HU University of Applied Sciences

Master of Informatics

MASTER'S THESIS

Efficiënter toezicht op compliance bij de verwerking van persoonsgegevens

Een onderzoek naar de toepasbaarheid van horizontaal toezicht op basis van Privacy by Design principes

Auteur
Dennis Teuben nr. 1189521

Supervisor
Dr. Bas van Gils

Datum
21-06-2021
HU University of Applied Sciences P.O. box 182
3500 AD UTRECHT
The Netherlands

Versie 1.0

Voorwoord

Privacy is steeds belangrijker. De waarde van data, zoals persoonsgegevens, zijn haast niet te overschatten. The Economist stelde in 2017 dat niet langer olie maar data de meest waardevolle grondstof ter wereld is.[1] Helaas zien we regelmatig dat het niet goed gaat met de bescherming van privacy bij de verwerking van persoonsgegevens. De schade bij privacy schendingen kan groot en soms onherstelbaar zijn. De recente datalekken in de GGD-registratiesystemen bij de bestrijding van de corona-pandemie is hier een pijnlijk actueel voorbeeld van.[2] Een dergelijk datalek ondermijnt daarnaast het vertrouwen in een betrouwbare overheid.

Aan de ene kant lijken consumenten bereid te zijn (meer) te betalen voor privacybescherming indien privacy-informatie zeer duidelijk aanwezig is op websites of applicaties (Tsai et al., 2011). Aan de andere kant komt een beeld naar voren dat consumenten geneigd zijn persoonlijke gegevens te delen als daar (economisch) gewin tegenover staat (Acquisto et al., 2006). Acquisti et al. (2013) laten in verschillende experimenten zien dat de waardebepaling van privacy en de keuze die de consument maakt zeer contextgevoelig is en afhangt van de 'framing' en het menselijk beslisgedrag.

Uit het Tweede Kamerdebat betreffende de toeslagenaffaire kwam onder andere naar voren dat het toezicht op de verwerking van persoonsgegevens te wensen over laat. Hier werd een verwijt gemaakt naar de toezichthouder, de Autoriteit Persoonsgegevens (AP), maar dat is niet helemaal terecht. De AP heeft te maken met capaciteitstekorten en kan daardoor bijna alleen reactief handelen. Er blijft nauwelijks tijd over om invulling te geven aan de adviserende functie van de AP ten aanzien van compliance.

In dit onderzoek wordt bezien of het toezicht effectiever en efficiënter ingezet kan worden door een 'horizontale' toezichtrelatie in te zetten. Daarvoor zal een intern controle-instrument ontwikkeld worden aan de hand van de principes van Privacy by Design.

Met dit onderzoek komt een eind aan een leerzame, interessante en intensieve periode. De parallel met een marathon is makkelijk gelegd, en geeft daarbij direct een doorkijkje naar mijn nieuwste ambitie voor de komende jaren. Dank gaat uit naar alle mensen die op een of andere manier hebben bijgedragen aan de totstandkoming van deze thesis. Bijzonder dank aan mijn begeleider Dr. Bas van Gils voor de niet aflatende steun en positieve woorden, medestudenten, en uiteraard mijn dappere dochter Sarah en lieve echtgenote Maaike voor hun eindeloze geduld.

Success is committing failure without losing enthusiasm. (Winston Churchill)

[1] https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.
[2] https://www.volkskrant.nl/nieuws-achtergrond/datalek-bij-ggd-gegevens-van-miljoenen-nederlanders-in-criminele-handen~b7f17bea/

Samenvatting

Deze thesis is geschreven als sluitstuk van een kwalitatief onderzoek met een tweetal doelstellingen. Enerzijds is het onderzoek erop gericht om te onderzoeken of de methode 'Privacy by Design' (PbD), gebruik makend van de zeven daarbij behorende principes, bij kunnen dragen aan het borgen van privacy compliance bij een overheidsorganisatie die persoonsgegevens verwerkt. Privacy by Design heeft als doel om al tijdens de ontwikkeling van informatiesystemen stil te staan bij privacy rechten van diegene wiens persoonsgegevens in het informatiesysteem worden verwerkt. Vragen als: "is het wel nodig om het geslacht te registeren" is een voorbeeld van een dergelijk punt van bewustwording.

Anderzijds wordt in dit onderzoek gekeken op welke manier het toezicht door de Autoriteit Persoonsgegevens verbeterd en versterkt kan worden. In de media verschijnen berichten vanuit de AP zelf met de strekking dat zij onvoldoende capaciteit hebben om goed toezicht te houden. Nog niet het topje van de ijsberg kan daadwerkelijk worden onderzocht, aldus de voorzitter van de AP. Laat staan dat de 'Autoriteit' persoonsgegevens zijn rol als kennisinstituut en adviseur daadkrachtig kan invullen. Daarom wordt een andere vorm van toezicht, die rond begin deze eeuw is ontwikkeld met als doel om toezicht te vereenvoudigen, zónder af te doen aan de eisen van wet- en regelgeving, onderzocht. Kan deze zogenaamde 'Horizontale Toezichtmethode' (HT) ertoe leiden dat organisaties zowel intrinsiek gemotiveerd raken om hun compliance te verhogen, en ertoe leiden dat de toezichthouder op een meer effectieve en efficiënte manier zijn rol als daadkrachtige autoriteit gestalte geeft.

Het onderzoek is op de volgende wijze uitgevoerd. Eerst worden de onderzoek elementen aangegeven die in samenhang worden bezien. De elementen worden uitgebreid toegelicht. Eerst wordt een nauwgezette kritische literatuurstudie uitgevoerd waarbij de elementen Privacy by Design (PbD) en Horizontaal Toezicht worden beschreven. Design science wordt gebruikt om het onderzoek te structureren. Literatuur en interviews geven de data. Uiteraard wordt het stil gestaan bij de ethische verantwoording van het onderzoek.
In hoofdstuk 3 van het onderzoek worden achtereenvolgens Privacy by Design, klassiek en horizontaal toezicht toegelicht. Vervolgens wordt het geheel vanuit zowel de constructieve als kritische kant belicht. Daarna volgt het construeren van het uiteindelijke artefact, het privacy control framework (PCF) aan de hand van de requirements ontleend aan de AVG en de criteria van HT. Daarbij wordt gekeken of deze requirements worden gedekt door de principes van PbD. Ook de respons uit de interviews worden in het ontwerp van het PCF meegenomen. Daarna volgt een validatie van het PCF waarbij het PCF is voorgelegd aan deskundigen door middel van interviews. Ten aanzien van HT vindt zelfs een dubbele validatie plaats. Volgens is bekeken of het ontworpen PCF bijdraagt aan het verhogen van de compliance en horizontaal toezicht. In het laatste hoofdstuk wordt discussie gevoerd of het PCF dan ook zorgt voor het verhogen van compliance, het inzetten van HT als toezicht vorm en wat de rol van de toezichthouder is en zou moeten zijn. Ook de deelvragen en de hoofdvraag wordt in dit laatste hoofdstuk beantwoord. Ten slotte wordt de contributie van het onderzoek, de beperkingen en suggesties voor vervolgonderzoek alsmede aanbevelingen voor vervolgonderzoek gegeven.

Inhoudsopgave

1. Inleiding

Dit inleidende hoofdstuk introduceert het onderzoek en schetst de context ervan voor de lezer. Het onderzoek start met in paragraaf één de introductie op het onderwerp waarna in paragraaf 1.2 de probleemstelling wordt toegelicht. In deze paragraaf zal tevens de doelstelling en vraagstelling voortkomend uit de probleemstelling geformuleerd worden. Vervolgens wordt in paragraaf 1.3 de afbakening van dit onderzoek beschreven en tot slot in paragraaf 1.4 de relevantie van dit onderzoek.

1.1 Introductie in het onderzoek

Privacy is in onze maatschappij steeds belangrijker. Als het mis gaat is de schade groot en soms onmogelijk te herstellen; 'Voorkomen is beter dan genezen'. Voldoen aan wet- en regelgeving wordt compliance genoemd. In dit onderzoek wordt compliance benaderd vanuit de context van de Koninklijke Marechaussee, een overheidsinstantie die ten behoeve van zijn taakstelling veel persoonsgegevens verwerken. Het probleem dat in dit onderzoek wordt onderzocht is op welke manier privacy beter kan worden geborgd en het toezicht op compliance effectiever en efficiënter kan worden. Hierbij wordt gekeken naar de privacy rechten voor individuen bij de verwerking van persoonsgegevens. Er wordt niet gekeken naar informatie-beveiligingsaspecten en cybersecurity. Het onderzoek wordt uitgevoerd aan de hand van de design science methode van Wieringa. Dit onderzoek is van belang omdat het toezicht op privacy en de schending van privacy rechten ten aanzien van individuen een actueel probleem is. Pijnlijke getuigen van de noodzaak van privacybescherming zijn onder andere:

- *Onderzoek door de Autoriteit Persoonsgegevens naar het UWV m.b.t. cliëntgegevens;*[3]
- *Berichtgeving rondom de registratie van persoonsgegevens van tienduizenden Nederlanders die onvoldoende beveiligd waren;*[4]
- *De boete van 440.000 euro die de AP oplegt aan het OLVG in Amsterdam voor ongeautoriseerde toegang tot patiëntendossiers.*[5]

1.1.1 Wat is privacy

Een persoonsgegeven wordt in de Algemene Verordening Gegevensbescherming (AVG) gedefinieerd als '*alle gegevens die iets zeggen over een persoon'*. Wanneer dit persoonsgegeven, al dan niet in combinatie met andere gegevens, iemand kan identificeren zonder dat daarvoor bijzondere inspanning moeten worden geleverd, dan is de privacy in het geding. Persoonsgegevens zijn te verdelen in twee soorten; *normale* persoonsgegevens en *bijzondere* persoonsgegevens. Privacy is een grondrecht en

[3] https://www.trouw.nl/economie/gegevens-miljoenen-oud-uwv-klanten-makkelijk-in-te-zien-het-interesseert-ze-niet-bij-uwv~b1af9852/.
[4] https://nos.nl/nieuwsuur/artikel/2365412-persoonsgegevens-tienduizenden-geteste-nederlanders-onvoldoende-beveiligd.html.
[5] https://autoriteitpersoonsgegevens.nl/nl/nieuws/ziekenhuis-olvg-beboet-om-onvoldoende-beveiliging-medische-dossiers.

verankerd in artikel 10 van de Grondwet. Dit artikel zegt: *"Ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op eerbiediging van zijn persoonlijke levenssfeer."* Daarnaast worden persoonsgegevens beschermd als onderdeel van het privéleven in de zin van artikel 8 van het Europees Verdrag voor de Rechten van de Mens (EVRM) en artikel 17 van het Internationaal Verdrag inzake Burgerlijke en Politieke Rechten (IVBPR). Om deze rechten te beschermen is de AVG opgesteld en wordt uitvoering gegeven aan verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016.

1.1.2 Compliance

De AVG zorgt voor strengere waarborgen op het gebied van gegevensbescherming, geeft burgers meer en sterkere rechten, biedt meer transparantie en zorgt ervoor dat alle personen die persoonsgegevens verwerken binnen het toepassingsgebied van de AVG, meer rekenschap moeten afleggen en een grotere verantwoordelijkheid dragen (Europees Parlement, 2020). De AVG geeft meer rechten aan individuen en verplicht organisaties meer verantwoordelijkheid zorgvuldigheid in acht te nemen in het verwerken van persoonsgegevens en burgers daarover goed te informeren. Denk hierbij bijvoorbeeld aan het recht op bezwaar tegen de verwerking van persoonsgegevens. Omdat het afstaan van persoonsgegevens vaak onbewust, ondoordacht of noodgedwongen plaatsvindt, is het belangrijk dat wetgeving rondom privacy door organisaties goed nageleefd wordt. Voor naleving wordt in deze thesis de term 'compliance' gehanteerd. Compliance moet ervoor zorgen dat de organisatie al haar verplichtingen nakomt en binnen de vastgestelde grenzen opereert (Vicente & Mira Da Silva, 2011).

Om privacy te borgen worden interne en externe controles uitgevoerd. Daartoe zijn organisaties (dus ook overheden) op grond van art. 37 AVG verplicht om een Functionaris Gegevensbescherming (FG) aan te stellen. Deze functionaris is de interne toezichthouder. De organisatie moet de Autoriteit Persoonsgegevens informeren over wie binnen hun organisatie de Functionaris Gegevensbescherming is. De AP zelf voert daarnaast externe controles, zgn. audits, uit ten aanzien van de verwerking van persoonsgegevens door organisaties.

1.1.3 Non-compliance

Non-compliance is het niet voldoen aan de wet- en regelgeving. Dit kan leiden tot sancties variërend van een aanzienlijke boete tot het intrekken van bijv. een vergunning, maar kan ook reputatieschade tot gevolg hebben. Daarom staat compliance bij organisaties steeds vaker hoog op de agenda. Compliance wordt hierbij vaak als een middel gezien om risico's te beheersen, in plaats van een doel op zich. Hiertoe ontwikkelen organisaties compliance programma's en stellen zij de wettelijk verplichte functionaris gegevensbescherming aan. Het is dus niet de vraag óf maar hóe non-compliant c.q. onrechtmatig gebruik van informatiesystemen voorkomen moet worden. Compliance is wat anders dan alle mogelijke risico's op non-compliance met een waslijst van maatregelen mitigeren.

1.1.4 Privacy Control Framework

Het primaire doel van een privacy control framework (PCF) is volgens Ridderbeekx om organisaties te begeleiden met betrekking tot privacy en bescherming van persoonsgegevens (Ridderbeekx & Scheuller, 2018). Als zodanig kan het PCF worden gebruikt als startpunt voor privacy audits. Het PCF bevat de voorgeschreven beheersingsdoelstellingen en beheersingsmaatregelen. In deze thesis zijn deze geformuleerd als requirements, strategieën en tactieken die daarvoor gebruikt worden. Daarnaast kan de PCF door een organisatie worden ingezet om de adequaatheid van privacy controles te beoordelen of om de hiaten te bepalen tussen de huidige staat van privacy controle en hun ambities in het licht van (veranderende) wetgevende kaders (bijv. De AVG).

Bij de verwerking van persoonsgegevens die waarschijnlijk een hoog privacy risico opleveren is een Data Protection Impact Assessment (DPIA) verplicht gesteld, ook wel de gegevensbeschermingseffectbeoordeling genoemd. Een DPIA is een methode die op een systematische en gestructureerde manier helpt om privacy risico's inzichtelijk te maken (Van Lieshout et al., 2012).

> *Definitie 1 – data Privacy Impact Assessment (DPIA) is een analyse-instrument om de privacy risico's voor personen te identificeren en te analyseren bij nieuwe of bestaande verwerkingen van persoonsgegevens door een organisatie* (Bieker et al., 2016).

Het belangrijkste doel van de DPIA is het creëren van bewustwording en inzicht in de privacy- en compliance-risico's die organisaties en personen kunnen lopen. Daarmee zijn de risico's onderkent maar niet gemitigeerd. Ridderbeekx & Scheuller (Ridderbeekx & Scheuller, 2018) noemen als nadeel van de DPIA-vragenlijst dat deze puur uitgaat van de wettelijke vereisten van de AVG. Dat terwijl de DPIA feitelijk een instrument is om privacy risico's van een gegevensverwerking inzichtelijk te maken en vervolgens te verkleinen of te mitigeren. Daarbij gaat het met name om de risico's voor personen van wie de gegevens worden verwerkt, maar ook om de gegevens van organisaties zelf. Om deze risico's weg te nemen of te verkleinen zullen beheersmaatregelen moeten worden opgesteld.

> *Definitie 2 – beheersmaatregel: activiteiten waarmee de kans van optreden of de gevolgen van risico's worden beïnvloed.*

Een dergelijk samenhangend geheel van beheersmaatregelen wordt ook wel een privacy control framework genoemd (Ridderbeekx & Scheuller, 2018). Een control framework enkel en alleen op de AVG gebaseerd zal dan ook in het beste geval de wettelijke privacy en compliance-risico's afdekken, maar ook niet meer dan dat (Ridderbeekx & Scheuller, 2018). Juist in dit onderzoek wordt bezien of de benadering vanuit Privacy by Design leidt tot niet alleen het verbeteren van compliance maar ook om de systeemtechnische risico's inzichtelijk te maken en te mitigeren. De organisatie gaat daarmee dus verder dan het enkel voldoen aan de juridische eisen uit de AVG, maar wil er ook voor zorgen dat het toezicht waaraan zij zijn onderworpen door het PCF wordt vereenvoudigd.

Informatiesystemen zouden volgens Julisch en Lohmann zo ontworpen moeten zijn dat zij geen onrechtmatig gebruik of toepassing toestaan, 'compliance vanuit het ontwerp' (Julisch et al., 2011) en (Lohmann, 2013). Er zijn voorbeelden van onrechtmatige gebruik te over, denk aan het exporteren van persoonsgegevens uit de GGD-database in de registratie van corona-vaccins. Deze systeem gebaseerde controle vereist een nieuwe auditaanpak waarbij organisaties moeten aantonen aan de controlerende instantie dat ze 'compliant' zijn. Organisaties moeten zelf de impact van regelgeving o.a. op hun informatiesystemen beschouwen, motiveren welke reeks beheersmaatregelen zij hebben genomen om hieraan te voldoen, en aantonen dat de beheersmaatregelen effectief zijn (Burgemeestre et al., 2011). Daarbij kan een PCF bruikbaar zijn. Deze fungeert daarbij als een gestructureerd beheersingskader dat de uitvoering van het toezicht faciliteert. In het PCF worden de beheersingsdoelstellingen als requirements opgenomen, de bijbehorende strategie en tactiek weergegeven. Het doel is uiteindelijk om op een eenduidige wijze verantwoording af te leggen. Een privacy control framework maar het mogelijk om met de controlerende instantie, in casu de Autoriteit Persoonsgegevens de dialoog aan te gaan over de vraag of de onderkende requirements voor het rechtmatig verwerken van persoonsgegevens, in toereikende mate wordt gehaald door het gebruik van een PCF.

1.1.5 Horizontaal toezicht

De manier waarop toezicht is vormgegeven kan eenvoudiger door middel van het overeenkomen van een horizontale toezichtrelatie, uitgaande van vertrouwen, begrip en transparantie. Horizontaal toezicht[6] gaat uit van een min- of meer gelijkwaardige relatie tussen de gecontroleerde en de toezichthouder. Horizontaal toezicht is in 2005 ontstaan als vorm van overheidstoezicht en wordt in de literatuur ook wel 'cooperative compliance' genoemd. Cooperative compliance kan in die zin beschouwd worden als een voorloper van horizontaal toezicht en is gericht op het vergroten van de vrijwillige naleving, van wet- en regelgeving (De Widt, 2017). In deze thesis wordt voor cooperative compliance een definitie ontleend aan Huiskers-Stoop en Gribnau en kan dit worden omschreven als:

> *Definitie 3 – cooperative compliance: De totstandkoming van een op wederzijds vertrouwen en vrijwillige regelnaleving gebaseerde relatie tussen een organisatie en toezichthouder, teneinde een juiste rechtspositie vast te stellen* (Huiskers & Gribnau, 2019)

Horizontaal toezicht kan worden gezien als een vorm van cooperative compliance maar zijn feitelijk elkaars gelijken en zullen beide resulteren in een eenvoudigere en efficiëntere naleving van wet- en regelgeving en toezicht daarop. In par. 2.3 wordt hierop uitgebreid ingegaan. In deze thesis wordt ten aanzien van Horizontaal Toezicht de volgende definitie, ontleend aan Huiskers-Stoop en Diekman (2012) aangehouden:

[6] Horizontaal toezicht wordt hier losjes gedefinieerd. In paragraaf 3.3 wordt hierbij uitgebreid stilgestaan.

Definitie 4 – horizontaal toezicht: (Overheids)toezicht gebaseerd op wederzijds vertrouwen, begrip en transparantie, waarbij de organisatie in ruil voor vrijwillige en actuele verstrekking van relevante gegevens snel zekerheid krijgt over zijn rechtspositie en gevrijwaard is van actieve controle achteraf door de toezichthouder.

1.2 Probleemstelling

Burgers staan er vaak niet bij stil dat organisaties hun persoonsgegevens verwerken, of zij hebben in veel gevallen geen andere keus dan hun persoonsgegevens af te staan ten einde toegang te krijgen tot een bepaald systeem of (geautomatiseerd) proces. Een voorbeeld is de geautomatiseerde grenspassagecontrole op de Luchthaven Schiphol waarbij de reiziger feitelijk geen keuze heeft in de persoonsgegevens die hij daarbij afstaat. Deze persoonsgegevens worden op dat moment door de Koninklijke Marechaussee (KMar) verwerkt. De KMar heeft niet de beschikking over een instrument dat ervoor zorgt dat bij het ontwikkelen en het gebruik van informatiesystemen aan compliance eisen wordt voldaan. Compliance wordt soms pas in ogenschouw genomen als een systeem al wordt gebruikt, en dat is te laat. Aanpassingen doen aan een informatiesysteem in een dermate laat stadium zijn vaak complex en onnodig kostbaar (Schaar, 2013). Daar komt bij dat het voor de KMar lastig is om bij de toezichthouder aan te tonen dat zij compliant zijn met betrekking tot de verwerking van persoonsgegevens. De KMar ontbeert een instrument waarmee het eenvoudiger is om intern de organisatie te onderzoeken of informatiesystemen compliant zijn ten aanzien van de verwerking van persoonsgegevens. Dit instrument zou de KMar moeten ondersteunen bij het aantonen aan de externe toezichthouder dat zij ‘compliant’ handelen ten aanzien van de verwerking van persoonsgegevens.

De hypothese van dit onderzoek is dat met het een privacy control framework de KMar meer grip krijgt op compliance ten aanzien van de verwerking van persoonsgegevens. Dit privacy control framework wordt ontwikkeld op basis van de principes van ‘Privacy by Design’. Daarnaast wordt onderzocht of het privacy control framework kan worden gebruikt om tot een horizontale toezichtrelatie met de AP te komen.

Deze thesis is een onderzoek naar een instrument welke een fundamentele bijdrage moet leveren aan compliance en het toezicht op de verwerking van persoonsgegevens moet verbeteren. Dit onderzoek richt zich op de volgende vraag:

Hoe kan een privacy control framework, op basis van Privacy by Design principes bijdragen aan implementatie van Horizontaal Toezicht?

De thesis betreft een ontwerpend onderzoek ook wel design science genoemd. De beantwoording van onderstaande deelvragen draagt bij aan zowel het ontwerpen van het artefact als aan de beantwoording

van de hoofdvraag. De deelvragen zijn verklarend (1 en 2) ontwerpend (3) en validerend (4 en 5) van aard. Deze onderverdeling van de deelvragen past op de design science methode van Wieringa die hieronder in paragraaf 1.2.1 wordt toegelicht.

1. Wat is een privacy control framework?
2. Hoe werkt horizontaal toezicht?
3. Hoe ziet een privacy control framework op basis van de principes van Privacy by Design eruit?
4. Hoe kan een privacy control framework bijdragen aan compliance?
5. Op welke manier kan een control framework bijdragen aan horizontaal toezicht?

1.2.1 Introductie in het onderzoek

Het onderzoek valt uiteen in een vijftal deelvragen waarvan de uitkomsten samen dienen ter beantwoording van de hoofdvraag. Deelvraag een en twee worden door middel van literatuuronderzoek beantwoord. Het betreft hier met name het verduidelijken van definities en het positioneren daarvan in hun specifieke context. In deelvraag drie komen zowel literatuur als reacties van respondenten bij elkaar. De design science methode van Wieringa wordt gebruikt om het privacy control framework te ontwerpen. Deze methode wordt in paragraaf 3.2.1 uitgewerkt. Op basis van de ontstane inzichten uit de literatuurstudie en interviews wordt, door gebruik te maken van de principes van Privacy by Design, een privacy control framework ontworpen. Deelvragen vier en vijf toetsen het ontworpen privacy control framework op bruikbaarheid. Het PCF wordt door middel van interviews met deskundigen uit de defensieorganisatie gevalideerd. Getoetst wordt of het framework bijdraagt aan compliance en of deze het mogelijk maakt om te komen tot horizontaal toezicht. Met name het laatste aspect is dubbel bevraagd in een gesprek met een autoriteit op het terrein van HT. Het onderzoek resulteert in een praktisch toepasbaar privacy control framework waarbinnen strategieën en tactieken zijn geformuleerd om concrete en praktische invulling te geven aan de zeven principes van Privacy by Design.

1.2.2 Probleem

Persoonsgegevens zijn een vorm van data en in veel gevallen privacygevoelig. Vanaf 25 mei 2018 moeten alle organisaties die met persoonsgegevens werken voldoen aan de Algemene Verordening Gegevensbescherming. De AVG is het Nederlandse equivalent van de Europese General Data Protection Regulation (GDPR). In deze thesis zal hierna gesproken worden over de AVG, tenzij het voor de nauwkeurigheid nodig is om de Europese benaming te hanteren. De AVG is een verordening waardoor deze automatisch na inwerkingtreding doorwerkt in de Nederlandse rechtsorde. De AVG heeft alleen betrekking op de verwerking van persoonsgegevens binnen EU-grondgebied, of als de verwerking gaat over onderdanen van de Europese Unie. De AVG is een set van regels om de privacy rechten van natuurlijke personen te beschermen. Organisaties die daar niet aan voldoen zijn niet compliant en riskeren zware boetes. In het geval van non-compliance kan een toezichthouder een boete

opleggen van ten hoogste 20 miljoen euro of van maximaal 4% van de wereldwijde jaaromzet van een organisatie. Artikel 51 van de AVG stelt;

> *'Elke lidstaat bepaalt dat één of meer onafhankelijke overheidsinstanties verantwoordelijk zijn voor het toezicht op de toepassing van de verordening, teneinde de grondrechten en fundamentele vrijheden van natuurlijke personen in verband met de verwerking van persoonsgegevens te beschermen en het vrije verkeer van persoonsgegevens binnen de Unie te vergemakkelijken'.*

Vervolgens is het de Uitvoeringswet AVG (UAVG) die in art. 6 lid 2 de Autoriteit Persoonsgegevens aanwijst als toezichthoudende instantie in Nederland. Volgens de site van de Rijksoverheid[7] is de AP de onafhankelijke toezichthouder in Nederland die de bescherming van persoonsgegevens bevordert en bewaakt. De AP houdt toezicht op de naleving van de wettelijke regels voor bescherming van persoonsgegevens. Echter, het is bijzonder slecht gesteld met de handhaving van deze privacywet, getuige o.a. het nieuwsbericht van 25 maart 2021.[8] De vraag is of meer geld dit probleem op zal lossen. Misschien is er een andere, meer effectieve en efficiëntere toezichtmethode nodig?
Andere belangrijke taken van de AP zijn onder meer adviseren over nieuwe regelgeving en voorlichting geven over de privacywetgeving. De AVG geeft aan dat een persoonsgegeven alle informatie is die herleidbaar is tot of iets kunnen zeggen over, een geïdentificeerde of identificeerbare natuurlijke persoon. Dit betekent dat deze gegevens ofwel direct over een persoon gaan, dan wel naar deze persoon te herleiden zijn. De formele definitie van persoonsgegeven is te vinden in art. 4 lid 1 AVG en luidt:

> *Definitie 5 - persoonsgegeven: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ("de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een 'identificator' zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.*

De belangrijkste bepalingen uit de AVG ten aanzien van de bescherming van persoonsgegevens zijn de privacy-rechten van natuurlijke personen, en de verantwoordelijkheid van organisaties om deze rechten te waarborgen. Er zijn in het kader van verwerking van persoonsgegevens een aantal belangrijke waarborgen af te leiden uit art. 5 van de AVG.

1. De AVG schrijft voor dat een organisatie altijd transparant moet zijn over de verwerking van persoonsgegevens.

---

7 https://www.rijksoverheid.nl/contact/contactgids/autoriteit-persoonsgegevens.
8 https://nos.nl/nieuwsuur/artikel/2374135-de-privacywet-wordt-amper-gehandhaafd-is-meer-geld-de-oplossing.html.

2. De AVG zegt daarnaast dat een organisatie alleen gegevens mag verzamelen voor gerechtvaardigde doeleinden de zogenaamde ‘doelbinding’.
3. De AVG schrijft verder dat alleen gegevens bewaard mogen worden die voor de bedrijfsvoering noodzakelijk zijn. Dit is het principe van ‘minimale gegevensverwerking’.
4. Voornoemd artikel uit de AVG voegt daar ten slotte aan toe dat er passende technische óf organisatorische maatregelen moeten worden genomen om een passende beveiliging (van persoonsgegevens) te waarborgen.

In dit kader speelt Privacy by Design een belangrijke rol. Deze ontwerpfilosofie ‘bakt’ privacy al door het hele systeem tijdens de ontwikkelingscyclus aldus Hoepman et.al (Colesky et al., 2016) Privacy by Design wordt in paragraaf 3.1 verder uitgewerkt.

Waarborg één en twee passen goed bij het recht op privacy van natuurlijke personen. Waarborg drie en vier geven een formele invulling aan de verantwoordelijkheid van organisaties om de privacy rechten te waarborgen. Om invulling te geven aan deze waarborgen is een gestructureerd beheersingskader nodig. Een privacy control framework biedt een dergelijk kader. Hierin worden de requirements, doelstellingen en de beheersmaatregelen in de vorm van strategieën van tactieken opgenomen. Onderstaande definitie, is gebaseerd op NOREA en wordt in deze thesis gehanteerd.

> *Definitie 6 – Privacy Control framework: is een instrument van interne beheersing dat is bedoeld om organisaties te ondersteunen bij het compliant verwerken van persoonsgegevens* (*NOREA*, 2019).

In het te ontwerpen PCF wordt uitgegaan van de invulling van deze waarborgen door middel van de principes van Privacy by Design. Privacy by Design is zoals o.a. Hoepman en Colesky (Koops et al., 2014; Colesky et al., 2016) schrijven een gebruikelijk en geaccepteerd uitgangspunt wanneer nagedacht wordt over privacy. Het PCF maakt de dialoog mogelijk tussen een organisatie en een toezichthouder over de vraag of daarmee de interne beheersingsmaatregelen voor de rechtmatige verwerking van persoonsgegevens in voldoende mate worden nageleefd. De dialoog kan ertoe leiden dat de partijen de toezichtrelatie horizontaler willen maken om redenen van efficiency en effectiviteit. Ervaring hiermee is opgedaan door de belastingdienst in de fiscale context en is een populair onderwerp van gesprek en onderzoek (Van der Hel & Siglé, 2019). Het ontwerpen van een PCF is niet eenvoudig, daarom wordt in deze thesis de design science methodologie van Wieringa toegepast, waarbij Privacy by Design geldt als bouwsteen waaruit principes ontleend worden.

1.3 Afbakening

Dit onderzoek bekijkt compliance met betrekking tot de verwerking van persoonsgegevens vanuit het perspectief van een grote overheidsorganisatie. De Koninklijke Marechaussee is in Nederland verantwoordelijk voor de grensbewaking. Dit is een wettelijke taak waarbij enorme hoeveelheden persoonsgegevens van reizigers die de grens willen passeren worden verwerkt, soms al voor de reiziger zich bij de grens meldt. Het is de KMar die als verwerkingsverantwoordelijke aan moet tonen dat de verwerking van persoonsgegevens rechtmatig en gerechtvaardigd is. Het is daarom voor de KMar van

belang dat zij aan de toezichthouder aan kunnen tonen dat zij bij de verwerking van persoonsgegevens compliant zijn. Het is dus waardevol om te onderzoeken of een instrument in de vorm van een privacy control framework hierbij helpt. Het perspectief van de betrokkene wiens persoonsgegevens worden verwerkt wordt niet onderzocht. Hier speelt met name een persoonlijk belang welke meer op het juridische vlak ligt. Het ontworpen instrument wordt gevalideerd tegen de requirements die de AVG stelt aan privacy, en aan de criteria van horizontaal toezicht. Er wordt niet gekeken naar de werking van het framework vanuit een implementatietraject, dat valt buiten de scope van deze thesis.

1.4 Relevantie

In een vrije democratische samenleving moeten mensen erop kunnen vertrouwen dat organisaties zorgvuldig omgaan met hun persoonsgegevens. Uit onderzoek dat in 2019 door de Autoriteit Persoonsgegevens is uitgevoerd blijkt dat Nederlanders zich zorgen maken over hun privacy. Uit dat onderzoek blijkt dat 94% van de mensen zich zorgen maakt over de bescherming van hun persoonsgegevens, en zich vooral zorgen maken over misbruik van het identiteitsbewijs, het volgen van online zoekgedrag en wifitracking. Op het moment van schrijven van deze thesis woedt een verhitte discussie over het gebruik van gevoelige (medische) persoonsgegevens ten aanzien van de bestrijding van de verspreiding van Covid-19. Hiervoor is een Corona-app ontwikkeld. De app helpt het contactonderzoek van de GGD door vroegtijdig te waarschuwen als de gebruiker ‘mogelijk’ besmet is. De app geeft dan advies wat de gebruiker het beste kan doen om te voorkomen dat hij of zij het virus onbewust op anderen overdraagt. In januari 2021 bleek dat het registratiesysteem van de GGD een lek te bevatten waardoor persoonsgegevens van duizenden Nederlanders op straat kwamen te liggen. Na onderzoek bleek dat het systeem een ‘export’ functie te bevatten waardoor dit mogelijk werd. Een functie in het systeem die onnodig is, en onderkent had kunnen worden als privacy principes al tijdens het ontwikkelen van het systeem in acht waren genomen. De ontwikkeling rondom de bestrijding van corona vallen buiten de scope van deze thesis, maar geven een actueel voorbeeld van een ontwikkeling waarbij privacy-issues zeer belangrijk zijn, en waarbij Privacy by Design principes toepasbaar zijn. De autoriteit persoonsgegevens blijft de ontwikkeling nauwgezet volgen.

De relevantie van dit onderzoek is drieledig, er is sprake van zowel praktische, maatschappelijke als wetenschappelijke relevantie. Deze drie gebieden worden hieronder geduid.

1.4.1 Praktische relevantie

Met het beantwoorden van de centrale vraag wordt duidelijk of, en zo ja onder welke omstandigheden, tot een nieuwe manier van toezicht kan worden gekomen door gebruik te maken van een privacy control framework. Met het PCF krijgt de KMar een instrument tot haar beschikking waarmee zij enerzijds beter in staat is om hun interne controles met betrekking tot compliance bij het verwerken van persoonsgegevens in te richten. Anderzijds zal dit instrument de KMar helpen bij het overleggen van bewijs aan de toezichthouder dat zij ‘compliant’ zijn ten aanzien van de verwerking van persoonsgegevens in haar informatiesystemen. Nu al worden er interne controles uitgevoerd door de

functionaris gegevensbescherming, maar deze beperken zich nog tot het bezien van de aanwezigheid van bijv. een DPIA en de actualiteit ervan. Een methode om diepgaand op de naleving van privacy rechten en informatiebeveiliging in te zoomen ontbreekt tot op heden, volgens een van de respondenten in een interview.

1.4.2 Maatschappelijke relevantie

Het ontworpen PCF moet ertoe leiden dat de privacy van individuen te allen tijde voldoet aan de eisen die wet- en regelgeving aan de verwerking stellen. De informatiesystemen die op dit moment worden gebruikt zijn waarschijnlijk niet allemaal compliant. Interne en externe controle kan ertoe leiden dat systemen moeten worden aangepast, wat vaak erg ingewikkeld en kostbaar is (Schaar, 2013). Daarnaast kan de toezichthouder, op het moment dat blijkt dat verwerking van persoonsgegevens echt onrechtmatig is de organisatie een boete toebedelen. Dit is niet alleen een financieel risico, maar leidt in veel gevallen ook tot imago-schade. Effecten die voor iedere organisatie onwenselijk zijn. Dit onderzoek moet eraan bijdragen dat deze ongewenste effecten zo min mogelijk voorkomen.

1.4.3 Wetenschappelijke relevantie

Er is redelijk veel onderzoek gedaan naar de efficiency en effectiviteit en de voor- en nadelen van horizontaal toezicht in met name de fiscale sector. De zorgsector maakt ook van deze methode gebruik, maar dat is nog betrekkelijk nieuw waardoor daar veel minder onderzoek voorradig is. Er zijn echter overeenkomsten en verschillen te ontdekken uit deze twee contexten. Uit onderzoek blijkt dat er geen of weinig onderzoek is gedaan naar de toepassing van horizontaal toezicht als het gaat om het toezicht op de verwerking van persoonsgegevens. Dat maakt dat dit onderzoek van toegevoegde waarde is voor de wetenschap omdat het de mogelijke toepassing van een dergelijke toezichtmethodiek beziet in een nieuw domein. Daarnaast is het relevant om te onderzoeken, als blijkt dat HT niet bruikbaar is, waarom dat dan zo is en welke randvoorwaarden ontbreken. Welke toezichtmethode dan wel bruikbaar is zou vervolgonderzoek kunnen zijn. Het is mogelijk dat horizontaal toezicht in theorie toepasbaar zou zijn, maar in de praktijk weerbarstig is.

1.5 Opbouw van de thesis

De thesis is na dit inleidende hoofdstuk als volgt opgebouwd:

- Hoofdstuk 2: Theoretisch kader
- Hoofdstuk 3: Methodologische verantwoording
- Hoofdstuk 4: Resultaten
- Hoofdstuk 5: Conclusie en aanbevelingen
- Hoofdstuk 6: Bronverwijzingen
- Hoofdstuk 7: Bijlagen

Hoofdstuk twee bevat het theoretisch kader van het onderzoek waarbij de elementen Privacy by Design, Toezicht en Horizontaal Toezicht, uitgebreid beschreven worden. Het gaat daarbij om definities en toelichting hierop. De gebruikte onderzoeksmethode en aanpak wordt behandeld in hoofdstuk drie. In de eerste paragraaf wordt kwalitatief onderzoek toegelicht en in paragraaf twee de onderzoeksmethode en technieken. Paragraaf drie bespreekt de ethische verantwoording van het onderzoek waarna uiteindelijk paragraaf vier de onderzoek betrouwbaarheid en validiteit behandeld. Hoofdstuk vier beschrijft welke resultaten het onderzoek naar respectievelijk horizontaal toezicht en het privacy control framework heeft opgeleverd. Daarbij worden ook de resultaten uit de interviews betrokken. In het vijfde hoofdstuk zijn conclusies geformuleerd naar aanleiding van de resultaten van het onderzoek en worden aanbevelingen gedaan. Daarnaast worden de deelvragen beantwoord en een antwoord geformuleerd op de hoofdvraag bij dit onderzoek. De wetenschappelijke en praktische contributie en de beperkingen komen vervolgens aan bod. Ten slotte wordt dit onderzoek afgesloten met suggesties voor het vervolgonderzoek en aanbevelingen daartoe.

2. Theoretisch kader

Volgens Oost en Markenhof (2010) wordt In het theoretisch kader beschreven binnen welk kennisgebied de probleemstelling een plek vindt. Daarmee wordt duidelijkheid gegeven over specifieke onderzoekthema's en wordt de relevante inhoudelijke keuze en vooronderstellingen en de belangrijkste thema's, en theorieën die de achtergrond vormen van het onderzoek belicht. In dit onderzoek zijn drie thema's; Privacy by Design, Toezicht, en Horizontaal Toezicht onderzocht.

2.1 Privacy by Design

Privacy by Design is een fundamentele benadering die rekening houdt met privacy al bij de ontwikkeling van informatiesystemen (Everson, 2017). Hoepman noemt Privacy by Design een ontwerpfilosofie (Hoepman, 2020). De principes van Privacy by Design vertonen gelijkenis met principes die door IT-architecten worden toegepast. Architectuurprincipes vullen de kloof tussen strategische intenties van hoger (strategisch) niveau en geven richting aan concrete ontwerpbeslissingen van organisaties (Fischer & Winter, 2010).

In Privacy by Design geldt een belangrijk principe: 'verzamel alleen datgene wat je écht nodig hebt'. Immers, gegevens die een organisatie niet verzameld kan het ook niet verliezen, zo stelt Koops (Koops et al., 2014) in zijn artikel. Dit principe staat ook wel bekend als dataminimalisatie, en wordt veelal gezien als het belangrijkste principe (Perera et al., 2016). Een voorbeeld van een privacy-verhogende maatregel is het gebruik van privacy enhancing technologies (PET). Dit zijn tools die helpen bij het borgen van privacy en security in informatiesystemen aldus Van Rossum (Van Rossum et al., 1995). Bij informatiesystemen is het belangrijk dat al tijdens het ontwikkelproces gebruik gemaakt wordt van privacy-verhogende maatregelen.

Ann Cavoukian (2009) ontwikkelde in 2009 de 7 principes van Privacy by Design, die in 2010 zijn aanvaard door de International Assembly of Privacy Commissioners and Data Protection Authorities (Data Protection and Privacy Commissioners, 2010). Deze principes, vertaald naar het Nederlands, zijn:

Nr.	Principe	Toelichting
PbD 1	Proactief niet reactief / preventief niet repressief	PbD geldt vanaf de initiatie van het ontwerp van een systeem en niet achteraf.
PbD 2	Privacy als standaardinstelling	Privacy criteria gelden per default. Daarbij is de regel "comply or complain".
PbD 3	Privacy geïntegreerd in ontwerp	Privacy maatregelen zijn integraal onderdeel van de informatieverwerking en zijn geen toevoeging.
PbD 4	Volledige functionaliteit	Het waarborgen van de privacy is een verantwoordelijkheid van alle betrokken partijen.
PbD 5	End-to-end beveiliging	PbD waarborgt het privacy management, inclusief de beveiliging, gedurende de gehele

		levenscyclus van de persoonsgegevens. Het is geen eenmalige actie.
PbD 6	Zichtbaarheid en transparantie	Inzicht en transparantie over de verwerking van persoonsgegevens moet mogelijk zijn voor zowel het individu als de eigen organisatie en toezichthouders.
PbD 7	Gebruiker staat centraal	Technische en organisatorische maatregelen zijn pas effectief, wanneer zij de persoonlijke levenssfeer van het individu beschermen.

Tabel 1, De principes van Privacy by Design (Cavoukian 2009).

Privacy by Design is ingebed in de General Data Protection Regulation (GDPR) die in Nederland is omgezet naar de AVG (European Data Protection Supervisor, 2018). Vanwege de formele inbedding en aanvaarding van de methode Privacy by Design en door het gebruik ervan door de Europese Commissie bij vaststelling van de GDPR wordt deze methode in dit onderzoek gehanteerd. De AVG geeft helaas geen scherpe criteria of definitie voor Privacy by Design (Hoel & Chen, 2016). In de AVG wordt Privacy by Design omschreven als; gegevensbescherming door ontwerp en door standaardinstellingen (EU general data protection regulation 2016/679 (GDPR) art. 25 en 47). Een vrij ruime en abstracte omschrijving die derhalve vraagt om concretisering en praktische invulling.

2.1.1 De principes van Privacy by Design

Bij de verwerking van persoonsgegevens die waarschijnlijk een hoog privacy risico opleveren is een Data Protection Impact Assessment (DPIA) verplicht gesteld. Dit wordt ook wel een gegevensbeschermingseffectbeoordeling genoemd. Een DPIA is een methode die op een systematische en gestructureerde manier helpt om privacy risico's inzichtelijk te maken.

Het belangrijkste doel van de DPIA is het creëren van bewustwording en inzicht in de privacy- en compliance-risico's die organisaties en personen kunnen lopen. Daarmee zijn de risico's onderkent maar niet gemitigeerd. Ridderbeekx & Scheuller (2018) noemen als nadeel van de DPIA-vragenlijst dat deze puur uitgaat van de wettelijke vereisten van de AVG. Dat terwijl de DPIA feitelijk een instrument is om privacy risico's van een gegevensverwerking inzichtelijk te maken en vervolgens te verkleinen of te mitigeren. Daarbij gaat het met name om de risico's voor personen van wie de gegevens worden verwerkt, maar ook om de gegevens van organisaties zelf. Om deze risico's weg te nemen of te verkleinen zullen beheersmaatregelen moeten worden opgesteld. In een privacy control framework op basis van PbD komen de beheermaatregelen samen (Ridderbeekx & Scheuller, 2018). Dat leidt ertoe dat niet allen aan de juridische eisen uit de AVG wordt voldaan maar zorgt er ook voor dat het toezicht effectiever en efficiënter wordt.

Informatiesystemen zouden zo ontworpen moeten zijn dat zij geen onrechtmatig gebruik of toepassing toestaan, 'compliance vanuit het ontwerp' volgens Julisch et al. 2011) en Lohmann (2013). Deze

systeem gebaseerde controle vereist een nieuwe auditaanpak waarbij organisaties moeten aantonen aan de toezichthoudende instantie dat ze 'compliant' zijn. Organisaties moeten zelf de impact van regelgeving o.a. op hun informatiesystemen beschouwen, motiveren welke reeks beheersmaatregelen zij hebben genomen om hieraan te voldoen, en aantonen dat de beheersmaatregelen effectief zijn (Burgemeestre et al., 2011). Daarbij kan een PCF bruikbaar zijn. Deze fungeert daarbij als een gestructureerd beheersingskader dat de uitvoering van het toezicht faciliteert. In het PCF worden de beheersingsdoelstellingen als requirements opgenomen, de bijbehorende strategie en tactiek weergegeven. Het doel is uiteindelijk om op een eenduidige wijze verantwoording af te leggen. Een privacy control framework maakt het mogelijk om met de controlerende instantie, i.c. de Autoriteit Persoonsgegevens de dialoog aan te gaan over de vraag of de onderkende requirements voor het rechtmatig verwerken van persoonsgegevens, in toereikende mate worden gehaald.

In de literatuur wordt door Schaar gesteld dat de standaardinstellingen van informatiesystemen altijd zo privacy vriendelijk mogelijk moeten zijn, en dat persoonsgegevens nooit standaard openbaar zichtbaar zijn (Schaar, 2013). Privacy by Design en by default zijn twee verschillende begrippen die met elkaar verbonden kunnen zijn. Het verschil is dat Privacy by Design in de *ontwerpfase* plaatsvindt en privacy by default gaat over privacy instelling bij *gebruik* van het systeem. Privacy by default beschouw ik daarom als onderdeel van Privacy by Design.

Volgens Duncan et al. kan Privacy by Design dienen als richtlijn over hoe organisaties om kunnen gaan met privacy-issues en risico's (Duncan, 2007). Volgens Schaar is het devies om al in een vroeg stadium van zowel de ontwikkeling als het gebruik van informatiesystemen een zorgvuldige omgang met persoonsgegevens af te dwingen (Schaar, 2013). Afdwingen betekent fundamentele principiële keuzes maken die voorkomen dat een systeem onrechtmatig gebruikt kan worden. Het is belangrijk dit al in de ontwikkeling mee te nemen omdat verborgen gebreken erg moeilijk te herstellen zijn als het systeem eenmaal in werking is, aldus Schaar (2013). Verschillende vraagstukken spelen daarbij volgens Kool (2011) een rol: hoe geeft een organisatie invulling aan dataminimalisatie? Is de verwerking van een persoonsgegevens door een organisatie écht nodig, denk aan de geboortedatum of geslachtsaanduiding ex. art. 5 lid 1 AVG. Hoe lang mag ik gegevens bewaren, of kan gewerkt worden met volledig geanonimiseerde gegevens? (Vermaas et al., 2010) Dat vraagt bij het ontwikkelen van informatiesystemen volgens de principes van Privacy by Design, om een generieke methode (Duncan, 2007).

Lieshout geeft in het TNO rapport van 2012 (Van Lieshout et al., 2012) duidelijk aan dat over Privacy by Design gesproken kan worden wanneer:

- De bescherming van de privacy van personen over wie gegevens verzameld worden al bij het (vroegste) ontwerp van een systeem wordt meegenomen;
- Er gebruik wordt gemaakt van organisatorische maatregelen om toegang tot en omgang met persoonsgegevens te regelen volgens bepaalde afspraken en voorschriften; en

- Er gebruik wordt gemaakt van technische maatregelen zoals versleuteling om toegang tot en omgang met persoonsgegevens af te schermen of te verhinderen.

2.1.2 De geschiedenis van privacywetgeving

Door de introductie van geavanceerde informatiesystemen krijgen organisaties de mogelijkheid om grote hoeveelheden persoonsgegevens gemakkelijk te verwerken en te bewaren. Daardoor ontstond in de jaren zeventig de behoefte aan meer algemene rechtsbescherming tegen privacy-schendingen wat uiteindelijk in 1981 leidt tot het Verdrag tot bescherming van personen. Dit is het eerste juridisch bindende internationale instrument voor gegevensbescherming. De contouren van de huidige AVG zijn daarin al te onderkennen. Bij de herziening van de Grondwet in 1983 wordt in artikel 10, eerste lid, de bescherming van de persoonlijke levenssfeer prominent als klassiek grondrecht geformuleerd. Daarnaast krijgt in het tweede en derde lid de wetgever de opdracht om regels op te stellen voor de bescherming van persoonsgegevens. De wet persoonsregistraties (WPR) uit 1989 is daarvan het resultaat. Met de komst van richtlijn 95/46/EG over de bescherming van natuurlijke personen in verband met de verwerking van hun persoonsgegevens, worden de lidstaten verplicht om hun privacywetgeving binnen de door de richtlijn aangegeven grenzen te harmoniseren. Nederland implementeert de richtlijn via de Wet bescherming persoonsgegevens (Wbp), en introduceert de functionaris voor de gegevensbescherming (FG). In april 2016 ziet de AVG het levenslicht en waarin vooral de verantwoordingsplicht nieuw is. Zij moeten kunnen aantonen dat zij ‘compliant’ zijn. Op bepaalde onderwerpen is de wetgeving moderner geworden en past de AVG beter in het digitale tijdperk. Doelbinding is daarvan een goed voorbeeld. Het zijn deze ontwikkelingen geweest die privacy van EU-burgers hebben beschermd en daarmee beperkingen hebben opgelegd aan organisaties die persoonsgegevens van EU-burger verwerken.

2.1.3 Verschillende in Privacy benaderingen

Privacy is een actueel thema en door de jaren heen zijn er verschillende pogingen gedaan om te definiëren wat privacy is met inachtneming van de specifieke context en de omgeving (Di Iorio et al., 2014). Warren en Brandeis omschreven privacy in 1890 al als het 'recht om met rust gelaten te worden' (Warren & Brandeis, 1890). In de jaren erna zijn er diverse pogingen gedaan om een sluitende definitie te formuleren o.a. door (Bambauer, 2013) en Lever (2006). Vooral juridisch werd privacy binnen de EU van land tot land verschillend gedefinieerd totdat het uiteindelijk werd opgenomen in art. 8 van de Europese Verklaring voor de Rechten van de Mens (EVRM). *“Everyone has the right to respect for his private and family life, his home and his correspondence”.*

Privacy by Design is niet te enige methode die toegepast wordt om privacy te waarborgen. In dit onderzoek zij een vijftal andere perspectieven bekeken aangaande privacy. Er is gekeken naar:

- ISO/IEC-29100:2011
- De AVG
- Databeschermingsrichtlijn uit 1995 (WBP)

- De principes van Schaar, en
- De privacy richtlijnen van de Organisatie voor Economische Samenwerking en Ontwikkeling (OESO) uit 1980.

In relatie tot Privacy by Design zijn er met bovengenoemde methoden gelijkenissen en verschillen te ontdekken. In tabel de tabel hieronder staan de alternatieven opgesomd en is een korte toelichting gegeven. Het voert in dit onderzoek te ver om alle methoden uitputtend te behandelen. Wel is in de volgende paragraaf aangegeven waarom voor de methode Privacy by Design gekozen is.

Methode	Toelichting (verkort)
ISO/IEC-29100:2011	ISO/IEC29100:2011 is een internationale norm en biedt een kader op hoog niveau voor de bescherming van persoonsgegevens binnen informatiesystemen. Het is algemeen van aard en plaatst organisatorische, technische en procedurele aspecten in een algemeen privacy kader. ISO is meer gebaseerd op de Plan-Do-Check-Act systematiek.
Algemene Verordening Gegevensbescherming (AVG) of General Data Protection Regulation (GDPR)	1. Legitimiteit en transparantie; Er moet een juridische basis zijn voor de verwerking van persoonlijke data. 2. Doelbinding; Persoonlijke gegevens morgen slechts worden verzameld voor legitieme doeleinden en alleen als je die expliciet hebt aangegeven en daar toestemming voor hebt gevraagd en gekregen. 3. Dataminimalisatie; Persoonlijke gegevens dienen adequaat en relevant te zijn voor de doelen die je hebt aangegeven. Je mag niet meer gegevens verzamelen dan nodig. 4. Accuraatheid; Je moet redelijke stappen ondernemen om de persoonlijke gegevens up-to-date te houden en bij te werken indien ze niet meer accuraat zijn. 5. Niet langer bewaren dan nodig; Je mag persoonlijke gegevens niet langer bewaren dan nodig is om aan de doeleinden te voldoen waarvoor je toestemming hebt verkregen. 6. Inzage-, correctie- en verwijderrecht en data-portabiliteit; Individuen hebben het recht om hun persoonlijke gegevens in te zien, te laten corrigeren en om reeds verstrekte toestemming voor bepaalde toepassingen zoals het gebruik voor direct marketing in te trekken.

	7. Beveiliging; Je bent verplicht om organisatorische, fysieke en technische maatregelen te treffen om persoonlijke data te beveiligen op een niveau dat overeenstemt met de gevoeligheid van die data. 8. Verantwoordelijkheid; In geval van een datalek ben je verplicht om dit binnen 72 uur te melden bij de Autoriteit Persoonsgegevens.
Databeschermingsrichtlijn uit 1995 (WBP)	De Wet Bescherming Persoonsgegevens (WBP) uit 1995 was de voorloper van de AVG. De regeling was enerzijds bedoeld als instrument om invulling en uitvoering te kunnen geven aan de WBP en anderzijds was het bedoeld is als instrument om de naleving van de WBP te bevorderen. Daarbij stond voorop dat persoonsgegevens in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze verwerkt moeten worden. Het grote verschil met de AVG is dat met name transparantie veel nadrukkelijker wordt benoemd. Organisaties krijgen onder de AVG zelf meer verantwoordelijkheid dan dat zij onder de WBP hadden. Deze verantwoordelijkheid is deels de legitimatie voor de verplichte functionaris gegevensbescherming (FG) in de AVG.
De principes van Schaar	Schaar somt in zijn standaard werk uit 2010 een zestal principes op die voor hem leidend zijn in de bescherming van privacy, deze zijn: 1. Data minimalisatie 2. Beheersbaarheid 3. Transparantie 4. (data) Vertrouwelijkheid 5. Datakwaliteit 6. Mogelijkheid van segregatie
De privacyrichtlijnen van de Organisatie voor Economische Samenwerking en Ontwikkeling (OESO) uit 1980.	De OECD stelt in haar privacy framework uit 2013 een achttal richtlijnen op die ‘nations’ moeten handhaven om de privacy van haar burgers op een juiste en daadkrachtige manier te beschermen. De OESO-richtlijnen bieden handvatten voor bedrijven om met kwesties om te gaan zoals ketenverantwoordelijkheid, mensenrechten.

Tabel 2, Privacy waarborg methodes vergeleken.

2.1.4 Waarom Privacy by Design?

In de wetenschappelijke literatuur was PbD geen gangbare term (Kool, van Schoonhoven et.al 2011). De Canadese toezichthouder op de dataprotectie-wetgeving Ann Cavoukian (2009) heeft de term in de jaren negentig geïntroduceerd in samenwerking met de Nederlandse toezichthouder (destijds de

Registratiekamer). Dit ging over de toepassingsmogelijkheden van Privacy Enhancing Technologies (PET) en verwees hierin naar het technisch inbouwen van privacybescherming in IT-systemen. PET is daarna echter uitgegroeid tot een bredere benadering (Cavoukian, 2009) waarbij het niet alleen gaat om technische waarborgen, maar ook om waarborgen in bedrijfsprocessen en een omslag in bedrijfscultuur. In 2010 hebben internationale toezichthouders op privacy en dataprotectie-wetgeving een 'Privacy by Design resolutie' aangenomen waarin PbD wordt omschreven als een holistisch concept dat kan worden toegepast in allerlei operaties van organisaties, inclusief de informatietechnologie, bedrijfspraktijken, bedrijfsprocessen, fysieke omgeving en genetwerkte infrastructuur (Cavoukian et al., 2010). Daarnaast is Privacy by Design in art. 25 AVG "Gegevensbescherming door ontwerp en door standaardinstellingen" met zoveel woorden genoemd als leidende maatregel ten einde "naleving van de voorschriften van deze verordening en ter bescherming van de rechten van de betrokkenen" te waarborgen. Dat alles wordt nog ondersteund door overweging 78 en 108 van de preambule bij verordening (EU) 2016/679. Gezien de brede omarming van PbD als concept en de formele inbedding in wet- en regelgeving is ook in dit onderzoek Privacy by Design als leidend gekozen om het privacy control framework vorm te geven.

2.2 Toezicht

Raaijmakers (2016) schrijft dat toezichthouders van oudsher worstelen met de vraag waar zij het accent van hun toezicht beleid moeten leggen en hoe zij zo effectief mogelijk hun toezicht capaciteit in kunnen zetten. Huisman en Beukelman (2007) en Denkers et al. (2013) hebben onderzoek gedaan en concluderen dat er weinig bekend is over de effectiviteit van sancties, controlestrategieën of handhavingsstijlen op de naleving van regelgeving door organisaties. Wel komt naar voren dat een toezichtrelatie een viertal specifieke kenmerken bezit, dit zijn; belangentegenstelling, ongelijke informatiepositie, machtsongelijkheid en on-vrijwilligheid.

2.2.1 Belangentegenstelling

Allereerst schrijven Huisman en Beukelman (2007) dat een organisatie andere belangen heeft dan de toezichthouder. Een toezichthouder is door de overheid ingesteld om bepaalde publieke waarden te versterken en te borgen. Daarbij past ook een adviesfunctie waar de toezichthouder invulling aan zou moeten geven. Een organisatie heeft ook te maken met de belangen van individuen. Dat kan ertoe leiden dat de organisatie niet dezelfde invulling geeft aan de publieke waarden als de toezichthouder die op de naleving toeziet. Dat resulteert in een spanningsveld tussen toezichthouder en de organisatie.

2.2.2 Ongelijke informatiepositie

Het tweede kenmerk is dat er sprake is van ongelijke informatieposities ook wel aangeduid als 'informatie-asymmetrie'. Organisaties weten welke risico's er zich intern manifesteren, welke risicobeheersing er getroffen is en voor welke uitdagingen zij staan. De toezichthouder heeft deze informatie niet en moet deze ontdekken. Anderzijds heeft de toezichthouder meer zicht op het

toezichtproces en waar de accenten liggen en hoe het reageert op tekortkomingen. Daarnaast gelden voor een toezichthouder allerlei wettelijke beperkingen met betrekking tot het delen van informatie.

2.2.3 Machtsongelijkheid

Toezichtrelaties kennen een machtsongelijkheid. Toezichthouders hebben op basis van de wet, in dit geval de AVG, instrumenten om compliance af te dwingen of de bevoegdheid om sanctionerend op te treden door bijv. een boete op te leggen. Deze bevoegdheden zijn nodig om te voorkomen dat een wet alleen een symboolfunctie heeft. Anderzijds kan een toezichthouder ook adviseren aldus Mendoza et.al (Mendoza & Wielhouwer, 2015) en Van der Hel en Siglé (2019).

2.2.4 On-vrijwilligheid

De toezichthouder en onder toezicht staande hebben elkaar niet zelf uitgekozen, maar zijn tot elkaar veroordeeld. In het geval van de naleving van privacywetgeving is de AP de wettelijk aangewezen toezichthouder. De AVG geeft de toezichthouder vanuit de wet democratische legitimiteit. Een positief effect voor organisaties is dat zij toezicht ook kunnen inzetten als kwaliteitsborging en daarmee een lerend vermogen aanspreken (Raaijmakers, 2016).

2.2.5 Inherente onvoorspelbaarheid

De optelsom van de kenmerken; belangentegenstelling, ongelijke informatiepositie, machtsongelijkheid en on-vrijwilligheid worden door Huisman en Beukelman (2007) samengevat als de ‘inherente onvoorspelbaarheid’ in toezichtrelaties. De organisatie en de toezichthouder kunnen elkaars gedrag niet voorzien. Deze onvoorspelbaarheid leidt tot een bureaucratische toezichtrelatie. Daarom wordt er voortdurend gezocht naar manieren om deze relatie voorspelbaarder en gelijkwaardiger te maken. Dit verklaart het ontstaan van horizontaal toezicht.

2.3 Horizontaal toezicht

Horizontaal toezicht was oorspronkelijk bekend als ‘enhanced relationship’ (Colon & Swagerman, 2015) en (Dabner & Burton, 2015) en kent internationale equivalenten. Sinds 2013 wordt de term ‘cooperative compliance’ gebezigd (Huiskers & Gribnau, 2019) en (De Widt & Oats, 2019). Er is weinig wetenschappelijke literatuur te vinden met betrekking tot horizontaal toezicht. De belangrijkste bijdragen aan de wetenschap m.b.t. horizontaal toezicht worden veelal gedaan in vakbladen of als onderzoekonderwerp ter hand genomen. Kenmerkend is dat er geen eenduidige definitie van horizontaal toezicht te vinden is. In alle definities die in onderstaande wetenschappelijke bijdragen zijn gevonden valt op dat termen als ‘werkwijze’ en ‘samenwerking’ terugkomen.

#	Jaar	Onderzoeker(s)	Onderzoek
R1	**2012**	Commissie horizontaal toezicht belastingdienst o.l.v. prof stevens	Fiscaal toezicht op maat
R2	**2014**	M.E. Oenema	Proefschrift - De formeelrechtelijke aspecten van horizontaal toezicht
R3	**2015**	E.A.M. Huiskers-Stoop	Proefschrift - De effectiviteit van horizontaal belastingtoezicht
R4	**2017**	Belastingdienst	Rapport - onderzoek toezicht grote ondernemingen
R5	**2013**	Dennis de Widt (university of Exeter), Fair tax project	Dutch horizontal monitoring - The handicap of a head start
R6	**2019**	M.A. Siglé	Proefschrift - The effects of cooperative compliance programmes

Tabel 3, Wetenschappelijke bijdragen m.b.t. horizontaal toezicht.

Horizontaal toezicht richt zich op het vergroten van 'wederzijds vertrouwen, begrip en transparantie' tussen de organisatie en de toezichthouder. Horizontaal toezicht gaat over toezicht ten aanzien van de uitvoering en naleving van wetgeving. In het Jaarboek Compliance 2012 (Commissie Horizontaal Toezicht Belastingdienst, 2012) van de belastingdienst wordt gesteld dat als horizontaal toezicht werkt, dit zou moeten leiden tot betere compliance, minder compliance-kosten en een versterkte samenwerking met controlerende instanties. In deze thesis wordt onderzocht of door gebruik van horizontaal toezicht deze positieve effecten ook gelden voor het toezicht op de verwerking van persoonsgegevens en het toezicht daarop.

Horizontaal toezicht wordt voornamelijk in fiscale sector toegepast tussen de belastingdienst en met name grote organisaties. De belastingdienst verlegt daarbij zijn koers van volledige controle van belastingplichtige organisaties naar beheersing van fiscale risico's. Er wordt alleen nog gecontroleerd als zich daadwerkelijk risico's voordoen. Door scherp onderscheid te maken tussen risicovolle en minder risicovolle ondernemingen (selectiever toezicht) ontstaat ruimte om controlecapaciteit in te zetten waar dat meest benodigd is. Horizontaal toezicht kenmerkt zich door zijn responsieve handhaving stijl, wat betekent dat er wordt ingegrepen waar nodig, en van eigen verantwoordelijkheid wordt uitgegaan waar dat kan. Horizontaal toezicht is in overeenstemming met de ontwikkelingen in de samenleving, waar de individuele verantwoordelijkheden van bijv. bedrijven en de overheid transparant zijn maar ook gehandhaafd worden (Burgemeestre et al., 2009). Sinds het begin van de deze eeuw is de belastingdienst corporate compliance programs (CCP) gaan gebruiken als onderdeel van hun overkoepelende compliance riskmanagementstrategie. De introductie van horizontaal toezicht past binnen deze ontwikkeling. Een corporate compliance program wordt door Majdanska omschreven als:

> *Definitie 7 – corporate compliance program: a relationship that favours collaboration over confrontation, and is anchored more on mutual trust than on enforceable obligations* (Bronżewska, K., & Majdańska, 2019).

Siglé schrijft in zijn proefschrift uit 2019 "*The effects of coorperative compliance programmes*" dat CCP's gezien worden als een reactie op sociale ontwikkelingen die vragen om meer focus op verantwoordelijkheid van organisaties, voor het naleven van wet- en regelgeving, en als een methode om te differentiëren tussen risicovolle en minder risicovolle organisaties. Siglé concludeert dat CCP's bijdragen aan de verbetering van compliance. 'Een CCP beoogt daarbij de relatie tussen toezichthouder en de organisatie te verbeteren waarbij beide partijen samenwerken om de naleving van de van toepassing zijnde wetgeving zo effectief en efficiënt mogelijk te handhaven, of te verbeteren'. Horizontaal toezicht is in overeenstemming met deze ontwikkeling in de samenleving, waar de individuele verantwoordelijkheden van bijv. bedrijven en de overheid transparant zijn maar ook gehandhaafd worden (Burgemeestre et al., 2009).

Horizontaal toezicht kenmerkt zich door het principe van 'voor wat, hoort wat'. De uitgangspunten zijn begrip, wederzijds vertrouwen en transparantie. De inherente onvoorspelbaarheid die voortvloeit uit ongelijke informatieposities en machtsongelijkheid, die zo kenmerkend is voor klassieke toezichtrelaties wordt hierdoor beperkt. Horizontaal toezicht heeft ten doel om toezicht te vereenvoudigen, naar voren te halen in het proces en efficiënter uit te kunnen voeren. Daarbij speelt vertrouwen een prominente rol (Burgemeestre et al., 2010). Afgelopen decennia hebben op vertrouwen gebaseerde toezichtstrategieën veel aandacht gekregen. Er is bewezen dat deze strategieën kunnen bijdragen aan betere compliance (Huiskers-Stoop, 2015). 'Een moderne controle-instantie moet een op vertrouwen gebaseerde toezicht methode opnemen in zijn compliance strategie. Met een coöperatief compliance programme (CCP) – zoals horizontaal toezicht – wordt de zekerheid vergroot en kunnen controle inspanningen worden verminderd' aldus Siglé (2019) in zijn voornoemde proefschrift.

2.3.1 Drie pilaren onder horizontaal toezicht

In dit onderzoek wordt een parallel getrokken met horizontaal toezicht door de belastingdienst in de fiscale context, en het toezicht door de AP op de verwerking van persoonsgegevens. Daarbij zijn de drie criteria; begrip, wederzijds vertrouwen en transparantie (Russo & Huiskers-stoop, 2020) de uitgangspunten.

'Wederzijds vertrouwen' gaat over het vertrouwen dat een toezichthouder kan ontlenen aan interne controle-instrumenten. Wederzijds vertrouwen is nodig bij een horizontale toezichtrelatie om de informatie-asymmetrie te verminderen (Belastingdienst, 2012, p. 8). In een horizontale toezichtrelatie moet de toezichthouder de organisatie vertrouwen, ondanks het feit dat de toezichthouder geen volledige informatie heeft over de compliance van de organisatie. Aan de andere kant moet de organisatie erop vertrouwen dat de toezichthouder zijn macht niet misbruikt bij het bereiken versterken

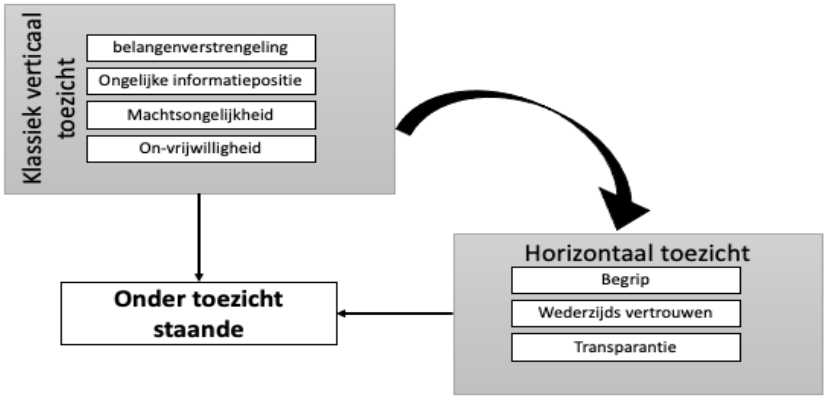
van zijn informatiepositie. Wederzijds vertrouwen vertoond daarmee gelijkenis met het vertrouwensbegrip uit art. 3:35 van het burgerlijk wetboek.

Begrip betekent begrijpen in welke omgeving en dynamiek een organisatie opereert en welke verwerking van persoonsgegevens noodzakelijk zijn voor de bedrijfsvoering. Wederzijds begrip gaat ook over het feit dat beide partijen elkaars positie en soms conflicterende belangen begrijpen. Huiskers-Stoop (2015) noemt begrip voor elkaars behoeftes en aspiraties het startpunt van de relatie tussen organisatie en toezichthouder bij een horizontale toezichtrelatie. Beeldvorming is daarbij een belangrijk aspect.

Het derde criterium is *transparantie*. Transparantie gaat over het geven van openheid over de risico's en de daartegenover staande maatregelen die een organisatie treft ten aanzien van deze risico's. Eerder werd al geschreven dat een toezichthouder binnen een horizontaal toezichtrelatie volledige openheid verwacht. Organisaties willen dat de openbaarheid en transparantie die zij binnen horizontaal toezicht verlenen, wordt beantwoord door de toezichthouder. Transparantie van de toezichthouder kan bijvoorbeeld betrekking hebben op het verstrekken van argumentatie voor vragen tijdens een audit of het aankondigen van veranderende regelgeving. Invulling geven aan de adviesfunctie past hier ook bij.

2.3.2 Horizontaal toezicht een paradigmaverschuiving

Het eerdergenoemde cooperative compliance richt zich op het realiseren van een meer gelijkwaardige 'horizontale' en coöperatieve relatie, waarin de naleving moet worden versterkt op andere manieren dan enkel controle en sanctiedreiging. Horizontaal toezicht is volgens Raaijmakers (2016) een lastig te duiden begrip, niet in de laatste plaats omdat het veel wegheeft van een 'contradictio in terminis'. De term 'horizontaal' suggereert een bepaalde mate van gelijkheid. Terwijl 'toezicht' zich juist kenmerkt door een bepaalde mate van machtsongelijkheid, oftewel een verticale relatie. Als je de verticale relatie als vertrekpunt neemt, is horizontaal toezicht eigenlijk een manier om te schuiven binnen de toezichtrelatie met als doel de relatie gelijkwaardiger te maken. Deze paradigma verschuiving ziet er als volgt uit:



Figuur 1, Paradigma verschuiving, van verticaal naar horizontaal toezicht.

De introductie van horizontaal toezicht past ook bij een ontwikkeling waarbij wordt gezocht naar alternatieve toezichtvormen om de beperkte toezichtcapaciteit van de Autoriteit Persoonsgegevens efficiënt in te zetten. Horizontaal toezicht wordt ingezet om het toezicht houden vanuit wantrouwen om te buigen naar toezicht houden vanuit vertrouwen (Huiskers & Gribnau, 2019). Zelfregulering en het geven van meer verantwoordelijkheid aan organisaties zijn hier producten van.

2.3.3 Beschouwingen horizontaal toezicht

Toelating tot horizontaal toezicht is voor een deel gebaseerd op de kwaliteit van het interne toezicht. Daarnaast moet het karakter van de onderneming wel passen bij de systematiek van horizontaal toezicht. Als beide in orde zijn kan de organisatie toegelaten worden tot HT met een verlaagde controledruk als positief gevolg. Wat betreft de doelen die de belastingdienst nastreeft met HT vinden we in de Leidraad Grote Ondernemingen het volgende – vaag geformuleerde – doel: ‘het creëren van een raamwerk voor compliance van grote organisaties, waarin naast de verbeterde relatie en transparantie ook aandacht bestaat voor de fiscale beheersing en de fiscale strategie’. Over de doelen die grote organisaties willen bereiken met HT is de Leidraad minder expliciet. De belastingdienst niet erg duidelijk is over het concept van HT en dan met name over de doelen die het nastreeft. Verwacht zou worden dat hier iets staat over verbetering van de toezichtrelatie in termen van effectiviteit en efficiency. De onduidelijkheid over de invulling van het concept is een voedingsbodem voor kritiek.

3. Methodologische verantwoording

Hoofdstuk drie beschrijft de methodische aanpak van deze thesis. In paragraaf 3.1 zal een toelichting op de keuze voor de aanpak worden gegeven. In paragraaf 3.2 worden de gebruikte onderzoeksmethode en technieken uiteengezet. In paragraaf 3.3 zal de ethische verantwoording worden bij deze thesis worden gegeven en ten slotte wordt in paragraaf 3.4. de betrouwbaarheid en validiteit van het onderzoek toegelicht.

3.1 Kwalitatief onderzoek

Als onderzoeker wil je begrijpen hoe mensen dingen ervaren en wat individuele standpunten en visies zijn (Boeije, 2014). Met name omdat in dit onderzoek perceptie over privacy en elementen zoals vertrouwen en begrip onderwerp zijn, is het in dit onderzoek belangrijk om ervaringen en standpunten van individuen te betrekken. Daarbij past een kwalitatief onderzoek, waarbij het belangrijk is om een open benadering te behouden en zo min mogelijk eigen aannames en veronderstellingen te gebruiken. Kwalitatief onderzoek richt zich op begrip van onderliggende drijfveren en geeft daarbij ruimte voor nuance en verfijnd inzicht. De interviews binnen dit kwalitatief onderzoek geeft de bevraagde doelgroep de ruimte voor toelichting en ervaringen waardoor het onderzoek niet in algemeenheden blijft hangen. Daarom is in dit onderzoek gekozen voor kwalitatief onderzoek. Het past bij het soort onderzoeken die vragen beantwoorden in het spectrum van complexiteit, perceptie en betekenis. De data in dit onderzoek is afkomstig uit literatuuronderzoek en interviews wat kwalitatieve onderzoeksmethoden zijn die bijzonder geschikt zijn voor het onderzoeken met een *open mind* (Edmondson & Mcmanus, 2007). Tijdens dit onderzoek is een literatuurstudie uitgevoerd om meer zicht te krijgen in de wetenschappelijke benadering van de onderzoekelementen en deze inzichten te gebruiken bij het uitvoeren van het onderzoek. Daarover wordt in 3.1.2 verslag gedaan van de wijze waarop dit is uitgevoerd. Het verzamelen van literatuur is op basis van empirische data gedaan. Het verkregen inzicht is verwerkt en gebruikt binnen het onderzoek. Aanvullend zal met een *open mind* gebruik worden gemaakt van semigestructureerde interviews. Hierover wordt in paragraaf 3.1.4 uitleg gegeven.

3.1.1 Onderzoek ontwerp

Het onderzoekontwerp wordt gebaseerd op de door Hevner beschreven ontwerpmethodiek voor informatiesystemen (Hevner et al., 2004). Deze ontwerpmethodiek is gekozen omdat deze gebruikt wordt voor het ontwikkelen van wetenschappelijke theorieën en artefacten voor informatiesystemen. Op de methode van Hevner is een praktische aanvulling gedaan door het toevoegen van de design science cycle van Wieringa (2014). Wieringa ontwikkelde op basis van de methode van Hevner zijn ‘engineering cycle’. In dit onderzoek en voor het ontwerpen van het artefact is gebruik gemaakt van een combinatie van de methoden waarbij Wieringa zijn design science methode leidend is. Wieringa geeft in zijn boek richtlijnen voor het doen van design science in informatiesystemen. In design science worden twee activiteiten onderkent: het ontwerpen van een artefact dat iets verbetert voor zijn stakeholders en empirisch onderzoek naar de prestaties van het artefact in een context. Een belangrijk kenmerk van de

benadering van Wieringa is dat het doel van het onderzoek is om een artefact in een (nieuwe) context te onderzoeken. Het artefact dat ontworpen wordt in dit onderzoek is een privacy control framework dat daarna op bruikbaarheid in een nieuwe context onderzocht wordt. In par 3.2.1 wordt uitgebreider stil gestaan bij de methode Wieringa in combinatie met Hevner.

Bestaande theorieën met betrekking tot compliance, vormen het startpunt van dit onderzoek. Dat betekent dat in dit onderzoek gekozen is voor een deductieve benadering. Deductief onderzoek gaat uit van een 'top-down' benadering, waarbij vanuit een algemene theorie gevolgtrekkingen worden gemaakt naar een bijzondere theorie. Vanuit deze redenatie is derhalve gestart met een literatuuronderzoek als fundering voor het kwalitatieve onderzoek. Daarbij worden met name definities verklaard, bestaande (toezicht)methoden uitgelegd en verbanden gelegd.

Volgens Wieringa (2014) is design science 'oplossing georiënteerd', dit in tegenstelling tot social science dat 'probleem-georiënteerd' is. Aangezien het resultaat van dit onderzoek een artefact is, welke een oplossing moet bieden voor het reeds genoemde probleem m.b.t. compliance bij de verwerking van persoonsgegevens én het toezicht daarop, wordt dit onderzoek gekenschetst als design science. De verschillende stappen die daarin worden gezet zijn worden in paragraaf 3.2.1 uitgebreid toegelicht.

De in- en exclusiecriteria alsmede de zoekopdrachten die zijn gedefinieerd voor dit onderzoek zijn in paragraaf 3.1.3 nader uitgewerkt. De zoekopdrachten zijn geformuleerd om antwoord te geven op de kennisvragen. Op basis van de literatuur en nadere theoretische verkenningen in o.a. rapporten van de autoriteit persoonsgegevens en interne onderzoeken door de belastingdienst, zijn vragen voor de semigestructureerde interviews geformuleerd. De data die in de interviews is vergaard vormen de bouwstenen voor zowel het artefact als beantwoording van deelvragen, en uiteindelijk centrale vraag.

3.1.2 Literatuur

Met betrekking tot Privacy by Design en horizontaal toezicht zijn wetenschappelijke artikelen geselecteerd op basis van een drietal criteria; tijd, taal en type. Er is voor gekozen om alleen artikelen te gebruiken die zijn geschreven na 2000 in de Nederlandse of Engelse taal. Het betreft wetenschappelijke artikelen, vakliteratuur en congresbijdragen. Een uitzondering hierop is het artikel van Warren en Brandeis uit 1890 met betrekking tot de oorsprong van privacy. Over horizontaal toezicht beperkt de literatuur zich voornamelijk tot artikelen in de fiscale context. Met betrekking tot PbD is veel literatuur te vinden die met name in gaat op de duiding van de principes en de toepassing ervan op het gebied van systeemontwikkeling. Uit zoekslagen gemaakt in Google scholar en HUGO, de online zoekmachine van de Hogeschool Utrecht, naar deze onderwerpen komen een groot aantal artikelen naar voren. Daarover is een selectie gemaakt op basis van eerdergenoemde criteria. Aan de hand van een beslismodel gebaseerd op de Prisma methode van Liberati (Liberati et al., 2009), is een selectie gemaakt van artikelen die uiteindelijk in deze literatuurstudie zullen worden gebruikt.

3.1.3 Zoekcriteria

De zoektermen vinden hun oorsprong in de onderzoeksvraag. Er is onderscheid gemaakt in kernbegrippen en afgeleide begrippen vanuit de deelvragen. Om goede literatuur te vinden zijn combinaties van deze kernbegrippen gemaakt, alsmede synoniemen en Engelstalige varianten. Gezocht is met zowel een 'AND' als een 'OR' tussen de zoektermen. Als kernbegrippen in mijn onderzoek is gekozen voor: Compliance/regelnaleving - Horizontaal toezicht - Control framework – Vertrouwen – Begrip - Transparantie – Privacy by Design.

De wetenschappelijke literatuur zijn in het Nederlands en Engels geschreven, waardoor ook een zoekslag met beide variant noodzakelijk is. Met name binnen het onderwerp horizontaal toezicht valt op dat een aanzienlijk deel van de wetenschappelijke literatuur in het Nederlands beschikbaar is en daarom in de sommige gevallen niet peer-reviewed is. Het gebrek aan peer-reviews is te verklaren door het feit dat HT als concept in Nederland, in vergelijking met andere landen, relatief lang als methode bekend is en derhalve al enige malen onderwerp van wetenschappelijk (promotie) onderzoek is geweest. De status van de auteurs (zie tabel 3) van deze literatuur maakt het gebruik van deze bronnen niet minder bruikbaar of van onvoldoende wetenschappelijk niveau, en zijn daarom in dit onderzoek gebruikt. In onderstaande tabel zijn de zoektermen, synoniemen en Engelstalige varianten opgesomd.

Zoekterm	**Synoniem/afgeleide**	**Engelstalige variant**
Compliance	Regel(naleving)	Compliancy, Compliant,
Horizontaal toezicht	Toezicht, Assessment	Horizontal monitoring, Cooperative compliance programmes
Control framework	Controlemechanisme	Control mechanism
Privacy by Design	Privacy by Default	
Privacy	AVG (Algemene Verordening Gegevensbescherming)	GDPR (General Data Protection Regulation)

Tabel 4, zoektermen, synoniemen en varianten in de literatuur.

Er is gebruik gemaakt van een tweetal informatiebronnen, die op hun beurt weer verwijzen naar andere bronnen. De primaire zoekslagen zijn gedaan in HUGO en Google Scholar.

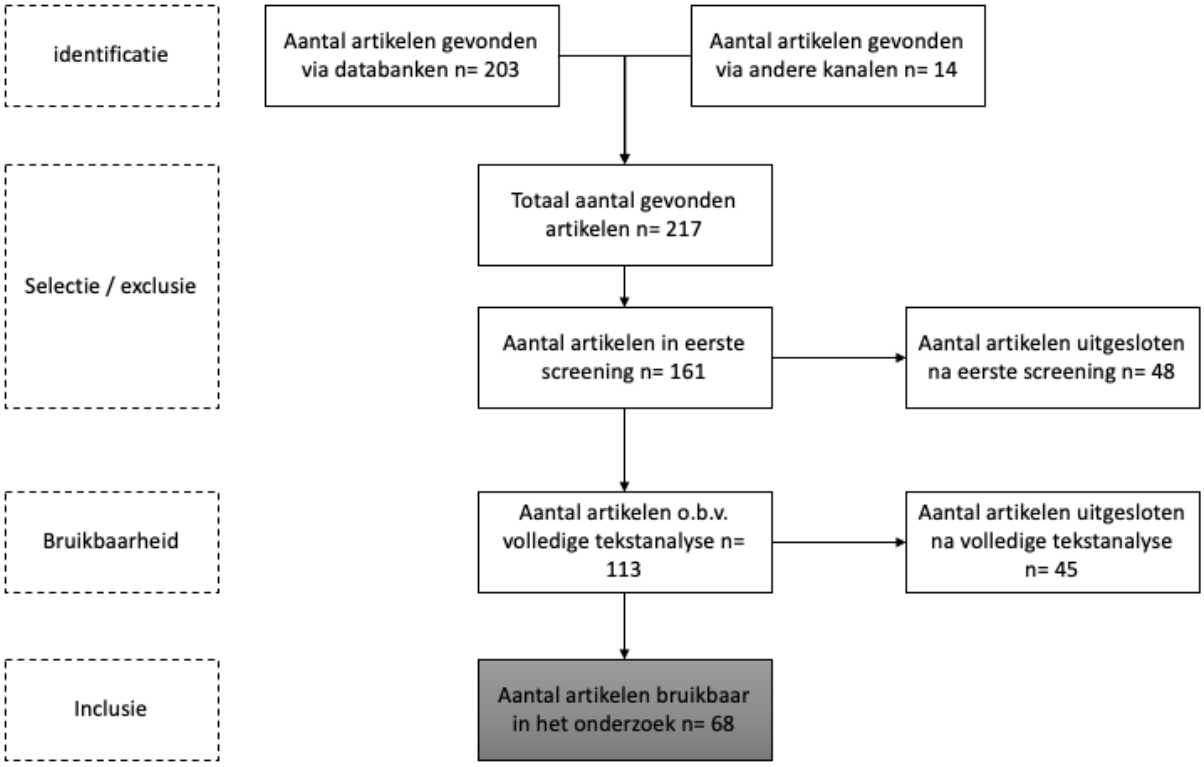
- HUGO; een onlinebibliotheek van de Hogeschool Utrecht waarmee wereldwijd in een groot aantal databanken kan worden gezocht. Voorbeelden zijn Narcis, Science-direct, MIS-Quarterly en Harvard Business Review.
- Google Scholar; een online zoekmachine van Google waarmee wetenschappelijke literatuur, proefschriften en (citaten uit) boeken kunnen worden gevonden op het internet. Google Scholar is laagdrempelig omdat het zonder abonnement te raadplegen is.

Om de juiste literatuur te selecteren zijn zij per stuk beoordeeld. Een belangrijk element in het doen van onderzoek is dat de gebruikte literatuur relevant en up tot date is. Daarnaast is van belang dat de literatuur een peer-review heeft ondergaan en in een taal is geschreven die voor de onderzoeker te begrijpen is. Zoals aangegeven zijn, met name in de context horizontaal toezicht, niet alle bronnen peer-reviewed. In onderstaande tabel is kort aangegeven op basis van welke criteria een artikel wel of niet is gebruikt in het onderzoek.

Criteria	Inclusie	Exclusie
Tijd	2000 – 2020	<2000
Taal	Nederlands en Engels	Anders dan Nederlands of Engelstalig
Type	Artikelen (peer-review) wetenschappelijke tijdschriften, congres papers, proefschriften	Niet- wetenschappelijke papers en artikelen

Tabel 5, In- en exclusiecriteria.

Uit de diverse zoekslagen zijn 203 artikelen naar voren gekomen, waaruit de 68 meest relevante artikelen zijn geselecteerd op basis van de in tabel 5 aangegeven criteria. De gekozen artikelen zijn geschreven in de periode 2000 – 2020 in het Nederlands of Engels. De geselecteerde artikelen zijn gelezen, bestudeerd en handmatig geanalyseerd. Vanuit een praktische overweging, die hieronder wordt toegelicht, is ervoor gekozen de analyse van de literatuur niet te verrichten middels een geautomatiseerde tool of volgens een vaste structuur. Alle gebruikte literatuur is opgenomen in de referentielijst bij dit onderzoek. De literatuur zal samen met de data afkomstig uit de interviews worden gebruikt om een antwoord te geven op de hoofdvraag, en om een artefact te ontwikkelen dat daadwerkelijk een oplossing biedt voor het actuele probleem. De uiteindelijke selectie van literatuur heeft plaatsgevonden volgens de PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) methode van Liberati (Liberati et al., 2009). Het doel van de PRISMA is om onderzoekers te helpen bij het rapporteren van een systematische review en meta-analyses in een onderzoek. PRISMA richt zich op manieren waarop auteurs kunnen zorgen voor een transparante en volledige rapportage van dit soort onderzoek. In figuur 2 zijn de stappen uitgewerkt. In de identificatie fase zijn alle artikelen uit de genoemde databases en via andere ‘onderhandse’ bronnen (bijvoorbeeld op verzoek via email aan de auteur of de bibliotheek van de HU) opgesomd. In totaal zijn in het begin 217 artikelen aan een snelle screening onderworpen. In deze screening zijn in totaal 56 artikelen uitgesloten, onder andere op basis van een onjuiste taal (3 in het Spaans, 1 in het Duits), irrelevante context of nadat bleek dat het gehele artikel niet online verkrijgbaar was. Vervolgens zijn de overgebleven 161 artikelen, op hoofdlijnen (samenvatting, tabellen, figuren en conclusies) aan een tweede screening onderworpen. In deze fase zijn 48 artikelen uitgesloten. De overgebleven 113 artikelen zijn integraal gelezen waarbij aantekeningen en verwijzingen op het fysieke document gemaakt zijn en accenten aangebracht. Ten slotte zijn ook in deze fase 45 artikelen uitgesloten, wat resulteert in een totaal bruikbare selectie voor het gehele onderzoek van 68 stuks.



Figuur 2, Prisma flow diagram voor selectie van gebruikte literatuur conform Liberati 2009.

3.1.4 Interviews

Khan onderscheidt drie typen interviews (Khan, 2014): het open interview, het semigestructureerde interview en het gestructureerde of gestandaardiseerde interview. Saunders et al. (2009) maken eenzelfde onderverdeling. Binnen dit onderzoek gebruik ik het semigestructureerde interview. De inhoud van de vragen, de formulering en de volgorde geeft aan hoe gestructureerd het interview uiteindelijk wordt (Boeije, 2012, p. 57). Semigestructureerde interviews worden gekenmerkt door het gebruik van een topiclijst, die een richtlijn voor onderwerpen gedurende interviews geeft (Cohen & Crabtree, 2006). In deze interviewvorm wordt structuur aangebracht door een zogenoemd interviewschema of door van tevoren precies geformuleerde open of halfopen vragen. De checklist zorgt ervoor dat alle onderwerpen worden geraakt. In bijlage F bij deze thesis worden de Interviewguide, Topiclist en de checklist gevoegd. De volgorde van de onderwerpen, de formulering van de vragen en de formulering van de antwoorden liggen niet vast. Deze methode laat ruimte voor persoonlijke opvattingen, ervaringen en belevingen van de respondenten. De interviewer bepaald hoe de vragen worden geformuleerd. Door het tonen van interesse, het doorvragen en het vragen om verduidelijking anticipeert de interviewer in op de situatie en stimuleert hij de voortgang van het gesprek (Khan 2014).

De eerste interviews zijn afgenomen onder een drietal medewerkers van de KMar in de periode januari en februari 2020. Het betreft een tweetal privacyfunctionarissen binnen de KMar en de functionaris gegevensbescherming. Deze functionarissen hebben allen vanuit hun functie te maken met de bescherming van privacy bij de verwerking van persoonsgegevens, compliance ten aanzien van het gebruik van informatiesystemen, en het afleggen van verantwoording aan de toezichthouder. De eerste drie respondenten hebben meerjarige ervaring in hun vakgebied. Deze drie interviews zijn in eerste

instantie gebruikt om de aanleiding van het onderzoek en de context te duiden. Uit de interviews is ook het daadwerkelijke probleem en de relevantie ervan aan bod gekomen. De corona-maatregelen maakte het in praktische zin onmogelijk om fysiek vervolginterviews te organiseren op dezelfde manier als in januari 2020, waarbij alle interviewdata op eenzelfde wijze verzameld zou worden zoals in de eerste drie interviews. Een fysieke bijeenkomst zou, naast spraak, meer non-verbale interactie (zoals een lach of een frons van een respondent) opleveren die ook als onderzoekdata moeten worden beschouwd. Gezien de beperkingen in de reisbewegingen en persoonlijke keuzes van respondenten hierin, hebben de vervolginterviews daarom zowel fysiek als digitaal plaatsgevonden. In december 2020 zijn een zestal interviews gehouden met privacy- en/of AVG-coördinatoren van de verschillende defensieonderdelen[9] om het concept framework scherper te krijgen, te valideren, en de bruikbaarheid in combinatie met horizontaal toezicht te bepalen. Deze functionarissen hebben zowel korte als langdurige ervaring met betrekking tot privacy en daaraan grenzende aspecten. Respondent nr. 2 en 3 zijn ook betrokken geweest bij de eerste serie interviews in de periode januari en februari 2020. In de tabel hieronder is een geanonimiseerd overzicht van respondenten opgenomen met informatie over de respondent en zijn of haar functie. De functiebenamingen zijn zoals deze in de organisatie worden gebruikt.

Respondent	Functie	Ervaring	Toelichting
Nr. 1 AH	WPG-functionaris	>3 jaar	Aandachtsgebied Wet Politie Gegevens (WPG)
Nr. 2 MS	AVG-functionaris	>1 jaar	Vreemdelingenrecht
Nr. 3 KW	Functionaris gegevensbescherming	2 jaar	Aanspreekpunt voor de Autoriteit Persoonsgegevens bij de organisatie
Nr. 4 AS	AVG-coördinator	1 jaar	Aanspreekpunt AVG bij de Kon. Marine
Nr. 5 CV	AVG-coördinator	>2 jaar	Aanspreekpunt AVG bij Kon. Luchtmacht
Nr. 6 JP en JD (duo)	AVG-coördinatoren	3 en <1 jaar	Aanspreekpunt HRM organisatie en juridische aangelegenheden
Nr. 7 OvO	AVG-coördinator	>3 jaar	Aanspreekpunt informatiebeveiliging
Nr. 8 JH	Assistant Professor, Tilburg School of Economics and Management	Onb.	Universitair docent Information Management / auteur (betreft gespreksnotitie)
Nr. 9 EH	Universitair docent	>5 jaar	Deskundige op het gebied van belastingrecht en gepromoveerd op onderzoek naar Horizontaal toezicht

Tabel 6, lijst van respondenten (geanonimiseerd), functies en toelichting.

Deze respondenten zijn geïnterviewd over de onderwerpen: privacy, Privacy by Design, het privacy control framework en horizontaal toezicht. Van alle fysieke en digitale interviews zijn geluidsopnames gemaakt die vervolgens door de onderzoeker zelf zijn getranscribeerd tot een analyseerbaar transcript. Een transcript is de weergave van het interview en een essentieel onderdeel van een kwalitatief onderzoek. Daarna volgt de digitale analyse van de interviewdata via de tool ATLAS_Ti.

[9] De Nederlandse defensieorganisatie bestaat uit een zevental zgn. defensieonderdelen waarbinnen de vier klassieke krijgsmachtonderdelen marine, landmacht, luchtmacht en marechaussee.

3.1.5 Analyse van literatuur en interviews

Zoals in par. 3.1.1 beschreven staat is de gebruikte literatuur handmatig geanalyseerd zonder gebruik te maken van een geautomatiseerde tool of volgens een vaste structuur. De interviews daarentegen zijn met gebruikmaking van de analysetool ATLAS_Ti geanalyseerd. Door middel van het open coderen, oftewel op pragmatische wijze coderen en labelen van uitspraken in de interviews, wordt een analyse gevormd. In de analyse van de interviews zijn onderstaande 17 'codes' of 'labels' gebruikt.

#	Code	Comment label
1	Advies(functie)	Er is behoefte aan advies / guidance vanuit de AP
2	Begrip	Begrip als een van de criteria van horizontaal toezicht
3	Behoefte systematiek	Er is behoefte aan een systematiek / methode om compliance te borgen
4	Bewustwording	Gaat over bewustworden m.b.t. privacy en de verwerking van persoonsgegevens bij de gebruikers van informatiesystemen
5	Borging	Gaat over de borging van met name AVG eisen bij de verwerking van persoonsgegevens
6	Capaciteit AP	Geeft aan dat de AP capaciteitsproblemen heeft t.a.v. hun taakstelling
7	Dataminimalisatie	Als principes om te voorkomen dat teveel persoonsgegevens worden verzameld en gebruikt
8	Doelbinding	Wettelijke grondslag voor de verwerking van persoonsgegevens
9	DPIA	Data Protection Impact Assessment
10	Intern toezicht	Toezicht wat intern de organisatie plaatsvindt
11	Privacy by Design	Methode of filosofie aan de hand waarvan het framework is ontworpen
12	Sancties	Sancties, boetes en handhaving vanuit de AP
13	Tastbaar maken	De behoefte om PbD principes praktische invulling te geven
14	Toezicht	Toezicht vanuit de AP
15	Transparantie	Transparantie als een van de criteria van horizontaal toezicht
16	Verantwoording	Het kunnen aantonen wat de risico's zijn incl. de mitigerende maatregelen
17	Vertrouwen	Vertrouwen als een van de criteria van horizontaal toezicht

Tabel 7, Atlas_Ti coding labels.

Door middel van het labelen van uitspraken of 'quotations' in de eerste drie interviews is een eerste praktische aanleiding voor het onderzoek en het te ontwerpen artefact geformuleerd. Daarnaast zijn in de later zes interviews de vereisten van het privacy control framework en de voorwaarden voor een horizontale toezicht relatie geanalyseerd. Twee voorbeelden van quotations die aanleiding geeft tot het ontwerpen van het privacy control framework zijn quotations behorende bij het codelabel 3 'behoefte systematiek' 1:34 en 4:18.

1:34 Voor de AVG hebben we het op dit moment uhmm uhmmm nog niet iets dergelijks. Uhmm ik kan me wel voor...

Content:
Voor de AVG hebben we het op dit moment uhmm uhmmm nog niet iets dergelijks. Uhmm ik kan me wel voorstellen dat het zeker bevordelijk zou zijn uhm alleen op dit moment is er nog gewoon te weinig kennis binnen de organisatie om zoiets uhmm om zoiets op gang te brengen

4:18 Als je een systeem eenmaal ontworpen hebt en je hebt die privacy by design niet gedaan, dan gaat dat...

Content:
Als je een systeem eenmaal ontworpen hebt en je hebt die privacy by design niet gedaan, dan gaat dat je niet meer lukken. Daarmee voldoet het systeem dus eigenlijk niet, en wij hebben dus ook heel veel systemen bij defensie, zoals peoplesoft die voldoen gewoon niet aan privacy by design en AVG. En dat komt omdat het oudere systemen zijn, maar even ombouwen is gewoon niet te doen.

Twee voorbeelden van quotations die duiden op het ‘tastbaar maken’ van het privacy control framework (codelabel 13) of ‘vertrouwen’ als onderdeel van horizontaal toezicht (codelabel 17) zijn quotations 11:2 en 4:24 uit de interviews.

11:2 Houd het concreet, overzichtelijk en begrijpelijk. Zoveel mogelijk wegblijven bij de vagere AVG begr...

Content:
Houd het concreet, overzichtelijk en begrijpelijk. Zoveel mogelijk wegblijven bij de vagere AVG begrippen als “transparantie”, want dat is te lastig meetbaar voor gebruikers.

4:24 Grote transparantie draagt bij aan vertrouwen.

Content:
Grote transparantie draagt bij aan vertrouwen.

In bijlage E zijn de gebruikte code labels uit de interviews in onderling verband getoond.
Een gedetailleerde conclusie op basis van de analyse van de interviews volgt in hoofdstuk 4.3.

3.2 Onderzoeksmethoden en technieken

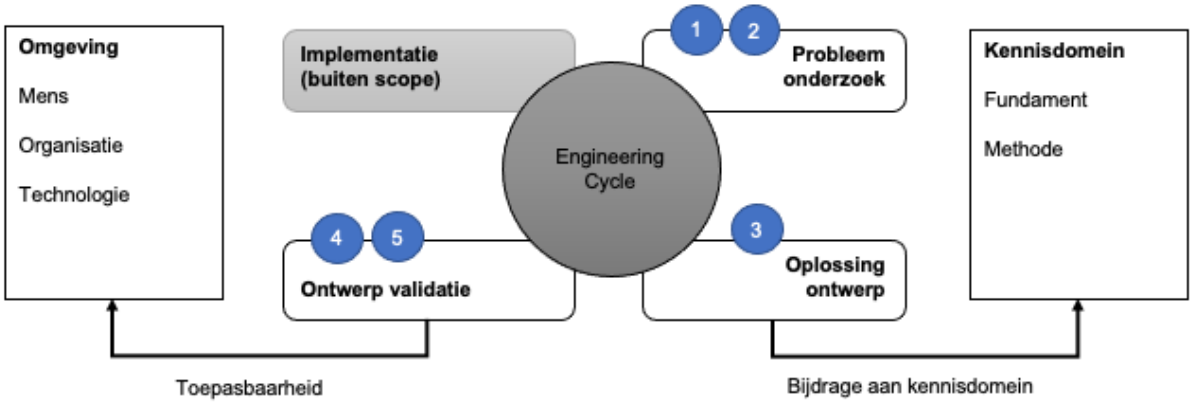
Dit onderzoek wordt de Design science cycle gebruikt om het PCF te ontwerpen. De design science cycle is door Wieringa ontworpen en uitgebreid beschreven in zijn boek ‘Design Science Methodology’ uit 2014. Deze methode vindt zijn herkomst in de Design Science methode van Hevner (Hevner et al., 2004). Design science stelt de onderzoeker in staat om niet alleen een bepaald fenomeen te verkennen, te beschrijven of uit te leggen, maar ook om oplossingen voor een bepaald probleem te ontwerpen of te adviseren (Dresch et al., 2019). In design science is er naast het ontwerpen van het artefact ook aandacht voor evaluatie van het artefact en communicatie hierover. In deze methode wordt de term ‘artefact’ gebezigd voor het PCF. In de beschrijving van de onderzoeksmethode wordt dit overgenomen. Hieronder wordt de design science methode van Wieringa nader toegelicht.

3.2.1 Design science cycle

De design science cyclus bestaat uit vier fases die worden doorlopen bij het ontwerpen van een artefact. Met de klok mee, beginnend rechtsboven zijn dit;

1. Problem investigation
2. Treatment design
3. Treatment validation
4. Treatment implementation (buiten scope)

In figuur 3 is daarbij ook aangegeven welke deelvragen in welke fase van de methode worden beantwoord.

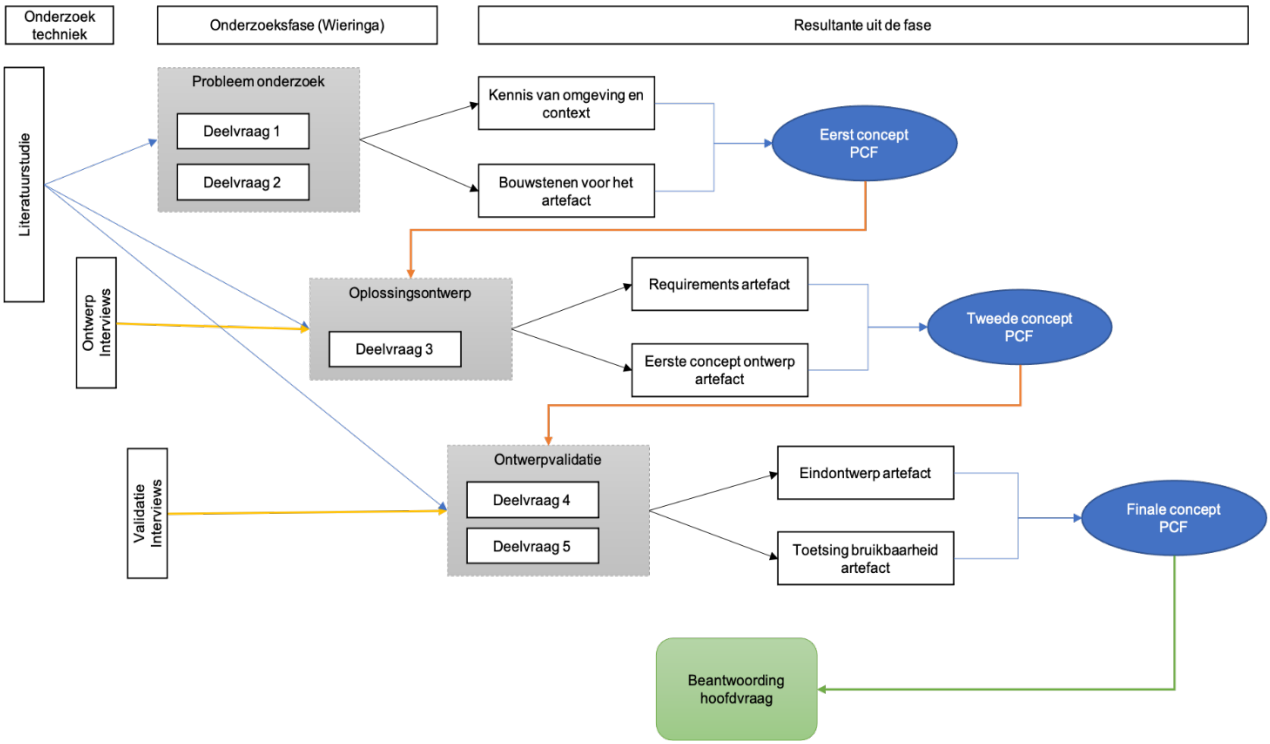


Figuur 3, Onderzoekmethodes van Hevner en Wieringa gecombineerd, daarin aangegeven de positie van de deelvragen uit het onderzoek.

Er worden twee activiteiten onderscheiden; het ontwerpen van een artefact en empirisch onderzoek naar de toepasbaarheid van het artefact. De implementatie van het artefact (linksboven in de afbeelding) wordt omwille van de omvang van het onderzoek buiten scope gelaten. In de probleemonderzoeksfase van dit onderzoek wordt onderzocht welke concepten er al bekend zijn en elders worden toegepast. Onderzocht wordt wat er in die context plaatsvindt, en welke oorzaken en gevolgen daarmee gemoeid gaan. Vervolgens wordt het effect van het privacy control framework onderzocht in relatie tot horizontaal toezicht. In de oplossingsontwerpfase worden de ontwerpvereisten gespecificeerd en verschillende contextvariabelen bezien. Belangrijk is om te onderzoeken welke bijdrage het artefact levert aan verbeteren van de compliance bij het verwerken van persoonsgegevens en het vereenvoudigen van toezicht. Op basis van literatuur en data uit o.a. interviews wordt een eerder ontwerp bijgesteld. In de laatste fase wordt het ontwerp gevalideerd en bezien of het PCF bruikbaar is als oplossing voor het geïdentificeerde probleem. Leidt het artefact in dit geval tot verbeterde compliance en een effectiever en efficiëntere toezichtmethodiek? Zoals gezegd wordt de implementatie van het artefact in dit onderzoek buiten scope geplaatst omwille van de tijd en omvang van deze thesis.

Aan de hand van literatuuronderzoek wordt nadere duiding gegeven aan de begrippen control framework, Privacy by Design en horizontaal toezicht. Het uitgevoerde literatuuronderzoek is vooral bedoeld om antwoord te geven op deelvraag 1 en 2. Deze eerste twee deelvragen zijn bedoeld om de context van het onderzoek te duiden en geven uitleg over zowel het privacy control framework als over horizontaal toezicht, en worden een aantal definities uitgewerkt. Op basis van de data die in deze fase is verzameld is een eerste concept van het PCF gemaakt. Een van de meest gebruikte technieken bij het verzamelen van gegevens is het uitvoeren van interviews. Door middel van interviews kan een onderwerp diepgaand verkend worden en kunnen ervaringen uit de praktijk worden gehaald die helpen bij het aanscherpen van het artefact. Charmaz (1996) vindt dat bij het uitvoeren van een interview nieuwe gebeurtenissen, opvattingen en gevoelens opnieuw onderzocht kunnen worden. Daarom zijn in in de eerste fase een drietal semigestructureerde interviews gehouden met respondenten uit de dagelijkse praktijk. Leidend in deze gesprekken is de beeldvorming bij en de aanleiding tot het onderzoek en het verzamelen van de eerste requirements. De data uit deze eerste interviews daarnaast interessant om de ontwerpende deelvraag 3 te beantwoorden. Op basis van het op dat moment

uitgevoerde literatuuronderzoek en interviews is een tweede concept van het framework ontwikkeld, waarna vervolginterviews zijn gehouden om het concept aan te scherpen. Met de data uit deze interviews wordt onderzocht of het PCF bijdraagt aan compliance (deelvraag 4) en vindt validatie van het PCF plaats naar de bruikbaarheid van horizontaal toezicht. Alles bij elkaar leidt tot beantwoording van de deelvragen en de hoofdvraag. Schematisch ziet het onderzoeksproces er als volgt uit.



Figuur 4, Onderzoeksproces: technieken, fases en resultanten.

Met de blauwe pijlen wordt aangegeven voor welke stap van het onderzoeksproces literatuurstudie wordt gebruikt, en met de gele pijlen de interviews. De blauwe lijnen leiden naar het product uit die processtap. De oranje pijlen volgen de chronologie van het onderzoek waarbij tot slot de groene pijl leidt naar de uiteindelijke beantwoording van de hoofdvraag.

3.3 Ethische verantwoording

Het onderzoek kan alleen goed worden uitgevoerd met medewerking van respondenten. Met name tijdens de interviews worden uitspraken en andere (gevoelige) data van andere personen vastgelegd. Daarom worden alle mogelijke maatregelen getroffen om de privacy van deze personen te waarborgen en om vanuit een ethisch oogpunt de verwerking van de data netjes te laten verlopen. Dat houdt onder andere in dat:

- Onderzoeksresultaten, met name uit de interviews geanonimiseerd worden indien dat is gewenst. Daarnaast is alleen wanneer dat relevant is naam en toenaam van respondenten vermeld worden.
- De interviews worden alleen na toestemming van de respondent opgenomen op een voice recorder of door opname van een digitale meeting vanwege de corona-pandemie. Deze

opnames worden verwerkt in tekst en waar nodig geanonimiseerd. Indien gewenst kunnen de opgenomen interviews worden vernietigd. De transcripties zullen ten behoeve van het onderzoek worden ingeleverd en bewaard blijven.

- Aan het begin van het interview wordt transparantie in acht genomen. Voordat de interviews worden afgenomen is informatie verstrekt over de doelstelling en de aanpak van het onderzoek.

3.4 Betrouwbaarheid en validiteit

Om een kwalitatief goed onderzoek uit te voeren zijn volgens Mortelmans (2009, pp. 428-430) drie zaken van belang; validiteit, betrouwbaarheid en generaliseerbaarheid. Een belangrijk aspect in validiteit is de triangulatie van de data en onderzoeksgegevens. Triangulatie, of ook wel driehoeksmeting, betekent dat onderzoek wordt verricht vanuit verschillende richtingen om een onderzoeksvraag te beantwoorden. De antwoorden uit de verschillende richtingen die elkaar overlappen of elkaar niet tegenspreken, zijn dan waarschijnlijk objectief waar. Het verhoogt de geldigheid van het onderzoeksresultaat (Verhoeven & Bik, 2014). Om de validiteit van het onderzoek te verhogen worden er meerdere validiteitsstrategieën toegepast.

3.4.1 Interne validiteit

Interne validiteit; als het onderzoek goed is opgezet en conform het plan is uitgevoerd kan de conclusie uit het onderzoek voor waar worden aangenomen of op zijn minst aannemelijk worden geacht. Interne validiteit wordt ook wel methodologische validiteit genoemd. Het geeft een oordeel over de kwaliteit van de onderzoeksmethode, dataverzameling en de daaruit volgende analyse (Charmaz, 1996; Boeije, 2012; Oost & Markenhof, 2016). Bryman en Bell noemen dit in hun boek ‘de match tussen onderzoek data en theoretische ideeën’.

Volgens Baarda (2013) en Boeije (2014) dient kwalitatief onderzoek te voldoen aan de gangbare kwaliteitseisen van betrouwbaarheid en validiteit. Resultaten moeten onafhankelijk zijn van toeval en een representatie van de werkelijkheid. In dit onderzoek is zoveel mogelijk gericht op objectiviteit echter wel rekening houdend dat enige vorm van subjectiviteit niet volledig kan worden voorkomen. Om dit toch zoveel mogelijk te voorkomen is het toepassen van peer-debriefing uitgevoerd waarbij aan medestudenten input is gevraagd en hypotheses zijn getoetst.

3.4.2 Externe validiteit

Externe validiteit; als de resultaten van het onderzoek gegeneraliseerd kunnen worden, zijn ze extern valide. In dit geval zouden de resultaten gegeneraliseerd kunnen worden als blijkt dat eenzelfde systematiek, zoals in de fiscale en zorgcontext wordt gebruikt, eveneens bruikbaar is voor informatiesystemen (Oost & Markenhof, 2016). Externe validiteit zegt ook iets over de repliceerbaarheid van het onderzoek, hoewel Bryman en Bell schrijven dat dit met name in kwalitatief onderzoek altijd lastig zal blijven, omdat met name de omgeving waarin het onderzoek zich afspeelt aan verandering

onderhevig is. In dit onderzoek wordt er gestreefd naar inhoudelijke generalisatie: in welke mate zijn de onderzoeksresultaten vergelijkbaar in soortgelijke situaties? In dit geval gaat het om de situatie in de fiscale context, in hoeverre zijn deze vergelijkbaar in de context van het onderhavig onderzoek? Op enig moment in het onderzoek bereikt de onderzoeker een moment van 'verzadiging'. Volgens Charmaz (2008) houdt dat in dat tijdens de analyse door het literatuuronderzoek en de interviews er geen nieuwe inzichten meer worden opgedaan. Met de beschikbare data kunnen derhalve de onderkende elementen worden onderbouwd om zo verschillende eigenschappen van de elementen zeer gedetailleerd vast te leggen. Op dat moment kan de onderzoeker aannemen dat de data die op dat moment is gegenereerd volstaat en er geen nieuwe data meer verzameld hoeft te worden. Het is belangrijk op te merken dat deze beslissing gedeeltelijk pragmatisch is, aangezien er altijd de mogelijkheid is dat er andere problemen zijn, maar men ergens moet stoppen. Charmaz (2008, p. 167) onderschrijft dit, met de bewering dat theoretische verzadiging een subjectieve oefening is en een interpretatieve benadering, zowel het belang als de beperkingen van dergelijke subjectiviteit erkent.

3.4.3 Betrouwbaarheid

De betrouwbaarheid van de resultaten heeft vooral te maken met de consistentie en repliceerbaarheid. Bij een kwalitatieve studie is van repliceerbaarheid geen sprake maar van uniekheid van onderzoeksgegevens. Mortelmans schrijf in zijn handboek kwalitatieve onderzoeksmethoden (pag. 433 – 436) (Mortelmans, 2009) dat betrouwbaarheid belangrijk is in kwalitatief onderzoek, en daarom is het goed om de betrouwbaarheid van dit onderzoek te vergroten door tijdens het onderzoek een nauwkeurige beschrijving te geven van het verloop van het onderzoek, de beslissingen die zijn genomen en eventueel de veranderingen die ten opzichte van het oorspronkelijke onderzoeksplan zijn ontstaan te benoemen. Om de betrouwbaarheid van het onderzoek te vergroten is er bijvoorbeeld voor gekozen om de transcripten van de interviews zelf te maken zodat er geen data verloren in een geautomatiseerd proces. Ook de eventuele non-verbale communicatie tijdens de fysieke interviews is zodoende onderkent en in de analyse verwerkt.

3.4.4 Objectivering

Het afnemen van de interviews en het analyseren van de daaruit gegenereerde data is zo objectief mogelijk uitgevoerd. Onoverkomelijk is dat hierbij persoonlijke opvattingen en ervaringen invloed zullen hebben gehad, echter is getracht om dit zo open mogelijk te doen. Gedurende het hele onderzoek is een open houding ten aanzien van andere perspectieven en invalshoeken aangehouden. Dit heeft er onder andere toe geleidt dat het ontworpen privacy control framework tijdens het onderzoek is aangepast en verbeterd. Daarmee voornamelijk doelend op het feit dat het belangrijk bleek om vooral niet te abstract te blijven, maar juist praktisch en pragmatisch te ontwerpen. Een andere stap in de objectivering is het voorleggen van gedachten of hypotheses aan medestudenten en deskundigen.

4. Resultaten

Horizontaal toezicht heeft geleid tot een paradigmawisseling in het toezicht, zie figuur 1 in paragraaf 2.3.2. Het heeft wel als risico dat HT een doel op zich wordt. Eerder werd al geschreven dat horizontaal toezicht ontstaan is uit een algemene maatschappelijk trend om de regeldruk te verlagen en de intrinsieke motivatie van onder toezicht staande aan te spreken (Commissie Horizontaal Toezicht Belastingdienst, 2012). Minder aandacht is er destijds geweest voor de concrete reden van de introductie van HT, namelijk een veelal inefficiënte en moeizame relatie tussen organisaties en toezichthouders. Veel informatie is hierover niet beschikbaar, maar het lijkt voor de hand te liggen dat deze hindernissen in de toezicht relatie verbeterd dienden te worden.

4.1 Resultaten uit het onderzoek naar horizontaal toezicht

De inherente onvoorspelbaarheid (zie par 2.2.5) van toezichtrelaties introduceert een klassiek kip/ei-probleem. De Commissie Horizontaal Toezicht Belastingdienst schrijft in haar rapport op pagina 94: “de één wil pas vertrouwen geven, als de andere het vertrouwen waard is, en omgekeerd” (Commissie Horizontaal Toezicht Belastingdienst, 2012). Toezichthouders die overwegen toezicht horizontaler in te richten moeten eerst bezien of en in hoeverre het realistisch is dat zij met de onder toezicht staande organisaties een situatie van wederzijds vertrouwen opbouwen, maar horizontaal toezicht kent zoals bekend nog twee andere uitgangspunten; begrip en transparantie. Ik ga hieronder op deze drie uitgangspunten nader in.

Wederzijds vertrouwen betekent in toezichtrelaties ‘de positieve verwachting van het gedrag van de ander (Belastingdienst, 2013)’. Door een positieve verwachting van het gedrag van organisaties als uitgangspunt te nemen en de belofte om passend en met begrip te zullen reageren, ontstaat bij organisaties als het goed is voldoende vertrouwen in de toezichthouder om open en transparant te zijn, althans zo zou het moeten. Dat vertrouwen groeit volgens de toezichthouder als partijen afstemmen of ze elkaar hebben begrepen, door aandacht voor elkaar te hebben en door wederzijds verantwoording af te leggen (Belastingdienst, 2008).

In modern overheidstoezicht is vertrouwen in organisaties het uitgangspunt. De moderne overheid geeft organisaties ruimte om eigen verantwoordelijkheid te dragen. Door organisaties vertrouwen te schenken, hoopt de toezichthouder zelf ook vertrouwen terug te krijgen. Six heeft zich in haar proefschrift ‘Trust and trouble; Building interpersonal trust within organizations’ uit 2004 gebogen over het begrip vertrouwen als het gaat om toezicht. Iemand vertrouwen betekent volgens Six ‘jezelf kwetsbaar maken voor het handelen van een ander, uitgaand van de verwachting dat hij bepaalde acties zal verrichten die voor jou belangrijk zijn en je het handelen van die ander niet volledig kan controleren of met zekerheid kan voorspellen’. Beide partijen moeten zich volgens Six kwetsbaar opstellen om ‘vertrouwen’ te bereiken. Six (2004) definieert vertrouwen als volgt:

> *Definitie 8 – Trust: Interpersonal trust is a psychological state comprising the intention to accept vulnerability to the actions of another party based upon the*

expectation that the other will perform a particular action important to you, irrespective of the ability to monitor or control that other party.

Voortbordurend op de definitie van Six, kan het begrip vertrouwen onder horizontaal toezicht volgens van der Hel – van Dijk (Van Der Hel & Pheijffer, 2012) als volgt worden ingevuld: van vertrouwen is sprake als zowel de toezichthouder als organisatie zich kwetsbaar opstellen voor het handelen van de ander, uitgaand van de verwachting dat beiden acties zullen verrichten die voor de ander belangrijk zijn, ongeacht de mogelijkheid om het handelen van die ander volledig te controleren of met zekerheid te voorspellen (Van der Hel & Siglé, 2019). Hoewel van der Hel – van Dijk meent dat vertrouwen een vorm van onzekerheid met zich brengt, denkt zij dat een 'minder weten' over feiten en omstandigheden te rechtvaardigen met een 'meer weten' over de organisatie en hoe deze de processen 'in control' heeft.

Bij **begrip** gaat het om de bereidheid van partijen zich in elkaars positie in te leven (Belastingdienst, 2013). Het gaat om een passende reactie op het gedrag van de ander (Belastingdienst, 2008). De Commissie Horizontaal Toezicht Belastingdienst spreekt - als het gaat over begrip voor elkaars belangen - over 'begrip voor het bedrijfsgebeuren' wat zoveel betekent als 'begrijpen hoe een organisatie in elkaar steekt (Commissie Horizontaal Toezicht Belastingdienst, 2012). Binnen een horizontaal toezichtrelatie is het ook van belang dat de Belastingdienst begrip heeft voor het spanningsveld waarin de organisatie en de toezichthouder zich bevinden. Ook speelt begrip een rol in het gezamenlijke overleg naar passende oplossingen en moeten partijen met begrip op elkaars fouten reageren. Dat betekent dat partijen met elkaar in gesprek moeten over de oorzaak van fouten en hoe fouten in de toekomst voorkomen kunnen worden (Commissie Horizontaal Toezicht Belastingdienst, 2012).

Bij **transparantie** gaat het erom dat organisaties en de toezichthouder elkaar informeren over relevante standpunten en de toezichthouder zijn visie geeft op de gevolgen ervan. Niet alleen de organisatie maar ook de toezichthouder moet open en transparant zijn (Belastingdienst, 2008). Voor wat betreft de transparantie van organisatie doet de toezichthouder een beroep op de eigen verantwoordelijkheid van de organisatie om een juiste een juiste voorstelling van zaken gegeven wordt. Om daaraan te voldoen moeten organisatie hun verwerkingsprocessen op orde hebben. De verwachtingen ten aanzien van fiscale transparantie kent ook een keerzijde, volgens Huiskers-Stoop (Huiskers-Stoop, 2015, p. 160). Zo kan de druk op transparantie - ter bevestiging van het in organisatie gestelde vertrouwen - stimuleren om juist die informatie te verstrekken die de betrouwbaarheid ten goede komt en informatie die de betrouwbaarheid aantast te verzwijgen; 'de toezichthouder weet immers niet wat hij niet weet' (Kaptein & Wempe, 2003). Daarnaast kan transparantie helpen bij het verdelen van verantwoordelijkheden, maar het kan die verantwoordelijkheden ook juist afschuiven (Kaptein & Wempe, 2003).

4.1.1 Constructieve effecten van horizontaal toezicht

Het naleven van wet- en regelgeving is volgens Mendoza en Wielhouwer (Mendoza & Wielhouwer, 2015) deels een gedragsuitkomst. Gedrag wordt bepaald door zowel intrinsieke als extrinsieke motivatie. Zelfs zonder intrinsieke motivatie en externe pressiemiddelen, denk aan de dreiging van

sancties, kan een op vertrouwen gebaseerd systeem efficiënt en effectief zijn. Maar dat vertrouwen is dan niet onbeperkt en niet voor iedereen, schrijven Mendoza en Wielhouwer in hun artikel 'Only the carrot, not the stick: incorporating trust in the enforcement of regulation' (Mendoza & Wielhouwer, 2015). Uit onderzoek blijkt (Accountant, 2017) dat compliance verbetert en horizontaal toezicht een waardevolle vorm van toezicht op grote organisaties is. De horizontale toezichtrelatie draagt positief bij aan een hogere bereidheid tot compliance.

4.1.2 Commentaar uit de wetenschap

In tabel 3 in paragraaf 2.3 is een overzicht gegeven van de wetenschappelijke bronnen die door diverse auteurs zijn geschreven. Het is derhalve interessant om te onderzoeken of de kritieken overeenkomen met het hetgeen door de wetenschap is geconstateerd. Allereerst is er de commissie onder leiding van Stevens (Commissie Horizontaal Toezicht Belastingdienst, 2012), die adviseert om heldere criteria te beschrijven waaraan organisaties moeten voldoen willen zij in aanmerking komen voor horizontaal toezicht. Het onderzoek van Huiskers-Stoop (Huiskers-Stoop, 2015) behandeld met name de effectiviteit van horizontaal toezicht. De effectiviteit van HT was eveneens een kritiekpunt uit de politiek. Huiskers-Stoop wijst er in haar onderzoek op dat het noodzakelijk is dat objectief kan worden getoetst waarom met de ene organisatie wel, en met de andere geen HT overeengekomen kan worden. Uit het eigen onderzoek van de belastingdienst in 2013 (Belastingdienst, 2013) komt met name de bevestiging naar voren dat organisaties meer gericht zijn om compliant te werken als de werkrelatie met de toezichthouder beter is.

Het onderzoek van De Widt (2017) is gericht op de resultaten van horizontaal toezicht en doet een aanbevelingen als het gaat om de werkwijze. De Widt schrijft: “This high level of interaction will especially occur during the initial stage of cooperative compliance, when a relatively large number of businesses are likely to be in need of more feedback to improve their level of control”. Het rapport adviseert dan ook dat organisaties niet te snel moeten worden toegelaten tot horizontaal toezicht totdat binnen de organisatie voldoende kennis en expertise aanwezig is om bijv. een PCF in te richten.

4.1.3 Kritiek uit praktijk, politiek en wetenschap

De kritiek uit politiek leidt zich toe te spitsen op twee zaken, de veronderstelde relatie tussen organisatie en toezichthouder, en het feit dat de toezichthouder minder controleert. De eerste conclusie wordt ook getrokken door de Commissie Horizontaal Toezicht Belastingdienst (Commissie Horizontaal Toezicht Belastingdienst, 2012) en het onderzoek van De Widt (2017). De Commissie Horizontaal Toezicht Belastingdienst noemt deze ‘verkleving’ zelfs een risico, die vragen om mitigerende maatregelen. De Widt op zijn beurt adviseert om meer openheid in de afspraken tussen organisaties en toezichthouder om discussies over dit punt voor te zijn. De wetenschap ziet geen causaal verband tussen de introductie van horizontaal toezicht en het verminderde aantal uitgevoerde controles door toezichthouders. Dat komt ook omdat, in deze onderzoeken de belastingdienst, al voor het introduceren van horizontaal toezicht, bezig was met het verminderen van de controles achteraf, maar deze aan de voorkant proberen te voorkomen.

De wetenschappelijke bijdragen gaan een tandje dieper en raken ook zaken als het concept, de uitvoering en de resultaten (in termen van effectiviteit en efficiency). Huiskers-Stoop en De Widt concentreren zich vooral op effectiviteit wat in het kader van onderhavig onderzoek relevant is.

De Widt concludeert dat horizontaal toezicht over het algemeen leidt tot een verbeterde relatie tussen organisaties en toezichthouder. Huiskers-Stoop voegt daaraan toe dat horizontaal toezicht ook leidt tot betere compliance. Volgens Siglé (2019) komt dat mede doordat de toezichthouder in een verbeterde relatie zijn adviesfunctie beter kan invullen. Een verbeterde adviesfunctie leidt immers ook tot een verhoging van de veiligheid van de persoonsgegevens in kwestie, en daarbij is zowel de organisatie als de toezichthouder gebaat. Dat is ook in lijn met de opzet van horizontaal toezicht; naar mate de werkrelatie beter is, is de mate van transparantie en beheersing ook beter.

Wat betreft het concept van horizontaal toezicht doen de Commissie Horizontaal Toezicht Belastingdienst, Huiskers-Stoop en De Widt eensluidende aanbevelingen. Zij adviseren om met name op het gebied van het toelaten van organisaties tot horizontaal toezicht duidelijke criteria op te stellen. De Widt acht dit raadzaam omdat horizontaal toezicht veel toezichtcapaciteit bespaard. De toezichthouder moet kunnen uitleggen aan welke criteria een organisatie moet voldoen voordat overgegaan kan worden tot horizontaal toezicht. Al met al lijkt het concept en de intentie van horizontaal toezicht niet ter discussie te staan, met name de effectiviteit blijkt in wetenschap nog onderbelicht.

Van der Hel-Van Dijk en Siglé (2019) besluiten in hun artikel ‘herijking horizontaal toezicht’ dat “voor andere organisaties die voornemens zijn om horizontaal toezicht te gaan implementeren het van belang is dat zij voorafgaand aan de invoering het begrip horizontaal toezicht duidelijk omschrijven als een vorm van toezicht die onderdeel uitmaakt van een omvattende toezicht strategie”. Daarnaast adviseren zij dat bij de implementatie er duidelijke doelen moeten worden gesteld, voor zowel de toezichthouder als de organisatie. Onderdeel van de implementatie moet zijn het maken van afspraken voor het meten van resultaten (effectiviteit en efficiency).

4.2 Resultaten uit het onderzoek naar het privacy control framework

In dit onderzoek wordt het framework ontwikkeld aan de hand van Privacy by Design. In dit onderzoek is overwogen om een andere methode van privacy borging te kiezen om het PCF te ontwikkelen, zoals in paragraaf 2.1.3 omschreven. De juridische voorwaarden voor privacy uit de AVG zijn nogal abstract geformuleerd en derhalve te weinig concreet. Een slag die in dit onderzoek juist wel is gemaakt. De AVG geeft meer een juridisch ‘afvinklijst’ en dat is in een ontwerponderzoek onpraktisch. De uitgangspunten van Schaar (2010) komen in grote mate overeen met de PbD principes maar zijn iets technischer van aard. Daarnaast is in dit onderzoek belangrijk gebleken dat privacyvraagstukken al in de ontwikkelingsfase van informatiesystemen worden bezien, waarbij Privacy by Design bij uitstek geschikt is.

Privacy by Design is een set van uitgangspunten en gezien de brede omarming van PbD als concept, plus de formele inbedding in wet- en regelgeving is in dit onderzoek Privacy by Design als leidend gekozen om het privacy control framework vorm te geven. In paragraaf 2.1.4 is hier al uitgebreider op in gegaan. Het houdt in dat een organisatie zich vragen stelt over potentiele privacy-implicaties aan de start van het ontwerp van een nieuw informatiesysteem (Van Lieshout et al., 2012). Aan deze uitgangspunten liggen zeven principes ten grondslag. Een privacy control framework is in par. 1.1.4 omschreven als een instrument van interne beheersing dat is bedoeld om organisaties te ondersteunen bij het compliant verwerken van persoonsgegevens. Door privacy direct in het verwerkingsproces van persoonsgegevens te borgen wordt voorkomen dat systemen persoonsgegevens verwerken of opslaan die niet rechtmatig verkregen zijn. Hoewel PbD vooral een principiële set van algemene theoretische uitgangspunten is, zonder duidelijkheid over de precieze toepassing in de praktijk, is voorzien dat het wel een belangrijke rol zal spelen bij beoordeling van de rechtmatigheid van verwerking van persoonsgegevens, aldus Lieshout et al.

4.2.1 Requirements engineering

In de afgelopen jaren is het belang van vastleggen van privacy vereisten en het modelleren van requirements om een hoge mate van privacybescherming te bieden steeds belangrijker geworden (Guarda & Zannone, 2009). Requirements geven volgens Wieringa ‘een doelstelling’ aan het te ontwerpen instrument, i.c. het PCF. Het gaat daarbij om criteria waaraan tegemoetgekomen moeten worden om aan de eisen, die aan het instrument worden gesteld door een belanghebbende, te voldoen. De belanghebbende is in dit geval de organisatie die met het PCF zijn compliance wil vergroten (in dit onderzoek de KMar) en dat wil aantonen aan de toezichthouder. Daarnaast is de organisatie gebaat bij effectiever toezicht van de toezichthouder. Het individu wiens privacy rechten gerespecteerd en geborgd moeten worden is ook een belanghebbende. Aan de genomen ontwerpbeslissingen moeten argumenten ten grondslag liggen die relevant zijn voor het te bereiken doel. Om redenen die in par. 3.1.1 zijn beschreven door Schaar (2013) en Duncan (2007) is het PCF in dit onderzoek wordt ontworpen o.b.v. de principes van PbD. Het PCF is opgebouwd uit de 7 principes van Privacy by Design, die op hun beurt de 11 opgestelde requirements dekken. Deze 11 requirements bestaan allereerst uit de acht requirements uit de AVG ontleend aan Wolters (Wolters, 2015), Colesky (Colesky et al., 2016) en Perera (Perera et al., 2016). Vervolgens zijn daaraan de drie algemeen bekende criteria vanuit HT, beschreven door o.a. Huiskers-Stoop (Huiskers-Stoop, 2015) en de Widt (2017) aan toegevoegd. De AVG requirements omvatten de rechten die een individu heeft ten aanzien van de verwerking van zijn of haar persoonsgegevens, en kennen derhalve een juridische verwijzing naar artikelen uit de AVG. Het is belangrijk te beseffen dat de AVG de bescherming van de persoonsgegevens ook in handen legt van het individu. Daarmee wordt getracht het individu beter in staat te stellen te bepalen door wie en waarvoor hun persoonsgegevens verwerkt worden (Wolters, 2015). De andere drie requirements hebben als *doelstelling* HT te bewerkstelligen. Het PCF moet uiteindelijk waarborgen dat de organisatie die het PCF gebruikt aan de gestelde 11 requirements voldoet. De 11 requirements staan in onderstaande tabel opgesomd en omschreven.

#	Requirement	AVG-artikel	Omschrijving
R01	Recht op informatie	13 - 14	Een betrokkene moet geïnformeerd worden dat zijn persoonsgegevens verwerkt worden en met welk doel.
R02	Recht van inzage	15.1	Betrokkene heeft het recht te weten of een organisatie zijn persoonsgegevens verwerkt en welke.
R03	Recht op rectificatie en aanvulling	16	Een betrokkene heeft het recht om rectificatie van hem betreffende onjuiste persoonsgegevens te krijgen.
R04	Recht op vergetelheid	17	Een organisatie moet persoonsgegevens wissen als deze niet langer nodig zijn, betrokkene zijn toestemming intrekt of onrechtmatig zijn verkregen.
R05	Recht op beperking van de verwerking	18	De persoonsgegevens worden na verwerking 'bevroren' en mogen niet verder worden verwerkt of gewijzigd.
R06	Recht op overdraagbaarheid (dataportabiliteit)	20	Een betrokkene heeft het recht zijn persoonsgegevens te verkrijgen om over te dragen.
R07	Recht van bezwaar	21	Een betrokkene heeft het recht bezwaar te maken tegen verwerking van zijn persoonsgegevens.
R08	Rechten op een menselijke blik	22	Organisaties mogen geen besluiten over betrokkenen nemen die uitsluitend op geautomatiseerde verwerking zijn gebaseerd.
R09	Begrip		Organisaties en toezichthouders begrijpen de context en dynamiek van elkaars positie en respecteren soms conflicterende belangen.
R10	Wederzijds vertrouwen		Organisaties en toezichthouders ontlenen vertrouwen aan de werking van het interne controlemechanisme.
R11	Transparantie		Organisatie geven openheid over de risico's en de daartegenover staande maatregelen, en toezichthouders over te controleren onderdelen.

Tabel 7, Requirements voor het Privacy Control Framework vanuit de AVG en Horizontaal Toezicht.

4.2.2 Privacy ontwerpstrategieën en tactieken

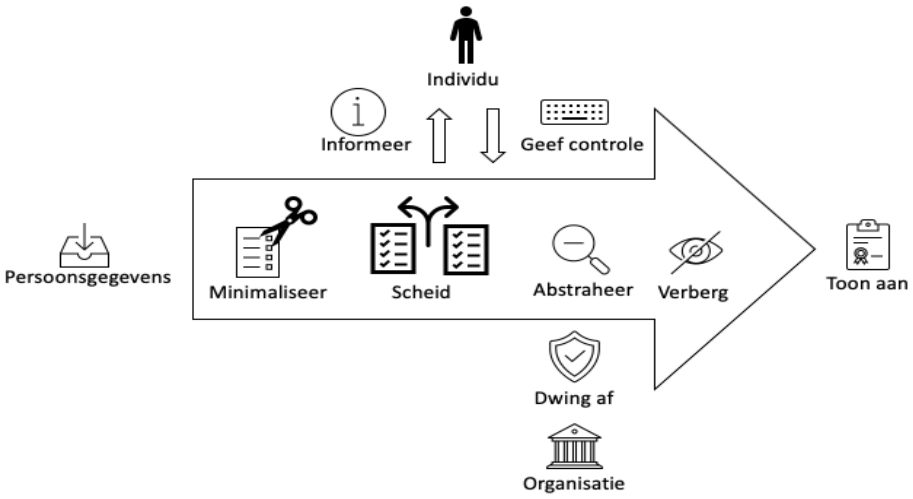
Zoals in paragraaf 4.2.1 is aangegeven bestaat het PCF uit de zeven Privacy by Design principes. Het PCF moeten waarborgen dat de organisaties die het gebruiken compliant zijn. Deze waarborgen zijn in de 11 geselecteerde requirements gevat. In het onderzoek is duidelijk geworden dat daar concrete en praktische invulling aan gegeven dient te worden. Een van de bezwaren op de methode Privacy by

Design was immers dat, zoals in par. 2.1 werd beschreven door Hoela (Hoela & Chen, 2016), de methode te vaag is en de principes te abstract geformuleerd zijn. Het is niet eenvoudig om deze wettelijke vereisten in privacy vriendelijke strategieën te vertalen. Daarom is in het onderzoek gezocht naar een vertaling van de 7 principes naar praktische strategieën. In het onderzoek is daarom aangesloten bij het onderzoek van Colesky et al. (2016) en Perera (Perera et al., 2016) die in hun artikel een extra abstractieniveau tussen privacy principes en strategieën hebben aangebracht die zij 'tactieken' noemen. Zij hebben een verzameling van dergelijke tactieken geïdentificeerd gebaseerd op uitgebreid literatuuronderzoek (van de door Hoepman en Colesky uitgevoerde literatuurstudie is een aparte referentielijst in de bijlage A opgenomen). De door Hoepman en Colesky geselecteerde strategieën zijn:

Nummer	***Strategie***	***Toelichting***
1	Minimaliseren	Beperk zoveel mogelijk de verwerking van persoonsgegevens
2	Scheid	Scheid de verwerking van persoonsgegevens zoveel mogelijk van elkaar
3	Abstraheer	Beperk zoveel mogelijk het detail waarin persoonsgegevens worden verwerkt
4	Verberg	Bescherm persoonsgegevens, of maak ze onherleidbaar of anonimiseer deze. Voorkom dat persoonsgegevens openbaar worden
5	Informeer	Informeer gebruikers over de verwerking van hun persoonsgegevens
6	Geef Controle	Geef gebruikers controle over de verwerking van hun persoonsgegevens
7	Dwing af	Committeer je aan een privacy vriendelijke verwerking van persoonsgegevens en dwing dit (systeem) technisch af
8	Toon aan	Laat zien dat je op een privacy vriendelijke wijze persoonsgegevens verwerkt

Tabel 8, Strategieën en toelichting volgens Hoepman en Colesky.

Deze strategieën worden in het PCF gebruikt om een eerste stap te zetten in het concretiseren van de PbD principes. Hoepman gebruikt 'privacy-ontwerpstrategieën' om vage juridische eisen te concretiseren (Hoepman, 2020). Privacy-ontwerpstrategieën stellen doelen die, als ze worden bereikt, de privacy in het systeem verbeteren, en zijn ook geschikt om een pakket van eisen op te stellen (Hoepman, 2020). De acht strategieën kunnen worden verdeeld in data-georiënteerde strategieën en proces-georiënteerde strategieën. De data-georiënteerde strategieën zijn technisch van aard en gaan over de verwerking van de persoonsgegevens zelf. Hieronder worden deze in figuur 5 binnenin de verwerking getoond. De proces-georiënteerde strategieën bevinden zich buiten de verwerking en gaan met name over organisatorische aspecten en noodzakelijke procedures.



Figuur 5, Het verschil in data-georiënteerde en proces-georiënteerde strategieën. (Naar: Hoepman, 2020).

De privacy ontwerpstrategieën vertalen vaag geformuleerde juridische eisen uit de AVG in concrete ontwerpeisen en laten zien hoe het te ontworpen systeem er uit moet zien. Vervolgens dienen deze strategieën vertaald te worden naar concrete tactieken om op die manier praktische invulling te geven aan de strategie. In totaal zijn er uit de literatuur van Hoepman en Colesky 25 tactieken geselecteerd. Als voorbeeld dient de strategie 'minimaliseren', waarbij volgens Hoepman en Colesky (Colesky et al., 2016) 'selecteren', 'uitsluiten', 'vernietigen' en 'verwijderen', praktische tactieken zijn om aan de strategie 'minimaliseren' te voldoen. In de tabel hieronder zijn per strategie de tactieken opgesomd die ingezet kunnen worden om de strategie praktisch toepasbaar te maken. Niet alle tactieken hoeven altijd ingezet te worden, er kan ook een keuze worden gemaakt die op dat moment het meest passend is. Op deze manier kan de strategie worden gezien als gereedschapskist en de tactiek als gereedschap.

Data Georiënteerd (technisch van aard)			Proces Georiënteerd (organisatorisch van aard)		
				Informeer	Meedelen
	Minimaliseer	Selecteer			Waarschuw
		Sluit uit			Verklaar
		Vernietig		Controleer	Consent
		Verwijder			Keuze
	Scheid	Isoleer			Corrigeer
		Distribueer			Verwijder
	Abstraheer	Groepeer		Dwing af	Stel vast
		Generaliseer			Dwing af
	Verberg	Beperk			Beheer
		Encrypt		Toon aan	Leg vast
		Dissociatie			Audit
		Anonimiseer			Rapporteer

Tabel 9, Strategieën en tactieken naar onderscheid data- en proces georiënteerd.

4.2.3 Requirements validatie

Het framework en de bruikbaarheid daarvan t.b.v. horizontaal toezicht is aan een validatieslag onderworpen. Daarvoor is een eerste concept van het framework aan de deskundigen uit het veld voorgelegd in een semigestructureerd interview. Daarin staan met name onderwerpen centraal die antwoord moeten geven op de vraag of een privacy control framework kan bijdragen aan compliance, op welke wijze het PCF dan moet worden ingezet, en of het PCF bij kan dragen aan horizontaal toezicht. De resultaten van deze interviews geven in eerste instantie een interessante en kijk op compliance en de toepassing van het framework in de praktijk. De respondenten geven aan dat een PCF bij kan dragen aan zowel het reeds in de ontwikkelfase van een informatiesysteem nadenken over privacyaspecten, als aan het compliant gebruik ervan. Daarnaast benoemen de respondenten dat bestaande systemen tegen het PCF aangehouden kunnen worden om te bezien of zij nog aan de vereisten van de AVG voldoen. De respondenten geven tevens aan dat zij van de toezichthouder graag een meer actieve rol zien. Zij begrijpen dat dit te maken heeft met gebrek aan capaciteit bij de AP waardoor taken zoals advisering onvoldoende tot hun recht komen. Volgens de respondenten zou het de toezichthouder helpen als zij een methode zouden hebben waarbij op een meer efficiënte en effectieve manier het toezicht vormgegeven kan worden. In hoofdstuk 6 wordt uitgebreid aandacht besteed aan de interviews.

4.2.4 Ontwerpkeuze

Het idee van een framework komt uit de fiscale context waar een tax control framework wordt gebruikt om toezicht horizontaal in te richten. In deze thesis is getracht de parallel te trekken tussen deze fiscale context en de privacy context bij het verwerken van persoonsgegevens. Fiscaal is horizontaal toezicht ontstaan uit een situatie van te weinig capaciteit bij de belastingdienst om toezicht te houden (De Widt, 2017). Dezelfde capaciteitstekorten zien we thans bij de AP, die zelf aangeeft te weinig capaciteit te hebben om goed toezicht te houden[10] aldus de voorzitter van de Autoriteit Persoonsgegevens. Een meer effectieve en efficiënte toezichtmethode kan daarvoor een oplossing zijn.

Voor het ontwerp van het privacy controle framework zijn een aantal ontwerpkeuze gemaakt. Allereerst moest er een keus gemaakt worden op basis van welke uitgangspunten het framework ontworpen zou gaan worden. In par. 2.1.4 is aangegeven en beargumenteerd dat de principes van Privacy by Design zijn gekozen als uitgangspunt. Vervolgens worden er requirements geformuleerd om het PCF een doel te geven. Daarbij is aangesloten op de rechten van het individu ten aanzien van de verwerking van persoonsgegevens conform de AVG. Op basis van de literatuur van Hoepman (2014) Danezis (Danezis et al., 2015) en Perera (Perera et al., 2016) en de handleiding AVG van de AP (Schermer et al., 2018, p. 73) zijn acht requirements vanuit de AVG en de drie criteria, begrip, wederzijds vertrouwen en transparantie, behorende bij horizontaal toezicht als requirements gedefinieerd. Daarna zijn de genoemde strategieën en tactieken uit de literatuur van bovengenoemde auteurs overgenomen en gebruikt om het PCF concreet en praktisch te maken. Er is voor de literatuur van Hoepman, Danezis en

[10] https://www.trouw.nl/binnenland/voorzitter-autoriteit-persoonsgegevens-de-achterstanden-zijn-zo-groot-dat-het-lachwekkend-is~bb44d7a8.

Perera in dit onderzoek gekozen omdat zij op een praktische wijze de vertaalslag maken van abstracte principes naar concrete en praktische tactieken. En dat is nodig om het framework meer te laten zijn dan een juridisch afvinklijstje, maar een praktisch instrument om compliance te vergroten.
De derde keuze is niet een inhoudelijke ontwerpkeuze, maar een voor de representatie van het ontwerp. Een framework in de vorm van een flowchart is in beginsel overwogen maar bleek niet haalbaar omdat er te veel verschillende strategieën en tactieken zijn. Dat maakt een flowchart bijzonder onoverzichtelijk. Om toch een overzichtelijk framework te maken is gekozen om de representatie in een tabelvorm te maken. Er zijn twee tabellen (zie tabel 10 en 11) ontworpen die tezamen het privacy control framework vormen. Het eerste deel van het PCF (tabel 10 hieronder) laat zien welke Privacy by Design principes (PbD 1 t/m Pbd 7) bijdragen aan het invullen van het desbetreffende requirement (R1, R2 etc.).[11] Met een kruis is in het framework aangegeven welke principe bijdraagt aan welk requirement.

			PbD01	PbD02	PbD03	PbD04	PbD05	PbD06	PbD07
			Proactief niet reactief	Privacy by default	Privacy by design	Behoud volledige functionaliteit	End-to-end security	Zichtbaar en transparant	Gebruiker centraal
Nr.	**Requirements AVG**								
R01	Recht op informatie	*Een betrokkene moet geinformeerd worden dat zijn persoonsgegevens verwerkt worden en met welk doel.*			x			X	X
R02	Recht op inzage	*Betrokkene heeft het recht te weten of een organisatie zijn persoonsgegevens verwerkt en welke.*						X	X
R03	Recht op rectificatie en aanvulling	*Een betrokkene heeft het recht om rectificatie van hem betreffende onjuiste persoonsgegevens te krijgen.*	X	x					X
R04	Recht op gegevenswissing	*Een organisatie moet persoonsgegevens wissen als deze niet langer nodig zijn, betrokkene zijn toestemming intrekt of onrechtmatig zijn verkregen.*	X	x		X	x		X
R05	Recht op beperking van de verwerking	*De persoonsgegevens worden na verwerking 'bevroren' en mogen niet verder worden verwerkt of gewijzigd.*		x	X		X	X	
R06	Recht op overdraagbaarheid / dataportabiliteit	*Een betrokkene heeft het recht zijn persoonsgegevens te verkrijgen om over te dragen.*	X		X		X		X
R07	Recht op bezwaar	*Een betrokkene heeft het recht bezwaar te maken tegen verwerking van zijn persoonsgegevens.*						X	X
R08	Recht m.b.t. geautomatiseerde besluitvorming en profilering	*Organisaties mogen geen besluiten over betrokkenen nemen die uitsluitend op geautomatiseerde verwerking zijn gebaseerd.*			X		X	x	X
	Requirements Horizontaal Toezicht								
R09	Begrip	*Organisaties en toezichthouders begrijpen de context en dynamiek van elkaars positie en respecteren soms conflicterende belangen*				x		X	x
R10	Wederzijds vertrouwen	*Organisaties en toezichthouders ontlenen vertrouwen aan de werking van het interne controlemechanisme*	X		X		X	X	X
R11	Transparantie	*Organisatie geven openheid over de risico's en de daartegenover staande maatregelen, en toezichthouders over te controleren onderdelen*	X	X	X			X	x

Tabel 10, Privacy Control Framework op basis van Privacy by Design principes

[11] In de bijlage is een variant van het framework uit tabel 6 opgenomen waarbij met een kruisje is aangegeven of het principe in meer (X) of mindere (0) mate bij draagt aan het desbetreffende requirement. Deze meer genuanceerde versie van het framework is onvoldoende reproduceerbaar en om die reden als bijlage opgenomen in dit onderzoek.

Hoepman en Perera bieden hiervoor bruikbare kaders. In de tabel 11 in de volgende paragraaf zijn de strategieën weergegeven die bij het desbetreffende Privacy by Design principe kunnen worden toegepast. In dit tweede deel van het PCF is per strategie aangegeven welke tactiek ervoor zorgt dat de strategie praktisch is én operationeel gemaakt kan worden. De werking van het PCF wordt hieronder verder uitgelegd.

4.2.5 Werking van het privacy control framework

Het privacy control framework moet op de volgende wijze worden toegepast. Aan de linkerzijde van het eerste deel (tabel 10) staan de requirements ofwel 'doelstelling', die zijn ontleend aan de AVG en de criteria van horizontaal toezicht. De organisatie kan een of meerdere doelstellingen willen nastreven, en zich afvragen welke principes van Privacy by Design daarin passen. Aan de bovenzijde van het PCF staan daarom de zeven principes van PbD opgenoemd. Per requirement is, aan de hand van de literatuur van o.a. Hoepman, Colesky en Danezis, bepaald welke principes bijdragen aan de invulling van het requirement. Vervolgens kan de organisatie kiezen welke strategie(ën) er beschikbaar is/zijn om aan de principes invulling te geven. Hoepman(2020), (Colesky et al., 2016) en (Danezis et al., 2015) schrijven hierover in hun artikelen dat het belangrijk is strategieën concreet te maken. De strategieën zorgen ervoor dat de op een hoog abstractieniveau geformuleerde principes tastbaar worden, en geven het PCF meer richting. Uit de interviews is gebleken dat het belangrijk is om vanuit de strategieën nog een niveau dieper te gaan en deze strategieën te voorzien van concrete en praktische tactieken. In totaal zijn er 25 tactieken die de strategie vormgeven en verduidelijken. Deze tactieken zijn door de voornoemde auteurs na uitgebreid literatuuronderzoek geformuleerd. Deze staan in de tabel 11 aangegeven,[12] en geven desbetreffende strategie meer handen en voeten. Zo valt af te leiden dat om de strategie 'abstraheren' te concretiseren, de tactieken 'groeperen en generaliseren' ingezet kunnen worden. Een uitwerking van iedere tactische invulling van de strategieën is in de bijlage C bij deze thesis gevoegd.

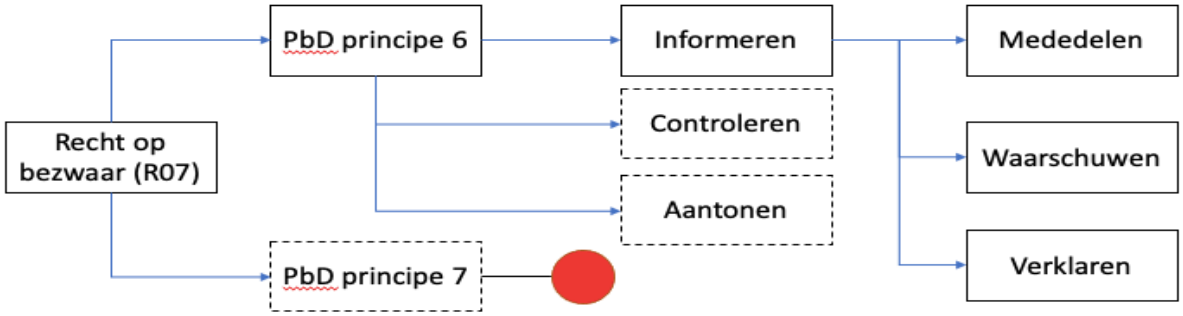
[12] In bijlage B en D is een variant van het framework uit tabel 10 en 11 opgenomen waarbij met een kruisje is aangegeven of het principe in meer (X) of mindere (0) mate bij draagt aan het desbetreffende requirement. Deze meer genuanceerde versie van het framework is onvoldoende reproduceerbaar en om die reden als bijlage opgenomen in dit onderzoek.

				PbD01	PbD02	PbD03	PbD04	PbD05	PbD06	PbD07
	Strategie	Tactiek		Proactief niet reactief	Privacy by default	Privacy by design	Behoud volledige functionaliteit	End-to-end security	Zichtbaar en transparant	Gebruiker centraal
Data Georienteerd (technisch van aard)	Minimaliseer	*Selecteert alleen strikt noodzakelijke persoonsgegevens.*	Selecteer	X	x		X	x		X
		Sluit op voorhand bepaalde persoonsgegevens uit die niet relevant zijn.	Sluit uit							
		Vernietig persoonsgegevens zodra deze niet langer nodig zijn.	Vernietig							
		Verwijder (deel)gegevens die niet langer nodig zijn. Hanteer	Verwijder							
	Scheid	*Verzamel en verwerk persoonsgegevens zoveel mogelijk in logisch gescheiden databases of systemen.*	Isoleer	x	X		X			X
		Verwerk persoonsgegevens zoveel mogelijk in verschillende fysieke locaties.	Distribueer							
	Abstraheer	*Aggregeer informatie over categorieen personen in plaats van per individu (bijv. Leeftijdscategorie).*	Groepeer		x	X		X		
		Voeg gedetailleerde persoonsgegevens zoveel mogelijk samen.	Generaliseer							
	Verberg	*Zorg ervoor dat de toegang tot persoonsgegevens beperkt en veilig is.*	Beperk	X	X	X	x	X		
		Maak persoonsgegevens onbegrijpbaar voor derden.	Encrypt							
		Verbreek de link of correlatie tussen data en persoonsgegevens, verwijder direct identificeerbare gegevens.	Dissociatie							
		Maak persoonsgegevens zoveel mogelijk onherleidbaar.	Anonimiseer							
Proces Georienteerd (organisatorisch van aard)	Informeer	*Laat, op verzoek, zien welke persoonsgegevens worden verwerkt, door wie en waarom.*	Meedelen	x					X	X
		Informeer betrokkenen als hun persoonsgegevens worden gebruikt en wanneer er belangrijke wijzigingen van gegevens plaatsvinden.	Waarschuw							
		Geef informatie over de verwerking van persoonsgegevens in een beknopte en begrijpelijke vorm.	Verklaar							
	Controleer	*Vraag betrokkenen om toestemming wanneer de verwerking dit toelaat en er geen andere grondslag is.*	Consent	X	x				X	X
		Geef het individu een reele keuze over de verwerking van persoonsgegevens.	Keuze							
		Geef betrokkenen de mogelijkheid om hun persoonsgegevens te corrigeren of te verwijderen.	Corrigeer							
		Geef de betrokkenen de mogelijkheid om persoonsgegevens te (laten) verwijderen.	Verwijder							
	Dwing af	*Stel beleid en verantwoordelijkheden rond privacy vast.*	Stel vast	X	X	x		X	x	
		Dwing beleid rond privacy af en zorg ervoor dat verantwoordelijkheden rond privacy waargemaakt worden.	Dwing af							
		Waarborg juistheid en integriteit bij vastlegging en uitwisseling van persoonsgegevens.	Beheer							
	Toon aan	*Documenteer maatregelen en beslissingen rond privacy.*	Leg vast	X					X	X
		Voer regelmatig audits uit op verwerkingen van persoonsgegevens.	Audit							
		Rapporteer over de implementatie van beleid en maatregelen rond privacy.	Rapporteer							

Tabel 11, Privacy by Design principes geconcretiseerd naar strategieën en tactieken.

Een voorbeeld: Requirements 'recht van bezwaar' (R07) is afkomstig uit de AVG. Een betrokkene heeft alleen iets aan deze rechten als de organisatie die als verwerkingsverantwoordelijke geldt die eerbiedigt op een wijze die bijdraagt aan de bescherming van en controle over de persoonsgegevens. Het individu heeft er bijvoorbeeld niets aan als hij de informatie ontvangt in een onbegrijpelijke taal, of als de organisatie voor deze informatie een vergoeding vraagt. In het PCF is met een kruis aangegeven dat principe PbD 6 en PbD 7 dit requirement invullen. In de tabel 11 staan vervolgens de diverse strategieën die de organisatie kan toepassen om deze principes gestalte te geven. Uit deze tabel is op te maken dat om PbD principes 6 en 7 in te vullen, de strategieën informeren, controleren en aantonen gekozen kunnen worden. De organisatie is vrij om een keuze te maken. Een volgende stap is het selecteren van de daarbij behorende tactieken. 'In het geval van de strategie 'informeren' kan daarvoor 'mededelen',

'waarschuwen' of 'verklaren' worden gekozen. Dit kan bijvoorbeeld inhouden dat de verwerkingsverantwoordelijke vertelt (mededeelt) welke persoonsgegevens worden verwerkt, op welke manier dat gebeurt (waarschuwt dat dit bijv. deels geautomatiseerd plaatsvindt) en met welke wettelijke grondslag (verklaring welk van toepassing is). Het informeren van het individu kan door eenvoudig het privacy beleid raadpleegbaar te maken op een website of in een app. Het hierboven beschreven voorbeeld 'Recht op bezwaar (R07) ziet er schematisch als in figuur 6 uit. Hierbij is het 'recht op bezwaar' het vertrekpunt en kiest de organisatie ervoor om dit vanuit privacy by design principe 6 te realiseren. Dit principe kent een drietal implementatie strategieën waar 'informeren' er 1 van is. Om de strategie 'informeren' verder te concretiseren kunnen de tactieken 'mededelen', 'waarschuwen' en 'verklaren' worden gebruikt.



Figuur 6, Voorbeeld requirement 'bezwaar' R07 in een flow weergegeven.

Een andere doelstellig van het PCF is om te bezien of door toepassing van dezelfde PbD-principes, met dezelfde strategieën en tastbare tactieken, aan de requirements van horizontaal toezicht kan worden voldaan. Dat zou er namelijk toe leiden dat zowel aan de AVG-compliance eisen wordt voldaan, maar ook dat het toezicht daarop verbeterd kan worden in termen van efficiëntie en effectiviteit.

Een voorbeeld om dit te illustreren aan de hand van het requirement 'transparantie' (R11). Dit requirement afkomstig uit HT wordt onder meer ingevuld door het PbD principe nr. 6 'zichtbaar en transparant'. Een PbD principe is onvoldoende concreet waardoor er een duidelijke strategie aan gekoppeld moet worden. Onder andere de strategie 'controleer' draagt ertoe bij dat de organisatie transparant is over de verwerking van persoonsgegevens, maar ook over de risico's die de organisatie onderkent. Controle is een fundamenteel principe om de privacy van gebruikers te beschermen (Hoepman, 2020). Het is belangrijk te beseffen dat organisaties in de selectie van strategieën en tactieken een keuzevrijheid hebben binnen het ontworpen privacy control framework. Privacy heeft niet als doel het onmogelijk maken om persoonlijke gegevens te delen en te gebruiken, maar dan wil de gebruiker wel controle en zeggenschap hebben over die persoonsgegevens die verwerkt worden. Gebruikers krijgen controle over de verwerking van hun persoonsgegevens bijvoorbeeld door het vragen van toestemming (consent) voor de verwerking van persoonsgegevens, ze te informeren over welke gegevens worden verwerkt, op welke manier en met welk doel. Het mogelijk te maken deze toestemming in te kunnen trekken, en uiteindelijk de gegevens te laten verwijderen.

4.3 Resultaten uit interviews

Ten aanzien van horizontaal toezicht is er een dubbele validatie gedaan. Op de eerste plaats zijn een zestal respondenten uit de organisatie (digitaal) bevraagd tijdens interviews of (vanwege de voorkeur van de respondent) op schrift, over horizontaal toezicht. Daarnaast heeft er ook een gesprek plaatsgevonden met een deskundige op het gebied van horizontaal toezicht vanuit de wetenschap.

Volgens de respondenten kan het privacy control framework ondersteunen bij aan het vergroten en opbouwen van transparantie vanuit de organisatie richting de toezichthouder. Ook kan het PCF worden ingezet om de risico's die in een bepaalde verwerking of systeem aanwezig zijn aan de toezichthouder te tonen en daarbij aan te geven welke mitigerende maatregelen daartegen worden genomen. Daarnaast versterkt, volgens de respondenten, het PCF het vertrouwen over en weer tussen organisaties en toezichthouders. Het PCF kan dan als een instrument worden gezien waarmee een inhoudelijk gesprek tot stand kan komen. Het vertrouwen groeit als blijkt dat het PCF ertoe leidt dat systemen geen onrechtmatig gebruik toelaat. Daarbij moet niet uit het oog worden verloren dat ook de volwassenheid en professionaliteit van het intern toezicht van de organisatie bijdraagt aan het vertrouwen tussen organisatie en toezichthouder.

Uit literatuur (Van Der Hel & Pheijffer, 2012) blijkt dat een belangrijk element in de fiscale context bij horizontaal toezicht is dat afspraken tussen de organisatie en toezichthouder worden gevat in een convenant. In het convenant worden de afspraken vastgelegd met betrekking tot de invulling van het toezicht op basis van de drie criteria. Aangezien in de context van dit onderzoek er überhaupt nog geen sprake is van normen omtrent deze drie begrippen is het onmogelijk om deze in dit stadium in een convenant vast te leggen dan wel enigszins meetbaar te maken. Er is immers nog helemaal geen sprake van een horizontale toezichtrelatie in de context van dit onderzoek c.q. de verwerking van persoonsgegevens. Ook voor de toezichthouder is een convenant van groot belang, immers als uit de toezicht relatie blijkt dat de organisatie de verwachtingen niet waar kan maken, dan kan de toezichthouder bij wijze van sanctie het convenant buiten werking stellen of een ander escalatietraject inzetten (Russo & Huiskers-stoop, 2020). Het convenant krijgt dan de kenmerken van een certificaat dat ingetrokken kan worden, maar dat is toekomst.

4.3.1 respondenten uit de praktijk

Een van de doelen van het onderzoek is om te kijken of het PCF bij kan dragen aan het efficiënter en effectiever inrichten van toezicht ten aanzien van de compliance bij verwerking van persoonsgegevens. De methode horizontaal toezicht kan hiervoor mogelijk geschikt zijn, maar dan moet aan de drie criteria van HT worden voldaan. De respondenten geven desgevraagd een paar interessante inzichten.

Als het gaat om het criterium 'vertrouwen' zijn de respondenten overwegend positief. Een respondent geeft aan dat: 'Er is tot nu toe zeer beperkt contact is tussen de KMar (organisatie) en de toezichthouder door gebrek aan capaciteit daarvoor aan de kant van de toezichthouder. Beperkt contact versterkt een vertrouwensband natuurlijk niet. Echter, een PCF zou kunnen bijdragen aan het versterken van de

vertrouwensband doordat de KMar zelf aangeeft en bijhoudt in hoeverre wordt voldaan aan wetgeving. Op die manier hoeft de toezichthouder bepaalde details niet zelf uit te zoeken en dat scheelt tijd'. Dat maakt het toezicht efficiënter en kan de capaciteit effectiever worden benut.
'Echter als blijkt dat het PCF niet waarheidsgetrouw blijkt te zijn, bijv. als bepaalde maatregelen niet zijn genomen waar dat wel had gemoeten, dan schaadt dat het vertrouwen'. Een tweede respondent vult aan: 'Een goed geïmplementeerd en toepasbaar framework leidt zonder meer tot verbeterde aantoonbaarheid van de naleving van de AVG/WPG, mits dit proces van het doorlopen en toepassen van het PCF gedocumenteerd is in de interne controles. Duidelijke transparantie en verantwoordingsbereidheid leiden uiteraard tot meer onderling vertrouwen'.

Een toezichtrelatie is tweerichtingsverkeer. Zolang er onzekerheid bestaat en de organisatie en de toezichthouder dus niet zeker weten hoe de wederpartij acteert, bestaat het risico dat het geven van (te) veel vertrouwen negatief uitpakt. Dit leidt ertoe dat veel toezichtrelaties blijven steken in de weliswaar suboptimale, maar stabiele situatie van wederzijds wantrouwen (Raaijmakers, 2016). In deze gedachtegang kan horizontaal toezicht beschouwd worden als de formalisering van een toezichtrelatie die reeds gestoeld is op 'wederzijds vertrouwen'. "Dit betekent dat er eerst sprake moet zijn van een door reputatie gevoed wederzijds vertrouwen, voordat het zinvol is afspraken in het kader van horizontaal toezicht te maken. En niet omgekeerd: we zetten horizontaal toezicht in om te bewerkstelligen dat er meer onderling vertrouwen komt in de toezichtrelatie. Dit is een behoorlijk hoge lat" aldus een respondent.

De respondenten geven aan dat een PCF bij kan dragen aan het vergroten van de 'transparantie' naar de toezichthouder m.b.t. compliance. Met het PCF kan worden aangetoond welke stappen worden genomen in het ontwerpen en ontwikkelen van informatiesystemen, om te voorkomen dat systemen onrechtmatigheden bevatten, of onrechtmatig gebruik toestaan. Eveneens kan het PCF ertoe bijdragen dat risico's worden ontdekt en gemitigeerd. Een respondent vat het als volgt samen: 'De AVG gaat, anders dan de WBP uit van een verantwoordingsplicht, de verwerkingsverantwoordelijke moet waarborgen en aantoonbaar kunnen maken te voldoen aan de wet. (zie artt. 24 en 25 AVG). Een goed geïmplementeerd PCF kan bijdragen aan de transparantie en maakt ook beleidskeuzes en inrichtingskeuzes inzichtelijk'. Een veel intensievere en ook meer controversiële manier om wederzijds transparantie te kweken, is het vergroten van duidelijkheid over norminvulling. In veel toezichtdomeinen is het gebruik van open normen (principle-based regelgeving) gangbaar. Open normen maken het makkelijker wetgeving te laten aansluiten op snel veranderende situaties en moedigen naleving in de geest van de wet (in plaats van de letter van de wet) aan, aldus Raaijmakers (Raaijmakers, 2016)

Het criterium 'begrip' is weerbarstig. Respondenten betwijfelen of het PCF bijdraagt aan het opbouwen of vergroten van begrip tussen organisatie en toezichthouder. Dit komt ook omdat 'begrip' een wat softe term is die lastig te normeren is. 'Begrip zorgt ervoor dat er bij de KMar meer besef komt van de zaken waar de toezichthouder op let. Echter dit is wel beperkt aangezien de KMar natuurlijk een hele andere kerntaak heeft dan beschermen van de privacy'. "Voor de meeste collega's is privacy puur een (lastige)

verplichting, een bijzaak" aldus een respondent. Een andere respondent twijfelt aan de meerwaarde van 'begrip' en zou eerder inzetten op het versterken van het vertrouwen. Weer een andere respondent merkt op dat het bij de toezichthouder ontbreekt aan 'organisatie-sensitiviteit' ten opzichte van de defensieorganisatie (waar de KMar deel van uitmaakt). De toezichthouder heeft geen goed beeld van de context waarbinnen de organisatie acteert. Huiskers-Stoop schreef al dat goede beeldvorming leidt tot beter begrip over en weer.
Begrip wordt ook niet in alle gevallen als relevant beschouwd. Immers, of de organisatie er nu wel of geen begrip voor heeft, als de toezichthouder op basis van wetgeving of beleidsmatige taakstelling is opgedragen om toezicht uit te oefenen dan is dat genoeg reden om toezicht te houden. Daarvoor hoeft het niet te wachten op begrip van een organisatie. Anderzijds hoeft de toezichthouder ook geen begrip op te brengen voor een organisatie die niet compliant is. Ten slotte wijst een respondent erop dat "de toezichthouder wel meer zou kunnen investeren in deskundigheid binnen een bepaalde context en op het vergroten van hun adviesfunctie naar de organisatie". Deze investeringen zouden wel bij kunnen dragen aan 'begrip' binnen een bepaalde context of toezicht dynamiek.

4.3.2 Respondent uit wetenschap

Huiskers geeft in het gesprek op 26 februari 2021 aan dat de horizontale toezichtrelatie in fiscale zin een voortvloeisel is van een heel oude relatie tussen belastingdienst en organisaties. De van oudsher hiërarchische relatie is na de Tweede Wereldoorlog verschoven naar een meer horizontale (zie ook pag. 27), en van een 100% controle naar een toezichtrelatie op basis van samenwerking. Het verschil met de context van dit onderzoek is dat de relatie tussen de organisatie en toezichthouder met betrekking tot de verwerking van persoonsgegevens nog relatief jong is. Volgens Huiskers zijn er twee cruciale factoren als organisatie en toezichthouder een horizontale toezichtrelatie ambiëren. Ten eerste een wederkerige relatie tussen de te controleren organisatie en de toezichthouder. Ten tweede een duidelijk motief vanuit de organisatie om een horizontale toezichtrelatie te willen.

Ten aanzien van het eerste punt concludeerde Siglé reeds in zijn aangehaalde onderzoek 'The effects of cooperative compliance programmes' dat horizontale toezichtrelaties goed kunnen werken voor grote organisaties: 'Zij zijn minder gevoelig voor de machtsmiddelen, zoals boetes en naheffingen, die door toezichthouders kunnen worden gebruikt. Huiskers sluit zicht hierbij aan en voegt eraan toe dat hoe groter de organisatie, hoe grotere de behoefte bestaat aan zekerheid. En juist deze zekerheid kan in een horizontale toezichtrelatie snel geboden worden. Een organisatie weet dan relatief snel dat zij compliant zijn - in deze context - in de verwerking van persoonsgegevens. Huiskers benadrukt dat het voordeel van een horizontale toezichtrelatie is dat aan de voorkant van het proces het toezicht plaatsvindt en niet achteraf, als het spreekwoordelijke kalf al verdronken is. Denk ook in deze aan het debacle met de GGD-registratiesystemen[13], waarbij toezicht aan de voorkant veel ellende had kunnen voorkomen.

[13]https://www.volkskrant.nl/nieuws-achtergrond/datalek-bij-ggd-gegevens-van-miljoenen-nederlanders-in-criminele-handen~b7f17bea/

De tweede factor betreft de (intrinsieke) motivatie die eigenlijk door beide partijen moet worden gevoeld om tot een bestendige horizontale toezichtrelatie te komen. Door gelijkwaardige én wederkerige interacties tussen partijen ontstaat er vertrouwen. Vertrouwen leidt tot transparantie en verbeterde processen. Voor de organisatie is het belangrijk bekend te zijn als betrouwbaar. De toezichthouder kan goed gedrag belonen met het verlagen van de toezichtdruk. “Dergelijke beloningen werken als een olievlek en kunnen andere organisaties een motivatie geven om beter te presteren”. De daarmee verbeterde beheersing levert meer zekerheid op. En dat is voor beide partijen een veel effectievere en efficiëntere werkwijze dan het traditionele toezicht achteraf.

4.3.3 Overige overwegingen

Alle respondenten binnen het ministerie van defensie geven aan dat zij in de praktijk weinig (extern) toezicht ervaren van de Autoriteit Persoonsgegevens. Zij ervaren dat als een gemis. Er is wel sprake van intern toezicht door bijv. de FG of door de Auditdienst Rijk (ADR). Deze is niet onbelangrijk, maar heeft toch een andere lading dan extern toezicht waarbij sancties kunnen worden opgelegd. Sancties die kunnen dienen als stok achter de deur. Extern toezicht komt, tot op heden, onvoldoende tot stand vanwege gebrek aan capaciteit bij de toezichthouder. Door de respondenten wordt ook aangegeven dat zij weinig deskundigheid bij de AP ervaren die weet hoe de defensieorganisatie werkt. Door het ontbreken van een juiste context wordt begrip over en weer bijvoorbeeld lastig.
Een ander erg opvallend gegeven is dat de respondenten vanuit de toezichthouder een erg passieve houding merken. Alleen op meldingen vanuit de organisatie wordt gereageerd, en ook dat niet eens altijd. Alleen op het moment dat de organisatie zelf een melding doet bijv. over een datalek, wil de toezichthouder nog wel contact zoeken met defensie, maar ook niet in alle gevallen. Daar komt bij dat er door de toezichthouder geen invulling wordt gegeven aan de adviesfunctie die zij m.b.t. compliance en/of AVG zouden kunnen innemen. Het invullen van de adviesfunctie draagt volgens Siglé (2019) ook weer bij aan transparantie. Respondenten vinden dit jammer, juist omdat de organisatie en de toezichthouder elkaar zouden kunnen ondersteunen in hun streven naar compliance. Een PCF zou wel kunnen helpen in het bijeenbrengen van de partijen en het faciliteren van een dialoog als het gaat om het op rechtmatige wijze verwerken van persoonsgegevens.

4.4 Discussie en analyse

Dit onderzoek is uitgevoerd om meer inzicht te krijgen hoe een privacy control framework bij kan dragen aan de borging van compliance bij de verwerking van persoonsgegevens én hoe het toezicht hierop verbeterd kan worden. De onderzoeksbevindingen laten zien dat een privacy controle framework ontworpen kan worden op basis van Privacy by Design. Het framework laat zien dat het helpt bij het vergroten van de transparantie vanuit de organisatie richting toezichthouder en dat dit het vertrouwen onderling versterkt. In relatie tot begrip, over en weer, heeft het zijn nut in mindere mate gediend. Aan het gebruik van het framework zijn wel een aantal randvoorwaarden gesteld zoals concretisering van principes in strategieën en tactieken. Daarnaast kan een voorzichtige conclusie getrokken worden

omtrent het gebruik van horizontaal toezicht als verbetering in het toezicht. In het volgende hoofdstuk worden de aanbevelingen en conclusies verder uitgewerkt.

Uit het onderzoek is verder naar voren gekomen dat een framework, opgebouwd uit de zeven principes van Privacy by Design alleen niet volstaat. Daartoe zijn de principes te abstract geformuleerd en biedt degene die ermee moet werken, systeemontwikkelaars, privacyfunctionarissen en toezichthouders te weinig houvast. Het is derhalve belangrijk om de principes te 'vertalen' naar praktisch en tastbare tactieken. In dit onderzoek is op basis van diverse literatuur een concretiseringsslag gemaakt naar eerst strategieën en vervolgens een diepere laag van tactieken. Dat maakt dat het framework praktisch en tastbaar wordt, en voor gebruikers hanteerbaar.

Vervolgens is onderzocht of het PCF bij kan dragen aan horizontaal toezicht. Een toezichtvorm die uitgaat van intensieve samenwerking met als pijlers, begrip, wederzijds vertrouwen en transparantie. Daarbij is van groot belang dat zowel organisatie als toezichthouder investeren in de relatie. Alleen op die manier kan een toezichtrelatie ontstaan gebaseerd op de drie genoemde pijlers. De combinatie tussen een PCF en een constructief inhoudelijk gesprek, kan ertoe leiden dat de twee partijen tot horizontaal toezicht komen. En van horizontaal toezicht is in diverse onderzoeken vastgesteld dat hierdoor effectiever en efficiënter toezicht ontstaat.

Een belangrijk besef bij het aangaan van een horizontale toezichtrelatie is dat de beide partijen dit wel moeten willen. Er is intrinsieke motivatie nodig om de relatie niet alleen op te zetten, maar ook te bestendigen. In een horizontale toezichtrelatie kan het toezicht verbeterd worden o.a. doordat de toezichthouder een meer adviserende rol aanneemt. Daaraan zitten voor beide partijen voordelen als dit leidt tot verhoogde compliance, "niemand is tegen het naleven van wettelijke regels". Echter, een horizontale toezichtrelatie, gebaseerd op elementen begrip, wederzijds vertrouwen en transparantie vraagt wel om een investering in tijd om de essentiële gesprekken te voeren die daarbij horen. Daar zal dus door de beide organisaties in geïnvesteerd moeten worden.

5. Conclusies en Aanbevelingen

In onderstaande paragrafen worden de deelvragen beantwoord aan de hand van de onderzochte literatuur en de data uit de interviews. Dat leidt uiteindelijk tot de beantwoording van de hoofdvraag.

5.1 Beantwoording van de deelvragen

De beantwoording van de vijf deelvragen vormen in samenhang het antwoord op de hoofdvraag. Hieronder volgt eerst in een opsomming de beantwoording van de deelvragen, waarin ook verwezen zal worden naar de uitgebreidere beantwoording in eerdere paragrafen.

De eerste deelvraag betreft de vraag *wat een privacy control framework nu is*? Het antwoord op die vraag wordt gegeven in hoofdstuk 4. Daar komt alles samen en blijkt dat het met name gaat om een framework die ervoor moet zorgen dat er een duidelijk overzicht is van privacyaspecten die in ogenschouw moeten worden genomen bij het ontwikkelen en het gebruik van informatiesystemen. De tweede vraag is die hoe de *methode horizontaal toezicht werkt.* Dit is onder andere relevant omdat het bijzonder actueel is. De toezichthouder kampt met grote capaciteitstekorten waardoor een horizontale toezicht methode, gestoeld op wederzijds vertrouwen, begrip en transparantie, uiterst bruikbaar is. Het antwoord is dat het hierbij gaat om een verondersteld effectievere en efficiëntere toezicht methode door een toezichthouder. Belangrijk daarbij is een toezichtrelatie op basis van gelijkwaardigheid in plaats van sterk hiërarchisch van bovenaf. In hoofdstuk 3 wordt uitgebreid op horizontaal toezicht ingegaan. In deelvraag drie wordt het antwoord gegeven op de vraag *hoe een privacy control framework op basis van principes van Privacy by Design er uit ziet*. Allereerst is het belangrijk dat het een framework is waarin op praktische en concrete wijze invulling gegeven wordt aan de bovenliggende principes. Principes zijn per definitie abstract geformuleerd waardoor het van belang is om deze operationeel te maken. Dat kan door strategieën en tactieken in het framework op te nemen die handen en voeten geven aan deze principes en het framework. In hoofdstuk 4 wordt het ontworpen framework getoond en ook in de bijlage is hierover informatie te vinden. De vierde vraag is of het *PCF bijdraagt aan compliance*, ofwel het voldoen aan wet- en regelgeving. Het antwoord op deze vraag is positief. Een PCF draagt bij aan compliance omdat met het een overzicht geeft van de privacyaspecten waaraan gedacht moet worden bij de ontwikkeling en het gebruik van informatiesystemen. Hier zit een belangrijk stuk bewustwording. Een voorbeeld is dataminimalisatie, een organisatie moet zich afvragen of een gevraagd persoonsgegeven daadwerkelijk benodigd is voor het doel van het informatiesysteem.

Een PCF is een instrument dat organisaties laat nadenken over het gebruik van informatiesystemen en over de vraag of deze systemen wellicht functionaliteiten in zich hebben die onrechtmatige handelingen accepteren. Een voorbeeld is de functie persoonsgegevens te exporteren, terwijl dit voor de werking van het systeem onnodig is of zelfs onrechtmatig. Als een organisatie met het PCF als kader stellend document hiervan meer bewust is, kan het ertoe bijdragen dat dergelijke functionaliteiten worden geblokkeerd.

De laatste deelvraag betreft de vraag of het PCF *helpt om tot horizontaal toezicht te komen*. Het PCF maakt volgens literatuur van o.a. Huiskers-Stoop (2015) en (De Widt, 2017) een onmisbaar onderdeel uit van horizontaal toezicht. Ook de respondenten in de interviews geven aan dat een PCF past bij aan een gelijkwaardiger toezicht. Met name wederzijds vertrouwen en transparantie kunnen daardoor worden vergroot. Daarnaast is belangrijk gebleken om in overleg naar passende oplossingen te zoeken en dat partijen met begrip op elkaars fouten reageren. Dat betekent dat partijen met elkaar in gesprek moeten over de oorzaak van fouten en hoe fouten in de toekomst, door het geven van advies, voorkomen kunnen worden (Commissie Horizontaal Toezicht Belastingdienst, 2012).

5.2 Beantwoording hoofdvraag

Ten slotte kom ik toe aan het beantwoorden van de hoofdvraag van dit onderzoek: **"Hoe kan een privacy control framework, op basis van Privacy by Design principes bijdragen aan implementatie van Horizontaal Toezicht?**

De eerste conclusie is dat het privacy control framework op basis van Privacy by Design principes de organisaties helpen bij compliance ten aanzien van de verwerking van persoonsgegevens. De principes van Privacy by Design geven de kaders aan waarmee wordt voldaan aan de requirements die door de AVG en vanuit horizontaal toezicht worden gesteld. De principes worden daarna concreet gemaakt in een set aan strategieën en tactieken. Dat maakt het PCF operationeel, waardoor het niet alleen uit de abstracte principes bestaat. Deze set moet gebruikt worden bij het ontwikkelen én gebruiken van informatiesystemen en zorgt ervoor dat organisaties grip krijgen op de verwerking van persoonsgegevens conform privacy wet- en regelgeving

Een tweede conclusie uit het onderzoek luidt dat het PCF bijdraagt, zij het soms beperkt, aan de invulling van de drie criteria van horizontaal toezicht; begrip, wederzijds vertrouwen en transparantie. Wederzijds vertrouwen en transparantie worden nadrukkelijk versterkt door het PCF. Het PCF dient als instrument om gesprekken tussen organisaties en toezichthouder te faciliteren. Het criterium 'begrip' blijft weerbarstig. Uit het onderzoek en de literatuur van o.a. Russo en Huiskers (Russo & Huiskers-Stoop, 2020) en Huiskers en Gribnau (Huiskers-Stoop & Gribnau, 2019) komt naar voren dat begrip alleen ontstaat als partijen elkaar (goed) kennen, transparant zijn en elkaar over en weer vertrouwen. Begrip wordt dus opgebouwd als vertrouwen en transparantie versterkt worden. En daarvoor zijn gesprekken nodig. Een cirkel gevormd door elkaar versterkende elementen.

Een derde conclusie is dat horizontaal toezicht ertoe bijdraagt aan efficiënter en effectiever toezicht. Dat komt omdat het toezicht gelijkwaardiger, minder hiërarchisch, ingezet wordt. Organisaties en toezichthouder moeten met elkaar in gesprek waarbij het PCF als instrument dient. Deze gelijkwaardigere vorm van toezicht heeft als positief effect dat het minder tijdrovend is. Gezien de capaciteitsproblemen bij de toezichthouder snijdt het mes dan aan twee kanten. Immers, de toezichthouder heeft meer capaciteit tot haar beschikking voor echt toezicht en handhaving bij

misstanden en het invullen van haar adviesfunctie vanuit haar positie als autoriteit. Daarbij dient wel opgemerkt te worden dat horizontaal toezicht op vrijwillige basis moet worden geïmplementeerd.

5.3 Wetenschappelijke en praktische contributie

Dit onderzoek heeft een tweeledige contributie; wetenschappelijk en praktisch. Zover bekend is er nog geen onderzoek gedaan naar de horizontaal toezicht methode in de context van compliance met AVG dan wel in de context van de verwerking van persoonsgegevens. Dit terwijl deze methode in de fiscale context uitgebreid is onderzocht en in veel gevallen leidt tot effectiever en efficiënter toezicht. De praktische contributie is een privacy control framework waarbij niet alleen AVG-aspecten maar ook aspecten uit horizontaal toezicht zijn samengebracht. Een dergelijk framework is nog onbekend.

5.4 Beperkingen van het onderzoek

Gedurende het onderzoek zijn er zowel praktische als inhoudelijke beperkingen opgetreden die het vervolmaken van het onderzoek in de weg hebben gestaan. In praktische zin heeft de Covid-19 pandemie er in negatieve zin toe bijgedragen dat de validatie interviews soms digitaal gehouden moesten worden waardoor met name non-verbale communicatie minder goed op te vangen is. Deskundigen waren terughoudend om fysiek af te spreken voor een interview.

Inhoudelijk ben ik er tegenaan gelopen dat horizontaal toezicht buiten de fiscale context minder bekend bleek te zijn dan vooraf ingeschat. Horizontaal toezicht is met name in de fiscale context bekend én in die hoedanigheid vanuit meerdere perspectieven onderzocht. Buiten de fiscale context is HT vrij onbekend. En onbekend maakt onbemind, waardoor dit onderzoek misschien aanleiding kan zijn om horizontaal toezicht in meerdere situaties te onderzoeken. Een tweede inhoudelijk beperking is gelegen in het feit dat het onmogelijk is gebleken om bij de toezichthouder binnen te komen. In een uitgebreide mail van de Autoriteit Persoonsgegevens werd aangegeven dat hiervoor helaas geen capaciteit beschikbaar was. Dit maakte de validatie vanuit het perspectief van de toezichthouder onmogelijk. Graag had ik mijn hypothese ook vanuit dat perspectief onderzocht.

5.5 Suggesties voor vervolgonderzoek

Een tweetal suggesties voor vervolgonderzoek zijn passend. Ten eerste is het interessant om te onderzoeken aan welke voorwaarden moet worden voldaan om HT goed in te richten in een nieuwe toezichtrelatie c.q. context. Daaraan is wel randvoorwaardelijk dat horizontaal toezicht door beide partijen wordt gewenst. Een tweede suggestie is om in een casestudy te onderzoeken of horizontaal toezicht daadwerkelijk bijdraagt aan effectiever en efficiënter toezicht, en welke risico's daaraan kleven.

5.6 Aanbevelingen voor de praktijk

Huiskers-Stoop (Huiskers-Stoop, 2015) schreef al in haar dissertatie: "dit betekent dat partijen met elkaar in gesprek moeten over de oorzaak van fouten en hoe fouten in de toekomst voorkomen kunnen worden". Zij doelt hiermee op de interactie tussen een organisatie en een toezichthouder in een horizontale toezichtrelatie. Daar liggen wat mij betreft twee heel belangrijke aanbevelingen, die

aansluiten bij hetgeen uit literatuuronderzoek en interviews naar voren is gekomen. Partijen moeten met elkaar in gesprek over de oorzaak van fouten, en hoe fouten voorkomen kunnen worden. Dat wil dus zeggen dat er actieve houding van beide partijen verwacht wordt. Waarom treden fouten op en welk gevolg hebben deze fouten, voor organisaties en het individu wiens persoonsgegevens worden verwerkt. Maar even belangrijk is het gesprek te voeren over het voorkomen van fouten. Daar past de adviesfunctie die de autoriteit persoonsgegevens moet innemen. De aanbeveling is daarom om de relatie te versterken door het voeren van (periodieke) toezichtgesprekken waarbij de organisatie vragen kan stellen en de autoriteit kan adviseren. Gesprekken die bijdragen aan het bestendigen van vertrouwen, begrip en transparantie over en weer. Het Privacy Control Framework kan daarbij worden ingezet om de gesprekken te faciliteren. Mijns inziens ligt daar voor beide partijen een inspanningsverplichting.

Een tweede aanbeveling is om het framework te combineren met het uitvoeren van de Data Protection Impact Analyses (DPIA's). Het framework zou kunnen helpen om privacy risico's van een gegevensverwerking in kaart te brengen. En om daarna maatregelen te kunnen nemen om de risico's te verkleinen. Ten slotte een advies voor de organisatie; start met een gestructureerde invoering van het privacy control framework en kies daarbij voor normen (AVG), principes (Privacy by Design) die bij de organisatie en het ecosysteem passen waar de organisatie deel van uitmaakt. Kies bewust voor één set aan privacy principes zoals in dit framework Privacy by Design is gebruikt en ontwikkel deze door. Privacy management inrichten is verstandig waarbij dit als life cycle management moet worden opgepakt. Dat betekent dat periodiek, bijvoorbeeld jaarlijks, een systeem tegen het licht gehouden moet worden om te bezien of de compliance nog geborgd is.

Als een organisatie daadwerkelijk wil overgaan op horizontaal toezicht dan zal het gesprek met de toezichthouder gevoerd moeten gaan worden. De functionaris gegevensbescherming zou deze gesprekken in eerste instantie kunnen faciliteren.

6. Bronverwijzingen

Accountant. (2017). *Horizontaal toezicht moet op de schop*. https://www.accountant.nl/nieuws/2017/5/horizontaal-toezicht-moet-op-de-schop/

Acquisti, A., John, L. K., & Loewenstein, G. (2013). What is privacy worth? *Journal of Legal Studies*, *42*(2), 249-274. https://doi.org/10.1086/671754

Acquisto, A., Friedman, A., & Telang, R. (2006). Is there a cost to privacy breaches? An event study. *ICIS 2006 Proceedings*, 94, 1563-1580. https://aisel.aisnet.org/icis2006/94

Bambauer, D. E. (2013). Privacy versus security. *Journal of Criminal Law and Criminology*, *103*(3), 667-684. https://scholarlycommons.law.northwestern.edu/jclc/vol103/iss3/2

Belastingdienst. (2008). *Tax control framework. Van risicogericht naar "in control": Het werk verandert*. Kennisgroep ZGO. http://www.wimlaman.nl/brochures/bel~alg~tax_control_framework.pdf

Belastingdienst. (2013). *Leidraad Toezicht Grote Ondernemingen*. http://duroi.nl/static/download/leidraad_toezicht_grote_ondernemingen_dv4231z1fd.pdf

Bieker, F., Friedewald, M., Hansen, M., Obersteller, H., & Rost, M. (2016). A process for data protection impact assessment under the European general data protection regulation. In S. Schiffner, J. Serna, D. Ikonomou, & K. Rannenberg (Eds.), *Lecture notes in computer science: Vol. 9857. Privacy technologies and policy* (pp. 21-37). Springer. https://doi.org/10.1007/978-3-319-44760-5_2

Boeije, H. (2012). Analyseren in kwalitatief onderzoek; *Denken en doen*. Den Haag: Boom Lemma.

Boeije, H. (2014). Stappenplan kwalitatief onderzoek. *Analyseren in Kwalitatief Onderzoek*.

Bronżewska, K., & Majdańska, A. (2019). The new wave of cooperative compliance programmes and the Impact of new technology. *European Taxation, 59*(2-3), 99-105. https://www.ibfd.org/sites/ibfd.org/files/content/pdf/Austria-Belgium-Poland-The-New-Wave-of-Cooperative-Compliance-Programmes-and-the-Impact-of-New-Technology.pdf

Burgemeestre, B., Hulstijn, J., & Tan, Y. H. (2009). Agent architectures for compliance. In H. Aldewereld, V. Dignum, & G. Picard (Eds.), *Lecture notes in computer science: Vol. 5881. Engineering societies in the agents world X* (pp. 68-83). Springer. https://doi.org/10.1007/978-3-642-10203-5_7

Burgemeestre, B., Hulstijn, J., & Tan, Y. H. (2010). The role of trust in government control of businesses. In H. D. Zimmermann (Ed.), *Proceedings of 23rd Bled eConference: eTrust implications for the individual, enterprises and society* (pp. 301-313). eBled.

Burgemeestre, B., Hulstijn, J., & Tan, Y. H. (2011). Value-based argumentation for justifying compliance. *Artificial Intelligence and Law*, *19*(2-3), 149-186. https://doi.org/10.1007/s10506-011-9113-4

Cavoukian, A. (2009). *Privacy by design: The 7 foundational principles*. Information and

Privacy Commissioner of Ontario, Canada. https://www.iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf

Cavoukian, A., Polonetsky, J., & Wolf, C. (2010). SmartPrivacy for the smart grid: Embedding privacy into the design of electricity conservation. *Identity in the Information Society*, *3*(2), 275-294. https://doi.org/10.1007/s12394-010-0046-y

Charmaz, K. (1996). The search for meanings- grounded theory. In J. A. Smith, R. Harré, & L. Van Langenhove (Eds.), *Rethinking methods in psychology*, (pp. 27-49). Sage.

Cohen, D., & Crabtree, B. (2006). *Qualitative research guidelines project*. Robert Wood Johnson Foundation. http://www.qualres.org/HomeEval-3664.html

Colesky, M., Hoepman, J. H., & Hillen, C. (2016). A critical analysis of privacy design strategies. In L. O'Conner (Ed.), *2016 IEEE Symposium on security and privacy workshops* (pp. 33-40). IEEE. https://doi.org/10.1109/SPW.2016.23

Colon, D. W., & Swagerman, D. M. (2015). Enhanced relationship preparedness in a Dutch multinational context: A tax control framework. *Journal of Accounting and Taxation*, *7*(1), 13-18. https://doi.org/10.5897/jat2014.0129

Commissie Horizontaal Toezicht Belastingdienst. (2012). *Fiscaal toezicht op maat: Soepel waar het kan, streng waar het moet*. https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2012/06/20/rapport-van-de-commissie-stevens-over-horizontaal-toezicht-bij-de-belastingdienst/rapport-van-de-commissie-stevens-over-horizontaal-toezicht-bij-de-belastingdienst.pdf

Dabner, J. H., & Burton, M. (2015). The "enhanced relationship" model collides with reality - the determinants of the relationship between tax administrators and tax intermediaries. In *The Law and Society Association Annual Conference* (pp. 1-17). https://doi.org/10.2139/ssrn.2701036

Danezis, G., Domingo-Ferrer, J., Hansen, M., Hoepman, J. H., Le Metayer, D., Tirtea, R., & Schiffner, S. (2014). *Privacy and data protection by design - from policy to engineering.* European Union Agency for Cybersecurity. https://doi.org/10.2824/38623

Data Protection and Privacy Commissioners. (2010). *Resolution on privacy by design*. https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf

De Widt, D. (2017). *Dutch horizontal monitoring: The handicap of a head Start*. Umeå universitet. https://www.diva-portal.org/smash/get/diva2:1142129/FULLTEXT01.pdf

De Widt, D., & Oats, L. (2019). *Co-operative compliance: Views of large business in the Netherlands and UK*. Umeå universitet. http://umu.diva-portal.org/smash/record.jsf?pid=diva2%3A1285489&dswid=7029

Denkers, A. J. M., Peeters, M. P., & Huisman, W. (2013). *Waarom organisaties de regels naleven*. *Over individuele motieven, de ethische bedrijfscultuur en de mores in de branche.* Boom Lemma.

Di Iorio, C. T., Carinci, F., & Oderkirk, J. (2013). Health research and systems' governance are

at risk: Should the right to data protection override health? *Journal of Medical Ethics*, *40*(7), 488-492. https://doi.org/10.1136/medethics-2013-101603

Dresch, A., Lacerda, D. P., & Cauchick-Miguel, P. A. (2019). Design science in operations management: Conceptual foundations and literature analysis. *Brazilian Journal of Operations & Production Management*, *16*(2), 333-346. https://doi.org/10.14488/bjopm.2019.v16.n2.a13

Duncan, G. (2007). Engineering: Privacy by design. *Science*, *317*(5842), 1178-1179. https://doi.org/10.1126/science.1143464

Edmondson, A. C., & Mcmanus, S. E. (2007). Methodological fit in management field research. *Academy of Management Review*. *32*(4), 1246-1264. https://doi.org/10.5465/AMR.2007.26586086

European Data Protection Supervisor. (2018). *Preliminary opinion on privacy by design*. https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf

Europees Parlement. (2020). *Gegevensbescherming als pijler van zeggenschap van de burger en de EU-aanpak van de digitale transformatie — twee jaar toepassing van de algemene verordening gegevensbescherming*. https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:52020DC0264&from=NL

Everson, E. (2017). Privacy by design: Taking ctrl of big data. *Cleveland State Law Review*, *65*(1), 27-43. https://engagedscholarship.csuohio.edu/clevstlrev/vol65/iss1/6

Fischer, C., Winter, R., & Aier, S. (2010). What is an enterprise architecture design principle? Towards a consolidated definition. In R. Lee (Ed.), *Studies in computational intelligence: Vol. 317. Computer and information science 2010* (pp. 193-205). Springer. https://doi.org/10.1007/978-3-642-15405-8_16

Guarda, P., & Zannone, N. (2009). Towards the development of privacy-aware systems. *Information and Software Technology*, *51*(2), 337-350. https://doi.org/10.1016/j.infsof.2008.04.004
Harvard Law Review, Vol. 4, No. 5. (Dec. 15, 1890), pp. 193-22

Hevner, A. R., March S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly*, *28*(1), 75-105. https://doi.org/10.2307/25148625

Hoel, T., & Chen, W. (2016). The principle of data protection by design and default as a lever for bringing pedagogy into the discourse on learning analytics. In W. Chen, J. C. Yang, S. Murthy, S. L. Wong, & S. Iyer (Eds.), *ICCE 2016 - 24th international conference on computers in education: Think global act local - workshop proceedings* (pp. 113-121). http://topicmaps.estandard.no/files/Hoel_Chen_LAEDM_ICCE16_final.pdf

Hoepman, J. H. (2014). *Privacy design strategies*. In N. Cuppens-Boulahia, F. Cuppens, S. Jajodia, A. Abou El Kalam, & Sans T. (Eds.), *IFIP advances in information and communication technology: Vol. 428. ICT systems security and privacy protection* (pp. 446-459). Springer. https://doi.org/10.1007/978-3-642-55415-5_38

Hoepman, J. H. (2020). *Privacyontwerpstrategieën (het blauwe boekje)*. Radboud University. https://repository.ubn.ru.nl/bitstream/handle/2066/195398/195398.pdf

Huiskers-Stoop, E. (2015). *De effectiviteit van horizontaal belastingtoezicht*. Erasmus University Rotterdam. https://repub.eur.nl/pub/79080/Huiskers_proefschrift_digitaal.pdf

Huiskers-Stoop, E., & Gribnau, J. (2019). Cooperative compliance and the Dutch horizontal monitoring model. *Journal of Tax Administration*, *5*(1), 66-110. http://jota.website/index.php/JoTA/article/view/219/158

Huisman, W. & A. Beukelman, Invloeden op regelnaleving door bedrijven. Inzichten in wetenschappelijke onderzoek, Den Haag: Boom Juridische uitgevers 2007, p. 14. Zie tevens Belasting- dienst.

Julisch, K., Suter, C., Woitalla, T., & Zimmermann, O. (2011). Compliance by design - bridging the chasm between auditors and IT architects. *Computers & Security*, *30*(6-7), 410-426. https://doi.org/10.1016/j.cose.2011.03.005

Kaptein, S. P., & Wempe, J. (2003). *De open onderneming: Een bedrijfsethisch vraagstuk*. Erasmus University Rotterdam. https://repub.eur.nl/pub/305

Khan, S. (2014). Qualitative research method: Grounded theory. *International Journal of Business and Management*, *9*(11), 224-233. https://doi.org/10.5539/ijbm.v9n11p224

Kool, L., van Schoonhoven, B., van Lieshout, M., Vedder, A. H., & Fleurke, F. M. (2011). Trusted technology: Een onderzoek naar de toepassings-voorwaarden voor Privacy by Design in de elektronische dienstverlening van de overheid. Rijksoverheid.

Koops, B. J., Hoepman, J. H., & Leenes, R. (2013). Open-source intelligence and privacy by design. *Computer Law & Security Review, 29*(6), 676-688. https://doi.org/10.1016/j.clsr.2013.09.005

Lever, A. (2006). Privacy rights and democracy: A contradiction in terms? *Contemporary Political Theory*, *5*(2), 142-162. https://doi.org/10.1057/palgrave.cpt.9300187

Liberati, A., Altman, D. G., Tetzlaff, J., Mulrow, C., Gøtzsche, P. C., Ioannidis, J. P., Clarke, M., Devereaux, P., Kleijnen, J., & Moher, D. (2009). The PRISMA statement for reporting systematic reviews and meta-analyses of studies that evaluate health care interventions: Explanation and elaboration. *Journal of Clinical Epidemiology, 62*(10), e1-e34. https://doi.org/10.1016/j.jclinepi.2009.06.006

Lohmann, N. (2013). Compliance by design for artifact-centric business processes. *Information Systems*, *38*(4), 606-618. https://doi.org/10.1016/j.is.2012.07.003

Mendoza, J. P., & Wielhouwer, J. L. (2015). Only the carrot, not the stick: Incorporating trust into the enforcement of regulation. *PLoS ONE*, *10*(2), Artikel e0117212. https://doi.org/10.1371/journal.pone.0117212

Mortelmans, D. (2009). *Handboek kwalitatieve onderzoeksmethoden.* Acco. http://library.wur.nl/WebQuery/clc/1975641

NOREA. (2019). *NOREA Handreiking Privacy Control Framework: Beheersingsdoelstellingen en beheersingsmaatregelen voor privacy audits en privacy-assuranceopdrachten*. https://www.norea.nl/download/?id=6041

Oost, H., en Markenhof. (2016). Een onderzoek voorbereiden. Amersfoort: ThiemeMeulenhoff.

Perera, C., McCormick, C., Bandara, A. K., Price, B. A., & Nuseibeh, B. (2016). Privacy-by-design framework for assessing internet of things applications and platforms. *Proceedings of the 6th International Conference on the Internet of Things* (pp. 83-92). ACM. https://doi.org/10.1145/2991561.2991566

Raaijmakers, K. (2016). Inherente onvoorspelbaarheid in toezichtrelaties: Kan horizontaal toezicht daaraan iets veranderen? In N. Boonstra (Ed.), *Jaarboek compliance 2016* (pp. 65-79). Nederlands Compliance Instituut.

Ridderbeekx, E., & Scheuller, S. (2017). *Privacy: Meer dan compliance en informatiebeveiliging.* Deitauditor. https://www.deitauditor.nl/informatiebeveiliging/privacy/

Russo, R., & Huiskers-Stoop, E. (2020). De doorontwikkeling van horizontaal. *MBB: Telastingbeschouwingen: Onafhankelijk Maandblad voor Belastingrecht en Belastingpraktijkt*. *2020*(9-30), 368-382.

Samuel D. Warren; Louis D. Brandeis

Saunders, M., Lewis, P., & Thornhill, A. (2009). *Research methods for business students* (5th ed.). Pearson.

Schaar, P. (2013). Privacy by design. *Identity in the Information Society, 3*(2), 267-274. https://doi.org/10.1007/s12394-010-0055-x

Schermer, B. W., Hagenauw, D., & Falot, N. (2018). *Handleiding algemene verordening gegevensbescherming en uitvoeringswet algemene verordening gegevensbescherming.* Ministerie van Justitie en Veiligheid. https://www.rijksoverheid.nl/documenten/rapporten/2018/01/22/handleiding-algemene-verordening-gegevensbescherming

Siglé, M. A., Dijk, E. C. J. M. H., & Nyenrode Business Universiteit (Breukelen). (2019). The Effects of Cooperative Compliance Programmes. Nyenrode.

Six, F. E. (2004). *Trust and trouble; Building interpersonal trust within organizations*. Erasmus University Rotterdam. http://repub.eur.nl/handle/1271

Tsai, J. Y., Egelman, S., Cranor, L., & Acquisti, A. (2011). The effect of online privacy information on purchasing behavior: An experimental study. *Information Systems Research*, *22*(2), 254-268. https://doi.org/10.1287/isre.1090.0260

Van der Hel, L., & Pheijffer, M. (2012). Evaluatie horizontaal toezicht: Fiscaal toezicht op maat. *Maandblad Voor Accountancy En Bedrijfseconomie*, *86*(7-8), 463-470. https://doi.org/10.5117/mab.86.20900

Van der Hel, L., & Siglé, M. (2019). Herijking horizontaal toezicht: Noodzakelijk kwaad of logisch gevolg? *Tijdschrift Voor Toezicht*, *10*(1), 13-25. https://doi.org/10.5553/tvt/187987052019010001004

Van Lieshout, M., Kool, L., Bodea, G., Schlechter, J., & Van Schoonhoven, B. (2012). *Stimulerende en remmende factoren van privacy by design in nederland* (Report No. TNO 2012 R10006). TNO. https://www.noraonline.nl/images/noraonline/5/5c/Stimulerende_en_remmende_factoren_van_Privacy_by_Design_in_Nederland.pdf

Van Rossum, H., Gardeniers, H., Borking, J. J., Cavoukian, A., Brans, J., Muttupulle, N., & Magistrale, N. (1995). *Privacy-enhancing technologies: The path to anonymity*. Registratiekamer.

Verhoeven, W. J., & Bik, J. (2014). Visualiseren van sociale netwerken op basis van kwalitatieve bronnen. *Kwalon*, *19*(3), 38-45. https://doi.org/10.5553/kwalon/138515352014019003005

Vermaas, P. E., Tan, Y. H., Van den Hoven, J., Burgemeestre, B., & Hulstijn, J. (2010). Designing for trust: A case of value-sensitive design. *Knowledge, Technology & Policy*, *23*(3-4), 491-505. https://doi.org/10.1007/s12130-010-9130-8

Vicente, P., & Mira Da Silva, M. (2011). A conceptual model for integrated governance, risk and compliance. In H. Mouratidis & C. Rolland (Eds.), *Lecture notes in computer science: Vol. 6741*. *Advanced Information Systems Engineering* (pp. 199-213). Springer. https://doi.org/10.1007/978-3-642-21640-4_16

Wieringa, R. J. (2014). *Design science methodology for information systems and software engineering*. Springer. https://doi.org/10.1007/978-3-662-43839-8

Wolters, P.T.J. (2015). *De rechten van de betrokkenen onder de AVG*. 3-6.

7. Bijlagen

A. Referenties in het onderzoek naar strategieën en tactieken door Hoepman en Colesky

Nr.	APA referentie literatuuronderzoek naar strategieen en tactieken door Hoepman
1	*T. Shümmer, "The Public Privacy – Patterns for Filtering Personal Information in Collaborative Systems," in Proceedings of CHI workshop on Human-Computer-Human-Interaction Patterns, 2004.*
2	*H. Baraki et al., Towards Interdisciplinary Design Patterns for Ubiquitous Computing Applications. Kassel, Germany: Kassel University Press GmbH, 2014.*
3	*C. Bier and E. Krempel, "Common Privacy Patterns in Video Surveillance and Smart Energy," in ICCCT-2012, 2012, pp. 610–615.*
4	*J.-H. Hoepman, "Privacy Design Strategies," IFIP SEC 2014, pp. 446–459, 2014.*
5	*M. Hafiz, "A Pattern Language for Developing Privacy Enhancing Technologies," Software - Practice and Experience, vol. 43, pp. 769–787,2013*
6	*C. Graf, P. Wolkerstorfer, A. Geven, and M. Tscheligi, "A Pattern Collection for Privacy Enhancing Technology," The Second International Conferences of Pervasive Patterns and Applications (Patterns 2010), vol.2, no. 1, pp. 72–77, 2010.*
7	*J. Porekar, A. Jerman-Blažič, and T. Klobučar, "Towards organizational privacy patterns," Proceedings - The 2nd International Conference on the Digital Society, ICDS 2008, 2008.*
8	*S. Ahern et al., "Over-Exposed ? Privacy Patterns and Considerations in Online and Mobile Photo Sharing," CHI '07, pp. 357–366, 2007.*
9	*F. Kelbert and A. Pretschner, "Towards a policy enforcement infrastructure for distributed usage control," Proceedings of the 17th ACM SACMAT (Symposium on Access Control Models And Technologies), p. 119, 2012.*
10	*L. Compagna, P. El Khoury, F. Massacci, R. Thomas, and N. Zannone, "How to capture, model, and verify the knowledge of legal, security, and privacy experts : a pattern-based approach," ICAIL '07, pp. 149–153, 2007.*
11	*E. S. Chung et al., "Development and Evaluation of Emerging Design Patterns for Ubiquitous Computing," DIS '04 Proceedings of the 5th conference on Designing interactive systems: processes, practices, methods, and techniques, pp. 233–242, 2004.*

B. Genuanceerd Privacy Control Framework

			PbD01	PbD02	PbD03	PbD04	PbD05	PbD06	PbD07
	X draagt in sterke mate bij / 0 draagt in mindere mate bij		Proactief niet reactief	Privacy by default	Privacy by design	Behoud volledige functionaliteit	End-to-end security	Zichtbaar en transparant	Gebruiker centraal
Nr.	**Requirements AVG**								
R01	Recht op informatie	*Een betrokkene moet geinformeerd worden dat zijn persoonsgegevens verwerkt worden en met welk doel.*			0			X	X
R02	Recht op inzage	*Betrokkene heeft het recht te weten of een organisatie zijn persoonsgegevens verwerkt en welke.*						X	X
R03	Recht op rectificatie en aanvulling	*Een betrokkene heeft het recht om rectificatie van hem betreffende onjuiste persoonsgegevens te krijgen.*	X	0					X
R04	Recht op gegevenswissing	*Een organisatie moet persoonsgegevens wissen als deze niet langer nodig zijn, betrokkene zijn toestemming intrekt of onrechtmatig zijn verkregen.*	X	0		X	0		X
R05	Recht op beperking van de verwerking	*De persoonsgegevens worden na verwerking 'bevroren' en mogen niet verder worden verwerkt of gewijzigd.*		0	X		X	X	
R06	Recht op overdraagbaarheid / dataportabiliteit	*Een betrokkene heeft het recht zijn persoonsgegevens te verkrijgen om over te dragen.*	0		X		X		X
R07	Recht op bezwaar	*Een betrokkene heeft het recht bezwaar te maken tegen verwerking van zijn persoonsgegevens.*						X	X
R08	Recht m.b.t. geautomatiseerde besluitvorming en profilering	*Organisaties mogen geen besluiten over betrokkenen nemen die uitsluitend op geautomatiseerde verwerking zijn gebaseerd.*			X		X	0	X
	Requirements Horizontaal Toezicht								
R09	Begrip	*Organisaties en toezichthouders begrijpen de context en dynamiek van elkaars positie en respecteren soms conflicterende belangen*				0		X	0
R10	Wederzijds vertrouwen	*Organisaties en toezichthouders ontlenen vertrouwen aan de werking van het interne controlemechanisme*	X		X		X	X	X
R11	Transparantie	*Organisatie geven openheid over de risico's en de daartegenover staande maatregelen, en toezichthouders over te controleren onderdelen*	X	X	0			X	0

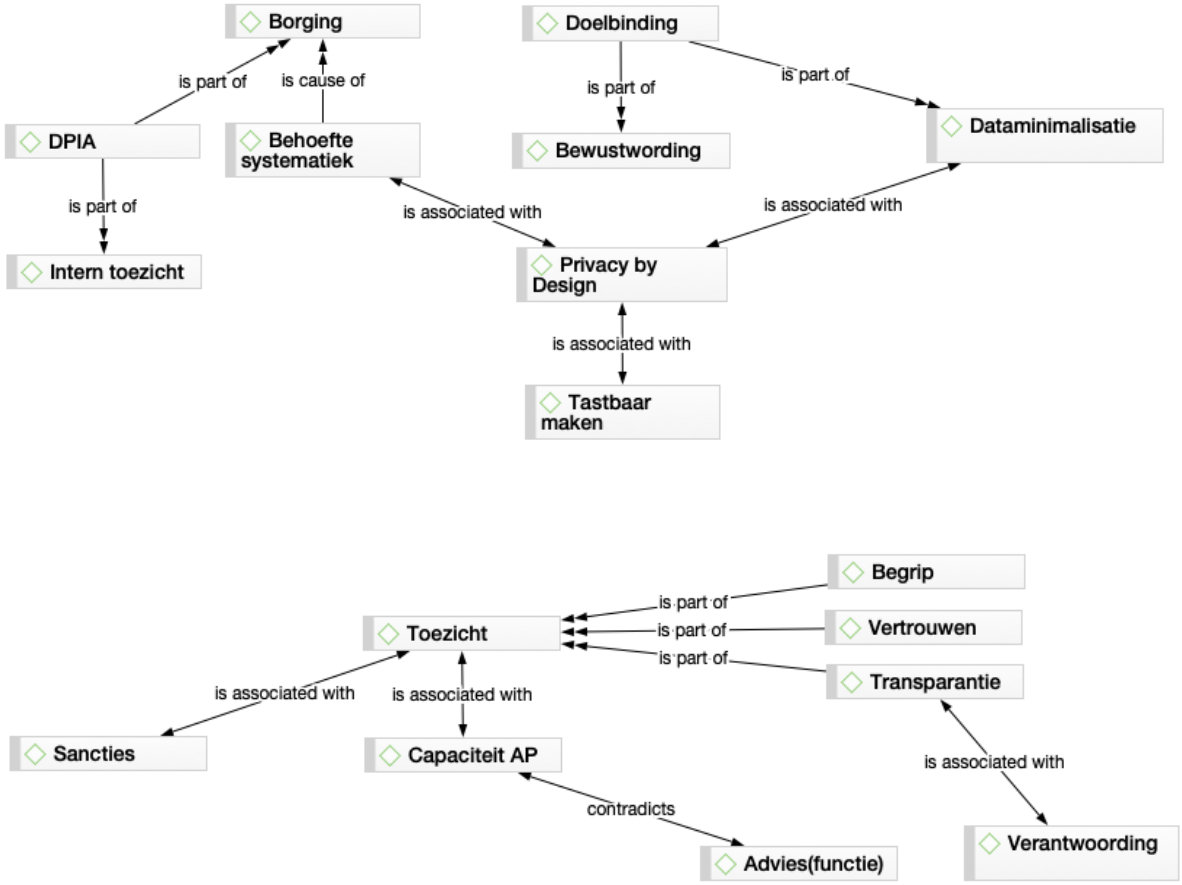
C. Tactieken en inhoudelijke toelichting

Tactiek	**Korte inhoudelijke toelichting**
Dissociatie	*Verbreek de link of correlatie tussen data en persoonsgegevens, verwijder direct identificeerbare gegevens.*
Anonimiseer	*Maak persoonsgegevens zoveel mogelijk onherleidbaar.*
Meedelen	*Laat, op verzoek, zien welke persoonsgegevens worden verwerkt, door wie en waarom.*
Waarschuw	*Informeer betrokkenen als hun persoonsgegevens worden gebruikt en wanneer er belangrijke wijzigingen van gegevens plaatsvinden.*
Verklaar	*Geef informatie over de verwerking van persoonsgegevens in een beknopte en begrijpelijke vorm.*
Consent	*Vraag betrokkenen om toestemming wanneer de verwerking dit toelaat en er geen andere grondslag is.*
Keuze	*Geef het individu een reele keuze over de verwerking van persoonsgegevens.*
Corrigeer	*Geef betrokkenen de mogelijkheid om hun persoonsgegevens te corrigeren of te verwijderen.*
Verwijder	*Geef de betrokkenen de mogelijkheid om persoonsgegevens te (laten) verwijderen.*
Stel vast	*Stel beleid en verantwoordelijkheden rond privacy vast.*
Dwing af	*Dwing beleid rond privacy af en zorg ervoor dat verantwoordelijkheden rond privacy waargemaakt worden.*
Beheer	*Waarborg juistheid en integriteit bij vastlegging en uitwisseling van persoonsgegevens.*
Leg vast	*Documenteer maatregelen en beslissingen rond privacy.*
Audit	*Voer regelmatig audits uit op verwerkingen van persoonsgegevens.*
Rapporteer	*Rapporteer over de implementatie van beleid en maatregelen rond privacy.*

D. Genuanceerd framework strategieën en technieken

	X draagt in sterke mate bij / 0 draagt in mindere mate bij			PbD01	PbD02	PbD03	PbD04	PbD05	PbD06	PbD07
	Strategie	**Tactiek**		Proactief niet reactief	Privacy by default	Privacy by design	Behoud volledige functionaliteit	End-to-end security	Zichtbaar en transparant	Gebruiker centraal
Data Georienteerd (technisch van aard)	**Minimaliseer**	*Selecteert alleen strikt noodzakelijke persoonsgegevens.*	Selecteer	X	0		X	0		X
		Sluit op voorhand bepaalde persoonsgegevens uit die niet relevant zijn.	Sluit uit							
		Vernietig persoonsgegevens zodra deze niet langer nodig zijn.	Vernietig							
		Verwijder (deel)gegevens die niet langer nodig zijn. Hanteer	Verwijder							
	Scheid	*Verzamel en verwerk persoonsgegevens zoveel mogelijk in logisch gescheiden databases of systemen.*	Isoleer	0	X		X			X
		Verwerk persoonsgegevens zoveel mogelijk in verschillende fysieke locaties.	Distribueer							
	Abstraheer	*Aggregeer informatie over categorieen personen in plaats van per individu (bijv. Leeftijdscategorie).*	Groepeer		0	X		X		
		Voeg gedetailleerde persoonsgegevens zoveel mogelijk samen.	Generaliseer							
	Verberg	*Zorg ervoor dat de toegang tot persoonsgegevens beperkt en veilig is.*	Beperk	X	X	X	0	X		
		Maak persoonsgegevens onbegrijpbaar voor derden.	Encrypt							
		Verbreek de link of correlatie tussen data en persoonsgegevens, verwijder direct identificeerbare gegevens.	Dissociatie							
		Maak persoonsgegevens zoveel mogelijk onherleidbaar.	Anonimiseer							
Proces Georienteerd (organisatorisch van aard)	**Informeer**	*Laat, op verzoek, zien welke persoonsgegevens worden verwerkt, door wie en waarom.*	Meedelen	0					X	X
		Informeer betrokkenen als hun persoonsgegevens worden gebruikt en wanneer er belangrijke wijzigingen van gegevens plaatsvinden.	Waarschuw							
		Geef informatie over de verwerking van persoonsgegevens in een beknopte en begrijpelijke vorm.	Verklaar							
	Controleer	*Vraag betrokkenen om toestemming wanneer de verwerking dit toelaat en er geen andere grondslag is.*	Consent	X	0				X	X
		Geef het individu een reele keuze over de verwerking van persoonsgegevens.	Keuze							
		Geef betrokkenen de mogelijkheid om hun persoonsgegevens te corrigeren of te verwijderen.	Corrigeer							
		Geef de betrokkenen de mogelijkheid om persoonsgegevens te (laten) verwijderen.	Verwijder							
	Dwing af	*Stel beleid en verantwoordelijkheden rond privacy vast.*	Stel vast	X	X	0		X	0	
		Dwing beleid rond privacy af en zorg ervoor dat verantwoordelijkheden rond privacy waargemaakt worden.	Dwing af							
		Waarborg juistheid en integriteit bij vastlegging en uitwisseling van persoonsgegevens.	Beheer							
	Toon aan	*Documenteer maatregelen en beslissingen rond privacy.*	Leg vast	0					X	X
		Voer regelmatig audits uit op verwerkingen van persoonsgegevens.	Audit							
		Rapporteer over de implementatie van beleid en maatregelen rond privacy.	Rapporteer							

E. Interview codelabels ATLAS_Ti in onderling verband



F. Interviewguide, Topiclist en checklist

Interviewguide/checklist

Introductie	
Introductie	• Voorstellen: Dennis Teuben, masterstudent aan de University of applied science Utrecht. • Danken voor bereidwilligheid. • Toepassingsmogelijkheden van horizontaal toezicht bij informatiesystemen. • U hebt van mij een e-mail ontvangen met daarin informatie over het onderzoek. • Heeft u op voorhand vragen over dit onderzoek?
Doel van het onderzoek	• Met dit interview neemt u deel aan het onderzoek naar de toepasbaarheid van horizontaal toezicht op basis van Privacy by Design principes. Informatiesystemen verwerken veel privacygevoelige data zoals persoonsgegevens, maar het toezicht hierop laat te wensen over. • Uit literatuurstudie en berichten in de dagelijkse media blijkt dat het voor organisaties lastig is om compliant en aan de autoriteit persoonsgegevens aan te tonen dat hun informatiesystemen worden ontwikkeld en gebruikt overeenkomstig wet- en regelgeving. Denk daarbij met name aan de AVG. • Hiervoor moeten complexe en tijdrovende procedures worden doorlopen die resulteren in standaard documenten. Ik onderzoek of door gebruik te maken van een privacy control framework op basis van de Privacy by design principes, dit eenvoudiger kan worden gemaakt. • Met dit onderzoek wil ik achterhalen of door het gebruik van horizontaal toezicht de controledruk kan worden verminderd. Horizontaal toezicht wordt al toegepast in m.n. de fiscale context, en leidt daar tot efficiencyverbetering.
Onderwerpen	Graag willen ik de volgende onderwerpen bespreken: • Horizontaal toezicht

	• Privacy by design • Control framework op basis van architectuur • Bruikbaarheid van control framework i.r.t. horizontaal toezicht
Vertrouwelijkheid	• In dit interview worden geen persoonlijke gegevens gebruikt Informatie welke u mij verteld zal enkel gebruikt worden voor dit onderzoek. Tijdens dit interview kunt u besluiten te stoppen en de verzamelde data te vernietigen.
Geluidsopname en	• Dit gesprek zal worden opgenomen. Hiervoor vragen wij uw toestemming tijdens de opnamen. • Na de data-collectie zal de opname worden vernietigd.

Topiclijst

Onderwerpen, vragen en subvragen	
1. Privacy en Privacy by design	• Kunt u wat vertellen over het privacy beleid binnen uw organisatie? • Bent u bekend met het privacy beleid binnen uw organisatie? • Slaagt uw organisatie erin om te voldoen aan wettelijke vereisten ten aanzien van privacy? • Wat moet uw organisatie daarvoor doen? • Bent u bekend met het concept 'privacy by design'? • Bent u bekend met de 7 principes van PbD?

2. P.1 Proactief / Preventief	Het eerste principe van PbD zegt dat vanaf de initiatie van het ontwerp van een IS er moet worden nagedacht over privacy, en niet achteraf.
	• Krijgt privacy voldoende aandacht bij de ontwikkeling of bij aanpassingen van informatiesystemen in uw organisatie.
	  • Zo ja waarom wel
	  • Zo nee waarom niet
	• Krijgt privacy op het juiste moment voldoende aandacht?
	• Welk risico loopt de organisatie als er niet tijdig aan privacyaspecten wordt gedacht?

3. P.2 Privacy als standaard instelling (default)	Privacycriteria gelden als standaard bij de verwerking van gegevens, waarbij de regel geldt: comply of explain.
	• Wordt privacy in de informatiesystemen binnen uw organisatie afdoende *automatisch* beschermt?
	  • Zo ja waarom wel
	  • Zo nee waarom niet
	• Wat houdt naar uw mening 'default' in als het gaat om privacy waarborgen in informatiesystemen?
	• Welke belang is leidend als het gaat om privacyaspecten in de informatiesystemen van uw organisatie?

4. P.3 Privacy geïntegreerd in het ontwerp (by design)	Privacy maatregelen zijn integraal onderdeel van de informatieverwerking. • Wat verstaat u onder privacy by design? • Welke voordelen kunt u noemen t.a.v. privacy by design? • Welke nadelen kunt u noemen t.a.v. privacy by design? • Wat kan er worden gedaan als privacy maatregelen niet of te laat worden onderkent in het ontwikkelproces?
5. P.4 Volledige functionaliteit	Het waarborgen van privacy is een verantwoordelijkheid van alle betrokken partijen. • Hoe verhouden privacy en veiligheid zich tot elkaar? • Hoe verhouden privacy en dienstverlening zich tot elkaar? • Welk belang is er gediend met het borgen van privacy? • Wie is uiteindelijk verantwoordelijk voor het borgen van privacy?
6. P.5 End-to-end beveiliging	Privacy by design geldt gedurende de hele levenscyclus per persoonsgegevens en is geen eenmalige actie. • Welke veiligheidsmaatregelen zijn essentieel voor het behouden van privacy? • Zijn deze maatregelen krachtig genoeg? • Op welk moment tijdens de verzameling van persoonsgegevens moeten deze maatregelen werken? • Is er bij de ontwikkeling van de informatiesystemen in uw organisatie voldoende nagedacht over veranderende omstandigheden (zoals wetgeving). • Wordt er vanuit architectuur nagedacht over deze maatregelen? • Hoe is de governance t.a.v. privacy geregeld?

7. P.6 Zichtbaarheid en transparantie	Inzicht en transparantie over persoonsgegevens moet mogelijk zijn voor alle betrokkenen. • Wie hebben er inzicht in de verwerking van persoonsgegevens in de informatiesystemen in uw organisatie? • Welke onafhankelijke derde houdt toezicht op de verwerking van persoonsgegevens? • Wat vindt u van deze controles? • Hoe toont uw organisatie aan dat zij persoonsgegevens verwerken conform de wettelijke vereisten van bijv. de AVG?
8. P7. Gebruiker staat centraal	De persoonlijke levenssfeer van de betrokkene moet worden beschermd. • Worden de belangen van het individu volgens u voldoende beschermd? • Zijn architecten voldoende betrokken bij de bescherming van de belangen van derden? • Zij de exploitanten zich voldoende bewust van de belangen van derden? • Welke technische maatregelen worden getroffen om de belangen van derden te beschermen? • Welke organisatorische maatregelen worden getroffen om de belangen van derden te beschermen?

Afsluiting	
Afsluiting	• Dit zijn alle vragen. Zijn er nog zaken welke niet aan bod zijn gekomen maar die u wel belangrijk vindt om te vermelden? • Wat is uw indruk van dit interview?
Bedanken	• Ik wil u hartelijk danken voor uw deelname aan dit onderzoek. Wanneer u naderhand nog vragen heeft over dit interview dan kunt u contact met mij opnemen middels dgc.teuben@gmail.com of telefonisch via 06-51912589