feit dat de samenleving steeds afhankelijker wordt van technologie, moeten technische maatregelen ongetwijfeld onderdeel zijn van die preventieve maatregelen. In het bedrijfsleven en de academische wereld worden die technieken al sinds 1995 ontwikkeld onder de naam 'Privacy Enhancing Technologies'.

2.3.1 Privacy Enhancing Technologies

De term wordt waarschijnlijk voor het eerst genoemd in 1995 in een rapport dat het resultaat is van een samenwerkingsverband tussen de Registratiekamer (destijds de Nederlandse privacy autoriteit) en de privacy autoriteit van Ontario, Canada (Hes & Borking, 1995). Met Privacy Enhancing Technologies (PET's) worden bedoeld: technologieën die de privacy van een persoon waarborgen door de hoeveelheid verwerkte persoonsgegevens (identificerende gegevens) te doen afnemen of te voorkomen dat deze wordt verwerkt. De anonimiteit en dus de privacy van een persoon zal hierdoor toenemen.

Voorbeelden van PET's uit het rapport zijn de digitale handtekening, het gebruik van pseudoniemen en trusted third parties. De digitale (blinde) handtekening kan onder andere gebruikt worden om documenten te ondertekenen zonder informatie vrij te geven over de identiteit van de persoon. Pseudonimisering is het vervangen van de identificerende gegevens door een pseudoniem waardoor gegevens niet meer te herleiden zijn tot de persoon. Een trusted third party kan gebruikt worden om de koppeling tussen het pseudoniem en de identificerende gegevens van een persoon te bewaren. Beide partijen vertrouwen die derde partij erop dat hij zorgvuldig met de gegevens omgaat. Een voorbeeld van een toegepaste PET is de IRMA kaart, gebaseerd op o.a. de PET attribute based credentials. De IRMA kaart is een smartcard die alleen de attributen laat zien die absoluut benodigd zijn[13]. Als iemand drank wil kopen in een slijterij wordt aan de hand van het attribuut 'leeftijd' berekend of de leeftijd hoger is dan 18 jaar. De

[12] Richtsnoeren beveiliging persoonsgegevens d.d. februari 2013
[13] I Reveal My Attributes d.d. 2012

leeftijd wordt niet getoond aan de winkelier. Dat is namelijk onnodig voor de controle maar zeker voor je privacy.

Door PET's te gebruiken wordt de privacy van mensen dus preventief beschermd. Als een informatiesysteem al is gebouwd en in gebruik is genomen is het vaak echter (te) kostbaar om PET's alsnog in te passen. Het is dus van belang om deze bij het bouwen van een informatiesysteem en dus in een nog eerder stadium (bij het ontwerpen) al mee te nemen. Hoe eerder, hoe beter. Deze gedachtegang wordt in de volgende paragraaf toegelicht.

2.3.2 Privacy by Design

In het eerder genoemde rapport waarin de term PET wordt genoemd wordt gezegd dat bij het ontwerpen van het systeem overwogen moet worden of de identiteit van personen benodigd is voor de werking van het systeem (Hes & Borking, 1995). Het aantal persoonsgegevens dat benodigd is voor een werkend systeem moet **van tevoren/vooraf** worden beperkt tot het absolute minimum. De gedachte om met rekening te houden met privacy voordat persoonsgegevens worden verzameld blijkt jaren later te worden gevangen in het concept Privacy by Design (PbD). PbD is dus: het meenemen van privacy in het gehele ontwikkelingsproces van informatiesystemen, van het vroege ontwerp tot de gerealiseerde productieomgeving.

Hoewel PbD vaak als synoniem wordt gebruikt van PET's, is PbD juist de gedachte achter PET's (Koops & Leenes, 2013). Volgens hen is de absolute kampioen van PbD Ann Cavoukian, een van de aandragers van het rapport over PET's uit 1995 en voormalig (in 2014) 'Information and Privacy Commissioner' van Ontario, Canada. PbD is vooral bekend geworden door de 7 fundamentele principes (Cavoukian, 2009). De principes die Cavoukian noemt zijn de volgende:

1. **Proactief** i.p.v. reactief; **Preventief** i.p.v. herstellend:
   Anticipeer op en voorkom inbreuken op iemands privacy voordat deze feitelijk plaatsvinden.

2. Privacy als **standaard** (by default):
   Ook als het individu zelf niets onderneemt zal toch zijn privacy zijn gewaarborgd.

3. Privacy **geïntegreerd** in het ontwerp:
   Privacy is geïntegreerd in het systeem, zonder aan functionaliteit te hoeven inleveren.

4. Volledige functionaliteit – **Positive-sum** i.p.v. Zero-sum:
   PbD vermijdt valse dichotomieën zoals privacy tegenover veiligheid door te demonstreren dat een combinatie van beiden wel degelijk mogelijk is.

5. Veiligheid van begin tot eind – **Bescherming tijdens de volledige levenscyclus**:
   Dit geeft de garantie dat alle gegevens op een veilige wijze zijn verkregen en op een tijdige en veilige wijze zijn vernietigd aan het eind van het proces.

6. **Zichtbaarheid** en **transparantie** – Houd het **open**:
   De technische componenten en het operationeel handelen blijven zichtbaar en transparant voor zowel de gebruikers als de dienstverleners. Onthoud: vertrouwen is de basis, maar nooit zonder controle.

7. **Respect** voor de privacy – laat de gebruiker **centraal** staan:
   PbD heeft boven alles architecten en exploitanten nodig die de belangen van het individu als hoogste prioriteit beschouwen door maatregelen in te stellen zoals krachtige privacy instellingen, passende informatievoorziening en gebruikersvriendelijke opties.

Rond dezelfde tijd als de publicatie van Cavoukian publiceren Spiekermann en Cranor (2009) hun denkwijze over het inbouwen van privacy. Zij noemen dit privacy engineering. In essentie komt het achterliggende idee van privacy engineering overeen met PbD. In privacy engineering staat het onderscheid tussen 'privacy-by-policy' en 'privacy-by-architecture' centraal, wat grofweg overeen komt met het onderscheid tussen respectievelijk privacybescherming in wetgeving en privacybescherming d.m.v. techniek. Deze andere invalshoek getuigt ervan dat het concept PbD in 2009 nog in de kinderschoenen staat. Volgens Gürses zou PbD bijvoorbeeld ook het dataminimalisatie principe moeten omvatten waar Cavoukian dit niet expliciet heeft opgenomen in haar principes (Gürses, Troncoso, & Diaz, 2011). Dataminimalisatie houdt in dat men altijd zo min mogelijk persoonsgegevens dient te verzamelen voor de werking van een systeem. Dataminimalisatie wordt gezien als ultieme vereiste om de privacy van personen te waarborgen en dient dus bij systeemontwerpers hoog in het vaandel te staan.

Systeemontwerpers hebben volgens Gürses (2014) echter te weinig verstand van privacy om privacyrequirements in PET's te vertalen. Dit is voornamelijk zo omdat privacy tegenwoordig een **sociaal** probleem is. Net als veiligheid, gebruiksvriendelijkheid en betrouwbaarheid, is privacy een ideaal dat is gedocumenteerd in wettelijke en sociale concepten. PbD probeert dit op te lossen met **techniek**. Het is onmogelijk om onze maatschappij te ontwerpen maar onze ontworpen systemen beïnvloeden wel onze maatschappij. Dus we moeten het toch proberen.

Het toenemende belang van privacy wordt door beleidsmakers over de hele wereld erkend. PET's worden bijvoorbeeld in 2007 door de Europese Commissie gepromoot[14]. Daarnaast wordt PbD in 2010[15], en in 2012[16] als essentieel onderdeel van fundamentele privacybescherming bestempeld. Dit heeft ertoe geleidt dat 'data protection by design and default' in de (eerder genoemde) aankomende Algemene Verordening Gegevensbescherming is opgenomen.

Er is echter nog steeds kritiek op PbD. Volgens van Rest en anderen (2014) is PbD een vaag concept, dat niet gemakkelijk toepasbaar is. Wegens een gebrek aan handvatten voor het vertalen van het concept PbD naar innovatieve PET's die privacy risico's bestrijden breiden zij de definitie van PbD uit naar: *"het toepassen van gevestigde privacy/gegevensbescherming patronen voor het passende doel, in het passende domein"*. Patronen zijn PET's beschreven op een abstract(er) niveau, toepasbaar op een specifiek probleem.

[14] Promoting data protection by privacy-enhancing technologies d.d. 14 mei 2007
[15] Privacy by Design Resolution d.d. 29 oktober 2010
[16] Protecting Consumer Privacy in an Era of Rapid Change d.d. maart 2012

Hiervoor dienen echter wel die privacy problemen, oftewel risico's, in kaart te zijn gebracht. Voor het in kaart brengen van de privacyrisico's van een project kan een Privacy Impact Assessment (PIA) worden uitgevoerd. Het uitvoeren van een PIA wordt door Kroener en Wright gezien als het sleutelconcept van PbD (Kroener & Wright, 2014). Het biedt een proces voor het *hoe* van PbD. Het assessment kan gedaan worden op verschillende momenten in het software engineering proces. Hoe eerder hoe beter. PIA's zijn de focus van deze thesis en worden in de volgende paragraaf omschreven.

2.3.3 Privacy Impact Assessment

Volgens Clarke is het concept van een PIA tussen 1995 en 2005 ontstaan en volwassen geworden. Het idee achter impact assessments is waarschijnlijk zelfs eerder ontstaan bijvoorbeeld in 1970: Men had de behoefte om voor de start van een groot project te schatten hoe groot de impact zou zijn op het milieu. Sinds midden 90'er jaren wordt met de term Privacy Impact Assessment bedoeld: een proces om in een vroege fase of voor de start van een project de impact op de privacy niet alleen te schatten maar ook te verkleinen (Clarke, 2009).

In Europa is het de gegevensbescherming autoriteit uit het Verenigd Koninkrijk (Information Commissioner's Office) die in 2007 als eerste een richtlijn publiceert om een PIA uit te voeren (Wright, 2012). Andere landen volgden, bijvoorbeeld Ierland in 2010. Uit België komt in 2011 de LINDDUN methode. Deze noemt zichzelf geen PIA maar een 'privacybedreiging analyseraamwerk' oftewel een methode voor privacy risico analyse (Deng, Wuyts, Scandariato, Preneel, & Joosen, 2011). Het idee is hetzelfde: Risico's of bedreigingen voor privacy identificeren en deze vervolgens proberen te bestrijden of compleet weg te nemen. In de LINDDUN methode worden de risico's bestreden door middel van het toepassen van PET's. Het identificeren wordt in de LINDDUN methode middels het opstellen van misuse-cases gedaan waar dit in een PIA vaak met een op nationale wetgeving gebaseerde stap-voor-stap vragenlijst wordt gedaan. Een recent ontwerp voor een PIA methode door Oetzel en Spiekermann (2014) doet juist weer afstand van een dergelijke vragenlijst georiënteerde methode maar zij benadrukken wel dat een PIA het sleutelconcept is van PbD. Hoewel het belang van PIA's hiermee is aangeduid, moge ook duidelijk zijn dat PIA's misschien nog niet zo volwassen zijn als Clarke in 2009 dacht.

In 2013 hebben Wright en anderen onderzoek gedaan naar acht PIA's uit zes verschillende landen op grond van 18 criteria waarvan zij vinden dat een 'goede' PIA eraan moet voldoen. Volgens deze criteria zou een 'goede' PIA standaard:

- aangeven dat het een proces is;
- een stel vragen bevatten om privacyrisico's te ontdekken;
- alle soorten privacy behandelen;
- aangeven dat het een vorm van risicomanagement is;
- privacyrisico's identificeren;
- mogelijke strategieën identificeren om de risico's te beperken;
- aangeven welke voordelen de uitvoering van een PIA heeft;
- aanbevelen om externe stakeholders te consulteren;
- aanmoedigen om de PIA te publiceren;
- vaststellen of uitvoering van de PIA benodigd is;
- voorzien in een structuur voor een PIA verslag/rapport;

- ook uitgevoerd kunnen worden op wetgeving of beleid;
- aangeven dat het PIA proces dynamisch is (constant corrigerend);
- expliciet aangeven dat een PIA meer is dan een compliance check;
- aangeven dat het rapport beoordeeld wordt door een derde, onafhankelijke partij;
- verplicht worden door de wet of gepaard moeten gaan met afstemming van het budget;
- ondertekend moeten worden door het senior management (ter verantwoording).

In de aankomende Algemene Verordening Gegevensbescherming wordt het in bepaalde gevallen verplicht een 'data protection impact assessment' uit te voeren. Dit is grofweg hetzelfde als een PIA. Spiekermann (2012) benadrukt dat het belangrijk is dat toepassing van PIA's verplicht moet worden vanwege de impuls die het PbD kan geven en het praktische hulpmiddel dat het kan zijn om compliance te bereiken. Een goed moment om te kijken naar de stand van zaken in Nederland. In Nederland zijn er op dit moment twee richtlijnen voor PIA's gepubliceerd:

Toetsmodel Privacy Impact Assessment Rijksdienst
Het toetsmodel vormt een nadere invulling en uitvoering van het regeerakkoord van 2012, de motie Franken van 17 mei 2011, de toezegging tot doorontwikkelen van een PIA en de in november 2011 aangekondigde maatregelen in het kader van iStrategie om aandacht voor privacy te versterken bij grote ICT-projecten. Het toetsmodel is verstrekt aan de Tweede Kamer op 21 juni 2013, en gepubliceerd op 1 oktober 2013[17]. Het toetsmodel wordt vanaf 1 september 2013 standaard toegepast (d.w.z. is verplicht binnen de Rijksdienst) bij het ontwikkelen van nieuwe wetgeving en beleid waarmee de bouw van nieuwe ICT-systemen of de aanleg van grote databestanden wordt voorzien[18].

Privacy Impact Assessment (NOREA)
De beroepsorganisatie van IT-auditors in Nederland (NOREA) heeft op 16 mei 2013 haar Privacy Impact Assessment gepresenteerd[19]. De NOREA is er van overtuigd dat zowel de publieke sector als de private sector baat kan hebben bij de uitvoering van een Privacy Impact Assessment. Het voorwoord van deze PIA is geschreven door de indiener van de bovengenoemde motie, prof. mr. Hans Franken, lid van de Eerste Kamer. Uit het voorwoord blijkt dat deze PIA ook is bedoeld voor toepassing in de particuliere sector waar het toetsmodel specifiek is geschreven voor toepassing binnen de Rijksdienst.

[17] Publicatie Toetsmodel Privacy Impact Assessment Rijksdienst d.d. 1 oktober 2013
[18] Kamerstuk over het Toetsmodel PIA Rijksdienst d.d. 19 juli 2013
[19] Handreiking Privacy Impact Assessment gepresenteerd d.d. 16 mei 2013

De NOREA PIA is de focus van deze thesis. De NOREA PIA bestaat inhoudelijk uit de volgende delen:

1. Deel 1: Introductie over het instrument PIA.
   Een algemene introductie waarin het doel, de achtergrond, het belang, en de verdere context van de PIA uiteen worden gezet. Ook wordt het begrip privacy gedefinieerd.
2. Deel 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 het stappenplan worden gevarieerd. Er wordt antwoord gegeven op vragen als: *"Uit welke stappen bestaat het PIA proces?"* en *"Wie kan ik betrekken bij de PIA?"*.
3. Deel 3: De PIA vragenlijst.
   Na het doorlopen van dit derde deel heeft men antwoorden op vragen als: *"Wat zijn de privacyrisico's van de verwerking van persoonsgegevens voor de betrokkenen en voor mijn organisatie?"* en *"Waar liggen deze risico's?"*. Dit derde deel bevat een vragenlijst op basis waarvan een aantal privacy relevante aspecten van het project én de privacyimpact van een project inzichtelijk worden.
4. Deel 4: De bijlagen.
   Deel 4 bevat vooral randzaken zoals een verklaring van de gebruikte begrippen en de succes- en faalfactoren voor het uitvoeren van een PIA.

In deze scriptie wordt op drie manieren onderzoek gedaan naar de NOREA PIA. De NOREA PIA wordt vergeleken met het toetsmodel voor de Rijksdienst, te vinden in H3. Vervolgens wordt beschreven tot welke inzichten de toepassing van de NOREA bij Nigella IT heeft geleid in H4. Ten slotte is gekeken in hoeverre de Nederlandse wetgeving voor gegevensbescherming is verwerkt in de vragenlijst van de NOREA PIA, te vinden in H5.

3 PIA VERGELIJKING

De eerste manier waarop onderzoek is gedaan naar de NOREA PIA is door deze te vergelijken met het Toetsmodel PIA Rijksdienst, het model voor een Privacy Impact Assessment van de Rijksoverheid. Daarmee wordt antwoord gegeven op de volgende onderzoeksvraag:

> *Hoe verhoudt de NOREA PIA zich tot de andere Nederlandse PIA, het Toetsmodel PIA van de Rijksdienst?*

De PIA's zullen op een aantal punten worden vergeleken. Deze worden hieronder omschreven.

3.1 AANPAK PIA VERGELIJKING

Recentelijk zijn acht PIA's uit zes verschillende landen onderzocht op een aantal criteria waaraan de ultieme PIA zou moeten voldoen (Wright et al., 2013). De 18 criteria zijn als uitgangspunt genomen om de twee verschillende Nederlandse PIA's te kunnen vergelijken. De Nederlandse PIA's zijn geen onderdeel geweest van bovengenoemd onderzoek. Om de leesbaarheid van de vergelijking te bevorderen zijn voor deze thesis de criteria van de oorspronkelijke vergelijking per onderwerp gecategoriseerd. De categorieën kunnen elkaar overlappen en sluiten elkaar niet uit. In de vergelijking van deze thesis worden de volgende categorieën (en criteria) gehanteerd:

Belangrijke functies van een PIA

Een PIA:

1. Bevat een stel vragen om privacyrisico's te ontdekken (meestal gerelateerd aan privacy principes);
2. Identificeert privacyrisico's;
3. Identificeert mogelijke strategieën om de risico's te beperken;

Privacy definitie

Een PIA:

4. Geeft expliciet aan dat een PIA meer is dan een compliance check (d.w.z. meer privacyaspecten behandeld dan alleen gegevensbescherming);
5. Behandelt alle soorten privacy (hiervoor wordt de definitie van Finn, Wright en Friedewald gebruikt);

Verantwoording en expertise

Een PIA:

6. Beveelt consultatie met externe stakeholder(s) aan;
7. Moedigt aan om de PIA te publiceren;
8. Geeft aan dat het PIA rapport beoordeeld moet worden door een derde, onafhankelijke partij;
9. Wordt verplicht door wetgeving/beleid of gaat gepaard met afstemming van het budget;
10. Moet ondertekend worden door het senior management (om verantwoording te bewerkstelligen);

Proces en structuur

Een PIA:

11. Geeft aan dat het een proces is;
12. Geeft aan dat het als een vorm van risicobeheer wordt bedoeld;

13. Voorziet in een structuur voor een PIA verslag/rapport;
14. Geeft aan dat het proces dynamisch is (constant corrigerend gedurende het gehele proces);

Randzaken

Een PIA:

15. Is gericht op het bedrijfsleven én de overheid;
16. Geeft aan welke voordelen de uitvoering heeft;
17. Stelt vast of uitvoering benodigd is;
18. Kan ook uitgevoerd worden op wetgeving of beleid;
19. Is leesbaar. In hoeverre zijn de teksten begrijpelijk? (zelf toegevoegd criterium)

3.2 VERGELIJKING

In paragraaf 3.2 wordt voor alle criteria beschreven hoe de twee PIA's scoren. Vermeld mag worden dat het toetsmodel een document is van elf pagina's en de NOREA PIA vijftig pagina's telt. Voor een snelle, overzichtelijke weergave van de score op elk criterium, zie paragraaf 3.3.

3.2.1 BELANGRIJKE FUNCTIES VAN EEN PIA

1. De PIA bevat een stel vragen om privacyrisico's te ontdekken (meestal gerelateerd aan privacy principes).
Toetsmodel Privacy Impact Assessment Rijksdienst
In het toetsmodel wordt een vragenlijst gebruikt om privacyrisico's te ontdekken. *"Een PIA is richtinggevend in de zin dat de (uitputtende) vragenreeks kan wijzen op relevante privacyrisico's die in de vroege fase van beleids- of systeemontwikkeling (wellicht nog) niet zijn onderkend."* Het toetsmodel voldoet aan het criterium.
Privacy Impact Assessment (NOREA)
De NOREA PIA voldoet aan dit criterium, vanwege: *"De PIA legt in de eerste plaats de risico's bloot van projecten die te maken hebben met privacy en dragen bij aan het vermijden of verminderen van deze privacyrisico's. Op basis van de antwoorden van de PIA wordt op systematische wijze inzichtelijk gemaakt of er een kans is dat de privacy van betrokkene wordt geschaad, hoe hoog deze is en op welke gebieden dit is."*

2. De PIA identificeert privacyrisico's.
Toetsmodel Privacy Impact Assessment Rijksdienst
Het toetsmodel is: *"richtinggevend in de zin dat de (uitputtende) vragenreeks kan wijzen op relevante privacyrisico's die in de vroege fase van beleids- of systeemontwikkeling (wellicht nog) niet zijn onderkend."* Tijdens het invullen van de vragenlijst moet bewustwording optreden van privacyaspecten en de betreffende risico's. Het toetsmodel voldoet dus aan het criterium.

Privacy Impact Assessment (NOREA)
In de PIA staat het volgende: *"De PIA legt in de eerste plaats de risico's bloot van projecten die te maken hebben met privacy en dragen bij aan het vermijden of verminderen van deze privacyrisico's. Op basis van de antwoorden van de PIA wordt op systematische wijze inzichtelijk gemaakt of er een kans is dat de privacy van betrokkene wordt geschaad, hoe hoog deze is en op welke gebieden dit is."* Dit blijkt na het doornemen van de vragenlijst ook zo te zijn. De PIA voldoet dus aan het criterium.

3. De PIA identificeert mogelijke strategieën om de risico's te beperken.
Toetsmodel Privacy Impact Assessment Rijksdienst
In de PIA staat het volgende: *"Vanwege het richtinggevende en corrigerende karakter van een PIA zal het invullen van de vragenlijst vaak een dynamisch proces zijn, waarbij concept-(beleids)oplossingen of het concept-functionele systeemontwerp geleidelijk worden aangescherpt."* Hoewel het toetsmodel bovenstaande aangeeft, voorziet het niet in mogelijkheden waarop oplossingen of ontwerpen worden aangescherpt. Het voldoet dus niet aan het criterium.
Privacy Impact Assessment (NOREA)
Na het identificeren van de risico's staat er het volgende: *"Op basis van de uitkomsten van de PIA kunt u gericht acties ondernemen om deze risico's te verminderen."* Bij de gedetailleerde omschrijving van de stap 'Beoordeel de impact en bedenk waar nodig (aanvullende) maatregelen' wordt globaal aangegeven op welke manieren dit kan. Er worden per OECD privacyprincipe voorbeelden gegeven van maatregelen/strategieën. Bij de geïdentificeerde risico's in de vragenlijst wordt ook vaak omschreven hoe ze kunnen worden voorkomen. Ook wordt er verwezen naar de PbD denkwijze en gerelateerde publicaties van het CBP. De PIA voldoet dus aan het criterium.

3.2.2 PRIVACY DEFINITIE

4. Er wordt expliciet aangegeven dat een PIA meer is dan een compliance check.
Toetsmodel Privacy Impact Assessment Rijksdienst
Nergens in het toetsmodel wordt er gesproken over compliance, over het voldoen aan de wet. In de vragenlijst zijn alleen diepgaande vragen opgenomen over artikelen van de Wbp, niet over andere privacyaspecten. Er wordt dus niet voldaan aan het criterium.
Privacy Impact Assessment (NOREA)
Zoals ook blijkt uit punt 4. worden niet alle privacyaspecten behandeld. Er staat ook: *"Deze PIA is geen nalevingsinstrument, maar een risicoanalyse-instrument waarmee privacyrisico's kunnen worden geïdentificeerd en gelokaliseerd. Ook in deze PIA wordt het uitvoeren van een dergelijke compliance check in veel gevallen aangeraden."* De PIA is dus niet eens een compliance check, en daarnaast worden niet **alle** privacyaspecten behandeld, maar enkele. De PIA voldoet dus niet aan het criterium.

5. De PIA behandelt alle soorten privacy (de definitie van Finn en anderen wordt gebruikt).
Toetsmodel Privacy Impact Assessment Rijksdienst
Privacy wordt in het toetsmodel vrijwel gelijk getrokken met gegevensbescherming. De definitie van gegevensbescherming wordt ontleend aan de Wet Bescherming Persoonsgegeven, of aan de definitie zoals deze in de bovenliggende Europese dataprotectierichtlijn 95/46 staat. Die definitie omvat niet alle vormen van privacy, dus voldoet het niet aan het criterium.
Privacy Impact Assessment (NOREA)
De definitie van privacy in de NOREA PIA wordt in eerste instantie breed opgezet, aan de hand van de privacy principes van de OECD, en met behulp van de vier definities van privacy die in de Nederlandse Grondwet staan (artikel 10 t/m 13). Uit de vragenlijst zelf blijkt dat privacy breder wordt opgevat dan de definitie van de Wbp. Echter, in de inleiding wordt gezegd dat in de PIA privacy vooral betrekking heeft op de bescherming van persoonsgegevens. Hiermee wordt bedoeld: *"het recht op eerlijke, veilige en betrouwbare informatieverwerking"*. Daarmee voldoet de PIA niet aan het criterium.

3.2.3 Verantwoording en expertise

6. De PIA beveelt consultatie met externe stakeholders aan.
Toetsmodel Privacy Impact Assessment Rijksdienst
Het toetsmodel raadt aan om contact op te nemen met de Functionaris Gegevensbescherming (FG) of de Chief Information Officer (CIO), maar dit zijn interne stakeholders. Verder wordt er nergens gesproken over externe stakeholders, dus voldoet het niet aan het criterium.
Privacy Impact Assessment (NOREA)
In de PIA staat: *"Tot slot kan het raadzaam zijn dat u de PIA rapportage (en de onderliggende ingevulde PIA vragenlijst) laat reviewen. Een review kan zowel intern als extern uitgevoerd worden."* Het is duidelijk dat de PIA voldoet aan het criterium.

7. Er wordt aangemoedigd om de PIA te publiceren.
Toetsmodel Privacy Impact Assessment Rijksdienst
In de PIA staat het volgende: *"Resultaten van een PIA moeten worden gezonden aan de betrokken FG en de CIO. (...) Bij wetgeving wordt over PIA-resultaten een passage opgenomen in de toelichting."* Bij wetgeving wordt er dus een gedeelte van de PIA opgenomen in de Memorie van Toelichting, die wordt gepubliceerd. Alle andere projecten worden aan de FG en CIO toegezonden. Dit staat echter niet gelijk aan publicatie. Het toetsmodel voldoet dus niet aan het criterium.
Privacy Impact Assessment (NOREA)
Er wordt nergens aangemoedigd om de PIA te publiceren. Er wordt dus niet voldaan aan het criterium.

8. Er wordt aangegeven dat een PIA beoordeeld moet worden door een derde, onafhankelijke partij.
Toetsmodel Privacy Impact Assessment Rijksdienst
Net zoals omschreven bij punt 9. wordt de PIA toegezonden aan de FG en CIO. Deze partij(en) zijn onafhankelijk, en worden niet of nauwelijks betrokken bij de uitvoering van de PIA. Er wordt dus voldaan aan het criterium.
Privacy Impact Assessment (NOREA)
Er staat letterlijk: *"Tot slot kan het raadzaam zijn dat u de PIA rapportage (en de onderliggende ingevulde PIA vragenlijst) laat reviewen. Een review kan zowel intern als extern uitgevoerd worden."* Vervolgens wordt toegelicht wanneer de review intern plaatsvindt, dit dient te gebeuren door aan onafhankelijke partij die niet is betrokken bij de uitvoering van de PIA. Er wordt dus voldaan aan het criterium.

9. De PIA wordt verplicht door wetgeving of beleid of gaat gepaard met afstemming van het budget voor projecten.
Toetsmodel Privacy Impact Assessment Rijksdienst
Uit een brief van de Tweede Kamer[20] op 21 juni 2013 blijkt dat het toetsmodel vanaf 1 september standaard toegepast dient te worden bij *"ontwikkeling van nieuwe wetgeving en beleid waarmee de bouw van nieuwe ICT-systemen of de aanleg van grote databestanden wordt voorzien"*. Het toetsmodel voldoet dus aan het criterium.
Privacy Impact Assessment (NOREA)
In de inleiding van de NOREA PIA staat het volgende: *"Deze PIA sluit nadrukkelijk aan bij de steeds sterker wordende politieke druk op het uitvoeren van PIA's voor verwerkingen die bijzondere privacyrisico'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."* Waar de NOREA beroepsgroep deze PIA aandraagt om de eisen van de motie te vervullen, is vanuit de Rijksdienst al het toetsmodel verplicht. De NOREA PIA wordt dus niet door wetgeving of beleid verplicht tot uitvoering, en voldoet dus niet aan het criterium.

[20] Brief Tweede Kamer over Toetsmodel d.d. 19 juli 2013

10. De PIA moet worden ondertekend door het senior management om verantwoording te bewerkstelligen.
Toetsmodel Privacy Impact Assessment Rijksdienst
Zoals eerder genoemd, dient het toetsmodel aan de FG of ICO te worden gezonden. Dit kan worden gezien als het laten ondertekenen van de uitgevoerde PIA. Aan het criterium wordt dus voldaan.
Privacy Impact Assessment (NOREA)
In de NOREA PIA staat letterlijk: *"Tot slot kan het raadzaam zijn dat u de PIA rapportage (en de onderliggende ingevulde PIA vragenlijst) laat reviewen. Een review kan zowel intern als extern uitgevoerd worden."* Omdat de NOREA PIA voor meer situaties gebruikt kan worden, omschrijft het niet dwingend dat een review verplicht is. De PIA voldoet dus niet aan het criterium.

3.2.4 PROCES EN STRUCTUUR

11. Er wordt gezegd dat de PIA een proces is.
Toetsmodel Privacy Impact Assessment Rijksdienst
In het toetsmodel wordt niet gesproken van een proces, maar alleen van een hulpmiddel of vragenlijst. Wel is er aangegeven dat het invullen van de vragenlijst een dynamisch proces is. Echter is de vragenlijst zelf geen onderdeel van een bovenliggend proces met een expliciet aangegeven fasering. Het toetsmodel voldoet dus niet aan dit criterium.
Privacy Impact Assessment (NOREA)
In de NOREA PIA wordt expliciet gezegd dat het een proces is. In het hoofdstuk *Handreiking* wordt omschreven uit welke stappen het proces bestaat. Er wordt dus voldaan aan het criterium.

12. De PIA wordt bedoeld als een vorm van risicobeheer.
Toetsmodel Privacy Impact Assessment Rijksdienst
Het toetsmodel is bedoeld om risico's op heldere en gestructureerde wijze in kaart te brengen. Er wordt echter nergens aangeduid dat de PIA bijdraagt aan risicomanagement. Het toetsmodel voldoet niet aan het criterium.
Privacy Impact Assessment (NOREA)
De volgende succesfactor wordt omschreven: *"de 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)."* Duidelijk moge zijn, dat voldaan wordt aan het criterium.

13. De PIA voorziet in een structuur voor een resulterend rapport/verslag.
Toetsmodel Privacy Impact Assessment Rijksdienst
Het toetsmodel zegt het volgende: *"Beantwoording van de PIA-vragenlijst resulteert in een geschreven document."* Het omschrijft verder geen structuur voor dat document, dus voldoet het niet aan het criterium.
Privacy Impact Assessment (NOREA)
De PIA zegt het volgende: *"De resultaten van de PIA worden vastgelegd in een verslag. Een voorbeeld voor een PIA-verslag is opgenomen in bijlage D."* In bijlage D van de NOREA PIA documentatie wordt op één pagina aangegeven wat er in het verslag in ieder geval aan de orde moet komen. Er wordt dus voldaan aan het criterium.

14. Er wordt aangegeven dat het PIA proces dynamisch is (constant corrigerend gedurende het gehele proces).
Toetsmodel Privacy Impact Assessment Rijksdienst
Hoewel er al is geconstateerd dat het toetsmodel niet als proces wordt benoemd staat er letterlijk: *"Vanwege het richtinggevende en corrigerende karakter van een PIA zal het invullen van de vragenlijst vaak een **dynamisch** proces zijn, waarbij concept-(beleids)oplossingen of het concept-functionele systeemontwerp geleidelijk worden aangescherpt."* Het toetsmodel voldoet dus wel aan het criterium.
Privacy Impact Assessment (NOREA)
Er staat letterlijk: *"Het PIA verslag kan een dynamisch document zijn. Hiermee wordt bedoeld dat in geval van wijzigingen in het project de PIA (deels) opnieuw doorlopen kan worden en waar nodig het verslag op onderdelen geactualiseerd kan worden."* Hier wordt het PIA verslag dynamisch genoemd maar het heeft betrekking op het gehele proces. De PIA voldoet aan het criterium.

3.2.5 Randzaken

15. De PIA is gericht op het bedrijfsleven én de overheid.
Toetsmodel Privacy Impact Assessment Rijksdienst
Het toetsmodel voldoet niet aan dit criterium: *"Het PIA-toetsmodel is specifiek gericht op de Rijksdienst en bedoeld voor toepassing op alle beleidsgebieden en binnen alle rechtsdomeinen."* Het is dus alleen bedoeld voor toepassing binnen de overheid.
Privacy Impact Assessment (NOREA)
De NOREA PIA spreekt niet van een specifieke doelgroep, maar: *"De PIA kan gebruikt worden door alle typen organisaties."* Dit betekent dat de PIA gebruikt kan worden voor het bedrijfsleven én de overheid, en voldoet dus aan het criterium.

16. Er wordt aangegeven welke voordelen uitvoering van de PIA heeft.

Toetsmodel Privacy Impact Assessment Rijksdienst

Het doel van het toetsmodel is *"om bij ontwikkeling van beleid, en de daarmee gepaard gaande wetgeving of bouw van ICT-systemen en aanleg van databestanden, privacyrisico's op gestructureerde en heldere wijze in kaart te brengen. (...) Het richt zo in een vroegtijdig stadium en op hoofdlijnen de aandacht op alle onderdelen van de beoogde verwerking van persoonsgegevens die aandacht en uitwerking behoeven. (...) In het bijzonder is de vragenlijst inhoudelijk gezien zowel richtinggevend als corrigerend bedoeld. Daarnaast moet het beantwoordingsproces als zodanig ook bewustwording stimuleren van de uiteenlopende privacyaspecten waarmee rekening moet worden gehouden."* Met richtinggevend wordt bedoeld dat de PIA richting geeft voor aanpassingen aan wat wordt ontwikkeld. Met corrigerend wordt bedoeld dat het proces zo is ontworpen dat in een later stadium kan blijken dat een eerdere stap opnieuw gedaan moet worden. Daarnaast is het doel: bewustwording van de aanwezige privacyrisico's bij de genoemde activiteiten. Het resulteert in een geschreven document. Het einddoel is: *"Dit heeft tot gevolg dat bij voorbereiding van wetgeving, beleid en overheidsICT-systemen privacyaspecten als zodanig onderdeel zijn geworden van het afwegingsproces."* Het toetsmodel voldoet dus aan het criterium.

Privacy Impact Assessment (NOREA)

Aangezien een specifieke paragraaf in de PIA over het doel gaat wordt hij hier geciteerd:
"De PIA kent een aantal belangrijke doelen. Het belangrijkste doel is:

1. *Het voorkomen van kostbare aanpassingen in processen, herontwerp van systemen of stopzetten van een project door vroegtijdig inzicht in de belangrijkste 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 privacybewustzijn 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."*

Deze PIA resulteert ook in een geschreven document. Voor de inhoud van het resulterend verslag worden suggesties gedaan. Er wordt in een losse paragraaf expliciet toegelicht dat de PIA niet bedoeld is om compliance na te gaan. De PIA is een risicoanalyse-instrument waarmee privacyrisico's kunnen worden geïdentificeerd en gelokaliseerd. Een compliance check zal in veel gevallen worden aangeraden. De NOREA PIA voldoet aan het criterium.

17. Er wordt vastgesteld of uitvoering van de PIA nodig is.
Toetsmodel Privacy Impact Assessment Rijksdienst
Het toetsmodel is van toepassing op projecten binnen de Rijksdienst waarin nieuw beleid wordt ontwikkeld voor wetgeving of een ICT systeem/databestand waarbij persoonsgegevens worden verwerkt door de verantwoordelijke. Er wordt van tevoren getoetst of de verwerking van persoonsgegevens noodzakelijk is voor het te bereiken doel. Hierbij zijn subsidiariteit en proportionaliteit van belang. Er wordt dus voldaan aan het criterium.
Privacy Impact Assessment (NOREA)
Deze PIA kan gebruikt worden door alle typen organisaties en is van toepassing op nieuwe projecten of grote wijzigingen aan bestaande systemen of processen waarbij persoonsgegevens worden verwerkt door de verantwoordelijke (eventueel door een bewerker). De PIA kan het beste in een zeer vroeg stadium van een project uitgevoerd worden door opdrachtnemers, opdrachtgevers of andere belanghebbenden. Of de gehele PIA uitgevoerd moet worden, wordt pas duidelijk als men aan de vragenlijst begint. Aan het begin van de vragenlijst zitten enkele vragen om vast te stellen of het risico groot genoeg is om de PIA geheel toe te passen. Er wordt dus aan het criterium voldaan.

18. De PIA kan ook worden uitgevoerd op wetgeving of beleid.
Toetsmodel Privacy Impact Assessment Rijksdienst
Volgens het toetsmodel doet een PIA het volgende: *"Een Privacy Impact Assessment (PIA) is een hulpmiddel om bij ontwikkeling van beleid, en de daarmee gepaard gaande wetgeving of bouw van ICT-systemen en aanleg van databestanden, privacyrisico's op gestructureerde en heldere wijze in kaart te brengen."* Juist het toetsmodel is dus van toepassing op de ontwikkeling van wetgeving of beleid, naast ICT-gerelateerde projecten. Het toetsmodel voldoet aan het criterium.
Privacy Impact Assessment (NOREA)
In de inleiding staat: *"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."* In de definities wordt vervolgens toegelicht dat: *"Het project kan bijvoorbeeld een initiatief, review, systeem, database, programma, applicatie, dienst dan wel **wets-** of **beleidsvoorstel** zijn."* De PIA voldoet dus aan het criterium.

19. De leesbaarheid van de PIA volgens de Accessibility Leesniveau Tool.
In 2013 is door Jansen en Boersma onderzoek gedaan naar de leesbaarheid/begrijpelijkheid van Nederlandse teksten (Jansen & Boersma, 2013). In dat onderzoek is een valide methode gebruikt, namelijk de *close test*. Vervolgens zijn de scores van dat onderzoek vergeleken met drie geautomatiseerde meetinstrumenten om de leesbaarheid van Nederlandse teksten te voorspellen. In die vergelijking is gebleken dat van de drie meetinstrumenten de *Accessibility Leesniveau Tool* de hoogste correlatie tussen voorspelling en leesniveau aangeeft. De correlatie is echter niet hoog genoeg om serieuze uitspraken te doen. Er wordt momenteel gewerkt aan een beter meetinstrument om de begrijpelijkheid van Nederlandse teksten te kunnen voorspellen, genaamd *LeesbaarheidIndex voor het Nederlands* (LIN). Dit onderzoek is echter nog niet afgerond dus bij gebrek aan beter is de tool van Accessibility gebruikt om toch iets over het leesniveau te kunnen zeggen. De stichting omschrijft het volgende: *"De Accessibility Leesniveau Tool geeft op basis van een ingevoerde tekst een indicatie van het niveau van de leesbaarheid."* Om de tool zijn werk te laten doen zijn minimaal tien goed gespelde, passend afgesloten zinnen benodigd. Daarnaast dient het aantal eigennamen aangegeven te worden, zodat de tool daar rekening mee kan houden in de berekening. Voor meer informatie over de tool en zijn functie zie de website van Accessibility[21]. Voor de twee PIA's wordt naast de besproken indicatie van de Accessibility tool ook de eigen ervaring besproken.
Toetsmodel Privacy Impact Assessment Rijksdienst
De context van het toetsmodel wordt heel kort, op één pagina uitgelegd. Op de tweede pagina wordt gelijk gesproken over subsidiariteit en proportionaliteit. Voor een beleidsmaker zijn dat wellicht bekende termen, maar voor een non-juridische medewerker van een ZBO kunnen dat onbekende begrippen zijn. De vragen in de vragenlijst worden uitgelegd aan de hand van verwijzingen naar de Wbp en waar ze onduidelijk zijn kan de FG of juridische afdeling van het betreffende ministerie ondersteuning bieden. Voor de indicatie van het leesniveau van het toetsmodel zijn de eerste tien zinnen genomen. Deze zijn vooraf gegaan door de woorden 'ten geleide' dus dienen als inleiding van het toetsmodel. Zelfs bij het invullen van 12 eigennamen, geeft de tool het leesniveau **C2** aan. Dit is het hoogste haalbare leesniveau in Nederland. De omschrijving van niveau C2 is: *"Ik kan moeiteloos vrijwel alle vormen van de geschreven taal lezen, inclusief abstracte, structurele of linguïstische complexe teksten, zoals handleidingen, gespecialiseerde artikelen en literaire werken."*
Privacy Impact Assessment (NOREA)
In de NOREA PIA wordt in een apart hoofdstuk de belangrijkste begrippen van de Wbp uitgelegd. In de vragenlijst worden diezelfde begrippen ook toegelicht aan de hand van definities van de Wbp. Waar ze niet direct worden uitgelegd wordt verwezen naar het specifieke artikel in de Wbp. Voor de voorspelling van het leesniveau van de NOREA PIA zijn de eerste tien zinnen van de inleiding genomen. Bij het invullen van 5 eigennamen geeft de tool het leesniveau **C1** aan. Dit is het op een na hoogste leesniveau in Nederland. De omschrijving van niveau C1 is: *"Ik kan lange en complexe feitelijke en literaire teksten begrijpen en het gebruik van verschillende stijlen waarderen. Ik kan gespecialiseerde artikelen en lange technische instructies begrijpen, zelfs wanneer deze geen betrekking hebben op mijn terrein."*

[21] Accessibility Leesniveau Tool d.d. 2009

3.3 Overzicht van de vergelijking

De scores van de twee PIA's voor de criteria zoals omschreven in de vorige paragrafen worden overzichtelijk weergegeven in onderstaande tabel. Een '●'-teken betekent dat de PIA voldoet aan het criterium.

#	PIA Criteria	Toetsmodel	NOREA
Belangrijke functies van een PIA			
1.	Bevat een stel vragen om privacyrisico's te ontdekken	●	●
2.	Identificeert privacyrisico's	●	●
3.	Identificeert mogelijk strategieën om de risico's te beperken		●
Privacy definitie			
4.	Geeft expliciet aan dat het meer is dan een compliance check		
5.	Behandelt alle soorten privacy		
Verantwoording en expertise			
6.	Beveelt consultatie met externe stakeholders aan		●
7.	Moedigt aan om de PIA te publiceren		
8.	Geeft aan dat het rapport door een onafhankelijke, derde partij beoordeeld moet worden	●	●
9.	Wordt verplicht door wetgeving/beleid of gaat gepaard met afstemming van het budget	●	
10.	Moet worden ondertekend door het senior management	●	
Proces en structuur			
11.	Zegt dat een PIA een proces is		●
12.	Wordt als een vorm van risicobeheer bedoeld		●
13.	Voorziet in een structuur voor een PIA verslag/rapport		●
14.	Geeft aan dat het PIA proces dynamisch is	●	●
Randzaken			
15.	Is gericht op het bedrijfsleven én de overheid		●
16.	Geeft aan welke voordelen uitvoering van de PIA heeft	●	●
17.	Stelt vast of uitvoering van de PIA nodig is.	●	●
18.	Kan ook worden uitgevoerd op wetgeving of beleid	●	●
19.	Het leesniveau van de PIA	**C2**	**C1**

3.4 CONCLUSIE VAN DE VERGELIJKING

Volgens de gemaakte vergelijking tussen de twee PIA's is te zien dat beide PIA's niet aan elk criterium voldoen. De NOREA PIA heeft wel de belangrijkste functies van een PIA verwerkt in zijn standaard. Het toetsmodel kan niet gebruikt worden om strategieën te identificeren om risico's te beperken. Qua privacy definitie missen beide PIA's een stuk. Ze leggen de focus op gegevensbescherming terwijl privacy een breder begrip is dan alleen gegevensbescherming. Een PIA zou in de breedte verder moeten gaan dan alleen een compliance check.

Op het gebied van verantwoording afdwingen doet het toetsmodel het weer iets beter. De PIA's zouden echter wel moeten aanraden om het PIA rapport te publiceren, zodat er transparantie wordt bewerkstelligd. Wat structuur/proces betreft scoort de NOREA PIA weer beter. Het toetsmodel voorziet namelijk niet in een structuur voor een document, terwijl er wel een document opgeleverd moet worden. Daarnaast is het toetsmodel alleen een vragenlijst en mist het een uitvoerige beschrijving van het bovenliggend proces. De NOREA PIA biedt dit wel.

Wat randzaken betreft is naar voren gekomen dat de NOREA PIA van toepassing is op de overheid en het bedrijfsleven waar het toetsmodel alleen voor de overheid bedoeld is. Ten slotte kan uit een indicatie voorzichtig geconcludeerd worden dat de NOREA PIA leesbaarder is dan het toetsmodel (geen hard bewijs hiervoor). Een algemene indruk is dat de NOREA PIA wat completer is. Dit is ook aan de omvang van de standaard af te leiden. Beide PIA's kunnen echter verbeterd worden.

In het volgende hoofdstuk worden de praktijkervaringen beschreven van de toepassing van de NOREA PIA bij Nigella IT.

4 UITVOERING VAN DE NOREA PIA BIJ NIGELLA IT

4.1 AANPAK

De NOREA PIA is bij Nigella IT toegepast op een informatiesysteem dat gedeeltelijk nog in ontwikkeling was. Dit heeft voor Nigella IT geresulteerd in een PIA rapport waarvan de inhoud (bijvoorbeeld geïdentificeerde risico's) belangrijk is. Voor deze thesis is die inhoud niet waardevol maar zijn vooral de bevindingen over de praktische uitvoering van het NOREA PIA proces van belang. Op de volgende onderzoeksvraag wordt daarom in dit hoofdstuk antwoord gegeven:

> *Tot welke inzichten over het NOREA PIA proces heeft de toepassing van de NOREA PIA bij Nigella IT geleid?*

Het NOREA PIA proces bestaat uit de volgende stappen:

1. Bepaal wie de PIA gaat uitvoeren en hoe dit moet gebeuren
2. Verzamel relevante informatie over het project
3. Vul de PIA vragenlijst in
4. Beoordeel de impact en bedenk waar nodig (aanvullende) maatregelen
5. Stel het PIA verslag op
6. Laat eventueel een (onafhankelijke) toets op de PIA uitvoeren

De methoden die zijn gebruikt om stap 2 van het proces uit te voeren zijn deskresearch en ad-hoc interviews met de projectmedewerkers van het EVS (zie volgende paragraaf). Voor stap 3 is de PIA vragenlijst uit de NOREA PIA documentatie gebruikt.

Om antwoord te geven op deze vraag is bij elke fase van het NOREA PIA proces geëvalueerd hoe deze is **uitgevoerd**, tegen welke **problemen** men is aangelopen en welke overige **aandachtspunten** geconcludeerd kunnen worden. De inzichten die bedoeld worden in de onderzoeksvraag zijn dus ingedeeld in daadwerkelijk opgetreden **problemen** en **aandachtspunten**:

- **Problemen** (deze hebben voor stagnatie, onduidelijkheid of een verkeerde conclusie gezorgd)
- **Aandachtspunten** (punten die mogelijk in een andere situatie tot een probleem kunnen leiden, maar bij deze casestudy niet tot problemen hebben geleid)

4.2 ACHTERGROND

Nigella IT is actief in de medische hulpmiddelenmarkt en ontwikkelt, implementeert en onderhoudt automatiseringsoplossingen voor een keur aan bedrijven en instellingen die te maken hebben met medische hulpmiddelen. Zij ontwikkelen momenteel een Elektronisch Voorschijf Systeem (EVS) dat ondersteuning biedt bij het voorschrijfproces van medische hulpmiddelen tussen onder andere zorgverleners, patiënten en leveranciers van medische hulpmiddelen. De digitale bewaring van dit proces dient als verantwoording voor de vergoeding van medische hulpmiddelen door de zorgverzekeraar.

Omdat in het systeem persoonsgegevens worden verwerkt is het van belang dat er aandacht wordt besteed aan de privacy van de patiënt. Het aantonen van mechanismen om de privacy te

beschermen is van belang om de vertrouwensrelatie met de gebruiker van het EVS te onderhouden. Omdat het systeem nog gedeeltelijk in ontwikkeling is, is het in theorie een uitgelezen mogelijkheid om een PIA uit te voeren. Sommige resultaten van de uitgevoerde PIA zijn vertrouwelijke gegevens. Deze zijn weggelaten uit de evaluatie.

4.3 Evaluatie van het NOREA PIA proces

Er is per processtap van de NOREA PIA beredeneerd tot welke inzichten men door de uitvoering in de praktijk is gekomen.

4.3.1 Stap 1: Bepaal wie de PIA gaat uitvoeren en hoe dit moet gebeuren

Uitvoering

Om praktische redenen is er gekozen om de PIA door één persoon uit te laten voeren. De PIA zou de waarheid moeten weerspiegelen door regelmatig de voortgang en de veronderstelde feiten terug te koppelen naar de personen die de relevante kennis bezitten. Aan de hand van bijlage B is beoordeeld welke personen betrokken moeten worden bij het verzamelen van de relevante informatie (stap 2). De succes- en faalfactoren van bijlage C zijn in acht genomen. Het resultaat van deze fase van de PIA is verwerkt in een plan van aanpak.

Problemen

Onduidelijke tijdsduur

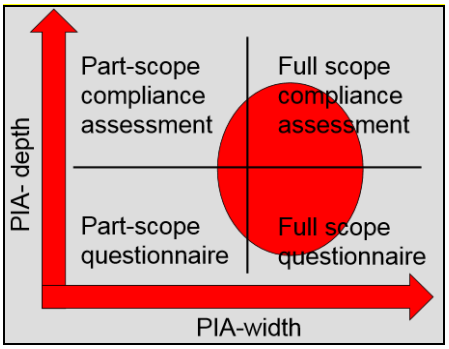
Op bladzijde 9 van de NOREA PIA staat omschreven dat het van veel factoren afhankelijk is hoe veel tijd de uitvoering van de PIA kost. Het is in de praktijk inderdaad lastig gebleken om op voorhand een accurate planning te maken voor de uit te voeren PIA. Het moment waaruit in de PIA blijkt hoe omvangrijk de uitvoering zal zijn is onderdeel van stap 3: het invullen van het eerste deel van de vragenlijst. Als dan blijkt dat de Wbp helemaal niet van toepassing is, is het uitvoeren van de PIA aanzienlijk minder werk dan wanneer de Wbp wel van toepassing is. Om het eerste deel van de vragenlijst in te kunnen vullen zal men dus eerst het vooronderzoek (stap 2) moeten doen. Als dat vooronderzoek veel tijd kost doet men er in ieder geval goed aan om een PIA uit te voeren aangezien er dan waarschijnlijk weinig is nagedacht en/of gedocumenteerd over de privacyaspecten van het project.

Aandachtspunten

Uitvoeren met juiste doelstelling

Uit een presentatie van de NOREA beroepsorganisatie[22] en de PIA documentatie blijkt dat de PIA niet gebruikt kan worden om met zekerheid vast te stellen of er compliance is met de Wbp. Onderstaande afbeelding (afkomstig uit die presentatie) beeldt de doelstelling van de PIA uit.

[22] Workshop Privacy Impact Assessments: "The NOREA PIA, design and experience" d.d. 5 december 2013



FIGUUR 2: BEREIK VAN DE NOREA PIA

Het is gebleken dat het voor een organisatie belangrijk is om compliant te zijn met privacywetgeving. Enerzijds omdat men de zaken goed geregeld wilt hebben. Anderzijds kan compliance belangrijk zijn omdat non-compliance een risico is wat (hoge) boetes en juridische rompslomp met zich mee kan brengen. Het behalen van compliance kan dus indirect ook een monetair belang zijn. De eisen van een gebruiker wat betreft privacy kunnen echter hoger zijn dan die van privacywetgeving. In een PIA is privacy ook breder gedefinieerd dan in de wetgeving. Een organisatie kan daarom een andere opvatting over privacy hebben dan de gebruiker van het systeem en de PIA zelf. Door het verschil in de opvatting van privacy en het belang van compliancy kan een organisatie haar prioriteiten anders stellen dan die van haar gebruikers en zelfs dan die van een PIA. Dit kan ervoor zorgen dat PIA's met de verkeerde doelstelling worden uitgevoerd. Het is dus zaak voor de uitvoerders van een PIA om goed van tevoren af te stemmen waarom een PIA wordt uitgevoerd, en ervoor te zorgen dat deze met de juiste doelstelling wordt uitgevoerd. Als compliance achterhalen het enige belang is, kan beter een compliance check of privacy audit worden uitgevoerd. Dit wordt ook onderstreept in een van de faalfactoren die de NOREA PIA zelf omschrijft.

4.3.2 Stap 2: Verzamel relevante informatie over het project

Uitvoering

Alle documentatie over het project is verzameld en bestudeerd. Vervolgens is contact opgenomen met het management van het project en zijn de projectleden benaderd met ad-hoc vragen waar verduidelijking benodigd was. Aan de hand van de verzamelde informatie zijn beschrijvingen gemaakt van: het proces waar het systeem onderdeel van is, de datastromen van het systeem, en de stakeholders en hun belang. De juridische aspecten van het project zijn in kaart gebracht tijdens het invullen van de vragenlijst. Voor alle juridische vragen is contact opgenomen met de directie.

Problemen

Geen privacy expertise leidt tot stagnatie

Als men geen ervaring heeft met wetteksten, zijn deze moeilijk te begrijpen. Uit de praktijk is dan ook gebleken dat het inlezen in de wetgeving veel tijd en moeite kost.

Aandachtspunten

Huidige situatie beschrijven aan de hand van gegevensstromen

Voor een organisatie is het vaak belangrijker om een werkend systeem op te leveren dan een systeem dat tot in de puntjes is gedocumenteerd. Stap 2 kan daarom een hoop tijd

kosten als er weinig tot geen documentatie beschikbaar is. Bij het beschrijven van het EVS is gebleken dat het nagaan van de datastromen een goed startpunt is. Deze datastromen zijn ook belangrijk voor de juridische analyse van het systeem. Door het volgen van de data, wordt duidelijk waar de verschillende verantwoordelijkheden van de Wbp dienen te liggen. De manier waarop verantwoordelijkheden op het moment zijn verdeeld, wil namelijk niet zeggen dat ze ook zo verdeeld zouden moeten zijn. Het is gebleken dat wanneer er weinig documentatie beschikbaar is, de gegevensstromen een goed startpunt zijn om het huidige systeem in kaart te brengen. In de NOREA PIA wordt dit impliciet aangeraden. Er wordt namelijk gezegd dat in het PIA rapport een gegevensstroomanalyse aan de orde moet komen.

4.3.3 Stap 3: Vul de PIA vragenlijst in

Uitvoering

De vragenlijst is vervolgens doorgelopen. Per vraag is zo compact mogelijk onderbouwd waarom voor het betreffende antwoord is gekozen. Dit is meteen gedocumenteerd, zodat dit in stap 5 (het opstellen van het totale PIA verslag) verwerkt kan worden.

Aandachtspunten

Afwegingsvermogen van uitvoerders is belangrijk

Het invullen van de vragenlijst wijst zich vanzelf. Hij is zo opgesteld dat hij makkelijk te begrijpen is en elke vraag met 'Ja' of 'Nee' beantwoord kan worden. Dit betekent echter niet dat het invullen weinig inspanning kost. Bij elk antwoord dient een zorgvuldige afweging gemaakt te worden en het uiteindelijke antwoord is zeer afhankelijk van de context en het standpunt van de organisatie. Een voorbeeld: vraag 1.8 luidt: *"Zijn er veel maatschappelijke belanghebbenden?".* Deze vraag kan alleen beantwoord worden als de organisatie een goede indruk heeft welke maatschappelijke belanghebbenden er zijn en waar de grens tussen 'veel' en 'niet veel' zich bevindt. Voor het grootste deel van de vragenlijst geldt dat zulke afwegingen gemaakt dienen te worden. De kwaliteit van de uitgevoerde PIA is dus sterk afhankelijk van het beoordelingsvermogen van de uitvoerders. Om dit met een citaat uit de eerdergenoemde presentatie van NOREA samen te vatten: *"A fool with a tool is still a fool"*[23]. Uit de succes- en faalfactoren blijkt dit ook, maar het wordt niet expliciet omschreven.

Zorgvuldige vastlegging van afweging kost tijd

Vanwege de omvang van de vragenlijst is het handig om bij elke afweging voor het antwoord de vraag nogmaals te vermelden. Het zou handig zijn als er een template beschikbaar zou zijn waarin het antwoord nog maar hoeft worden ingevuld/toegelicht en de vragen al staan vermeld. Doordat er geen standaard wordt geboden waarin de afweging voor elk antwoord zorgvuldig vastgelegd kan worden, wordt niet aangemoedigd om elk antwoord zorgvuldig af te wegen.

Creatief zijn bij documenteren

Bij het maken van de afwegingen kan het handig zijn om deze overzichtelijk weer te geven. Bijvoorbeeld bij vraag 2.1 *"Zijn alle gegevens nodig om het doel te bereiken (worden er*

[23] Workshop Privacy Impact Assessments: "The NOREA PIA, design and experience" d.d. 5 december 2013

zo min mogelijk gegevens verzameld)?" is het handig om voor elk data-element na te lopen of deze toegevoegde waarde heeft en of deze noodzakelijk is. Als er veel data-elementen zijn is het handig om de afwegingen overzichtelijk weer te geven in een tabel.

4.3.4 Stap 4: Beoordeel de impact en bedenk (aanvullende) maatregelen

Uitvoering

Nadat de vragenlijst is doorlopen zijn mogelijke risico's geïdentificeerd. Voor elke belanghebbende is vervolgens beoordeeld welke impact het risico heeft. Bij het bepalen van de impact maakt de NOREA PIA een onderscheid tussen 'impact op de betrokkene' en 'impact op de organisatie'. Vanuit de ingeschatte impact van de risico's op de betrokkene is indirect de impact op de organisatie geschat. Bij sommige risico's gaf de vragenlijst aan wat er ondernomen kon worden om het risico weg te nemen of de impact te verkleinen. Waar niet direct werd omschreven welke maatregelen getroffen konden worden is indirect via de OECD principes[24] nagegaan met welk privacy principe het risico te maken heeft. Deze principes boden vervolgens een startpunt bij het bedenken van de maatregelen.

Problemen

Weinig expertise van de uitvoerder qua impactbepaling leidt tot stagnatie

Het bereiken van compliance betekent nog niet per se dat de privacy van de betrokkene wordt gewaarborgd. Non-compliance kan eveneens impact hebben op de organisatie, terwijl het geen impact heeft op de betrokkene. Deze complexiteit en de huidige maatschappelijke aandacht voor privacy maken impactbepaling geen gemakkelijke opgave, en een zeer context-afhankelijke activiteit. Het is gebleken dat de impactbepaling afhankelijk is van de expertise van de uitvoerder.

Weinig expertise van de uitvoerder qua risicobeperking bepaalt de kwaliteit

De NOREA PIA geeft buiten een aantal voorbeelden[25] weinig houvast bij het bedenken van maatregelen. Het woord 'bedenken' duidt ook op een ad-hoc activiteit. Het is gebleken dat het bedenken van maatregelen die de risico's verkleinen of helemaal uitsluiten dan ook volledig op de expertise van de uitvoerders van de PIA leunt. Vandaar dat een van de succesfactoren van de PIA is: *"PIA's zijn voorts meer effectief: (…) 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 deze expertise in mindere mate aanwezig is leidt dat tot een uitgevoerde PIA van lagere kwaliteit.

[24] te vinden in bijlage H van de NOREA PIA
[25] pagina 13 en 14 in de NOREA PIA

4.3.5 Stap 5: Stel het PIA verslag op

Uitvoering

De structuur van het PIA verslag/rapport is gebaseerd op bijlage D van de NOREA PIA. Het rapport opstellen was volgens de NOREA PIA en volgens de praktijk een dynamische activiteit.

Aandachtspunten

Documenteren bij elke stap

Ervaring wijst uit, dat het opstellen van het PIA verslag een activiteit is die gedeeltelijk tijdens elke voorgaande processtap wordt uitgevoerd. Uiteraard wordt de definitieve versie pas na afloop van het gehele proces gemaakt, maar delen van het verslag worden al tijdens eerdere processtappen opgesteld. Deze voorgaande stappen dienen namelijk toch gedocumenteerd te worden.

4.3.6 Stap 6: Laat eventueel een (onafhankelijke) toets op de PIA uitvoeren

Uitvoering

Vooraf aan de uitvoering van de PIA bij Nigella IT is om praktische redenen ervoor gekozen om geen onafhankelijke toets uit te laten voeren. Het PIA verslag is na de vorige stap ingeleverd bij de opdrachtgever en daarmee is de betrokkenheid bij de uitvoering van de PIA beëindigd.

Aandachtspunten

PIA kan uitgevoerd worden om te legitimeren

Als echter blijkt dat de resultaten van de vragenlijst erop wijzen dat er weinig tot geen privacyrisico's zijn, kan de opdrachtgever ertoe neigen om geen onafhankelijke toets op de uitgevoerde PIA uit te laten voeren. Er is dan immers een indicatie dat de impact op de privacy klein is dus er is geen aanleiding tot paniek. Echter, de constatering van de vragenlijst kan fout zijn. In dat geval is het besluit tot het niet laten uitvoeren van een onafhankelijke toets gevaarlijk aangezien de impact op de privacy groter kan zijn dan beoogd. Dit geldt natuurlijk net zo goed in het geval de vragenlijst een groot privacyrisico aantoont. De privacy maatregelen die dan getroffen worden op basis van de PIA kunnen overbodig zijn.

4.4 Conclusie van de evaluatie

De uitvoering van de NOREA PIA zorgt in de context van het EVS niet voor verrassingen. De problemen waar men in de uitvoering bij Nigella IT tegenaan is gelopen waren omschreven in de NOREA PIA documentatie onder de succes- of faalfactoren, maar waren desondanks niet te voorkomen. Er zijn aandachtspunten die bij een volgende uitvoering in deze context van belang kunnen zijn, maar het is bepaald geen noodzakelijke voorkennis. Hieronder zijn de **problemen** en **aandachtspunten** kort samengevat.

De volgende **problemen** zijn opgetreden tijdens de uitvoering:

- Het is lastig om op voorhand een strakke planning te maken voor de PIA, waardoor de geschatte tijdsduur onduidelijk is.
- Het ontbreken van juridische voorkennis van privacy wetgeving leidt tot stagnatie. Een manier om dit probleem te voorkomen is om binnen de organisatie met eventuele juridische expertise contact op te nemen. Dit wordt ook in de succesfactoren van de NOREA PIA omschreven.
- De aanwezige expertise was helaas laag, waardoor de kwaliteit van de uitgevoerde PIA lager uitvalt dan wanneer hij door bijvoorbeeld beveiligingsexperts zou zijn uitgevoerd. Deze expertise is vooral nodig voor de impactbepaling en het bedenken van maatregelen die de risico's verkleinen of wegnemen. Dit probleem kan voorkomen worden door uitvoerders aan te stellen met een kritische mindset die ook van pas komt bij andere vormen van risicobeheer. Meer uitvoerders betrekken bij de PIA wil niet zeggen dat de expertise toeneemt maar het kan wel extra invalshoeken bieden.

Algemene **aandachtspunten** die in deze casus niet voor problemen hebben gezorgd tijdens de uitvoering zijn de volgende:

- Het is gebleken dat het belangrijk is om goed na te gaan met welk doel de NOREA PIA wordt uitgevoerd, en of dat het juiste doel is.
- Bij het uitvoeren van het vooronderzoek van stap 2 is gebleken dat het volgen van de datastromen een goed uitgangspunt is om de beschrijving van een systeem vorm te geven. Dit is vooral handig in geval goede documentatie niet aanwezig is.
- Bij het doorlopen van de vragenlijst is het belangrijk om de antwoorden goed af te wegen. Hiervoor is een goed beoordelingsvermogen benodigd.
- Het is gebleken dat het documenteren van deze afwegingen een hoop tijd kost, ongeacht de expertise van de uitvoerders.
- Bij het documenteren is het verstandig om vraag 2.1 van de vragenlijst in tabelvorm te verwerken.
- Het PIA verslag kan gaandeweg het PIA proces worden opgebouwd en wordt na het bedenken van de maatregelen definitief gemaakt.
- Tenslotte is het verstandig om de PIA altijd door een onafhankelijke (eventueel externe) partij te laten reviewen, ook al is dat niet verplicht. Er is dan beter voorkomen dat de PIA de verkeerde conclusie trekt.

5 VALIDITEITSANALYSE NOREA PIA VRAGENLIJST

In de NOREA PIA zit een vragenlijst verwerkt die privacyrisico's moet identificeren. Deze vragenlijst is onderworpen aan een inhoudelijke validiteitsanalyse (of hij meet wat hoe dient te meten). Voor de definitie van (data) privacy voor deze validiteitsanalyse is de Wet bescherming persoonsgegevens (Wbp) als uitgangspunt genomen, omdat dit in Nederland de geldende wetgeving is wat betreft gegevensbescherming. Een privacyrisico is dan: een risico tot non-compliance met de Wbp. In de validiteitsanalyse is echter niet beoordeeld in hoeverre er een risico tot non-compliance is, maar of er voor 100% vastgesteld kan worden of er non-compliance is. De vragenlijst is dus zo geanalyseerd dat duidelijk is geworden in hoeverre er met 100% zekerheid compliance met de Wbp wordt vastgesteld. Er wordt dus in dit hoofdstuk antwoord gegeven op de volgende onderzoeksvraag:

> *In hoeverre trekt de vragenlijst van de NOREA PIA de juiste conclusie wat betreft compliance met de Wbp?*

Bij de beoordeling of de vragenlijst valide is, is gevalsonderscheiding toegepast. Positive betekent dat er een risico is, dus dat er non-compliance is vastgesteld. Negative is de tegenovergestelde conclusie; compliance. **True positive** en **true negative** zijn dus gevallen waarin de vragenlijst de juiste conclusies trekt. **False positives** zijn de gevallen waarin de vragenlijst de verkeerde conclusie trekt (non-compliance) terwijl er in werkelijkheid compliance is. Dit kan vervelend zijn, aangezien er wellicht maatregelen genomen worden die niet genomen hoeven te worden. **False negative** zijn de gevallen die echt niet aanwezig mogen zijn aangezien de vragenlijst aangeeft dat er compliance is, terwijl er in werkelijkheid non-compliance is met de wet.

5.1 AANPAK

De validiteitsanalyse is gedaan in drie stappen.

Stap 1 is de voorbereiding, waarin twee stroomschema's zijn gemaakt. De definitie van privacy (de Wbp) is omgezet van de tekstuele vorm naar een stroomschema aan de hand van het document 'Raamwerk Privacy Audit'. Door de Wbp te vertalen naar een stroomschema is het makkelijker af te lezen hoe artikelen zich verhouden tot elkaar. Het stroomschema is gebruikt in stap 2 om te bepalen wanneer bepaalde artikelen van de wet niet meer van toepassing zijn, en dus vervolgens in de vragenlijst niet meer aan de orde hoeven te komen. In de voorbereiding is ook de vragenlijst van de NOREA PIA omgezet naar een stroomschema. Dit tweede stroomschema is net zoals het stroomschema van de Wbp gemaakt om overzicht creëren, maar in het bijzonder om in stap 3 te kunnen beoordelen op hoeveel manier de vragenlijst doorlopen kan worden. Voor meer informatie over de stroomschema's, zie paragraaf 5.2.

Stap 2 van de validiteitsanalyse is de analyse per vraag en antwoord. Hiervoor is het stroomschema van de Wbp van stap 1 gebruikt. Per vraag van de vragenlijst is beoordeeld met welk artikel van de Wbp raakvlakken zijn en wat de conclusie per antwoord is wat betreft compliance. Stap 2 is tekstueel beschreven in paragraaf 5.3. Daarnaast is stap 2 ook verwerkt in een spreadsheet, te vinden in bijlage III. In die spreadsheet geeft het commentaar in de meest rechtse kolom aan of de vragenlijst met zekerheid (non-)compliance heeft vastgesteld (true false of true positive). De spreadsheet is benodigd geweest om het overzicht tussen de vragenlijst en

de Wbp te bewaren en om vervolgens na te kunnen gaan welke onderdeel van de wet in welke vraag terug komt. Tijdens de analyse van stap 2 zijn een aantal punten over de vragenlijst opgevallen die invloed hebben op de validiteit. Deze zijn opgesomd in paragraaf 5.3.1.

Stap 3 omvat het nagaan van alle mogelijke paden waarop de vragenlijst doorlopen kan worden. Stap 2 diende eerst te worden gedaan, omdat in stap 3 complete paden worden geanalyseerd. Een pad is een aaneenschakeling van beantwoorde vragen tot een punt waar de vragenlijst eindigt. Ook de aaneenschakeling van beantwoorde vragen dient in zijn geheel doorlopen te worden om te beoordelen in welke situaties de vragenlijst de juiste conclusie trekt. Voor de beoordeling hoeveel paden er zijn is het stroomschema van de PIA vragenlijst van stap 1 gebruikt. Stap 3 wordt belicht in paragraaf 5.4.

De algemene conclusie van dit hoofdstuk wordt in paragraaf 5.5 samengevat.

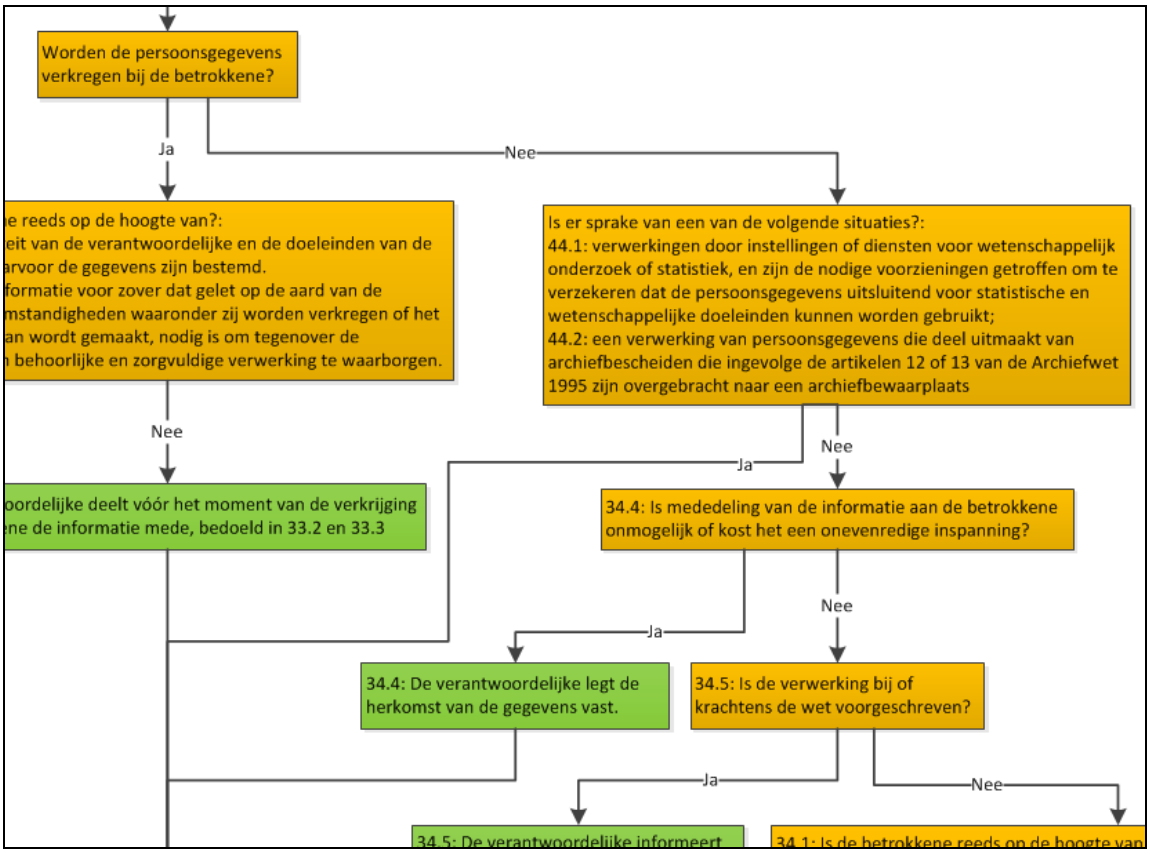
5.2 Stap 1: Omzetten naar stroomschema's

Zoals in de aanpak omschreven is het stroomschema van de Wbp gebaseerd op het Raamwerk Privacy Audit. Dit raamwerk dient als handboek bij het uitvoeren van een privacy audit. Een privacy audit is een controle of men voldoet aan de Wbp (voornamelijk bedoeld voor bestaande situaties). Een verantwoordelijke betekent in de Wbp: degene die verantwoordelijk is voor de gegevensbescherming en het doel en de middelen van de verwerking bepaalt. In het raamwerk is maar een selectie artikelen van de Wbp verwerkt, aangezien een aantal artikelen niet van toepassing is op een verantwoordelijke.

Het raamwerk heeft de geselecteerde artikelen gecategoriseerd per onderwerp. Dezelfde selectie en groepering van artikelen is ook aangehouden voor het stroomschema van de Wbp. Een voorbeeld: Als het verbod van artikel 16 niet van toepassing is, is er compliance met artikel 17 t/m 23 want deze zijn dan niet van toepassing. Ook al dateert het Raamwerk uit 2000, is het nog steeds van toepassing aangezien de Wbp geen drastische veranderingen heeft ondergaan. Om de kleine aanpassingen aan de Wbp in de analyse mee te nemen, is de op dat moment actuele versie van de Wbp gebruikt voor de analyse. Dit is de versie van 28 oktober 2014[26].

Het gemaakte stroomschema van de Wbp is niet opgenomen in de thesis vanwege de omvang en de dynamische vorm. De volgende afbeelding laat een klein deel van het schema zien om toch een indruk te krijgen:

[26] Wet Bescherming Persoonsgegevens d.d. 28 oktober 2014



FIGUUR 3: VOORBEELD STROOMSCHEMA WBP

Het stroomschema aanpassen zodat het in deze thesis past zou afdoen aan de waarde ervan. Het is te raadplegen als Visio bestand in het master thesis archive op de website van de Radboud Universiteit Nijmegen[27].

Het stroomschema van de PIA vragenlijst is wel opgenomen in de thesis, in bijlage IV. Dit tweede stroomschema is een overzichtsweergave van de vragenlijst waarop in een oogwenk te zien is hoe de vragenlijst doorlopen kan worden. De vragen en de antwoorden zijn letterlijk overgenomen uit de vragenlijst, maar de toelichting is weggelaten vanwege de beoogde omvang dat het stroomschema dan zou krijgen.

[27] Archive of Master Thesis Reports laatst bezocht 6 maart 2015

5.3 Stap 2: Analyse per vraag en antwoord

In deze paragraaf wordt per vraag bediscussieerd welke artikelen worden afgedekt en welke onterecht worden uitgesloten door het gegeven antwoord. Vanwege de lengte van de vragenlijst is deze paragraaf ook omvangrijk. Er wordt aangeraden om deze paragraaf alleen aandachtig te lezen als men is geïnteresseerd in de specifieke validiteitsbeoordeling per antwoord.

1.1: Is er sprake van het verwerken van persoonsgegevens?

Deze vraag heeft raakvlakken met artikel 1, onderdeel b, en artikel 2.

Ja: Is er sprake van een verwerking van persoonsgegevens, ga je verder. In de Wbp staat echter nog een aantal uitzonderingen dat is vrijgesteld. Die worden niet gevangen in de vragenlijst als dit antwoord is gegeven. Artikelen die nog uitzonderingen omschrijven worden niet behandeld (artikel 3 en 4).

Nee: Als er geen sprake is van het verwerken van persoonsgegevens, is de Wbp niet van toepassing. Er zijn dan ook geen compliancy risico's m.b.t. de Wbp. Antwoord nee komt in dit geval overeen met de Wbp, omdat de vragenlijst stopt.

1.2: Is het duidelijk wie verantwoordelijk is voor de verwerking van de gegevens?

Deze vraag heeft raakvlakken met artikel 1, onderdeel d, waarin 'verantwoordelijke' wordt gedefinieerd.

Ja: Als het duidelijk is wie de verantwoordelijke is, dan kan met zekerheid antwoord gegeven worden op de vervolgvragen en zijn er geen onduidelijkheden. Het zegt verder niets over compliance.

Nee: Als het niet duidelijk is wie de verantwoordelijke is, kan het zijn dat je dat zelf bent. En de verantwoordelijke moet aan een aantal verplichtingen voldoen. Deze vraag gaat verder niet in op die verplichtingen. Het antwoord 'nee' op deze vraag betekent dat je zelf de verantwoordelijke kunt zijn en dat er dus een kans op non-compliance is.

1.2.1: Verwerkt uw organisatie de persoonsgegevens in opdracht en onder verantwoordelijkheid van een andere organisatie? Treedt uw organisatie op als bewerker?

Deze vraag heeft raakvlakken met artikel 1, onderdeel c, waarin 'bewerker' wordt gedefinieerd.

Ja: Als je een bewerker bent, gelden alleen de verplichtingen die de verantwoordelijke op jou afdwingt door middel van een contract. Dit staat omschreven in artikel 14, lid 2. Het antwoord ja betekent dat je kunt stoppen met de vragenlijst. De Wbp dwingt in geen enkel artikel verplichtingen af op de bewerker, dus is verder niet van toepassing. De verplichtingen die de bewerker na dient te komen vallen dus buiten de vragenlijst.

Nee: Als je geen bewerker bent, is je organisatie of een specifiek(e) persoon/afdeling binnen je organisatie verantwoordelijk voor de verwerking en in de zin van de Wbp een

verantwoordelijke. Aan de hand van de rest van de vragenlijst kunnen nog compliance risico's worden geïdentificeerd.

1.3: Is het duidelijk wie na afloop van het project verantwoordelijk is voor het in stand houden en evalueren van de getroffen maatregelen?

De 'getroffen' maatregelen zijn bedoeld om de risico's te verkleinen die de PIA identificeert. Deze vraag komt op een raar moment. Het is namelijk nog onduidelijk waar de risico's zich bevinden en dus is het nog onduidelijk wie de maatregelen zou moeten treffen. Met maatregelen worden waarschijnlijk ook bedoeld de maatregelen omschreven in artikel 13 van de Wbp en de naleving ervan in artikel 15, maar ook maatregelen die daar niet onder vallen, maar wel zijn benodigd om compliancy risico's te verkleinen.

Ja: Als het duidelijk is wie er verantwoordelijk is voor de naleving, wil dat impliciet zeggen dat toezicht op naleving ook gedaan zal worden. Het risico dat niet voor naleving gezorgd gaat worden, is dan niet aanwezig. Hier wordt alleen niet duidelijk gemaakt wat concreet wordt bedoeld met de maatregelen, waardoor antwoord 'ja' niet betekent dat er compliance met artikel 15 is.

Nee: Als het niet duidelijk is wie de maatregelen in stand moet houden, zou dat kunnen betekenen dat het niet duidelijk is wie de verantwoordelijke is in de zin van de Wbp. De verantwoordelijke is namelijk volgens artikel 15 van de Wbp verantwoordelijk voor het toezicht op naleving van een aantal artikelen. Dit antwoord zou dan tegenstrijdig zijn met antwoord 'ja' op vraag 1.2. Het kan ook zo zijn dat de verantwoordelijke wel weet dat hij de verantwoordelijke is, maar niet weet wat zijn verplichtingen zijn. Antwoord 'nee' wil dus zeggen: er is een kans op non-compliance.

1.4: Is het doel van de verwerking van persoonsgegevens voldoende SMART omschreven?

Hiermee wordt gedoeld op artikel 7 van de Wbp: *"Persoonsgegevens worden voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden verzameld"*. In het artikel wordt niet gesproken over SMART, maar SMART is een methode hoe je een doel welbepaald en uitdrukkelijk kunt omschrijven.

Ja: Is het doel SMART omschreven, moet er nog altijd een gerechtvaardigd doeleinde voor de verwerking zijn. Is het antwoord dus 'ja', wil dat nog niet betekenen dat er compliance is met artikel 7, alleen gedeeltelijke compliance.

Nee: Is het doel niet precies genoeg omschreven, voldoe je niet aan de wetgeving. Indien het antwoord nee is, is er non-compliance.

1.5: Is er sprake van:
a. Gebruik van nieuwe technologie?
b. Gebruik van technologie die bij het publiek vragen of weerstand op kan roepen?
c. De invoering van bestaande technologie in nieuwe context?

d. (Andere) grote verschuivingen in de werkwijze van de organisatie, de manier waarop persoonsgegevens worden verwerkt en/of de technologie die daarbij gebruikt wordt?

De concepten genoemd in bovenstaande vragen komen nergens concreet terug in de Wbp, maar in veel gevallen is de Wbp van toepassing omdat er toch persoonsgegevens worden verwerkt. Per vraag een toelichting:

a. Dit kunnen gevoelige gegevens zijn die niet per definitie onder de noemer bijzondere persoonsgegevens vallen van artikel 16. Maar ook voor die gegevens geldt dat er aan de eisen van de Wbp voldaan moet worden. Voornamelijk de concepten doelbinding en dataminimalisatie en een wettelijke grondslag zijn van groot belang.

b. In geval van biometrie kunnen dit medische gegevens zijn, gegevens m.b.t. RFID kunnen divers zijn, en profilering heeft te maken met artikel 42, waarin eisen worden gesteld aan besluiten gebaseerd op geautomatiseerde verwerkingen.

c. Concreet zegt de Wbp niks over cameratoezicht of drugscontrole, maar dit zijn toch persoonsgegevens en dus geldt de Wbp gewoon.

d. Als door de manier waarop persoonsgegevens worden verwerkt, nieuwe conclusies kunnen worden getrokken, worden er dus meer persoonsgegevens verzameld. Ook voor die nieuwe persoonsgegevens geldt de Wbp.

Ook is het mogelijk dat er sectorspecifieke zelfregulering of wetgeving is die op de concepten in de vragen in gaat. Artikel 26, lid 1 zegt dat er nadere regels voor bepaalde sectoren kunnen gelden, en artikel 25 zegt dat er gedragscodes kunnen zijn die door het CBP goedkeuring hebben gekregen voor de sector waarin jouw organisatie actief is.

Ja: Het antwoord 'ja' wilt niets zeggen over de mate van compliance met de Wbp. Er zal goed gekeken moeten worden naar de doelen van de verwerkingen en de eventuele nieuwe informatie die wordt gegenereerd over personen. Voor alle vragen geldt dat er goed gekeken moet worden naar compliance.

Nee: Hetzelfde geldt voor antwoord 'nee': voor (bestaande) verwerkingen geldt dat ze moeten voldoen aan de wet. Het verschil met antwoord 'ja' is dat de projecten die met gegevens werken genoemd in a. t/m d., gevoeliger liggen bij de betrokkene en toezichthouders en handhavers en deze eerder weerstand zullen leveren of terughoudend zijn met het geven van toestemming.

1.5: Is er sprake van:
e. Een nieuwe verwerking van persoonsgegevens?
f. Het verzamelen van meer of andere persoonsgegevens dan voorheen of een nieuwe manier van verzamelen?
g. Gebruik van al verzamelde gegevens voor een nieuw doel of een nieuwe manier van gebruiken?

Deze drie vragen verwijzen naar een nieuwe situatie waarin meer gegevens voor hetzelfde doel, dezelfde gegevens voor andere of meerdere doelen, of beiden, worden gebruikt. In een nieuwe situatie zal je, net als in de oude situatie, moeten voldoen aan de Wbp. Dus zal je moeten nagaan of je compliant bent met de Wbp. Indien de verwerking dusdanig verandert als in één van de drie vraagstellingen wordt geschetst, wordt een compliance check aangeraden.

Ja: Wanneer een van de hierboven omschreven nieuwe situaties het geval is wordt een compliance check aangeraden. Het antwoord 'ja' zorgt er dan natuurlijk voor dat alle artikelen van de Wbp aan de orde komen.

Nee: Wanneer op een van de vragen het antwoord 'nee' is, zal er weinig tot niets veranderd zijn aan de al bestaande verwerking van persoonsgegevens. Maar als dit verkeerd in wordt geschat, kan de conclusie getrokken worden dat er geen grondige compliance check nodig is terwijl er wel iets verandert. Het antwoord 'nee' betekent overigens niet dat de bestaande verwerking van persoonsgegevens compliant is met de Wbp. Hoewel de vragenlijst vooral bedoeld is om te toetsen of nieuwe projecten grondig getoetst moeten worden (middels een compliance check), stel ik als uitgangspunt dat de vragenlijst alle situaties zou moeten toetsen op compliance. In dat geval schiet de vragenlijst tekort, omdat bestaande situaties van grondige toetsing (compliance check) worden vrijgesteld.

1.6: Heeft u op alle bovenstaande (a t/m g) nee geantwoord?

Ja: Wanneer er op alle vragen van 1.5 nee is geantwoord, wordt verondersteld dat het privacyrisico voor de verwerking zo laag is, dat de vragenlijst verder doorlopen van weinig waarde is. Er wordt wel benadrukt dat compliance met de Wbp nog niet is gegarandeerd, dus dat moet buiten het verkleinen van de risico's nog worden nagegaan. Het antwoord wil daarom niets zeggen over compliance. Omdat ik de vragenlijst analyseer op validiteit m.b.t. de Wbp, moet ik hier constateren dat een groot gedeelte van de Wbp niet doorlopen zal worden indien het een bestaande verwerking, zonder nieuwe technologieën betreft.

Nee: Als het een verwerking betreft met nieuwe technologieën, maar niet in een nieuwe situatie met nieuwe verwerkingen (vrij geïnterpreteerd), dan zal de vragenlijst verder wel uitgevoerd worden, maar zal er geen compliance check worden gedaan. Er zullen dan niet alle artikelen van de Wbp worden nagelopen, alleen die wat in de PIA zijn verwerkt. Om te achterhalen welke dat zijn, lopen we de vragenlijst verder door.

1.7: Is er (naast de Wbp) veel wet en regelgeving ten aanzien van persoonsgegevens waar het project mee te maken heeft?

De toelichting bij deze vraag doelt op alle regelgevende aspecten die bij de Wbp komen kijken. Sectorale wetgeving kan nadere regels stellen aan de Wbp (artikel 26), gedragscodes goedgekeurd door het CBP kunnen gelden voor jouw sector (artikel 25), algemene maatregelen van bestuur kunnen van toepassing zijn (gehele Wbp), jurisprudentie kan invulling geven aan de onduidelijkheid van de Wbp, en er zijn internationale aspecten van de Wbp (artikel 76 en 77). Deze open eindes van de Wbp vallen echter buiten de scope van dit onderzoek, omdat alleen de

pure vorm van de Wbp in de analyse is meegenomen. Andere wetgeving is dus niet relevant. De antwoorden op deze vraag hebben verder geen functie, want er worden geen vragen uitgesloten.

1.8: Zijn er veel maatschappelijke belanghebbenden?

Deze vraag behandelt geen Wbp gerelateerde aspecten. De antwoorden sluiten geen vragen uit dus het antwoord is niet relevant.

1.9: Zijn er veel partijen betrokken bij de uitvoering van het project?

Hier gaat het erom of het duidelijk is welke verantwoordelijkheden elke partij heeft en of ze deze nakomen. Elke partij die niet zorgvuldig met gegevens omgaat, is een risico. Dit heeft natuurlijk alles met de Wbp te maken, maar behandeld geen artikel specifiek. Om na te gaan of er compliance is, zijn verdere vragen benodigd.

Ja: Indien er veel partijen zijn betrokken bij het project, maar deze houden zich allen netjes aan de afspraken, is er geen risico. Om echt na te gaan of er een risico is, zijn meer specifieke vragen benodigd.

Nee: Indien er weinig partijen zijn betrokken bij het project, maar deze houden zich niet aan de afspraken, is er wel een risico. Net als bij antwoord 'ja', zijn er meer vragen benodigd om te constateren dat er een risico is.

1.10: Is er een geschillenregeling/partij waar betrokkene terecht kan bij vragen of klachten?

Deze vraag heeft raakvlakken met gedragscodes (bedoeld in artikel 25) waarin eventueel ook de afhandeling van geschillen wordt besproken. Verder verplicht de Wbp geen partij aan te stellen in geval van klachten, het voorziet alleen in de beschrijving van de rechten die een betrokkene heeft. In geval van een geschil tussen belanghebbende en verantwoordelijke met betrekking tot een bestuurlijk besluit van de verantwoordelijke, kan de belanghebbende zich ook tot het CBP richten.

Ja: Indien er een geschillenregeling is, zal de verantwoordelijke zich hierbij moeten aansluiten. Of de verantwoordelijke dit doet wordt echter niet vastgesteld bij deze vraag. Aangezien bij dit onderzoek de gedragscodes niet worden meegenomen, wordt dit niet gezien als een punt waarbij de vragenlijst tekort schiet in het achterhalen van compliance.

Nee: Een ingericht contactpunt voor klachten wordt niet verplicht in de Wbp. Je dient echter wel te reageren op verzoeken van betrokkenen die worden omschreven in de Wbp. Er is dus geen compliancy risico indien het antwoord 'nee' is. De Wbp verwijst wel naar gedragscodes met een geschillenregeling, waarin het misschien verplicht wordt om een contactpunt voor geschillen in te richten. De gedragscodes vallen buiten dit onderzoek, dus wordt dit niet gezien als een punt waarin de vragenlijst tekort schiet in het achterhalen van compliance.

2.1: Zijn alle gegevens nodig om het doel te bereiken (worden er zo min mogelijk gegevens verzameld)?

De vraag heeft te maken met het principe dataminimalisatie. Als het doel ook bereikt kan worden met minder gegevens, dienen er minder gegevens te worden verzameld. In de Wbp wordt dit omschreven in artikel 11, lid 1. Persoonsgegevens dienen toereikend, ter zake dienend en niet bovenmatig te zijn.

Ja: Als het antwoord 'ja' is, is er sprake van compliance. De toelichting zorgt ervoor dat het vrij duidelijk is wat met zo min mogelijk bedoeld wordt, dus kan er niet getwijfeld worden aan de conclusie dat er compliance is met artikel 11, lid 1.

Nee: Als het antwoord 'nee' is, dan is sprake van non-compliance met artikel 11, lid 1.

2.2: Kan het doel met geanonimiseerde of gepseudonimiseerde gegevens worden bereikt (terwijl daar op dit moment geen gebruik van wordt gemaakt)?

Ja: Wanneer deze vraag met ja wordt beantwoord, bestaat er de mogelijkheid om de verwerking niet onder de Wbp te vallen. Is dat het geval, heeft het geen zin om te checken of men compliant is met de Wbp. Er dient dan wel goed te worden nagegaan of de gegevens niet indirect herleidbaar zijn naar een persoon. Als de gegevens worden geanonimiseerd, is de Wbp niet meer van toepassing. Daarmee is het verder toepassen van de vragenlijst eigenlijk niet nodig, terwijl dit niet wordt aangegeven bij het antwoord.

Als ze niet worden geanonimiseerd, terwijl dat wel tot de mogelijkheden behoort, is er sprake van non-compliance met artikel 11. Lid 1. Dus als er toch tot een uniek persoon herleidbare gegevens worden gebruikt, terwijl dat om het doel te bereiken niet nodig is, is er non-compliance.

Nee: Wanneer deze vraag met nee beantwoord wordt, dient toch compliance met de Wbp te worden bewerkstelligd. Maar dit hebben we bij vraag 1.1 al vastgesteld. Daarom dekt deze vraag verder geen inhoud van de Wbp af. We gingen er namelijk al vanuit dat er persoonsgegevens verwerkt worden.

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)?

Deze vraag gaat in op een verplichting die valt onder artikel 22. Het gaat om een volgsysteem, waarbij mogelijk strafrechtelijke gegevens over het gedrag worden verzameld die in het geval van personeelsgegevens vallen onder de noemer bijzondere persoonsgegevens en dus het verbod van artikel 16. Ook heeft de vraag raakvlakken met een geautomatiseerd systeem waarop een besluit genomen wordt, zoals bedoeld in artikel 42.

Ja: Als de gegevens die worden verzameld strafrechtelijke gegevens zijn, en ze vallen niet onder de uitzonderingen van artikel 22, is er non-compliance. De strafrechtelijke gegevens omschreven in artikel 22 mogen alleen onder bepaalde voorwaarden verwerkt worden. Om dit vast te stellen zijn echter nog aanvullende vragen vereist. Met dit antwoord is alleen vastgesteld dat er mogelijk strafrechtelijke gegevens worden verzameld.

Nee: Het antwoord 'nee' geeft alleen aan dat er waarschijnlijk geen strafrechtelijke gegevens worden verzameld, dus is het verbod van artikel 16 niet van toepassing, wat deze vorm van bijzondere persoonsgegevens betreft.

2.4.a: Is er sprake van verwerken van bijzondere persoonsgegevens?

Deze vraag gaat over artikel 16 Wbp. Wanneer bijzondere persoonsgegevens verwerkt worden dient er een aanvullende wettelijke grondslag te zijn, bovenop de wettelijke grondslag bedoeld in artikel 8.

Ja: Met het antwoord 'ja' op deze vraag wordt alleen vastgesteld dat er een kans op non-compliance is. Om na te gaan of er compliance is zijn aanvullende vragen over de uitzonderingen (art. 17 t/m 23) op het verbod (art. 16) vereist.

Nee: Als het antwoord 'nee' is, is vastgesteld dat artikel 16 t/m 23 niet van toepassing zijn. Men is dan ook compliant met deze artikelen.

2.4.b: Is er sprake van verwerken van uniek identificerende gegevens?

Met deze vraag wordt het verbod op medische gegevens bedoeld, in het bijzonder de medische gegevens die erfelijke eigenschappen van een betrokkene beschrijven (artikel 21, lid 4).

Ja: Als het antwoord 'ja' is, is alleen vastgesteld dat er een kans op non-compliance is. Er wordt wel aangegeven dat de verwerking alleen is toegestaan onder bepaalde wettelijke voorwaarden, maar aanvullende vragen zijn vereist om na te gaan of aan deze voorwaarden is voldaan.

Nee: Als het antwoord 'nee' is, is er compliance met een gedeelte van artikel 21.

2.4.c: Is er sprake van verwerken van een wettelijk voorgeschreven persoonsnummer?

Met deze vraag wordt bedoeld *"een nummer dat ter identificatie van een persoon bij wet is voorgeschreven"* zoals dat wordt omschreven in artikel 24.

Ja: Het antwoord ja op deze vraag betekent dat er moet worden nagegaan of er een wettelijke grondslag is. Daarnaast zou men moeten kijken of er aanvullende eisen worden gesteld aan de verwerking in een algemene maatregel van bestuur. Deze valt echter buiten de vraagstelling, dus zijn aanvullende vragen vereist.

Nee: Het antwoord 'nee' betekent dat er compliance is met artikel 24.

2.4.d: Is er sprake van verwerken van andere gegevens dan hiervoor beschreven waarvoor geldt dat sprake is van een (gepercipieerde) verhoogde gevoeligheid?

In de toelichting worden meerdere voorbeelden genoemd. Een daarvan is 'gegevens waarvoor een geheimhoudingspicht geldt'. Al die voorbeelden worden niet expliciet genoemd in de Wbp, behalve gegevens waarvoor een geheimhoudingsplicht geldt. Deze mogen volgens artikel 9, lid 4 niet verwerkt worden.

Ja: Voor deze gegevens kan een gedragscode of andere wet en regelgeving gelden, maar deze vallen buiten deze validiteitsanalyse. Dit betekent dat er in de afweging van artikel 13 (beveiligingsmaatregelen) hogere eisen worden gesteld. Om te bepalen of hieraan wordt voldaan zijn aanvullende vragen vereist. Als uit het antwoord blijkt dat er een geheimhoudingsplicht geldt, wordt er niet aangegeven dat er non-compliance is, terwijl dat op grond van artikel 9, lid 4 wel zo is.

Nee: Het antwoord 'nee' op deze vraag betekent dat er geen geheimhoudingsplicht geldt, en dus wordt voldaan aan compliance met artikel 9, lid 4.

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?

Deze vraag is een herhaalvraag over dataminimalisatie (zie vraag 2.1). Hier wordt gevraagd of er **andere** gegevens gebruikt kunnen worden om hetzelfde doel te bereiken. Het heeft ook met de hoeveelheid van gegevens te maken, aangezien er gevoeligere gegevens verwerkt worden dan nodig is om het doel te bereiken. Gevoeliger betekent dat de gegevens meer prijsgeven over een persoon dan nodig is. Impliciet betekent het dus dat er meer gegevens worden verwerkt dan nodig is. Het gaat over hetzelfde artikel van de Wbp, namelijk artikel 11, lid 1.

Ja: Er is non-compliance met artikel 11, lid 1.

Nee: Als alle gegevens nodig zijn om het doel te bereiken, is er compliance met art. 11, lid 1.

2.5: Verwerkt u gegevens over kwetsbare groepen of personen?

In de toelichting worden genoemd: minderjarige personen, verstandelijk gehandicapten, gedetineerden, onder toezicht gestelden, en mensen van wie de fysieke veiligheid in gevaar is. Voor sommigen van de net opgesomde personen geldt volgens artikel 5, lid 1 dat in geval de verwerking gebaseerd is op toestemming, de toestemming van een wettelijk vertegenwoordiger vereist is. Deze toestemming kan te allen tijden worden ingetrokken (lid 2). Dit geldt ook voor betrokkenen die niet onder de opgesomde personen vallen.

Ja: Indien het een van de personen betreft die in artikel 5, lid 1 worden genoemd, geldt er een verplichting voor de verantwoordelijke. Deze wordt niet genoemd in het antwoord. Er zijn dus aanvullende vragen vereist om dit na te gaan.

Nee: Als er geen gegevens worden verzameld over de opgesomde personen, is er compliance met artikel 5, lid 1.

2.6: Hebben de gegevens betrekking op de gehele of grote delen van de bevolking?

In de Wbp wordt niet gesproken over verwerkingen op grote schaal. Het enige dat impliciet in de wet staat is dat er passende maatregelen genomen moeten worden (artikel 13) gelet op de stand van de techniek, de kosten van de uitvoering en de risico's die de verwerking en de aard van de gegevens met zich mee brengen. Onnodige verzameling en verdere verwerking moeten voorkomen worden. Indien het antwoord ja is, staat er: *"U loopt een verhoogd risico. De kans op*

misbruik van de gegevens wordt groter naarmate u meer gegevens verwerkt." Als 'meer gegevens' wordt gelezen in de zin van de vraag, heeft dat als betekenis dat er puur van **meer personen** gegevens worden verzameld, niet meer gegevens per persoon. Dit betekent dat de beveiligingsmaatregelen moeten inspelen op bedreigingen van kwaadwillenden. Denk aan fysieke splitsing van de gegevens en een duidelijk autorisatiebeleid. Met de vraag wordt deze afweging echter niet beoordeeld.

Ja: Indien het antwoord ja is, is alleen vastgesteld dat er een grotere kans op non-compliance is, omdat de lat voor de afweging van beveiligingsmaatregelen hoger ligt.

Nee: Dit antwoord wil niets zeggen over compliance.

3.1: Zijn er (na afronding van het project) bij het verzamelen en verder verwerken van de gegevens meerdere interne partijen betrokken?

Ongeacht het antwoord op deze vraag, mogen persoonsgegevens alleen worden verwerkt onder de verantwoordelijkheid van de verantwoordelijke of de bewerker. Als dit nog niet het geval was uit hoofde van ambt, beroep of wettelijke verplichting geldt er een geheimhoudingsplicht voor gegevens die onder dezelfde verantwoordelijkheid worden verwerkt. De verantwoordelijke verwerkt persoonsgegevens alleen als hij daarvoor een wettelijke grondslag heeft. Wanneer er meerdere interne partijen bij zijn betrokken, dient er dus voor gezorgd te worden dat het hierboven besprokene in stand wordt gehouden.

Ja: Indien het antwoord op deze vraag ja is, wordt dus alleen vastgesteld dat er een hogere kans op non-compliance is.

Nee: De kans op non-compliance is kleiner.

3.2: Zijn er (na afronding van het project) bij het verzamelen en verder verwerken van de gegevens meerdere externe partijen betrokken?

Dezelfde redenering die voor de vorige vraag geldt, is hier ook van toepassing. Daarbij komt ook nog kijken dat externe partijen niet zomaar onder de directe verantwoordelijkheid vallen van de verantwoordelijke, tenzij het een bewerker is. Met een bewerker dienen dan duidelijke contractuele afspraken te worden gemaakt, zodat de huidige organisatie als het ware wordt uitgebreid naar de bewerker voor wat betreft de verwerking van persoonsgegevens. Die contractuele afspraken dienen onder andere de maatregelen van artikel 13 af te dwingen op de bewerker. Het kan ook zijn dat de externe partij zelf een verantwoordelijke is. Maar dan dient deze zelf zorg ervoor te dragen dat hij de gegevens op grond van de wet, en met een goede beveiliging verwerkt. Het valt dan niet meer onder de verantwoordelijkheid van de oorspronkelijke verantwoordelijke.

Ja: Indien het antwoord op deze vraag 'ja' is, wil dat zeggen dat de kans op non-compliance aanwezig is.

Nee: Is het antwoord 'nee', is die kans ook aanwezig, maar deze is kleiner.

3.2.1: Zijn er partijen betrokken (in het project of bij de verwerking) die zich niet aan met Nederland vergelijkbare privacywetgeving hoeven te houden?

Deze vraag gaat over de verwerking van gegevens buiten landen van de Europese Economische Ruimte (EER).

Ja: Indien het antwoord 'ja' is dient een aantal dingen te worden nagegaan die in de toelichtingen van de vraag en het antwoord worden beschreven (bron artikel 76). Aanvullende vragen zouden kunnen nagaan of er compliance met de Wbp is. Artikel 77 is hierbij ook van belang. Nu wordt bij antwoord ja alleen vastgesteld of er een kans op non-compliance is.

Nee: Indien het antwoord 'nee' is, worden gegevens verwerkt binnen Nederland, of een land binnen de EER. Er is dan compliance met artikel 76 en 77.

3.2.2: Is de verstrekking van de gegevens aan derde partijen in lijn met het doel waarvoor de gegevens oorspronkelijk zijn verzameld?

Het verstrekken van gegevens aan derden is een vorm van een verwerking van gegevens. Voor alle verwerkingen geldt dat het doel in lijn moet zijn met het doel waar de gegevens voor verzameld worden, tenzij het een uitzondering is. Dit staat omschreven in artikel 9, lid 1 en 2 en wordt vaak aangehaald als 'doelbinding'. Bij deze vraag wordt echter alleen naar de doelbinding gevraagd van een specifieke vorm van verwerking, namelijk verstrekking aan derden (uit de toelichting kan worden geïnterpreteerd worden dat bewerkers ook worden bedoeld). Bij deze vraag wordt echter wel direct gevraagd of er compliance is met artikel 9, lid 1 en 2 voor de verwerking. De beoordeling of er doelbinding is, moet de invuller zelf maken op basis van een aantal criteria (artikel 9, lid 2). Er zijn echter nog uitzonderingen op artikel 9, die staan in artikel 43.

Ja: Indien antwoord 'ja' is gegeven, zou er compliance moeten zijn met artikel 9, lid 1 en 2, voor de specifieke verwerking van de gegevens: verstrekking van de gegevens aan derden (inclusief bewerkers). Artikel 41 wordt onterecht uitgesloten (zie volgende vraag).

Nee: Als er 'nee' wordt geantwoord, is er kans op non-compliance met artikel 9, lid 1 en 2, m.b.t. de verstrekking aan derden (inclusief bewerkers). Aanvullende vragen zijn vereist om vast te stellen of de uitzonderingen van artikel 43 gelden.

3.2.3: Worden de gegevens verkocht aan de derde partijen?

Deze vraag heeft te maken met artikel 41. Wanneer uit de vorige vraag blijkt dat de verstrekking in lijn is met het oorspronkelijke doel van de verwerking, wordt deze vraag onterecht overgeslagen. Als het verkopen van gegevens aan derden voor commerciële of charitatieve doelen het gerechtvaardigde doel is dat in lijn is met het doel bij verzamelen, moet deze vraag toch worden behandeld. De voorwaarden die de Wbp stelt aan een verwerking met dat doel zijn namelijk ook van toepassing wanneer er wel doelbinding is.

Ja: Als antwoord 'ja' van toepassing is, kan afhankelijk van de situatie een aantal verplichtingen gelden. Aanvullende vragen zijn vereist om na te gaan of er compliance is.

Nee: Indien antwoord 'nee' van toepassing is, is vastgesteld dat artikel 41 niet van toepassing is en er dus compliance is.

4.1: Kan de manier waarop de gegevens worden verzameld worden opgevat als privacy gevoelig?

Deze vraag heeft verschillende raakvlakken met de Wbp. Privacy gevoelig is niet duidelijk gespecificeerd, maar uit de toelichting kan worden opgemaakt dat heel diverse manieren worden bedoeld. De Wbp geldt hoe dan ook voor de gevallen die worden genoemd in de toelichting zolang het persoonsgegevens betreft. Voor die manieren van verzamelen zal de betrokkene zelf ook een afweging moeten maken of hij de gegevens allemaal wil prijsgeven in ruil voor de dienst die hij ervoor terugkrijgt. Hoe gevoeliger de gegevens en de manier van verzamelen, hoe hoger de lat zal liggen bij het maken van de afweging van het niveau van beveiliging (artikel 13).

Ja: Aanvullende vragen zijn vereist om iets te kunnen zeggen over de mate van compliance.

Nee: Ook voor niet privacy gevoelige gegevens en manieren van verzamelen moet een passend niveau van beveiliging zijn. Aanvullende vragen zijn vereist om de mate van compliance te kunnen vaststellen.

4.2: Is het doel van het verzamelen van de gegevens publiekelijk bekend of kan het publiekelijk bekend gemaakt worden?

Deze vraag heeft raakvlakken met de meldingsplicht die te vinden is in artikel 32 van de Wbp. Een organisatie zal na moeten gaan of het verplicht is de verwerking te melden bij het CBP of een functionaris gegevensbescherming. Dit staat in het Vrijstellingsbesluit, dat buiten deze analyse valt. Is een organisatie niet verplicht om de verwerking te melden, kan het alsnog overwegen dat te doen. Voordat een organisatie kan overwegen of het gaat melden, zal het eerst na moeten gaan of melding verplicht is.

Ja: Dit antwoord zegt niets over compliancy omdat niet duidelijk is of melding verplicht is. Daar zijn meer vragen voor benodigd.

Nee: Dit antwoord zegt niets over compliancy omdat niet duidelijk is of melding verplicht is. Daar zijn meer vragen voor benodigd.

4.3: Verzamelt u de gegevens op basis van een van de wettelijke grondslagen?

Deze vraag heeft alles te maken met artikel 8.

Ja: Als het antwoord 'ja' is, ben je compliant met artikel 8.

Nee: Als het antwoord 'nee' is, is er niet zomaar een risico op non-compliance, maar ben je non-compliant.

4.3.1: Is duidelijk of u de gegevens verzamelt op basis van toestemming (opt-in) of op basis van een andere grondslag (opt-out)?

Deze vraag is verwarrend. Met antwoord 'nee' wordt waarschijnlijk bedoeld dat er een andere grondslag is voor de verwerking dan toestemming. Letterlijk gezien wordt er iets anders gevraagd.

Ja: Indien het antwoord 'ja' is, heeft de betrokkene toestemming gegevens voor de verwerking. Aanvullende vragen zijn benodigd om compliancy te kunnen vaststellen.

Nee: Indien het antwoord 'nee' is, kan de betrokkene bezwaar maken tegen de verwerking. Er wordt geen compliance vastgesteld, daar zijn aanvullende vragen voor nodig.

4.3.2: Indien u toestemming aan de betrokkene vraagt (opt-in) kunnen de betrokkenen de toestemming op een later tijdstip intrekken (opt-out)?

Deze vraag doelt op artikel 5, lid 2: *"Een toestemming kan door de betrokkene of zijn wettelijk vertegenwoordiger te allen tijde worden ingetrokken"*.

Ja: Antwoord 'ja' wil zeggen dat er compliance is met deze specifieke verplichting.

Nee: Antwoord 'nee' wil zeggen dat er non-compliance is.

4.3.3: Is de impact van het intrekken van de toestemming groot voor de betrokkene?

Deze vraag kan ook worden opgevat als: Is de toestemming (die als wettelijke grondslag wordt gebruikt) geen **vrije** wilsuiting? Als de verwerking is gebaseerd op toestemming en de gebruiker wordt min of meer gedwongen om deze te geven omdat hij anders de dienst niet kan gebruiken, is het in feite geen toestemming in de zin van artikel 8 en artikel 1, lid i. De verwerking is dan onrechtmatig. De toelichting van antwoord 'nee' in de vragenlijst staat bij antwoord 'ja' en andersom.

Ja: Als het antwoord op de vraag 'ja' is, kan de verwerking dus onrechtmatig zijn, dus kan er non-compliance zijn. Aanvullende vragen zijn vereist om dit na te gaan.

Nee: Er wordt vanuit gegaan dat als de impact klein is, dat het een vrije wilsuiting is. Dit hoeft niet zo te zijn. Aanvullende vragen zijn vereist om compliance vast te stellen.

4.4: Vertelt u tegen de betrokkene dat de gegevens worden verzameld?

Deze vraag heeft raakvlakken met informatieverstrekking aan de betrokkene. Deze vraag stelt vast of dit gedaan wordt.

Ja: Aanvullende vragen zijn vereist, daarom wordt verwezen naar vraag 4.4.2.

Nee: Aanvullende vragen zijn vereist. Daarom wordt verwezen naar vraag 4.4.1.

4.4.1: Bij nee: Kunnen de betrokkenen op de hoogte zijn van het verzamelen van de gegevens?

Ja: Informatieverstrekking is mogelijk. Aanvullende vragen zijn benodigd om vast te stellen of er compliance is.

Nee: Als de betrokkenen niet op de hoogte kunnen zijn van de verwerking, is er niet gelijk een compliance issue. Hiervoor zijn aanvullende vragen vereist.

4.4.2: Bij Ja (op vraag 4.4): Vertelt u tegen de betrokkene waarom de gegevens worden verzameld (wat u er mee gaat doen)?

Deze vraag heeft raakvlakken met artikel 33 en 34, waarin wordt omschreven aan welke eisen informatieverstrekking dient te voldoen.

Ja: In geval van informatieverstrekking dient naast de doeleinden van de verwerking nog meer te worden meegedeeld, maar dit wordt niet gevraagd. Met deze vraag wordt dus gedeeltelijk vastgesteld in hoeverre er compliance is m.b.t. informatieverstrekking (artikel 33/34).

Nee: Indien niet wordt meegedeeld wat de doeleinden zijn, kan het zo zijn dat informatieverstrekking niet vereist is. Aanvullende vragen zijn vereist om compliance vast te kunnen stellen.

4.4.3: Bij ja: (op vraag 4.4): Vertelt u tegen de betrokkene aan wie de gegevens worden verstrekt (daar waar dit geen wettelijke verplichting is)?

Zoals de vraag zelf al aangeeft, is het meedelen van de ontvangers van de gegevens waarschijnlijk niet verplicht. Artikel 33, lid 2 en 34, lid 2 verplichten bij informatieverstrekking o.a. het volgende: "*nadere informatie voor zover dat gelet op de aard van de gegevens, de omstandigheden waaronder zij worden verkregen of het gebruik dat ervan wordt gemaakt, nodig is om tegenover de betrokkene een behoorlijke en zorgvuldige verwerking te waarborgen."* Het verstrekken van de ontvangers valt daar waarschijnlijk niet onder. Als de betrokkene een verzoek om inzage van zijn gegevens plaatst, ben je wel verplicht mee te delen wie de ontvangers zijn. Ik ga ervan uit dat dit ook wordt bedoeld in de vraagstelling, aangezien artikel 33 en 34 al zijn behandeld in voorgaande vragen.

Ja: Het antwoord 'ja' zegt iets over compliance. Wanneer de betrokkene erom vraagt wordt hem medegedeeld aan wie de gegevens worden verstrekt. Dit betekent gedeeltelijke compliance met artikel 35, lid 2.

Nee: Het antwoord 'nee' zegt niets over compliance. Daar zijn aanvullende vragen voor vereist.

4.5: Zou de betrokkene kunnen worden verrast door de verwerking (op het moment dat hij daarover wordt geïnformeerd)?

Deze vraag gaat in op de verwachtingen van een betrokkene. Als de verwachtingen van de betrokkene niet overeen komen met de werkelijke verwerking, kan hij bij informatieverstrekking verrast worden en weerstand leveren. Daarom is het goed om transparant te zijn naar de betrokkene over de verwerking en de doelen van de verwerking, nog voor de gegevens worden

verzameld. Als je compliant bent met de Wbp zal je die afwegingen al gemaakt hebben en ervoor gezorgd hebben dat de betrokkene nergens door verrast zal worden. Deze vraag heeft echter nergens concrete uitwerkingen in de Wbp, dus het antwoord zal niets zeggen over de mate van compliance.

Ja: Dit antwoord zegt niets over de mate van compliance. Het wil alleen iets zeggen over de kans op eventuele terugtrekking van toestemming of bezwaar op de verwerking.

Nee: Dit antwoord zegt niets over de mate van compliance. Het wil alleen iets zeggen over de kans op eventuele terugtrekking van toestemming of bezwaar op de verwerking.

5.1: Is het gebruik van de gegevens verenigbaar (in lijn) met het doel van het verzamelen?

Deze vraag omvat het begrip doelbinding. Doelbinding houdt in dat de werkelijke verwerking in lijn moet zijn met het doel van de verwerking, dat verenigbaar moet zijn met het doel van de verwerking op het moment van verzamelen. Doelbinding is omschreven in artikel 9, lid 1 en 2. Dit dient voor elk gegeven te worden nagegaan. Tenzij de verdere verwerking onder bepaalde voorwaarden voor historische, statistische of wetenschappelijke doelen geschiedt en er geen geheimhoudingsplicht in de weg staat, mogen gegevens dus alleen gebruikt worden voor de doelen die bij verzameling duidelijk zijn gespecificeerd. Gebeurt dit toch, is er non-compliance.

Ja: Is het antwoord 'ja', is er compliance met artikel 9, lid 1 en 2.

Nee: Wordt er met 'nee' geantwoord op deze vraag is er vastgesteld dat er wellicht non-compliance is. Er zijn nog uitzonderingen waarbij er geen doelbinding hoeft te zijn. De uitzonderingen worden niet in de toelichting of vraagstelling genoemd. Aanvullende vragen zijn vereist.

5.2: Worden gegevens gebruikt voor andere bedrijfsprocessen of doelen dan waar ze oorspronkelijk voor verzameld zijn?

Deze vraag dient naar mijn idee meer als controlevraag op vraag 5.1 want in principe is deze al beantwoord. Deze vraag gaat weer in op doelbinding, artikel 9 lid 1 en 2 van de Wbp. Het gebruik van de gegevens voor andere bedrijfsprocessen of doelen dan het doel bij verzameling kan betekenen dat de doelen niet verenigbaar zijn. Maar dit wordt niet specifiek gevraagd. Dit wordt gevraagd bij vraag 5.2.1.

Ja: Indien het antwoord 'ja' is op deze vraag impliceert dat een kans op non-compliance. Aanvullende vraag 5.2.1 is vereist.

Nee: Bij antwoord 'nee' is nogmaals bevestigd dat er sprake is van doelbinding.

5.2.1: Past het doel van dit bedrijfsproces bij het oorspronkelijke doel van verzamelen?

Het antwoord op deze vraag maakt controlevraag 5.2 compleet.

Ja: Indien het antwoord 'ja' is, is er compliance met artikel 9, lid 1 en 2. Dit is eigenlijk al vastgesteld bij vraag 5.1.

Nee: Is het antwoord nee, betekent dit dat er non-compliance is.

5.3: Is de kwaliteit van de gegevens gewaarborgd, dat wil zeggen: zijn de gegevens actueel, juist en volledig?

De kwaliteit van de gegevens wordt behandeld in artikel 6 en artikel 11, lid 1 en 2. Artikel 6 omschrijft dat ze zorgvuldig verwerkt moeten worden. Artikel 11 omschrijft in lid 1 dat gegevens ter zake dienend moeten zijn, wat impliciet betekent dat ze actueel moeten zijn. Lid 1 omschrijft ook dat gegevens toereikend moeten zijn, wat betekent dat ze volledig moeten zijn. Lid 2 beschrijft dat maatregelen getroffen moeten worden zodat gegevens juist (en nauwkeurig) verwerkt worden. Een kanttekening voor artikel 11 is dat lid 1 en 2 moeten worden opgevat, gelet op de doeleinden waarvoor ze verzameld en vervolgens verwerkt worden. Dit betekent dat gegevens niet altijd de beste kwaliteit hoeven te hebben, zolang ze maar de geschikte kwaliteit hebben met het oog op het doel.

Ja: Antwoord 'ja' duidt op gedeeltelijke compliance met artikel 6, artikel 11, lid 1 en 2.

Nee: Wanneer het antwoord op deze vraag nee is, duidt dat op een kans op non-compliance.

5.4: Worden op basis van de gegevens beslissingen genomen over de betrokkene(n)?

Als er op basis van de gegevens belangrijke beslissingen worden genomen, zal de kwaliteit van de gegevens beter gewaarborgd moeten worden. Worden er geen beslissingen genomen, zal de kwaliteit minder gewaarborgd moeten worden. In vraag 5.4.1 wordt daar dieper op ingegaan. Daarnaast is het zo dat er een besluit kan worden genomen dat de betrokkene aangaat, gebaseerd op alleen een geautomatiseerde verwerking (artikel 42). Dit mag alleen onder bepaalde voorwaarden.

Ja: Als er een besluit wordt genomen, zullen er aanvullende vragen gesteld moeten worden om te beoordelen welke artikelen van toepassing zijn. Er is een kans op non-compliance.

Nee: Als er geen beslissingen worden genomen op basis van de persoonsgegevens, zal de kwaliteit minder gewaarborgd te hoeven worden. In hoeverre minder, is afhankelijk van de situatie. In ieder geval worden er geen geautomatiseerde besluiten genomen, dus is artikel 42 niet van toepassing.

5.4.1: Bij ja: leveren de gegevens een volledig en actueel beeld van de betrokkenen op?

Dit is in principe dezelfde vraag als 5.3, alleen is nu duidelijk dat de kwaliteit van de gegevens goed gewaarborgd moet zijn. Het is lastig om te bepalen of de kwaliteit genoeg is gewaarborgd, omdat een afdoend niveau van gegevenskwaliteit zeer context-specifiek is.

Ja: Antwoord 'ja' duidt op gedeeltelijke compliance met artikel 6, artikel 11, lid 1 en 2. Daarnaast zijn aanvullende vragen benodigd om na te gaan of er geautomatiseerde beslissingen worden genomen over de betrokkene.

Nee: Er is een kans op non-compliance. Aanvullende vragen zijn vereist om te beoordelen of de kwaliteit afdoende wordt gewaarborgd. Daarnaast zijn aanvullende vragen benodigd om na te gaan of er geautomatiseerde beslissingen worden genomen over de betrokkene.

5.5: Is sprake van koppeling, verrijking of vergelijking van gegevens uit verschillende bronnen?

De toelichting in geval van antwoord 'ja' noemt het risico dat de gegevens worden gebruikt voor andere doelen dan waar ze voor verzameld zijn, voor of nadat het oorspronkelijke doel is behaald. Bewaartermijnen worden aangedragen als maatregel om misbruik tegen te gaan nadat het oorspronkelijke doel is behaald. Doelbinding is naar mijn idee de maatregel die voorkomt dat gegevens niet worden gebruikt voor andere doelen waarvoor ze zijn verzameld, voordat het oorspronkelijke doel is behaald. Bewaartermijnen zijn echter volgens de wet in de meeste gevallen verplicht, en doelbinding is ook volgens de wet verplicht. Doelbinding is al behandeld in vraag 5.1. Bewaartermijnen worden behandeld in onderdeel 6 van de vragenlijst.

Ja: Indien gegevens op deze manier worden verwerkt, dient goed te worden nagegaan of er doelbinding is, en of bewaartermijnen worden gehanteerd. Verder kun je geen conclusie trekken naar aanleiding van dit antwoord.

Nee: Indien antwoord 'nee', is er geen kans op non-compliance wat betreft deze verwerking van persoonsgegevens.

5.6: Worden gegevens breed verspreid binnen de organisatie?

In principe is deze vraag vergelijkbaar met vraag 3.1. De conclusie daar is:

Ongeacht het antwoord op deze vraag, mogen persoonsgegevens alleen worden verwerkt onder de verantwoordelijkheid van de verantwoordelijke of de bewerker. Als dit nog niet het geval was uit hoofde van ambt, beroep of wettelijke verplichting geldt er een geheimhoudingsplicht voor gegevens die onder dezelfde verantwoordelijkheid worden verwerkt. De verantwoordelijke verwerkt persoonsgegevens alleen als hij daarvoor een wettelijke grondslag heeft. Wanneer er meerdere interne partijen bij zijn betrokken, dient er dus voor gezorgd te worden dat het hierboven besprokene in stand wordt gehouden.

Ja: Indien het antwoord op deze vraag ja is, wordt dus alleen vastgesteld dat er een hogere kans op non-compliance is.

Nee: De kans op non-compliance is kleiner.

5.7: Worden gegevens breed verspreid buiten de organisatie?

In principe is deze vraag vergelijkbaar met vraag 3.2. De conclusie daar is:

Dezelfde redenering die voor de vorige vraag geldt, is hier ook van toepassing. Daarbij komt ook nog kijken dat externe partijen niet zomaar onder de directe verantwoordelijkheid vallen van de verantwoordelijke, tenzij het een bewerker is. Met een bewerker dienen dan duidelijke contractuele afspraken te worden gemaakt, zodat de huidige organisatie als het ware wordt

uitgebreid naar de bewerker voor wat betreft de verwerking van persoonsgegevens. Die contractuele afspraken dienen onder andere de maatregelen van artikel 13 af te dwingen op de bewerker. Het kan ook zijn dat de externe partij zelf een verantwoordelijke is. Maar dan dient deze zelf zorg ervoor te dragen dat hij de gegevens op grond van de wet, en met een goede beveiliging verwerkt. Het valt dan niet meer onder de verantwoordelijkheid van de oorspronkelijke verantwoordelijke.

Ja: Indien het antwoord op deze vraag 'ja' is, wil dat zeggen dat de kans op non-compliance aanwezig is.

Nee: Is het antwoord 'nee', is die kans ook aanwezig, maar is deze kleiner. Artikel 34, lid 1 wordt onterecht uitgesloten (zie volgende vraag).

5.7.1: Is het doorgeven van de gegevens aan partijen buiten de organisatie in lijn met de verwachtingen van de betrokkene?

Net zoals in vraag 4.5 wordt hier ingegaan op de verwachtingen van de betrokkene. Met verwachtingen wordt bedoeld, de verwachtingen op basis van de informatieverstrekking aan de betrokkene. De toelichting bij antwoord nee geeft aan dat er een kans is op non-compliance met artikel 34, lid 1, onderdeel b. Deze omschrijft informatieverstrekking in geval van verzameling via een andere partij dan de betrokkene. Artikel 33 wordt niet behandeld, terwijl nog niet is vastgesteld of artikel 33 of 34 van toepassing is. Artikel 33 gaat over informatieverstrekking in het geval de gegevens rechtstreeks bij de betrokkene zijn verzameld. Dit staat in principe los van de verstrekking aan derden. Ook wordt er niet ingegaan op de inhoud van de informatieverstrekking.

Ja: De verwachtingen van de betrokkene zijn nergens verwerkt in de wet. Dat de verwachtingen overeen komen met de informatieverstrekking wil niets zeggen over de mate van compliance van die informatieverstrekking. Daarom is er met dit antwoord nog niet vastgesteld dat er compliance is met artikel 33 of 34.

Nee: Het kan zo zijn dat informatieverstrekking is gedaan en niet overeen komt met de verwachtingen van de betrokkene. Dat wil nog niet zeggen dat de informatieverstrekking niet overeen komt met de wet. Daarom is er met dit antwoord nog niet vastgesteld dat er non-compliance is met artikel 33 of 34.

5.8: Stelt uw organisatie profielen op van de betrokkenen, al dan niet geanonimiseerd?

Ja: Als er aan profilering wordt gedaan, zijn er aanvullende vragen nodig om te beoordelen of dit mag volgens de wet. Zie 5.8.1.

Nee: Als er geen profielen worden opgesteld, is het niet mogelijk om een besluit te nemen gebaseerd op geautomatiseerde verwerkingen met betrekking tot een betrokkene. Artikel 42 is dan niet van toepassing.

5.8.1: Indien profielen worden opgesteld, kan het profiel tot uitsluiting of stigmatisering leiden?

In de Wbp wordt op geautomatiseerde profilering ingegaan in artikel 42. Wanneer aan de hand van een profiel een besluit wordt genomen *"waaraan voor hem rechtsgevolgen zijn verbonden of dat hem in aanmerkelijke mate treft"*, geldt dit artikel. Een dergelijk besluit mag alleen geautomatiseerd genomen worden onder bepaalde voorwaarden.

Ja: Het nemen van beslissingen op basis van profilering mag alleen onder bepaalde voorwaarden (artikel 42, lid 2 en 3). Aanvullende vragen zijn vereist om vast te stellen of hieraan wordt voldaan.

Nee: Wanneer het niet kan leiden tot stigmatisering of uitsluiting, zal het besluit de betrokkene niet in aanmerkelijke mate treffen. Artikel 42 is dan niet van toepassing.

5.9: Kunnen de betrokkenen hun gegevens inzien of daarom vragen?

Deze vraag heeft te maken met het inzagerecht, te vinden in artikel 35, 37, 39 en 43.

Ja: Naast het feit dat betrokkenen het recht op inzage kunnen effectueren, moet de informatieverstrekking aan de betrokkene ook een minimale inhoud hebben. Daar wordt niet op ingegaan in de vraag. Er is dus vastgesteld dat er gedeeltelijke compliance is met bovenstaande artikelen.

Nee: Er is een aantal uitgezonderde situaties waarin de verantwoordelijke niet hoeft te voldoen aan het recht van inzage, die niet in de overweging worden meegenomen. Aanvullende vragen zijn vereist om vast te stellen of er non-compliance is.

5.10: Kunnen de betrokkenen hun gegevens corrigeren of daarom vragen (verbeteren, aanvullen)?

Wat wordt bedoeld in deze vraag is het recht dat betrokkenen kunnen vragen om verbetering, aanvulling, verwijdering, of afscherming van hun persoonsgegevens indien ze feitelijk onjuist, onvolledig of niet meer ter zake dienend zijn voor het doel van de verwerking of de verwerking is in strijd met een wettelijk voorschrift (artikel 36). In deze vraag wordt alleen expliciet gevraagd naar verbeteren of aanvullen. Dit recht is eigenlijk alleen van toepassing als het verzoek om inzage ook van toepassing is. De vraag gaat echter niet in op de uitzonderingen die gelden op het correctierecht (vrijelijk zo genoemd).

Ja: Als ze de mogelijkheid hebben om te verbeteren of aan te vullen zijn er nog aanvullende vragen die doorgelopen moeten worden om na te gaan of er compliance is met artikel 36.

Nee: Er dient nog te worden nagegaan of het inzagerecht ook van toepassing is en of er een uitzondering op artikel 36 van toepassing is, voordat gezegd kan worden dat er gedeeltelijke non-compliance is met artikel 36. Aanvullende vragen zijn benodigd om na te gaan of alle voorwaarden van het correctierecht worden nageleefd.

5.11: Kunnen de betrokkenen hun gegevens verwijderen of daarom vragen?

Deze vraag is een vervolg op vraag 5.10 waarin een onderdeel van artikel 36 wordt behandeld: verwijdering. Er wordt nog steeds geen aandacht besteed aan de uitzonderingen op artikel 36. Daarnaast wordt het gedeelte van artikel 36 dat gaat over het vragen om afscherming niet behandeld, en dit is de laatste vraag van deze categorie.

Ja: Als ze de mogelijkheid hebben om te verbeteren of aan te vullen zijn er nog aanvullende vragen die doorgelopen moeten worden om na te gaan of er compliance is met artikel 36.

Nee: Er dient nog te worden nagegaan of het inzagerecht ook van toepassing is en of er een uitzondering op artikel 36 van toepassing is, voordat gezegd kan worden dat er gedeeltelijke non-compliance is met artikel 36. Aanvullende vragen zijn benodigd om na te gaan of alle voorwaarden van het correctierecht worden nageleefd.

6.1: Is een bewaartermijn voor de gegevens vastgesteld?

In de Wbp wordt het onderwerp bewaartermijn behandeld in artikel 10. Het volgende wordt gezegd: *"Persoonsgegevens worden niet langer bewaard in een vorm die het mogelijk maakt de betrokkene te identificeren, dan noodzakelijk is voor de verwerkelijking van de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt."* Persoonsgegevens zijn per definitie gegevens betreffende een geïdentificeerd of identificeerbaar persoon, dus wanneer ze geanonimiseerd worden geldt artikel 10 niet meer, in ieder geval geldt de Wbp in zijn geheel dan niet meer. Naast de Wbp kan er bijzondere wetgeving gelden die de bewaartermijn voor de persoonsgegevens bepaalt. De vraag doelt op de bewaartermijn die vanuit de wet is ingesteld (soll), niet op de bewaartermijn die de organisatie op dit moment aanhoudt (ist). Maar uit de toelichtingen kan worden afgeleid dat er wordt verwacht om een vergelijking te maken tussen de twee. De vraag kan dan geïnterpreteerd worden als de volgende: "Komt de bewaartermijn die wordt aangehouden overeen met de wettelijk vereiste bewaartermijn?".

Ja: Als het antwoord 'ja' is, is er misschien compliance met artikel 10. Daar zijn nog aanvullende vragen voor nodig, zie 6.2 en 6.3.

Nee: Als het antwoord 'nee' is, kan het nog steeds zo zijn dat de gegevens langer worden bewaard voor een uitzondering op artikel 10. Aanvullende vragen zijn vereist.

6.2: Kunnen de gegevens na afloop van de bewaartermijn fysiek worden verwijderd (uit een bestand) of worden vernietigd (papier)?

Dit heeft raakvlakken met artikel 10. Het is voor compliance niet relevant of gegevens **kunnen** worden verwijderd na afloop van de bewaartermijn, maar of ze dat ook daadwerkelijk worden.

Ja: Aanvullende vragen zijn vereist om vast te stellen of dit gebeurt in compliance met de Wbp, zie vraag 6.3.

Nee: Gegevens hoeven niet altijd volledig te worden verwijderd na afloop van de bewaartermijn. Het gaat er om dat de gegevens geen persoonsgegevens meer zijn na de

bewaartermijn, zodat ze niet meer herleidbaar zijn tot een persoon. Er dient dan ook in de toekomst ervoor gezorgd te worden dat ze niet herleidbaar zijn tot een persoon. Aanvullende vragen zijn dus vereist om vast te stellen of ze met recht niet verwijderd kunnen worden.

6.3: Zo ja, worden de gegevens na verstrijken van de bewaartermijn op een dergelijke manier vernietigd of verwijderd dat ze niet meer te benaderen en te gebruiken zijn?

Deze vraag gaat in op het daadwerkelijke verwijderen nadat de bewaartermijn is afgelopen.

Ja: Dit antwoord wil zeggen dat er compliance is met artikel 10.

Nee: De uitzondering op de bewaartermijn voor historische, statistische of wetenschappelijke doeleinden wordt niet overwogen (artikel 10, lid 2). Aanvullende vragen zijn dus vereist om vast te stellen of er non-compliance is.

7.1: Is sprake van intern geformuleerd beleid over het beveiligen van informatie?

In de Wbp wordt nergens gesproken over beleid, maar uit de vraagstelling en de toelichting kan worden opgemaakt dat deze vraag te maken heeft met artikel 13. De toelichting zegt: *"Beveiligingsbeleid is noodzakelijk voor het maken van keuzes en het effectief en efficiënt nemen van maatregelen die de gegevens beveiligen"*. Vrij geïnterpreteerd: "Is er geen beveiligingsbeleid, is er waarschijnlijk geen compliance met artikel 13." Dit is natuurlijk sterk afhankelijk van de organisatie en de context. In ieder geval wordt met deze vraag niet direct de compliance getoetst.

Ja: Aanvullende vragen zijn vereist om compliance met artikel 13 na te gaan.

Nee: Aanvullende vragen zijn vereist om na te gaan of er non-compliance is met artikel 13. Hiermee komt een einde aan de vragenlijst, hoewel dit niet erg duidelijk blijkt uit de toelichting bij dit antwoord.

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?

In de toelichting wordt een informatiebeveiligingsplan genoemd, wat het beleid zou moeten concretiseren in te treffen maatregelen. De wet geeft echter geen concrete invulling aan de in artikel 13 genoemde passende maatregelen. Vanuit de wet is dus ook niet gemakkelijk vast te stellen of een organisatie compliant is. Dit zal een organisatie zelf goed moeten afwegen. Het zal in ieder geval ervoor moeten zorgen dat er geen datalekken plaatsvinden of grote zwakheden in de beveiliging van de informatie-infrastructuur van de organisatie worden voorkomen.

Ja: Is het antwoord op de vraag 'ja', wil dit nog niet zeggen dat er compliance is omdat dit per context een verschillende afweging is.

Nee: Is het antwoord op de vraag 'nee', zal de kans op non-compliance groter zijn. Aanvullende vragen zijn vereist om dit vast te stellen.

5.3.1 Bevindingen vragenlijst

In deze paragraaf staan bevindingen die zijn opgevallen bij de analyse per vraag en antwoord (stap 2). Deze hebben invloed hebben op de validiteit van de vragenlijst. Naast onderstaande bevindingen over de validiteit van de vragenlijst zijn in bijlage II nog andere aandachtspunten over de vragenlijst opgesomd die door de analyse naar voren zijn gekomen. Die aandachtspunten hebben bijvoorbeeld te maken met het soms onduidelijke verloop van de vragenlijst, maar hebben geen invloed op de validiteit.

5.3.1.1 Onterecht uitgesloten artikelen

Als vraag 3.2.2 met 'ja' wordt beantwoord, wordt vraag 3.2.3 uitgesloten door het verloop van de vragenlijst. Echter kan vraag 3.2.3 kan nog altijd van toepassing zijn als vraag 3.2.2 met 'ja' wordt beantwoord. In vraag 3.2.3 wordt artikel 40 onterecht uitgesloten en wordt dus niet behandeld.

5.3.1.2 Niet behandelde artikelen

Artikel 3 en 4 worden niet behandeld. In vraag 1.1 wordt bij antwoord 'ja' geconcludeerd dat de Wbp van toepassing is, terwijl nog niet is vastgesteld of er sprake is van een uitzondering op de Wbp (artikel 3 en 4).

Zodra vraag 2.4.a met 'ja' beantwoord wordt, is duidelijk dat het verbod op verwerking van bijzondere persoonsgegevens van toepassing is. Om na te gaan of er compliance is, dienen de uitzonderingen op dit verbod te worden nagelopen. Afgezien van enkele verwijzingen naar deze uitzonderingen (2.3, 2.4.b), worden ze niet behandeld. Dit wil zeggen dat artikelen 17 tot en met 23 niet goed worden nagegaan.

De melding aan het CBP/Functionaris voor de Gegevensbescherming en het bijbehorende Voorafgaand Onderzoek over de verwerking van de persoonsgegevens, worden niet behandeld in de vragenlijst afgezien van een enkele verwijzing naar artikel 32 (in vraag 4.2). Dat wil zeggen dat artikel 27 tot en met 32 niet (goed) worden nagegaan.

Artikel 38 en 40 worden niet behandeld in de vragenlijst, en na gedetailleerd onderzoek worden artikel 37 en 39 nauwelijks afgedekt. Artikel 37 tot en met 40 hebben betrekking op de rechten van betrokkenen.

Voor alle niet-behandelde artikelen geldt dat het na invullen van de vragenlijst niet duidelijk is of er compliance is of niet. Dit betekent dat er niet is vastgesteld of true negative of false negative het geval is voor die artikelen. In geval van een false negative kan het zijn dat er verondersteld compliance is, terwijl non-compliance het geval is.

5.4 Stap 3: Analyse van de gehele vragenlijst

Bij de beoordeling van de validiteit van de gehele vragenlijst zouden in theorie alle mogelijke paden van de vragenlijst nagelopen moeten worden. Met een pad wordt bedoeld: een aaneenschakeling van vragen en antwoorden waardoor de vragenlijst op een specifieke manier wordt doorlopen. Een berekening toont aan dat er in totaal meer dan 24×10^{15} paden zijn waardoor het onmogelijk was om elk pad gescheiden door te lopen. Door paden te groeperen in verzamelingen kon vervolgens per verzameling een uitspraak over de validiteit gedaan worden. Die verzamelingen zijn gebaseerd op de mogelijke manieren waarop de vragenlijst kan eindigen. De vragenlijst kan bij vier vragen eindigen. Voor elk van deze mogelijke einden is een verzameling of het totale aantal paden uitgelicht. De berekeningen daarvan alsook de berekening van het bovengenoemde totale aantal paden zijn te raadplegen in bijlage I.

5.4.1 Einde na vraag 1.1

De eerste vraag waarbij de vragenlijst kan eindigen is 1.1. De specifieke conclusie van antwoord 'nee' op vraag 1.1 is: de Wbp is niet van toepassing. Daarmee is vanzelf vastgesteld dat verdere vaststelling van compliance overbodig is. De validiteit van dit specifieke pad is dus in orde, want de conclusie komt overeen met die van de Wbp (true negative). Dit pad kan maar op één manier worden belopen. De totale dekking is weergegeven in de volgende tabellen:

Legenda	
●	Compleet afgedekt
◌	Gedeeltelijk afgedekt

Artikelen	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Dekking	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●

Artikelen	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	76	77
Dekking	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●

5.4.2 Einde na vraag 1.2.1

De tweede mogelijkheid waarop de vragenlijst kan eindigen is na vraag 1.2.1. De conclusie bij antwoord 'ja' op 1.2.1 is: U kunt stoppen. Ze omschrijven vervolgens niet wat de risico's zijn voor een bewerker, maar zeggen dat de vragenlijst niet meer van toepassing is voor een bewerker. Volgens de Wbp moeten bewerkers echter wel voldoen aan de verplichtingen die de verantwoordelijke contractueel op hen afdwingt in een bewerkersovereenkomst. Dit wordt omschreven in artikel 14. De verantwoordelijke draagt zorg voor de naleving van deze verplichtingen en kan juridische stappen nemen als er geen naleving plaatsvindt. Er is dus wel een compliance risico voor een bewerker. Niet i.v.m. de Wbp, maar i.v.m. de bewerkersovereenkomst met de verantwoordelijke. Dit valt daarom buiten de Wbp. De validiteit van deze verzameling paden is dus in orde, want de conclusie komt overeen met die van de Wbp (true negative). De totale dekking is weergegeven in de volgende tabellen:

Artikelen	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Dekking	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●

Artikelen	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	76	77
Dekking	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●

5.4.3 EINDE NA VRAAG 1.6

De derde mogelijkheid waarop de vragenlijst kan eindigen is na vraag 1.6. Alle paden eindigen door antwoord 'ja' op vraag 1.6. De conclusie is dan als volgt: '*De privacyrisico's zijn laag, verder uitvoeren heeft weinig toegevoegde waarde. Let op! U dient wel aan de eisen van de Wbp te voldoen.*' Daarmee wordt aangegeven dat compliance met de Wbp nog niet is nagegaan. De enige antwoorden die duidelijkheid geven over de mate van compliance zijn vraag 1.1 en 1.4. Vraag 1.1 kan in deze verzameling alleen met 'ja' beantwoord worden. Voor vraag 1.4 maakt het niet uit welk antwoord gegeven wordt, de Wbp wordt in elk geval evenveel afgedekt (true positive of true false). De conclusie m.b.t. compliance die getrokken wordt in de paden met antwoord 'ja' op vraag 1.4 is als volgt: Er is gedeeltelijk compliance met artikel 7. Er is alleen niet nagegaan of persoonsgegevens voor gerechtvaardigde doeleinden zijn verzameld, vandaar 'gedeeltelijk'. Bij alle paden waarin antwoord 'nee' op vraag 1.4 is gegeven, is vastgesteld dat er geen compliance is met een gedeelte van artikel 7. De validiteit van deze verzameling paden is daarmee vastgesteld en is erg laag. De totale dekking van deze verzameling paden wordt weergegeven in de volgende tabel:

Artikelen	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Dekking		●					◌																

Artikelen	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	76	77
Dekking																							

Voor alle artikelen die niet worden afgedekt in bovenstaande tabel is niet duidelijk of er compliance is. Er worden voor de overige artikelen geen risico's geïdentificeerd. Dit zou betekenen dat na eindiging van de vragenlijst, voor heel veel artikelen niet duidelijk is of er een false negative of een true negative is vastgesteld.

5.4.4 EINDE NA VRAAG 7.2

De derde mogelijkheid waarop de vragenlijst kan eindigen is na vraag 7.2, de laatste vraag. Alle resterende paden doorlopen is te veel werk, aangezien dit er nog ruim 24×10^{15} zijn (zie bijlage I voor de precieze berekening). Zelfs als deze gegroepeerd worden doorlopen, is het te veel werk. Om toch iets over de validiteit van deze overige paden te kunnen zeggen, is gekeken wat de maximale validiteit is van deze verzameling. De resterende paden hebben namelijk een nóg lagere validiteit. De dekking van de verzameling met de hoogste validiteit is weergegeven in onderstaande tabellen. Voor uitleg over de manier waarop deze validiteit behaald kan worden, zie bijlage I.

Artikelen	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Dekking	○	●			○	○	○	●	○	●	●					●	●	●	●	●	●	●	●

Artikelen	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	76	77
Dekking	●											○						●	●			●	●

Door de PIA te gebruiken om privacyrisico's te identificeren, kun je dus (afgezien van de mogelijkheden in hoofdstuk 5.4.1 en 5.4.2) nooit een hogere validiteit behalen dan hierboven weergegeven. Dat wil zeggen dat in de complexere gevallen waarbij privacy juist van belang is, van heel veel artikelen niet wordt nagegaan of er wel of geen compliance is (true negative of false negative). De privacyrisico's met betrekking tot de Wet bescherming persoonsgegevens worden dan maar deels vastgesteld, terwijl compliance belangrijk is om de privacy van gebruikers te kunnen waarborgen. Er is geen steekproef genomen omdat men niets kan zeggen over de kans waarop precies een dergelijk pad wordt doorlopen. Elke situatie is namelijk verschillend.

5.5 Conclusie van de validiteitsanalyse

Om antwoord te kunnen geven op de laatste onderzoeksvraag is de validiteit van de vragenlijst van de NOREA PIA in drie stappen onderzocht. De eerste stap omvatte het omzetten van de Wet bescherming persoonsgegevens naar een stroomschema zodat beoordeeld kon worden wanneer een bepaald artikel nog van toepassing is. Daarnaast is de PIA vragenlijst ook omgezet naar een stroomschema. In de tweede stap is voor elk antwoord op de vragen vastgesteld in hoeverre er compliance met de Wbp wordt vastgesteld. De derde stap omvatte het analyseren van bijna alle mogelijkheden om de vragenlijst te doorlopen om te beoordelen of een dergelijk pad een valide oordeel geeft over de mate van compliance. Daaruit is gebleken dat de vragenlijst alleen in de gevallen waarin geen persoonsgegevens worden verwerkt, of waarin de PIA wordt uitgevoerd door een bewerker een volledige en juiste conclusie trekt wat betreft compliance. In de overige gevallen waarin persoonsgegevens worden verwerkt door een verantwoordelijke worden veel artikelen van de Wbp niet behandeld, waardoor men nooit met zekerheid heeft vastgesteld of er volledige compliance is. Een aantal voorbeelden uit de Wbp waarvan dan niet is vastgesteld of men compliant is:

- de meldplicht (artikel 27 t/m 30 Wbp)
- de informatieverstrekking aan de betrokkene (artikel 33 en 34 Wbp)
- de rechten van de betrokkene (artikel 35 t/m 40 Wbp)

Als het onduidelijk is of er compliance is met bijvoorbeeld bovengenoemde artikelen loopt een verantwoordelijke het risico dat hij non-compliant is. Een verantwoordelijke die ervan uitgaat dat er na uitvoering van de PIA geen privacyrisico's meer zijn, kan dus (hoewel misschien onwetend) toch non-compliant zijn. Non-compliance met de Wbp betekent dat er door het CBP bestuurlijke boetes van maximaal €810.000 opgelegd kunnen worden.

Kortom, de NOREA PIA vragenlijst kan niet gebruikt worden als een betrouwbare compliance check. In de relevante gevallen (als persoonsgegevens verwerkt worden) wordt namelijk niet vastgesteld of er voldaan wordt (of gaat worden) aan alle artikelen van de Wbp.

6 CONCLUSIE

In deze thesis is getracht de volgende hoofd-onderzoeksvraag te beantwoorden:

Hoe geschikt is de NOREA PIA om privacyrequirements vast te stellen?

Om deze vraag te kunnen beantwoorden zijn drie aspecten van de NOREA PIA onderzocht. Ten eerste, *hoe verhoudt de NOREA PIA zich tot de andere Nederlandse PIA, het Toetsmodel van de Rijksdienst?* Het is gebleken dat beide PIA's niet aan alle criteria van de vergelijking voldoen maar de NOREA PIA is wel completer. De NOREA PIA zou nog moeten aanraden om het resulterende rapport te publiceren om transparantie te bewerkstelligen. Daarnaast zou de focus van privacy verbreedt moeten worden zodat deze verder reikt dan gegevensbescherming. Ook zou de NOREA PIA beter moeten afdwingen om verantwoording af te leggen, want dit is belangrijk om privacy te waarborgen. Een voorzichtige indicatie geeft aan dat de NOREA PIA leesbaarder is dan het toetsmodel. Al met al kan geconcludeerd worden dat de NOREA PIA in Nederland de meest complete PIA is, maar hij kan nog op bovengenoemde punten verbeterd worden.

Ten tweede, w*elke inzichten levert de uitvoering van het NOREA PIA proces bij Nigella IT op?* Er kunnen twee soorten inzichten worden onderscheiden: problemen en aandachtspunten. Tijdens de uitvoering zijn een drietal problemen opgetreden. Vooraf aan de uitvoering van de PIA is het onduidelijk hoe lang het gaat duren. Dit probleem kan men helaas niet voorkomen zoals ook wordt erkend in de NOREA PIA documentatie. Daarnaast is gebleken dat een gebrek aan juridische expertise leidt tot stagnatie. Een gebrek aan expertise op gebied van impactbepaling en risicobeheersing leidt tot een uitgevoerde PIA van lagere kwaliteit. Deze twee problemen kan men voorkomen door de genoemde expertise bij de uitvoering te betrekken. Naast de genoemde problemen kan er een aantal aandachtspunten aangeduid worden waaruit o.a. bleek dat uitvoering van een PIA met de juiste doelstelling zeer belangrijk is. Een ander aandachtspunt is dat de kwaliteit van de resultaten van de PIA zeer afhankelijk is van de expertise van de uitvoerders. Dit staat ook als succesfactor omschreven in de documentatie. Al met al zijn er bij de uitvoering van de NOREA PIA geen grote verrassingen geweest en worden deze ook niet verwacht bij uitvoering in een soortgelijke context.

Het derde onderzochte aspect is de validiteit van de vragenlijst van de NOREA PIA. Uit die analyse kan worden geconcludeerd dat de vragenlijst maar in een klein aantal gevallen de juiste conclusie trekt. Als er geen persoonsgegevens worden verwerkt is de conclusie snel en vaak juist, echter als er wél persoonsgegevens worden verwerkt is er meestal geen volledige conclusie. Wanneer er persoonsgegevens worden verwerkt is het juist belangrijk dat er wordt vastgesteld of er compliance is.

Concluderend betekent dit dat de NOREA PIA in Nederland momenteel de beste standaard is om privacyrequirements vast te stellen door middel van een Privacy Impact Assessment. Compliance wordt er echter niet mee vastgesteld, dus niet alle juridische eisen van de Wbp worden meegenomen. Ook biedt de NOREA PIA documentatie geen stap-voor-stap omschrijving om risico's in maatregelen te vertalen en is de kwaliteit van de resulterende privacyrequirements zeer afhankelijk van de expertise van de uitvoerder(s).

7 Discussie, aanbevelingen en verder onderzoek

7.1 Discussie

Vanwege het dynamische karakter van IT en de zeer recente ontwikkelingen op het gebied van PIA's en PbD is er maar weinig actuele literatuur beschikbaar. Veel onderzoek op het gebied van PbD en PIA's is namelijk kwalitatief en vooral nog exploratief. Vanwege het Nederlandse karakter van de NOREA PIA en de geassocieerde wetgeving is gekozen om de thesis in het Nederlands te schrijven. Daarom zijn waar nodig Engelse termen vertaald naar het Nederlands. Mogelijk hebben Engelse woorden door deze vertaling een deel van hun betekenis verloren.

Deelvraag 1: PIA vergelijking
De vergelijking tussen de PIA's is gedaan aan de hand van criteria uit de literatuur. De beoordeling of de PIA's voldoen aan die criteria is echter afhankelijk geweest van het persoonlijk beoordelingsvermogen. De afwegingen zijn zorgvuldig gedocumenteerd om de transparantie te bevorderen. Het is gebleken dat sommige criteria overlap vertonen of overbodig zijn. Daarnaast kunnen nog meer criteria worden aangedragen om PIA's te vergelijken. Deze aanbevelingen zijn te vinden in paragraaf 7.2.

Deelvraag 2: Casestudy bij Nigella IT
De toepassing van de NOREA PIA bij Nigella IT is zeer afhankelijk geweest van de expertise van de uitvoerder. De inzichten van deelvraag 2 zijn daarom ook niet ontleend aan de inhoud maar aan het doorgelopen proces. Een casestudy is echter maar één onderzoekseenheid, dus zullen er in andere situaties problemen op kunnen treden die op grond van de evaluatie in deze thesis niet zijn voorspeld. Alle opgetreden problemen en sommige aandachtspunten staan omschreven in de NOREA PIA documentatie, in de vorm van succes- en faalfactoren. De NOREA PIA documentatie is dus, op een aantal aandachtspunten na, duidelijk over de eventuele problemen die kunnen optreden.

Deelvraag 3: Validiteitsanalyse PIA vragenlijst
Voor de validiteitsanalyse is een aantal hulpartefacten opgesteld aan de hand van bestaande documentatie waarmee een privacy audit uitgevoerd kan worden. Die documentatie wordt aangeraden door de gegevensbescherming autoriteit van Nederland, het College Bescherming Persoonsgegevens. Er is een aantal beslissingen genomen om de analyse praktisch te houden, bijvoorbeeld de selectie van een deel van de artikelen van de Wbp, of het analyseren van de maximale validiteit vanwege het te grote aantal mogelijkheden om de vragenlijst te doorlopen. De beoordeling in hoeverre de wet is verwerkt in de vragenlijst is zorgvuldig gedocumenteerd om de transparantie te bevorderen. Het vervolgens nagaan van de validiteit is gestructureerd gedaan. De gedetailleerde berekening is te vinden in bijlage I. Vanwege het gecompliceerde en zeer specifieke onderzoek bij deze handelingen is er geen literatuur te vinden wat soortgelijk onderzoek beschrijft. Daarom zijn alle stappen zo zorgvuldig mogelijk beschreven om mogelijke twijfel weg te nemen.

Niet elk pad van de vragenlijst is beoordeeld op zijn validiteit, vanwege de te grote hoeveelheid paden. Een bepaalde verzameling paden (zie paragraaf 5.4.4) is daarom op een andere manier beoordeeld om toch een uitspraak over de mate van validiteit te kunnen doen. Van die

verzameling is de maximale validiteit onderzocht, door de vragenlijst op een manier te doorlopen waardoor de hoogste validiteit wordt behaald. Dit houdt in dat bij elke vraag het antwoord is gekozen dat het meeste vaststelt over compliance. De keuze om de maximale validiteit te onderzoeken is gebaseerd op het gevoel dat de validiteit erg laag zou zijn. Het onderzoek wijst uit dat de maximale validiteit relatief laag is waardoor de werkelijke validiteit alleen nog maar lager kan zijn. De maximale validiteit impliceert dat een verantwoordelijke die persoonsgegevens verwerkt en die alleen uitgaat van de risico's die aan de hand van de NOREA PIA worden geïdentificeerd bijvoorbeeld niet weet of er compliance is met de meldplicht, de informatie-verstrekking aan de betrokkene, of de rechten van de betrokkene. Dit betekent dat er non-compliance kan zijn, wat vervolgens betekent dat de verantwoordelijke het risico loopt om een bestuurlijke boete door het CBP opgelegd te krijgen ter hoogte van maximaal €810.000.

7.2 Aanbevelingen

Criteria vergelijking

Wanneer men onderzoek doet naar een PIA kan men de criteria gebruiken van Wright (2013), die omschrijven waar een goede PIA aan zou moeten voldoen. De criteria stellen een onderzoeker in staat om een PIA met diepgang te onderzoeken, echter kunnen zij nog verbeterd worden. Er zijn een aantal criteria die overlap vertonen waardoor sommige criteria overbodig zijn, zoals *"bevat een stel vragen om privacyrisico's te ontdekken"* en *"identificeert privacyrisico's"*, of *"geeft aan dat een PIA meer is dan een compliance check"* en *"behandelt alle soorten privacy"*. Deze kan men samentrekken naar: *"bevat een stel vragen om privacyrisico's te identificeren"* en *"behandelt alle soorten privacy, is meer dan een compliance check"*. Ook is gebleken dat een PIA erg moeilijk leesbaar kan zijn door alle juridische termen die erin gebruikt worden. Daarom kan leesniveau een aanvullend criterium zijn om PIA's te vergelijken. Voor Nederlandse PIA's kan bij gebrek aan beter bijvoorbeeld de Accessibility Leesniveau Tool[28] gebruikt worden.

PIA uitvoerder

De persoon die de NOREA PIA gaat uitvoeren in een nieuwe situatie doet er goed aan om de problemen en aandachtspunten van hoofdstuk 4 door te nemen zodat hij zich goed voorbereidt.

Aanpassing NOREA PIA vragenlijst

De NOREA PIA vragenlijst kan nog op een aantal punten verbeterd worden. Bij een aantal vragen is het onduidelijk naar welke vraag men vervolgens moet doorgaan. Dit zijn vraag 1.2, 4.3, 4.4.1, 5.2 en 5.7. Ook staat bij vraag 4.3.3 de toelichting van het antwoord bij 'nee', terwijl het bij 'ja' hoort te staan. Ook worden onderdelen van de Wbp in meerdere vragen bevraagd, waardoor het mogelijk is om tegenstrijdige conclusies te trekken. Zie hiervoor bijlage II, onderdeel 'Dubbele vragen'. Daarnaast kan artikel 40 uitgesloten worden door vraag 3.2.2 met 'ja' te beantwoorden terwijl deze wel nog van toepassing is. Ook zijn er artikelen die in de gehele vragenlijst niet worden behandeld. Zie hiervoor paragraaf 5.3.1.2.

Het is het wenselijk als met de NOREA PIA volledig compliance wordt nagegaan zodat na uitvoering van de NOREA PIA in ieder geval alle juridische implicaties worden meegenomen in de vertaalslag naar PET's. Op dit moment is de vragenlijst van de NOREA PIA namelijk vrij omvangrijk

[28] Accessibility Leesniveau Tool d.d. 2009

terwijl hij tegelijkertijd niet eens volledig vaststelt of er compliance is met de wet. De diepgang van de huidige vragenlijst lijkt daardoor geen doel te hebben. Door hem uit te breiden kan ervoor gezorgd worden dat in alle gevallen juist wordt nagegaan of er compliance is.

7.3 VERDER ONDERZOEK

Het is gebleken dat het bedenken van maatregelen voor risicobeperking tijdens de uitvoering van de NOREA PIA zeer afhankelijk is van de expertise van de uitvoerders. In 2009 was er ook al de aandrang om deze vertaalslag beter te kunnen begeleiden zodat privacy beter wordt vertaald in ontwerpdoelen (Wuyts, Scandariato, De Decker, & Joosen, 2009). Een invalshoek om vanuit privacybedreigingen oplossingen te formuleren zoals in de LINDDUN methode wordt gedaan is al een stap in de goede richting (Deng et al., 2011). Ook het nieuwe PIA raamwerk van van Rest et al. lijkt een tussenstap in die vertaalslag te willen inbouwen door ontwerppatronen te betrekken bij het ontwerpproces (van Rest et al., 2014). Hoepman bouwt verder op dit idee door drie abstractielagen aan te brengen: privacy design strategies, privacy design patterns en als laatste PET's (Hoepman, 2014). Voor de vertaling van strategieën naar patronen en van strategieën naar PET's is een goede opzet gemaakt, maar dit concept zal nog verder doorontwikkeld moeten worden om echt bruikbaar te worden voor de PbD gedachte.

8 Bibliografie

Cavoukian, A. (2009). *Privacy by Design: The 7 Foundational Principles (revised 2011)*. *Information and Privacy Commissioner of Ontario, Canada*. Retrieved from https://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples-dutch.pdf

Clarke, R. (2006). What's "Privacy"? In *Proceedings of the Workshop at the Australian Law Reform Commission*. Retrieved from http://www.rogerclarke.com/DV/Privacy.html

Clarke, R. (2009). Privacy impact assessment: Its origins and development. *Computer Law and Security Review*, *25*(2), 123–135. doi:10.1016/j.clsr.2009.02.002

Deng, M., Wuyts, K., Scandariato, R., Preneel, B., & Joosen, W. (2011). A privacy threat analysis framework: Supporting the elicitation and fulfillment of privacy requirements. *Requirements Engineering*, *16*(1), 3–32. doi:10.1007/s00766-010-0115-7

Felt, A., Ha, E., Egelman, S., Haney, A., Erika, C., & Wagner, D. (2012). Android Permissions : User Attention , Comprehension , and Behavior. In *Proceedings of the Eighth Symposium on Usable Privacy and Security* (p. 3).

Finn, R. L., Wright, D., & Friedewald, M. (2013). Seven Types of Privacy. In *In European data protection: coming of age* (pp. 3–32). doi:10.1007/978-94-007-5170-5

Gürses, S. (2014). Can you engineer privacy? *Communications of the ACM*, *57*(8), 20–23. doi:10.1145/2633029

Gürses, S., Troncoso, C., & Diaz, C. (2011). Engineering Privacy by Design. In *Conference on Computers, Privacy & Data Protection, CPDP*.

Hes, R., & Borking, J. (1995). *Privacy-enhancing technologies: The path to anonymity.* Retrieved from https://www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=329

Hoepman, J. H. (2014). Privacy Design Strategies. In *ICT Systems Security and Privacy Protection, 29th IFIP TC 11 International Conference, SEC 2014, Marrakech, Morocco* (pp. 446–459). Retrieved from http://arxiv.org/abs/1210.6621

Jansen, C., & Boersma, N. (2013). Meten is weten? Over de waarde van de leesbaarheidsvoorspellingen van drie geautomatiseerde Nederlandse meetinstrumenten. *Tijdschrift Voor Taalbeheersing*, *35*, 47–62.

Koops, B.-J., & Leenes, R. (2013). Privacy regulation cannot be hardcoded. A critical comment on the "privacy by design" provision in data-protection law. *International Review of Law, Computers & Technology*, *28*(September 2014), 159–171. doi:10.1080/13600869.2013.801589

Kosinski, M., Stillwell, D., & Graepel, T. (2013). Private traits and attributes are predictable from digital records of human behavior. In *Proceedings of the National Academy of Sciences of the United States of America* (Vol. 110, pp. 5802–5). doi:10.1073/pnas.1218772110

Kroener, I., & Wright, D. (2014). A Strategy for Operationalizing Privacy by Design. *The Information Society: An International Journal*, *30*(5), 355–365. doi:10.1080/01972243.2014.944730

Landau, S. (2014). Summing Up. *Communications of the ACM*, *57*(11), 37–39. doi:10.1145/2668901

Oetzel, M. C., & Spiekermann, S. (2014). A systematic methodology for privacy impact assessments: a design science approach. *European Journal of Information Systems*, *23*(2), 126–150. doi:10.1057/ejis.2013.18

Shapiro, S. S. (2010). Privacy by design: Moving from Art to Practice. *Communications of the ACM*, *53*, 27. doi:10.1145/1743546.1743559

Spiekermann, S. (2012). The challenges of privacy by design. *Communications of the ACM*, *55*(7), 38. doi:10.1145/2209249.2209263

Spiekermann, S., & Cranor, L. F. (2009). Engineering privacy. *IEEE Transactions on Software Engineering*, *35*(1), 67–82.

Van Rest, J., Boonstra, D., Everts, M., van Rijn, M., & van Paassen, R. (2014). Designing Privacy-by-Design. In *Privacy Technologies and Policy* (pp. 55–72). doi:10.1007/978-3-642-54069-1_4

Wright, D. (2012). The state of the art in privacy impact assessment. *Computer Law and Security Review*, *28*(1), 54–61. doi:10.1016/j.clsr.2011.11.007

Wright, D., Finn, R., & Rodrigues, R. (2013). A comparative analysis of privacy impact assessment in six countries. *Journal of Contemporary European Research*, *9*(1), 160–180.

Wuyts, K., Scandariato, R., De Decker, B., & Joosen, W. (2009). Linking privacy solutions to developer goals. In *Proceedings - International Conference on Availability, Reliability and Security, ARES 2009* (pp. 847–852). doi:10.1109/ARES.2009.51

BIJLAGEN

I. BEREKENINGEN VALIDITEIT

Einde na vraag 1.1
Het gaat zich om het volgende pad:

Vraag	Antwoord/mogelijkheden
1.1	Nee

Dit kan op één manier worden doorlopen. Door 'nee' te antwoorden op vraag 1.1.

Einde na vraag 1.2.1
Het gaat zich om de volgende verzameling paden:

Vraag	Antwoord/mogelijkheden
1.1	Ja
1.2	2 (ja of nee)
1.2.1	Ja

Het aantal manieren waarop de vragenlijst kan eindigen is 2^1, vanwege de 2 mogelijke antwoorden die bij vraag 1.2 gegeven kunnen worden.

Einde na vraag 1.6
Het gaat zich om de volgende verzameling paden:

Vraag	Antwoord/mogelijkheden
1.1	Ja
1.2	2
1.2.1	Nee
1.3	2
1.4	2
1.5	Nee (op alle)
1.6	Ja

Het aantal manieren waarop de vragenlijst kan eindigen is $2^3=8$.

Einde na vraag 7.2
Buiten de 11 mogelijkheden die hierboven zijn berekend besproken, kan de vragenlijst op nog veel meer manieren worden doorlopen. Deze mogelijkheden zijn helaas niet gemakkelijk uit te drukken in een verzameling van paden omdat na vraag 1.6 sommige vragen worden overgeslagen door bepaalde antwoorden te geven. De berekening van het totaal aantal paden is in onderstaande tabel weergegeven. Er is te zien op hoeveel verschillende manieren men van de weergegeven vraag naar de vraag kan gaan die een rij lager staat. Waar nodig, staat er uitleg bij de berekening.

Vraag	Berekening	Toelichting
1.1	2^3	Vraag 1.1 moet met 'ja' worden beantwoord en 1.2.1 moet met 'nee' worden beantwoord, anders stopt de vragenlijst. Vraag 1.2, 1.3 en 1.4 kunnen willekeurig worden beantwoord, vandaar de 2^3 manieren om van 1.1 **tot** 1.5 te komen.
1.5	$2^6 * 7$	Minimaal één van de 7 vragen van 1.5 moet met 'ja' beantwoord worden. Dit betekent dat 6 vragen willekeurig beantwoord kunnen worden en één met 'ja', maar dit kan op 7 verschillende manieren.
1.6	2^{15}	Van vraag 1.6 tot 3.2 zijn er alleen vragen die willekeurig beantwoord kunnen worden. Dit zijn er in totaal 15, vandaar 2^{15}.
3.2	7	Om van vraag 3.2 naar 4.1 te komen zijn meerdere mogelijkheden. Een mogelijkheid is om 'nee' te antwoorden op 3.2. Een tweede mogelijkheid is om 'ja' op 3.2, 3.2.1 willekeurig en vervolgens 3.2.2 met 'ja' te beantwoorden. Dit kan op twee manieren vanwege vraag 3.2.1. De laatste mogelijkheid is door 3.2 met 'ja', 3.2.1 willekeurig, 3.2.2 met 'nee', en 3.2.3 willekeurig te beantwoorden. Dit kan door 3.2.1 en 3.2.3 op 2^2 manieren. Dit zijn er 7 ($1+2+2^2$) in totaal.
4.1	2^2	Tussen 4.1 en 4.3 zitten twee vragen die willekeurig beantwoord kunnen worden (4.1 en 4.2). Dit kan op 2^2 manieren.
4.3	5	Tussen 4.3 en 4.4. zitten vier vragen die elk beantwoord kunnen worden zodat ze uitkomen op 4.4, of doorgaan naar de volgende vraag. Zo zijn er in totaal vijf mogelijkheden om op 4.4 uit te komen.
4.4	9	Als vraag 4.4 met 'ja' beantwoord wordt, kunnen 4.4.2 en 4.4.3 elk willekeurig worden beantwoord om op 4.5 uit te komen. Dit kan op 2^2 manieren. Als 4.4 met 'nee' wordt beantwoord, kan 4.4.1 met 'nee' beantwoord worden om op 4.5 uit te komen, of met 'ja', waardoor dezelfde twee willekeurige te beantwoorden vragen doorlopen moeten worden. In totaal $2^2+2^2+1=9$ manieren in totaal.
4.5	2^2	Door twee willekeurig te beantwoorden vragen kun je op 2^2 manieren tot vraag 5.2 komen.
5.2	3	Via 5.2 'nee' kan op één manier, via 5.2 'ja' kan op twee manieren vanwege de willekeurig te beantwoorden vraag 5.2.1. In totaal $1+2=3$ manieren.
5.3	2	De willekeurige vraag 5.3 kan op twee manieren beantwoord worden.
5.4	3	Volgens dezelfde redenering als bij 5.2 naar 5.3, zijn er drie mogelijkheden.
5.5	2^4	Tussen 5.5 en 5.8 zijn vier vragen die willekeurig beantwoord kunnen worden, vandaar 2^4 mogelijkheden.
5.8	3	Volgens dezelfde redenering als bij 5.2 naar 5.3, zijn er drie mogelijkheden.
5.9	2^4	Tussen 5.9 en 6.2 zijn vier vragen die willekeurig beantwoord kunnen worden, vandaar 2^4 mogelijkheden.
6.2	3	Volgens dezelfde redenering als bij 5.2 naar 5.3, zijn er drie mogelijkheden.
7.1	3	Volgens dezelfde redenering als bij 5.2 naar 5.3, zijn er drie mogelijkheden.
einde		

Totaal aantal paden/mogelijkheden om de vragenlijst te doorlopen

Het totale aantal mogelijkheden om de vragenlijst te doorlopen is dan een vermenigvuldiging van de in bovenstaande tabel weergegeven aantal mogelijkheden, plus de mogelijkheden behandeld in hoofdstuk 4.2.1, 4.2.2 en 4.2.3. Dit komt neer op het volgende aantal:

Aantal mogelijkheden met einde na 7.2:
$2^{37} * 3^5 * 5 * 7^2 * 9 = 24547284280000000 = 2454728428 * 10^{16}$
Totaal aantal mogelijkheden om de vragenlijst te doorlopen: 24547284280000000 + 11 = 24547284280000011

Aantal paden waarop de vragenlijst eindigt na vraag 7.2, met hoogste validiteit

Deze berekening wordt hetzelfde weergegeven als hierboven, aangezien de hoogste validiteit behaald kan worden met verschillende paden die niet altijd dezelfde vragen bevatten. Waar er verschillende paden mogelijk zijn waarbij dezelfde validiteit wordt behaald, zal dit worden aangegeven in de toelichting.

Vraag	Berekening	Toelichting
1.1	$2^{18} * 7 * 2^6$	In deze aaneenschakeling van vragen en antwoorden, kunnen er nog geen vragen worden uitgesloten door een specifiek antwoord. Daarom geldt hier dezelfde berekening als bij de berekening voor het totale aantal paden.
3.2	2	Tussen 3.2 en 4.1 kan de conclusie getrokken worden dat er compliance is met artikel 41, 76 en 77. Dit kan op twee manieren. De eerste manier is heel kort, namelijk door 'nee' te antwoorden op vraag 3.2. De tweede manier is door op alle vragen tussen 3.2 en 4.1 'nee' te antwoorden.
4.1	2^2	Om van 4.1 naar 4.3.1 te komen, kan er twee keer willekeurig geantwoord worden, en vervolgens met 'ja' op 4.3. 4.3 moet namelijk met 'ja' beantwoord worden om bij de vragen te komen die nog inhoud van de Wbp afdekken die nergens anders in de vragenlijst worden afgedekt. Dit kan op 2^2 manieren.
4.3.1	$4 = 2^2$	Tussen 4.3.1 en 4.4 wordt er vastgesteld of er compliance is met artikel 5, lid 2. Dit wordt in alle mogelijke paden gedaan en dit zijn er 4 in totaal.
4.4	2	Om tussen 4.4 en 4.5 iets te kunnen zeggen over de Wbp, moet vraag 4.4.3 met 'ja' worden beantwoord. Dit kan op 2 manieren, vanwege vraag 4.4.2, die willekeurig ingevuld kan worden.
4.5	$2^2 * 3$	Tussen 4.5 en 5.3 wordt altijd dezelfde conclusies getrokken over de Wbp, dus kunnen deze samengetrokken worden. Zie de vorige berekening om de toelichting voor de berekening te zien.

Vraag	Berekening	Toelichting
5.3	192	Tussen 5.3 en 5.9 kan een aantal conclusies worden getrokken: gedeeltelijke compliance met art. 6 en compliance met art. 11, lid 1 en 2, en compliance met art. 42. Dit kan op 3 verschillende mogelijkheden: **1.** De eerste mogelijkheid is door 'ja' te antwoorden op 5.3, 'ja' op 5.4, en vervolgens zijn er 2^5 verschillende manieren om tot 5.8 te komen. 5.8 of 5.8.1 dient vervolgens met 'nee' beantwoord te worden. Dit kan op 2 manieren, waardoor de 1e mogelijkheid kan in een totaal van $2^5 * 2 = 2^6$ manieren. **2.** De tweede mogelijkheid is door 5.3 met 'ja' te beantwoorden, 5.4 met 'nee', en vervolgens zijn er nog 2^5 manieren om tot 5.8 te komen, en 3 manieren om tot 5.9 te komen. Dit komt neer op een totaal van: $2^5 * 3$ manieren. **3.** De derde mogelijkheid is door 5.3 met 'nee' te beantwoorden, 5.4 met 'ja', 5.4.1 met 'ja', en vervolgens zijn er 2^4 manieren om tot 5.8 te komen en weer 2 manieren om tot 5.9 te komen. In totaal 2^5 manieren. In totaal komen deze drie mogelijkheden om met de hoogste validiteit tot vraag 5.9 te komen, neer op het volgende totale aantal: $(2^6) + (2^5 * 3) + (2^5) = 64 + 96 + 32 = 192$ manieren.
5.9	2^4	Er zijn 4 willekeurige vragen tot 6.2, dus dit kan op 2^4 manieren.
6.2	1	6.2 dient met 'ja' beantwoord te worden en 6.3 ook met 'ja', dus is er maar één manier om naar vraag 7.1 te komen.
7.1	3	Vraag 7.1 kan met 'nee' beantwoord worden om tot het einde te komen, of met 'ja' en vervolgens 7.2 met een willekeurig antwoord. In totaal 3 manieren.
Einde		

Het totale aantal manieren waarop de hoogste validiteit behaald kan worden is:

$2^{18} * 7 * 2^6 * 2 * 2^2 * 2^2 * 2 * 2^2 * 3 * 192 * 2^4 * 1 * 3 = 2^{36} * 3^2 * 7 * 192 =$ 831230790598656

Dit is ongeveer 3,39% van het totale aantal manieren om de vragenlijst te doorlopen.

Manier waarop maximale validiteit wordt behaald

De validiteit van de verzameling paden hierboven omschreven is als volgt:

- Door antwoord 'ja' op 1.1: artikel 2 wordt volledig afgedekt
- Door willekeurig antwoord op 1.4: artikel 7 wordt gedeeltelijk afgedekt
- Door willekeurig antwoord op 2.1: artikel 11, lid 1 wordt afgedekt
- Door antwoord 'nee' op 2.4.a: artikel 16 t/m 23 worden volledig afgedekt
- Door antwoord 'nee' op 2.4.c: artikel 24 wordt volledig afgedekt
- Door antwoord 'nee' op 2.4.d: artikel 9, lid 4 wordt afgedekt
- Door antwoord 'nee' op 2.5: artikel 5, lid 1 wordt gedeeltelijk afgedekt
- Door antwoord 'nee' op 3.2 of op andere manieren: artikel 41, 76 en 77 worden volledig afgedekt
- Door willekeurig antwoord op 4.3: artikel 8 wordt volledig afgedekt
- Door antwoord 'nee' op 4.3.1 of op andere manieren: artikel 5, lid 2 wordt afgedekt
- Door antwoord 'ja' op 4.4.3: artikel 35, lid 2 wordt gedeeltelijk afgedekt
- Door antwoord 'nee' op 5.2 of op andere manieren: artikel 9, lid 1 en 2 worden afgedekt
- Door antwoord 'ja' op 5.3 of op andere manieren: artikel 6 wordt gedeeltelijk afgedekt en artikel 11 wordt volledig afgedekt

- Door antwoord 'nee' op 5.4 of op andere manieren: artikel 42 wordt afgedekt
- Door antwoord 'ja' op 6.3: artikel 10 wordt afgedekt.

II. AANDACHTSPUNTEN VRAGENLIJST

In deze bijlage zijn meerdere punten opgesomd die zijn geconcludeerd bij de validiteitsanalyse van de vragenlijst.

Onduidelijk verloop

Wanneer vraag 1.2 wordt beantwoord is het onduidelijk of de volgende vraag 1.2.1 of 1.3 is. Wanneer je niet weet wie de verantwoordelijke is, kan het zo zijn dat je wel weet dat je bewerker bent. Wanneer je wel weet wie de verantwoordelijke is, weet je ook of je een bewerker bent of niet. Ik ben er dus vanuit gegaan dat vraag 1.2.1 in ieder geval gesteld wordt, ongeacht het antwoord op 1.2.

Wanneer vraag 4.3 met 'nee' wordt beantwoord is het onduidelijk of de volgende vraag 4.3.1 of 4.4 is. Logisch gezien zijn 4.3.1 tot en met 4.3.3 niet meer van toepassing als er geen wettelijke grondslag is. Ik ben er dus vanuit gegaan dat vanuit antwoord 'nee' op vraag 4.3, vraag 4.4 het logisch vervolg is.

Wanneer vraag 4.4.1 wordt beantwoord is het onduidelijk of de volgende vraag 4.4.2 of 4.5 is. Aangezien er door het beantwoorden van 4.4 met 'nee' is vastgesteld dat er geen informatieverstrekking naar de betrokkene wordt gedaan, zijn 4.4.2 en 4.4.3 niet van toepassing. Er kan daar namelijk toch geen antwoord op worden gegeven. Ik ben er dus vanuit gegaan dat vanuit vraag 4.4.1, vraag 4.5 het logisch vervolg is.

Wanneer vraag 5.2 met 'nee' wordt beantwoord is het onduidelijk of de volgende vraag 5.2.1 of 5.3 is. Uit de vraagstelling van 5.2.1 kan worden verondersteld dat deze alleen van toepassing is als op vraag 5.2 'ja' is geantwoord. Ik ben er dus vanuit gegaan dat vanuit antwoord 'nee' op vraag 5.2, vraag 5.3 het logisch vervolg is.

Wanneer vraag 5.7 met 'nee' wordt beantwoord is het onduidelijk of de volgende vraag 5.7.1 of 5.8 is. In de vraagstelling van 5.7 staat: 'Worden gegevens breed verspreid buiten de organisatie?'. Als daarop het antwoord 'nee' is, is verspreiding buiten de organisatie nog niet uitgesloten. Vandaar dat ik ervan ben uitgegaan dat 5.7.1 het logisch vervolg is, als 5.7 met 'nee' wordt beantwoord.

Fout antwoord

In de vraagstelling van 4.3.3 staat: 'Is de impact van het intrekken van de toestemming groot voor de betrokkene?'. Vervolgens staat de toelichting die je zou verwachten bij antwoord 'ja', bij antwoord 'nee'. Deze is waarschijnlijk in het verkeerde vak gezet.

Dubbele vragen

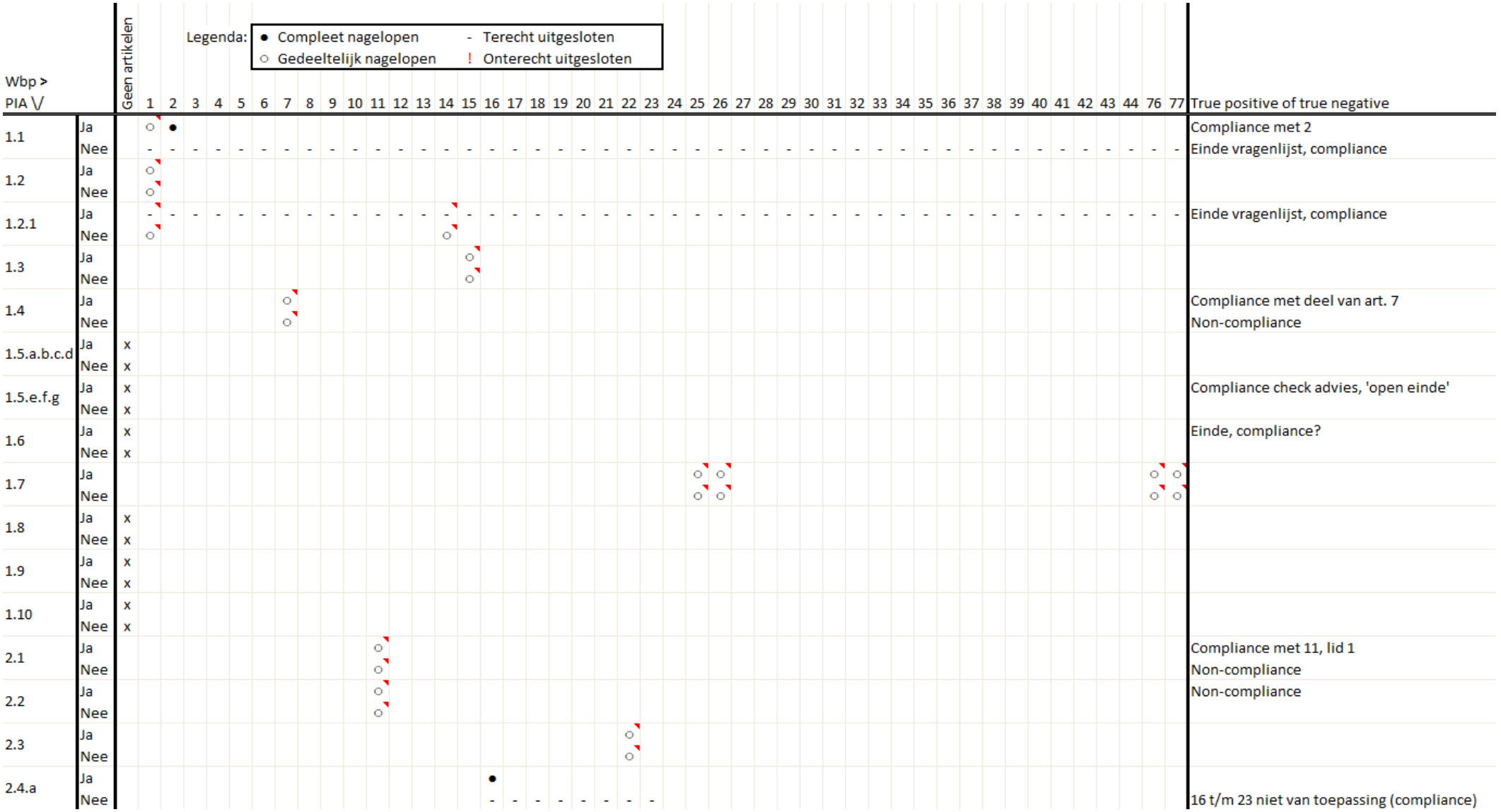
De vragenlijst maakt het mogelijk om tegenstrijdige conclusies te trekken. De mogelijkheid dat door het invullen tegenstrijdige conclusies kunnen worden getrokken duidt op de aanwezigheid van overbodige vragen.

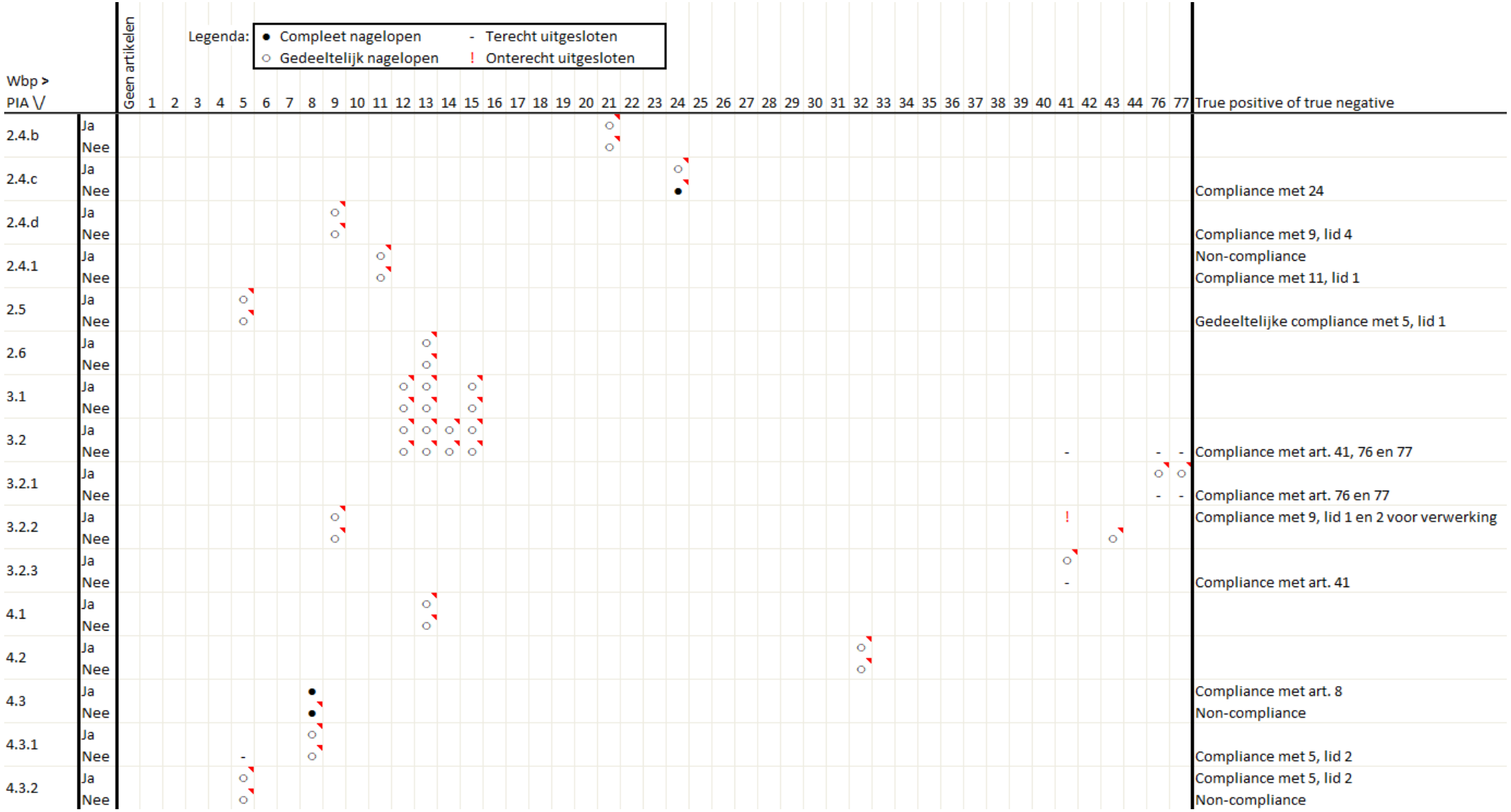
Als vraag 2.1 wordt geantwoord met 'ja', is de conclusie: er is compliance met artikel 11, lid 1 (dataminimalisatie). Als vervolgens vraag 2.2 ook met 'ja' beantwoord wordt, wordt er een tegenstrijdige conclusie getrokken, namelijk dat er geen compliance is met artikel 11, lid 1. Deze tegenstrijdigheid betekent dat een van de twee vragen overbodig is. Met vraag 2.1 kan compliance of non-compliance worden vastgesteld, maar met vraag 2.2 kan alleen non-compliance worden vastgesteld. Vraag 2.2 heeft wel toegevoegde waarde, aangezien het de concepten anonimiseren en pseudonimisering aankaart. Een betere oplossing zou daarom zijn om dit te verwerken in vraag 2.1 en om vraag 2.2 vervolgens te schrappen.

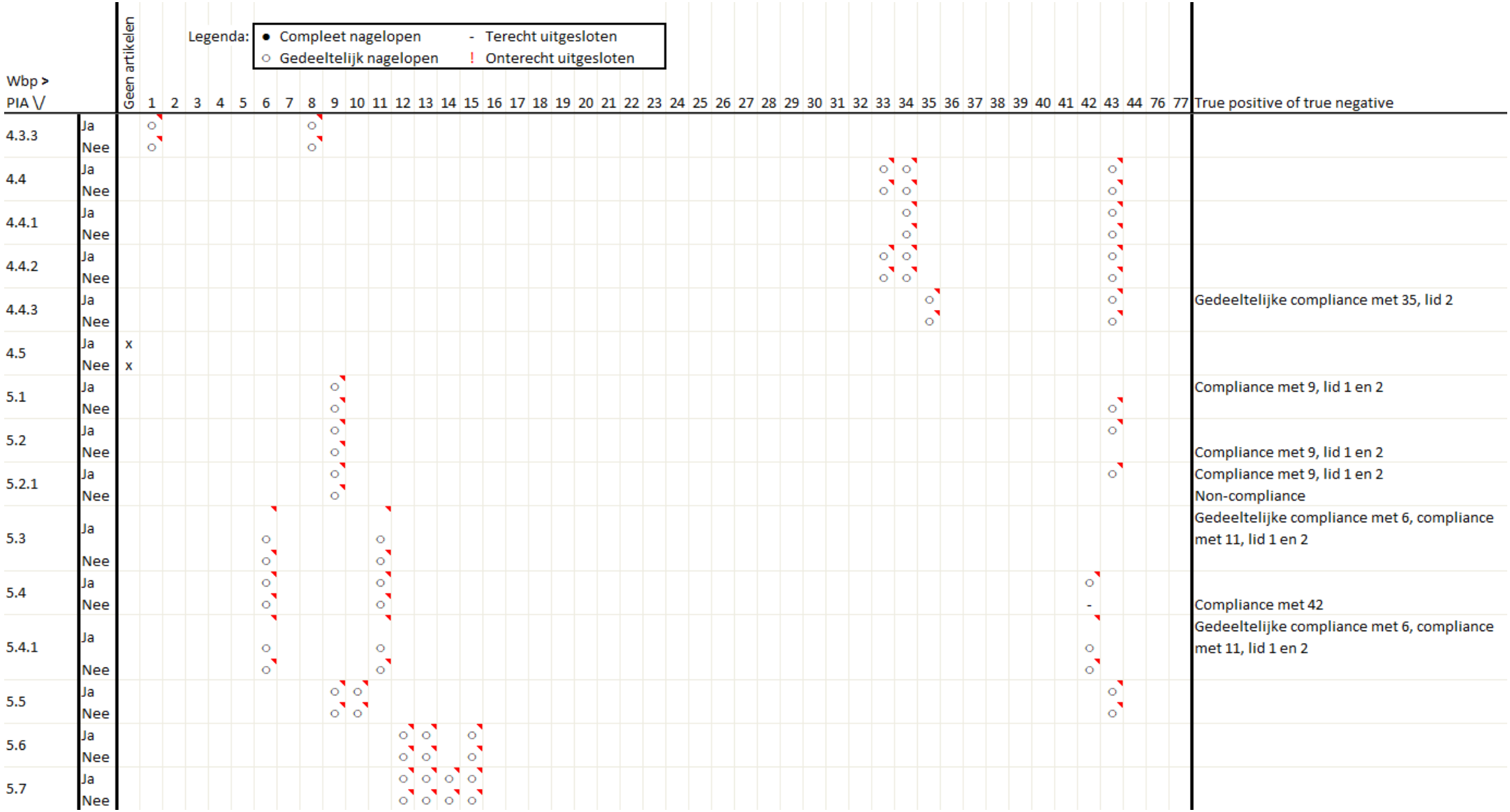
Dezelfde redenering geldt ook voor vraag 2.4.1. Als in de vraag 2.1 en 2.2 de conclusie getrokken wordt dat er sprake is dataminimalisatie, kan antwoord 'ja' op vraag 2.4.1 alsnog een tegenstrijdige conclusie opleveren. In vraag 2.4.1 wordt gevraagd of er 'andere gegevens, die een verminder risico op misbruik met zich mee brengen' gebruikt kunnen worden om hetzelfde doel te realiseren. Wanneer het risico op misbruik groter is dan met andere gegevens, zullen deze gegevens meer zeggen over een persoon dan gezegd kan worden met die andere gegevens. Met andere woorden: Er is niet voldaan aan dataminimalisatie, want dataminimalisatie houdt in dat gegevens niet bovenmatig mogen zijn. En dataminimalisatie is al in vraag 2.1 en 2.2 behandeld. Ik zou vraag 2.4.1 ook verwerken in vraag 2.1, zodat er geen overbodige vragen worden gesteld.

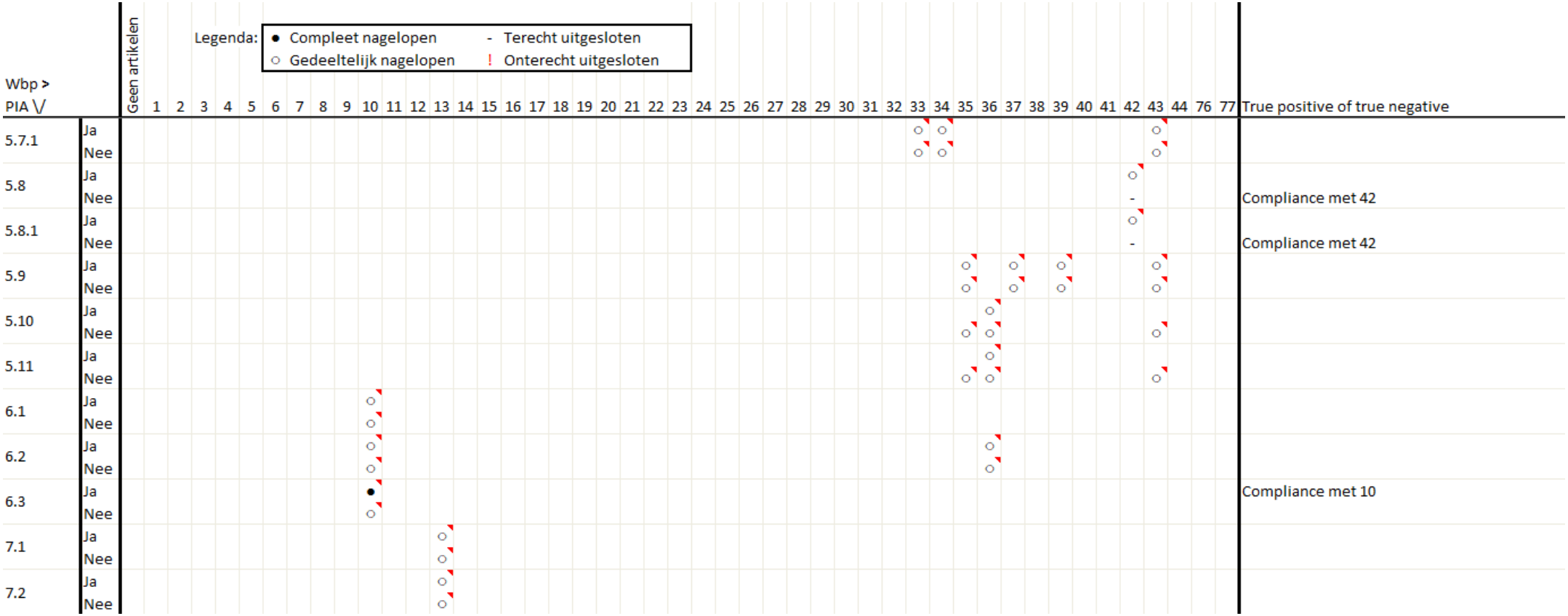
Als vraag 5.1 wordt beantwoord met 'ja', is de conclusie: er is compliance met artikel 9, lid 1 en 2 (doelbinding). Als vervolgens vraag 5.2 met 'ja' wordt beantwoord en vraag 5.2.1 met 'nee', is de conclusie: er is non-compliance met artikel 9, lid 1 en 2. Vraag 5.2 en 5.2.1 zijn daarom overbodig.

III. VERGELIJKING WBP – NOREA PIA

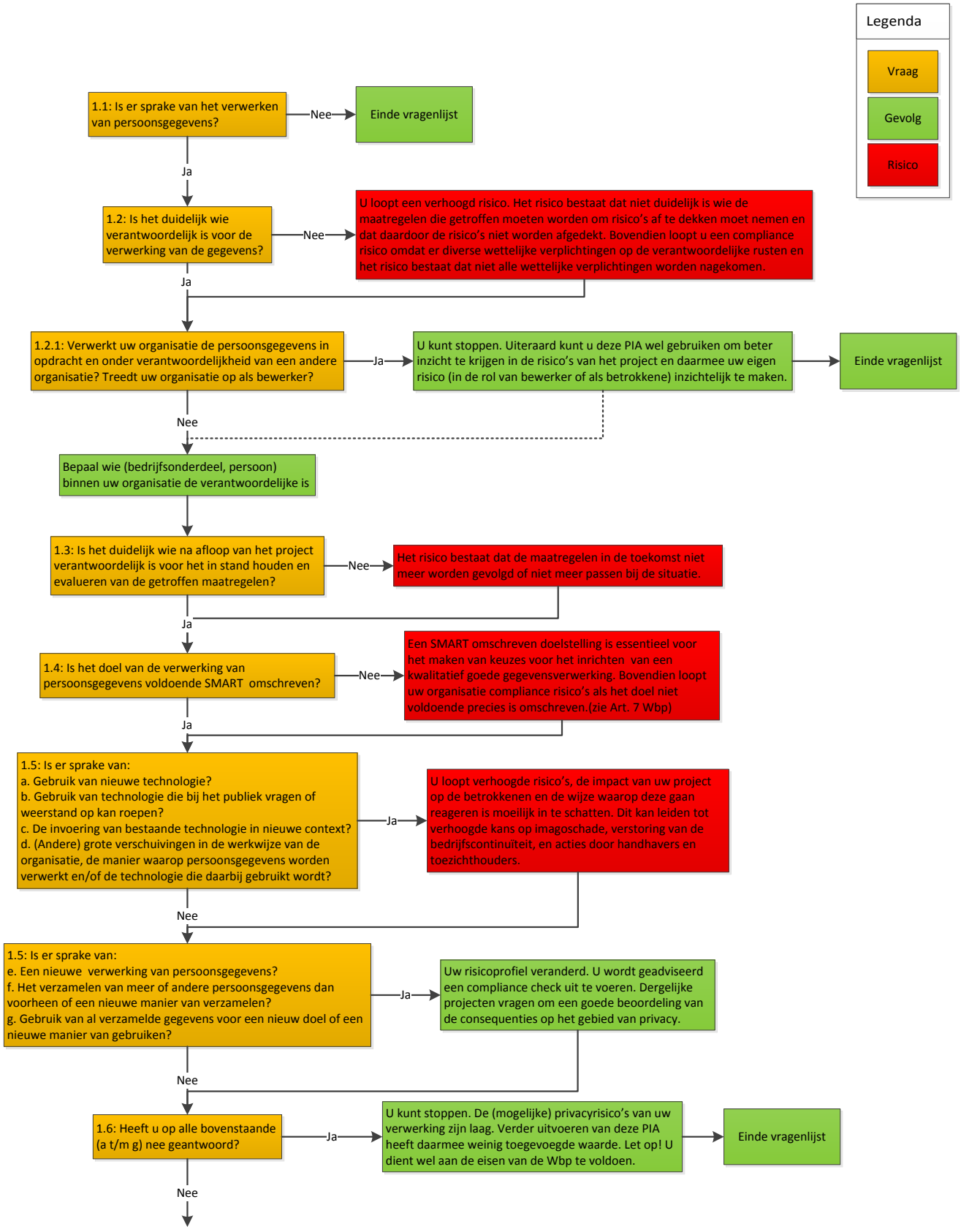


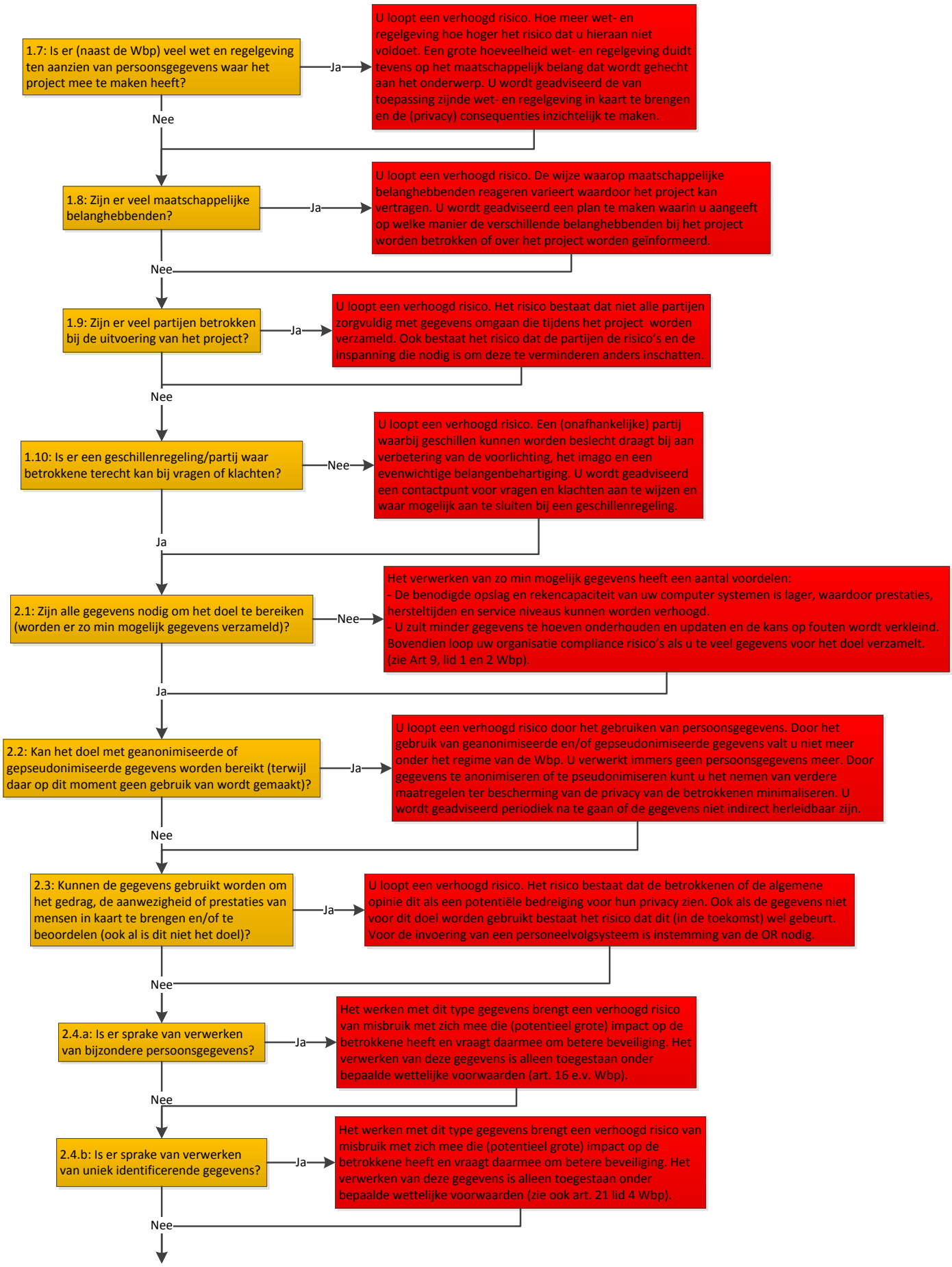

Legenda:
● Compleet nagelopen
○ Gedeeltelijk nagelopen
- Terecht uitgesloten
! Onterecht uitgesloten
Wbp >
PIA \/
Geen artikelen
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 76 77
True positive of true negative
2.4.b Ja
Nee
2.4.c Ja
Nee
Compliance met 24
2.4.d Ja
Nee
Compliance met 9, lid 4
2.4.1 Ja
Non-compliance
Nee
Compliance met 11, lid 1
2.5 Ja
Nee
Gedeeltelijke compliance met 5, lid 1
2.6 Ja
Nee
3.1 Ja
Nee
3.2 Ja
Nee
Compliance met art. 41, 76 en 77
3.2.1 Ja
Nee
Compliance met art. 76 en 77
3.2.2 Ja
Compliance met 9, lid 1 en 2 voor verwerking
Nee
3.2.3 Ja
Nee
Compliance met art. 41
4.1 Ja
Nee
4.2 Ja
Nee
4.3 Ja
Compliance met art. 8
Nee
Non-compliance
4.3.1 Ja
Nee
Compliance met 5, lid 2
4.3.2 Ja
Compliance met 5, lid 2
Nee
Non-compliance

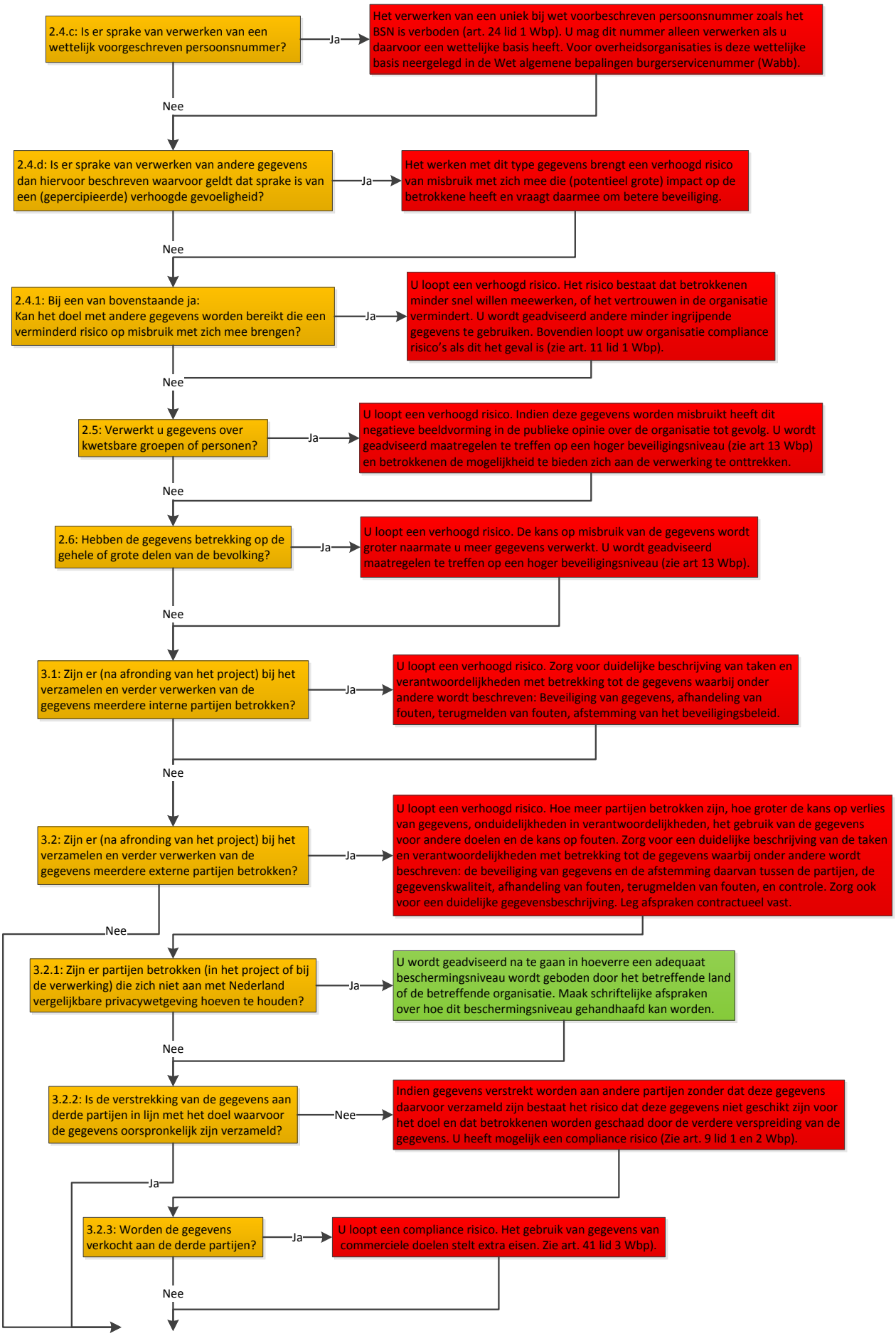

Legenda:
● Compleet nagelopen
○ Gedeeltelijk nagelopen
- Terecht uitgesloten
! Onterecht uitgesloten
Wbp >
PIA \/
Geen artikelen
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 76 77
True positive of true negative
4.3.3 Ja
Nee
4.4 Ja
Nee
4.4.1 Ja
Nee
4.4.2 Ja
Nee
4.4.3 Ja
Nee
Gedeeltelijke compliance met 35, lid 2
4.5 Ja x
Nee x
5.1 Ja
Nee
Compliance met 9, lid 1 en 2
5.2 Ja
Nee
Compliance met 9, lid 1 en 2
5.2.1 Ja
Nee
Compliance met 9, lid 1 en 2
Non-compliance
5.3 Ja
Nee
Gedeeltelijke compliance met 6, compliance met 11, lid 1 en 2
5.4 Ja
Nee
Compliance met 42
5.4.1 Ja
Nee
Gedeeltelijke compliance met 6, compliance met 11, lid 1 en 2
5.5 Ja
Nee
5.6 Ja
Nee
5.7 Ja
Nee

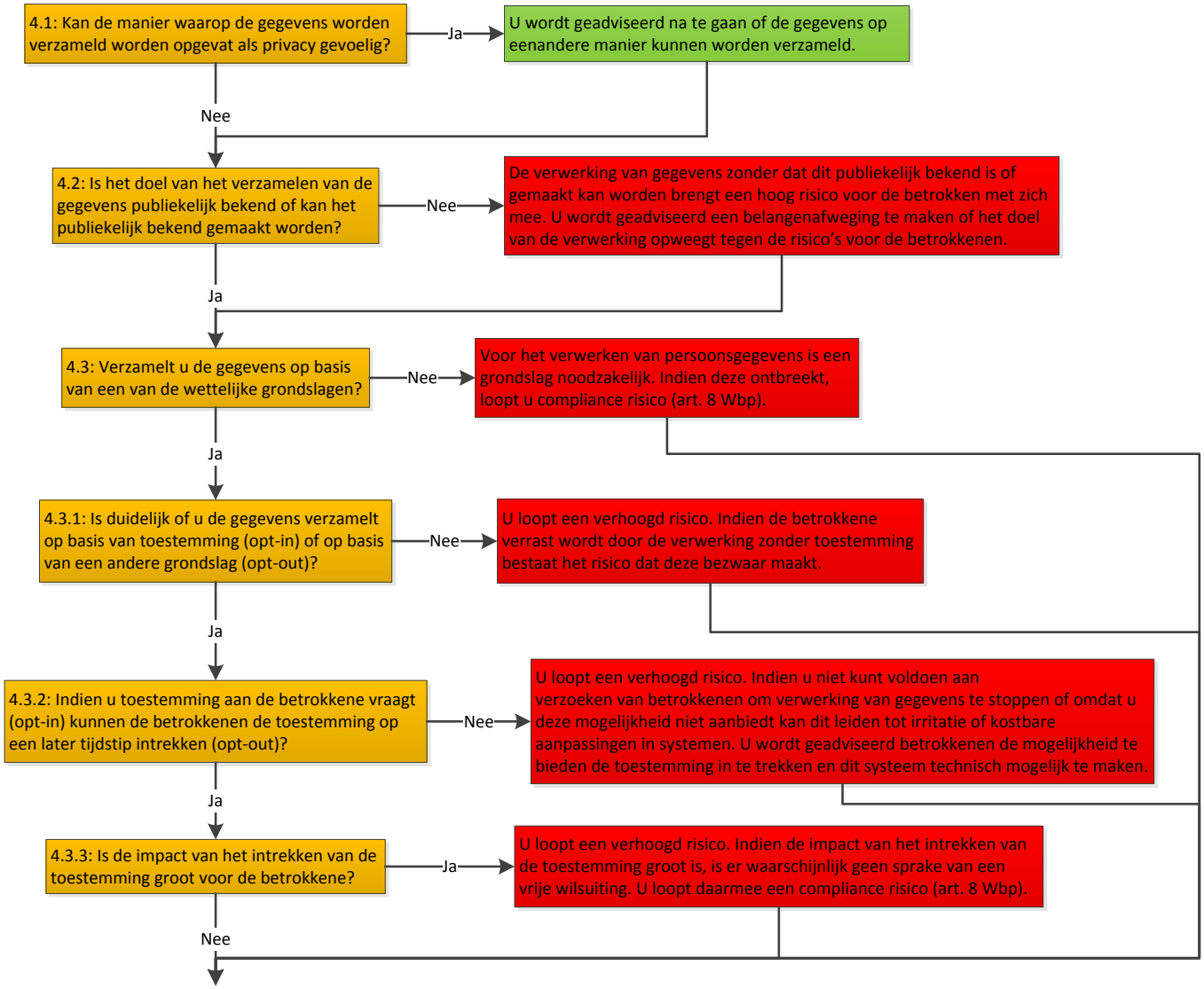

Legenda:
● Compleet nagelopen
○ Gedeeltelijk nagelopen
- Terecht uitgesloten
! Onterecht uitgesloten
Wbp >
PIA \/
Geen artikelen
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 76 77
True positive of true negative
5.7.1 Ja Nee
5.8 Ja Nee
Compliance met 42
5.8.1 Ja Nee
Compliance met 42
5.9 Ja Nee
5.10 Ja Nee
5.11 Ja Nee
6.1 Ja Nee
6.2 Ja Nee
6.3 Ja Nee
Compliance met 10
7.1 Ja Nee
7.2 Ja Nee

IV. Stroomschema PIA

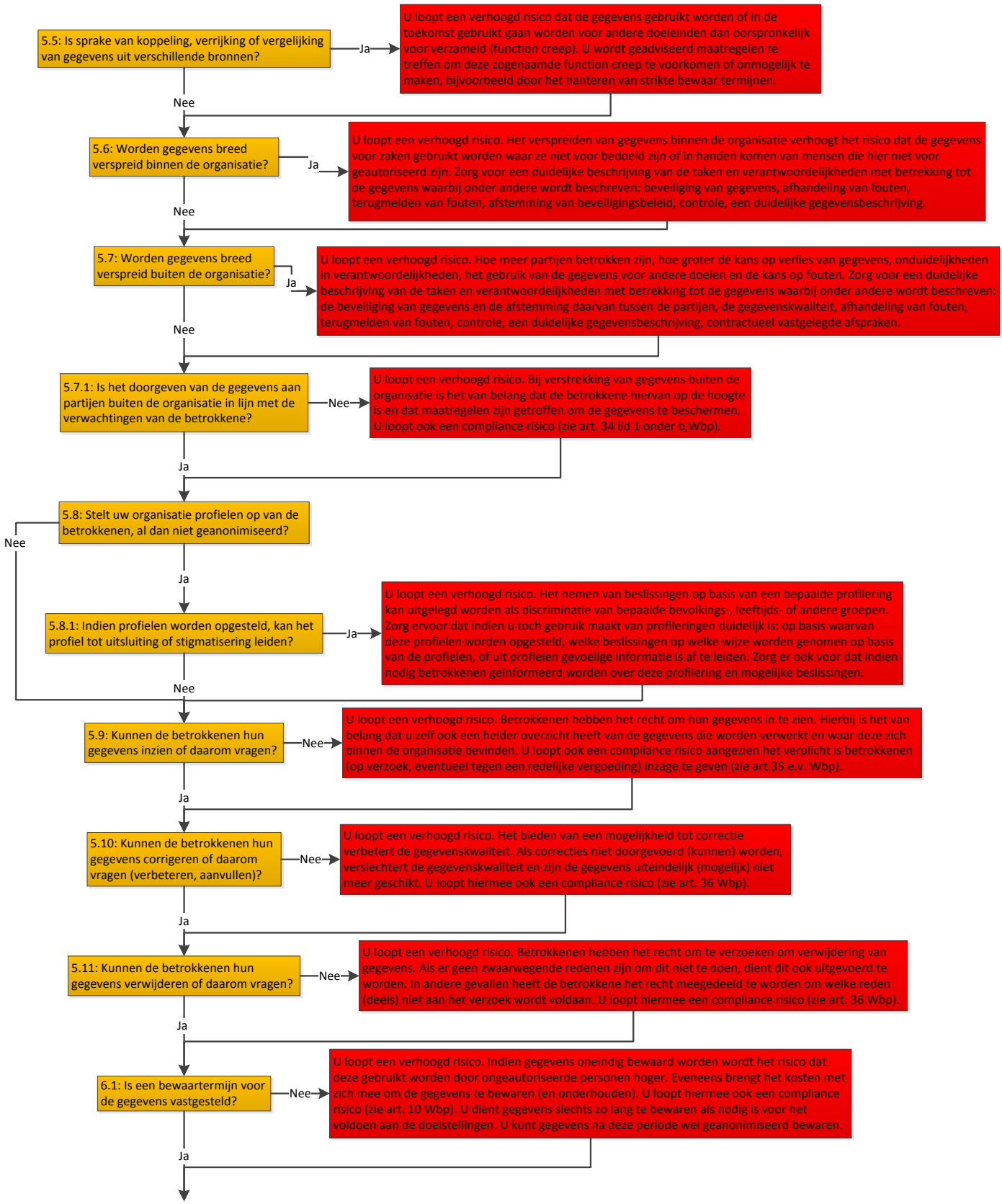


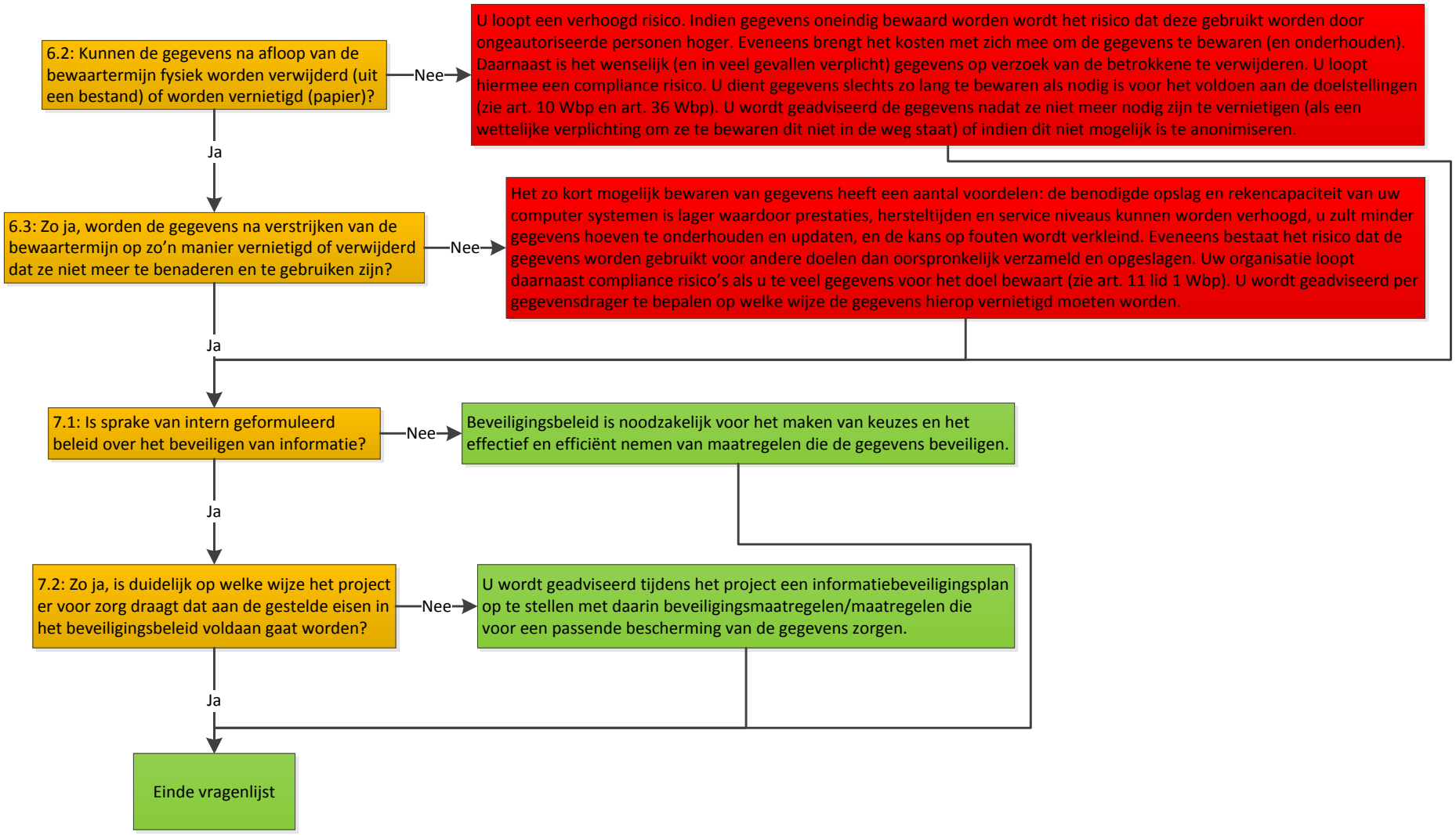

1.7: Is er (naast de Wbp) veel wet en regelgeving ten aanzien van persoonsgegevens waar het project mee te maken heeft?
Ja
U loopt een verhoogd risico. Hoe meer wet- en regelgeving hoe hoger het risico dat u hieraan niet voldoet. Een grote hoeveelheid wet- en regelgeving duidt tevens op het maatschappelijk belang dat wordt gehecht aan het onderwerp. U wordt geadviseerd de van toepassing zijnde wet- en regelgeving in kaart te brengen en de (privacy) consequenties inzichtelijk te maken.
Nee
1.8: Zijn er veel maatschappelijke belanghebbenden?
Ja
U loopt een verhoogd risico. De wijze waarop maatschappelijke belanghebbenden reageren varieert waardoor het project kan vertragen. U wordt geadviseerd een plan te maken waarin u aangeeft op welke manier de verschillende belanghebbenden bij het project worden betrokken of over het project worden geïnformeerd.
Nee
1.9: Zijn er veel partijen betrokken bij de uitvoering van het project?
Ja
U loopt een verhoogd risico. Het risico bestaat dat niet alle partijen zorgvuldig met gegevens omgaan die tijdens het project worden verzameld. Ook bestaat het risico dat de partijen de risico's en de inspanning die nodig is om deze te verminderen anders inschatten.
Nee
1.10: Is er een geschillenregeling/partij waar betrokkene terecht kan bij vragen of klachten?
Nee
U loopt een verhoogd risico. Een (onafhankelijke) partij waarbij geschillen kunnen worden beslecht draagt bij aan verbetering van de voorlichting, het imago en een evenwichtige belangenbehartiging. U wordt geadviseerd een contactpunt voor vragen en klachten aan te wijzen en waar mogelijk aan te sluiten bij een geschillenregeling.
Ja
2.1: Zijn alle gegevens nodig om het doel te bereiken (worden er zo min mogelijk gegevens verzameld)?
Nee
Het verwerken van zo min mogelijk gegevens heeft een aantal voordelen:
- De benodigde opslag en rekencapaciteit van uw computer systemen is lager, waardoor prestaties, hersteltijden en service niveaus kunnen worden verhoogd.
- U zult minder gegevens te hoeven onderhouden en updaten en de kans op fouten wordt verkleind.
Bovendien loop uw organisatie compliance risico's als u te veel gegevens voor het doel verzamelt. (zie Art 9, lid 1 en 2 Wbp).
Ja
2.2: Kan het doel met geanonimiseerde of gepseudonimiseerde gegevens worden bereikt (terwijl daar op dit moment geen gebruik van wordt gemaakt)?
Ja
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 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.
Nee
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)?
Ja
U loopt een verhoogd risico. Het risico bestaat dat de betrokkenen of de algemene opinie dit als een potentiële bedreiging voor hun privacy zien. Ook als de gegevens niet voor dit doel worden gebruikt bestaat het risico dat dit (in de toekomst) wel gebeurt. Voor de invoering van een personeelvolgsysteem is instemming van de OR nodig.
Nee
2.4.a: Is er sprake van verwerken van bijzondere persoonsgegevens?
Ja
Het werken met dit type gegevens brengt een verhoogd risico van misbruik met zich mee die (potentieel grote) impact op de betrokkene heeft en vraagt daarmee om betere beveiliging. Het verwerken van deze gegevens is alleen toegestaan onder bepaalde wettelijke voorwaarden (art. 16 e.v. Wbp).
Nee
2.4.b: Is er sprake van verwerken van uniek identificerende gegevens?
Ja
Het werken met dit type gegevens brengt een verhoogd risico van misbruik met zich mee die (potentieel grote) impact op de betrokkene heeft en vraagt daarmee om betere beveiliging. Het verwerken van deze gegevens is alleen toegestaan onder bepaalde wettelijke voorwaarden (zie ook art. 21 lid 4 Wbp).
Nee


2.4.c: Is er sprake van verwerken van een wettelijk voorgeschreven persoonsnummer?
Ja
Het verwerken van een uniek bij wet voorbeschreven 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).
Nee
2.4.d: Is er sprake van verwerken van andere gegevens dan hiervoor beschreven waarvoor geldt dat sprake is van een (gepercipieerde) verhoogde gevoeligheid?
Ja
Het werken met dit type gegevens brengt een verhoogd risico van misbruik met zich mee die (potentieel grote) impact op de betrokkene heeft en vraagt daarmee om betere beveiliging.
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?
Ja
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).
Nee
2.5: Verwerkt u gegevens over kwetsbare groepen of personen?
Ja
U loopt een verhoogd risico. Indien deze gegevens worden misbruikt heeft dit negatieve beeldvorming in de publieke opinie over de organisatie tot gevolg. U wordt geadviseerd maatregelen te treffen op een hoger beveiligingsniveau (zie art 13 Wbp) en betrokkenen de mogelijkheid te bieden zich aan de verwerking te onttrekken.
Nee
2.6: Hebben de gegevens betrekking op de gehele of grote delen van de bevolking?
Ja
U loopt een verhoogd risico. De kans op misbruik van de gegevens wordt groter naarmate u meer gegevens verwerkt. U wordt geadviseerd maatregelen te treffen op een hoger beveiligingsniveau (zie art 13 Wbp).
Nee
3.1: Zijn er (na afronding van het project) bij het verzamelen en verder verwerken van de gegevens meerdere interne partijen betrokken?
Ja
U loopt een verhoogd risico. Zorg voor duidelijke beschrijving van taken en verantwoordelijkheden met betrekking tot de gegevens waarbij onder andere wordt beschreven: Beveiliging van gegevens, afhandeling van fouten, terugmelden van fouten, afstemming van het beveiligingsbeleid.
Nee
3.2: Zijn er (na afronding van het project) bij het verzamelen en verder verwerken van de gegevens meerdere externe partijen betrokken?
Ja
U loopt een verhoogd risico. Hoe meer partijen betrokken zijn, hoe groter de kans op verlies van gegevens, onduidelijkheden in verantwoordelijkheden, het gebruik van de gegevens voor andere doelen en de kans op fouten. Zorg voor een duidelijke beschrijving van de taken en verantwoordelijkheden met betrekking tot de gegevens waarbij onder andere wordt beschreven: de beveiliging van gegevens en de afstemming daarvan tussen de partijen, de gegevenskwaliteit, afhandeling van fouten, terugmelden van fouten, en controle. Zorg ook voor een duidelijke gegevensbeschrijving. Leg afspraken contractueel vast.
Nee
3.2.1: Zijn er partijen betrokken (in het project of bij de verwerking) die zich niet aan met Nederland vergelijkbare privacywetgeving hoeven te houden?
Ja
U wordt geadviseerd na te gaan in hoeverre een adequaat beschermingsniveau wordt geboden door het betreffende land of de betreffende organisatie. Maak schriftelijke afspraken over hoe dit beschermingsniveau gehandhaafd kan worden.
Nee
3.2.2: Is de verstrekking van de gegevens aan derde partijen in lijn met het doel waarvoor de gegevens oorspronkelijk zijn verzameld?
Nee
Indien gegevens verstrekt worden aan andere partijen zonder dat deze gegevens daarvoor verzameld zijn bestaat het risico dat deze gegevens niet geschikt zijn voor het doel en dat betrokkenen worden geschaad door de verdere verspreiding van de gegevens. U heeft mogelijk een compliance risico (Zie art. 9 lid 1 en 2 Wbp).
Ja
3.2.3: Worden de gegevens verkocht aan de derde partijen?
Ja
U loopt een compliance risico. Het gebruik van gegevens van commerciele doelen stelt extra eisen. Zie art. 41 lid 3 Wbp).
Nee


4.1: Kan de manier waarop de gegevens worden verzameld worden opgevat als privacy gevoelig?
Ja
U wordt geadviseerd na te gaan of de gegevens op eenandere manier kunnen worden verzameld.
Nee
4.2: Is het doel van het verzamelen van de gegevens publiekelijk bekend of kan het publiekelijk bekend gemaakt worden?
Nee
De verwerking van gegevens zonder dat dit publiekelijk bekend is of gemaakt kan worden brengt een hoog risico voor de betrokken met zich mee. U wordt geadviseerd een belangenafweging te maken of het doel van de verwerking opweegt tegen de risico's voor de betrokkenen.
Ja
4.3: Verzamelt u de gegevens op basis van een van de wettelijke grondslagen?
Nee
Voor het verwerken van persoonsgegevens is een grondslag noodzakelijk. Indien deze ontbreekt, loopt u compliance risico (art. 8 Wbp).
Ja
4.3.1: Is duidelijk of u de gegevens verzamelt op basis van toestemming (opt-in) of op basis van een andere grondslag (opt-out)?
Nee
U loopt een verhoogd risico. Indien de betrokkene verrast wordt door de verwerking zonder toestemming bestaat het risico dat deze bezwaar maakt.
Ja
4.3.2: Indien u toestemming aan de betrokkene vraagt (opt-in) kunnen de betrokkenen de toestemming op een later tijdstip intrekken (opt-out)?
Nee
U loopt een verhoogd risico. Indien u niet kunt voldoen aan verzoeken van betrokkenen om verwerking van gegevens te stoppen of omdat u deze mogelijkheid niet aanbiedt kan dit leiden tot irritatie of kostbare aanpassingen in systemen. U wordt geadviseerd betrokkenen de mogelijkheid te bieden de toestemming in te trekken en dit systeem technisch mogelijk te maken.
Ja
4.3.3: Is de impact van het intrekken van de toestemming groot voor de betrokkene?
Ja
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).
Nee


4.4: Vertelt u tegen de betrokkene dat de gegevens worden verzameld?
Ja
Nee
4.4.1: Bij nee: Kunnen de betrokkenen op de hoogte zijn van het verzamelen van de gegevens?
Nee
Het verstrekken van informatie over welke gegevens worden verzameld draagt bij aan de transparantie en wekt vertrouwen bij de betrokkenen. Bovendien loopt u een compliance risico indien de informatie niet wordt verstrekt (zie art 33 e.v. Wbp).
Ja
4.4.2: Bij Ja (op vraag 4.4): Vertelt u tegen de betrokkene waarom de gegevens worden verzameld (wat u er mee gaat doen)?
Nee
Het verstrekken van informatie over wat u met de verzamelde gegevens gaat doen draagt bij aan de transparantie en wekt vertrouwen bij de betrokkenen. Bovendien loopt u een compliance risico indien de informatie niet wordt verstrekt (zie art. 33 e.v. Wbp).
Ja
4.4.3: Bij ja: (op vraag 4.4): Vertelt u tegen de betrokkene aan wie de gegevens worden verstrekt (daar waar dit geen wettelijke verplichting is)?
Nee
U wordt geadviseerd (per verstrekking) vast te leggen aan wie gegevens worden verstrekt. Eveneens wordt u geadviseerd om op het moment dat de gegevens worden verzameld, de betrokkenen te vertellen aan welke partijen de gegevens verstrekt zullenworden. Als laatste wordt u geadviseerd om als betrokkenen daarom vraagt hem te vertellen welke informatie wanneer aan wie is verstrekt.
Ja
4.5: Zou de betrokkene kunnen worden verrast door de verwerking (op het moment dat hij daarover wordt geïnformeerd)?
Ja
U loopt een verhoogd risico. Indien betrokkenen worden verrast door de gegevens verwerking bijvoorbeeld omdat meer gegevens worden verzameld dan op het eerste gezicht noodzakelijk is, of omdat het verdere gebruik niet in lijn is met het doel van verzamelen bestaat het risico dat de betrokkene de gegevens niet wil verstrekken of bezwaar maakt tegen het gebruik. U wordt geadviseerd na te gaan of de gegevens via een andere weg kunnen worden verzameld, of minder gegevens worden verzameld of dat de doelen van verder gebruik in lijn zijn met het doel van verzamelen.
Nee
5.1: Is het gebruik van de gegevens verenigbaar (in lijn) met het doel van het verzamelen?
Nee
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).
Ja
5.2: Worden gegevens gebruikt voor andere bedrijfsprocessen of doelen dan waar ze oorspronkelijk voor verzameld zijn?
Ja
Nee
5.2.1: Past het doel van dit bedrijfsproces bij het oorspronkelijke doel van verzamelen?
Nee
Het gebruik van de gegevens dient in overeenstemming met het oorspronkelijke 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).
Ja
5.3: Is de kwaliteit van de gegevens gewaarborgd, dat wil zeggen: zijn de gegevens actueel, juist en volledig?
Nee
U loopt een verhoogd risico. Het is van belang dat de verwerkte gegevens juist zijn om ervoor te zorgen dat geen verkeerde conclusies worden getrokken of verkeerde acties worden ondernomen. U loopt hiermee ook een compliance risico (zie art. 11 lid 2 Wbp).
Ja
5.4: Worden op basis van de gegevens beslissingen genomen over de betrokkene(n)?
Nee
Ja
5.4.1: Bij ja: leveren de gegevens een volledig en actueel beeld van de betrokkenen op?
Nee
Er bestaat een verhoogd risico dat er foutieve beslissingen genomen worden op basis van de gegevens waardoor schade voor betrokkenen of de organisatie kan ontstaan als gegevens onjuist, verouderd of onvolledig zijn.
Ja


5.5: Is sprake van koppeling, verrijking of vergelijking van gegevens uit verschillende bronnen?
Ja
U loopt een verhoogd risico dat de gegevens gebruikt worden of in de toekomst gebruikt gaan worden voor andere doeleinden dan oorspronkelijk voor verzameld (function creep). U wordt geadviseerd maatregelen te treffen om deze zogenaamde function creep te voorkomen of onmogelijk te maken, bijvoorbeeld door het hanteren van strikte bewaar termijnen.
Nee
5.6: Worden gegevens breed verspreid binnen de organisatie?
Ja
U loopt een verhoogd risico. Het verspreiden van gegevens binnen de organisatie verhoogt het risico dat de gegevens voor zaken gebruikt worden waar ze niet voor bedoeld zijn of in handen komen van mensen die hier niet voor geautoriseerd zijn. Zorg voor een duidelijke beschrijving van de taken en verantwoordelijkheden met betrekking tot de gegevens waarbij onder andere wordt beschreven: beveiliging van gegevens, afhandeling van fouten, terugmelden van fouten, afstemming van beveiligingsbeleid, controle, een duidelijke gegevensbeschrijving.
Nee
5.7: Worden gegevens breed verspreid buiten de organisatie?
Ja
U loopt een verhoogd risico. Hoe meer partijen betrokken zijn, hoe groter de kans op verlies van gegevens, onduidelijkheden in verantwoordelijkheden, het gebruik van de gegevens voor andere doelen en de kans op fouten. Zorg voor een duidelijke beschrijving van de taken en verantwoordelijkheden met betrekking tot de gegevens waarbij onder andere wordt beschreven: de beveiliging van gegevens en de afstemming daarvan tussen de partijen, de gegevenskwaliteit, afhandeling van fouten, terugmelden van fouten, controle, een duidelijke gegevensbeschrijving, contractueel vastgelegde afspraken.
Nee
5.7.1: Is het doorgeven van de gegevens aan partijen buiten de organisatie in lijn met de verwachtingen van de betrokkene?
Nee
U loopt een verhoogd risico. Bij verstrekking van gegevens buiten de organisatie is het van belang dat de betrokkene hiervan op de hoogte is en dat maatregelen zijn getroffen om de gegevens te beschermen. U loopt ook een compliance risico (zie art. 34 lid 1 onder b,Wbp).
Ja
5.8: Stelt uw organisatie profielen op van de betrokkenen, al dan niet geanonimiseerd?
Nee
Ja
5.8.1: Indien profielen worden opgesteld, kan het profiel tot uitsluiting of stigmatisering leiden?
Ja
U loopt een verhoogd risico. Het nemen van beslissingen op basis van een bepaalde profilering kan uitgelegd worden als discriminatie van bepaalde bevolkings-, leeftijds- of andere groepen. Zorg ervoor dat indien u toch gebruik maakt van profileringen duidelijk is: op basis waarvan deze profielen 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.
Nee
5.9: Kunnen de betrokkenen hun gegevens inzien of daarom vragen?
Nee
U loopt een verhoogd risico. Betrokkenen hebben het recht om hun gegevens in te zien. Hierbij is het van belang dat u zelf ook een helder overzicht heeft van de gegevens die worden verwerkt en waar deze zich binnen de organisatie bevinden. U loopt ook een compliance risico aangezien het verplicht is betrokkenen (op verzoek, eventueel tegen een redelijke vergoeding) inzage te geven (zie art.35 e.v. Wbp).
Ja
5.10: Kunnen de betrokkenen hun gegevens corrigeren of daarom vragen (verbeteren, aanvullen)?
Nee
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).
Ja
5.11: Kunnen de betrokkenen hun gegevens verwijderen of daarom vragen?
Nee
U loopt een verhoogd risico. Betrokkenen hebben het recht om te verzoeken om verwijdering van gegevens. Als er geen zwaarwegende redenen zijn om dit niet te doen, dient dit ook uitgevoerd te worden. In andere gevallen heeft de betrokkene het recht meegedeeld te worden om welke reden (deels) niet aan het verzoek wordt voldaan. U loopt hiermee een compliance risico (zie art. 36 Wbp).
Ja
6.1: Is een bewaartermijn voor de gegevens vastgesteld?
Nee
U loopt een verhoogd risico. Indien gegevens oneindig bewaard worden wordt het risico dat deze gebruikt worden door ongeautoriseerde personen hoger. Eveneens brengt het kosten met zich mee om de gegevens te bewaren (en onderhouden). 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.
Ja


6.2: Kunnen de gegevens na afloop van de bewaartermijn fysiek worden verwijderd (uit een bestand) of worden vernietigd (papier)?
Nee
U loopt een verhoogd risico. Indien gegevens oneindig bewaard worden wordt het risico dat deze gebruikt worden door ongeautoriseerde personen hoger. Eveneens brengt het kosten met zich mee om de gegevens te bewaren (en onderhouden). Daarnaast is het wenselijk (en in veel gevallen verplicht) gegevens op verzoek van de betrokkene te verwijderen. U loopt hiermee een compliance risico. U dient gegevens slechts zo lang te bewaren als nodig is voor het voldoen aan de doelstellingen (zie art. 10 Wbp en art. 36 Wbp). U wordt geadviseerd de gegevens nadat ze niet meer nodig zijn te vernietigen (als een wettelijke verplichting om ze te bewaren dit niet in de weg staat) of indien dit niet mogelijk is te anonimiseren.
Ja
6.3: 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?
Nee
Het zo kort mogelijk bewaren van gegevens heeft een aantal voordelen: de benodigde opslag en rekencapaciteit van uw computer systemen is lager waardoor prestaties, 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.
Ja
7.1: Is sprake van intern geformuleerd beleid over het beveiligen van informatie?
Nee
Beveiligingsbeleid is noodzakelijk voor het maken van keuzes en het effectief en efficiënt nemen van maatregelen die de gegevens beveiligen.
Ja
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?
Nee
U wordt geadviseerd tijdens het project een informatiebeveiligingsplan op te stellen met daarin beveiligingsmaatregelen/maatregelen die voor een passende bescherming van de gegevens zorgen.
Ja
Einde vragenlijst