MASTER'S THESIS

Implementeren ISO-gecertificeerde organisaties de GDPR grondiger?

Ebeltjes, E.G. (Rene)

Award date:
2020

Implementeren ISO-gecertificeerde organisaties de GDPR grondiger?

Do ISO certified organisations implement the GDPR more substantive ?

Opleiding:	Open Universiteit, faculteit Management, Science & Technology Masteropleiding Business Process Management & IT
Programma:	Open University of the Netherlands, faculty of Management, Science & Technology Master Business Process Management & IT
Cursus:	IM0602 Voorbereiden Afstuderen BPMIT IM9806 Afstudeertraject Business Process Management and IT
Student:	E.G. Ebeltjes
Identiteitsnummer:	
Datum:	23 Augustus 2020
Afstudeerbegeleider	dr. L. Bollen
Meelezer	dr. R. Bosua
Versie nummer:	1.1
Status:	Final

Abstract

Dit onderzoeksrapport focust zich op de relatie van ISO en niet-ISO-gecertificeerde organisaties op de implementatiekwaliteit van de Europese privacy wet; de GDPR. En onderzoekt hiermee de vraag die centraal staat in mijn onderzoek dat voornamelijk ISO 9001, ISO 14001 en/of ISO 27001 gecertificeerde organisaties een grondiger GDPR implementatie hebben uitgevoerd dan niet-ISO-gecertificeerde organisaties. Op basis van literatuuronderzoek over Total Quality Management- en ISO implementaties is gebleken dat de determinanten voor een grondige implementatie en voor een symbolische implementatie duidelijk zijn echter er is geen literatuur beschikbaar met bevindingen over de grondigheid van GDPR implementaties. Met dit rapport tracht de onderzoeker aanvullende wetenschappelijke informatie te verschaffen over de GDPR-implementatiekwaliteit bij ISO- en niet-ISO-gecertificeerde organisaties. Uit het kwantitatieve onderzoek is aangetoond dat vanuit de verschillende invalshoeken er tussen ISO- en niet-ISO-gecertificeerde organisaties met de mate van hun GDPR-implementatiekwaliteit geen relatie is gevonden.

Sleutelbegrippen

GDPR, ISO-27001, ISO-9001, ISO-14001, symbolic versus substantive, symbolisch versus grondig

Samenvatting

Door de Europese verordening; de General Data Protection Regulation (GDPR) die in mei 2016 in werking is getreden en vanaf 25 Mei 2018 van toepassing is, zijn bedrijven verplicht alle benodigde organisatorische en technische maatregelen rondom de bescherming van natuurlijke personen uit de Europese Unie te implementeren. In dit onderzoeksrapport tracht de onderzoeker te verklaren hoe kwalitatief ISO- en niet-ISO-gecertificeerde ondernemingen de GDPR verordening hebben geïmplementeerd. De probleemstelling schuilt dan ook in het vinden van de verschillen in de implementatiekwaliteit van de GDPR bij niet-ISO-gecertificeerde ondernemingen ten opzichte van organisaties die ISO gecertificeerd zijn. Bij ISO-gecertificeerde ondernemingen worden ISO 9001, ISO 27001 en ISO 14001 gecertificeerde ondernemingen onder de loep genomen omdat zij namelijk al ervaring hebben opgedaan in het nemen van de benodigde organisatorische en technische maatregelen om deze ISO-certificering te realiseren en te behouden.

Het doel van dit onderzoek is om de kwaliteit van de GDPR implementatie te analyseren bij Nederlandse organisaties. Hiervoor is de volgende onderzoeksvraag opgesteld: "*Hebben ISO-gecertificeerde organisaties een grondige GDPR-implementatiestrategie dan niet-ISO-gecertificeerde organisaties?*" Hierbij wordt gekeken hoe de verschillen in implementatiekwaliteit van de GDPR bepaald kunnen worden en gecategoriseerd kunnen worden in symbolische- en grondige implementatiekwaliteit. Tevens wordt bezien in hoeverre de bedrijfsgrootte invloed heeft op de implementatiekwaliteit.

Om antwoord te kunnen geven op de onderzoeksvraag heeft er een uitgebreid literatuuronderzoek plaats gevonden naar de implementatiekwaliteit van ISO standaarden en kwaliteitsmanagement alvorens er een kwantitatief onderzoek is uitgevoerd. Voor dit onderzoek zijn de privacy statements van meer dan 80 organisaties via hun publieke bronnen grondig doorgelezen en zijn de certificeringen opgezocht. De onderzochte organisaties variëren van 20 tot 10.000 medewerkers. De privacy statements zijn vergeleken met 25 geselecteerde bepalingen uit 13 van de 99 artikelen van de GDPR verordening. Uit de resultaten bleek dat er geen significantie is tussen het voldoen aan ISO-certificatie en de GDPR-implementatiestrategie van bedrijven, er geen verband is tussen de grootte van een organisatie en de ISO-certificering op de implementatiestrategie en er geen multicollineariteit is tussen de twee onafhankelijke variabelen. Hierdoor kan geconcludeerd worden dat er geen verband is tussen organisaties met minimaal één ISO certificaat en zonder ISO certificaat als het gaat om de kwaliteit van de GDPR implementatie.

De Nederlandse gegevensbeschermingsautoriteit Autoriteit Persoonsgegevens of een geaccrediteerde ISO-certificatie-instelling kan er dus niet van uitgaan dat ISO-gecertificeerde organisaties de GDPR grondiger hebben geïmplementeerd dan niet-ISO-gecertificeerde organisaties. Op basis van de literatuur en de bevindingen uit dit onderzoek wordt een drietal aanbevelingen voor de praktijk voorgesteld en een viertal voordrachten voor verder onderzoek. De GDPR is in Nederland ook bekend onder de naam Algemene Verordening Gegevensbescherming (AVG).

Summary

By the European regulation; the General Data Protection Regulation (GDPR) that came into force in May 2016 and applies from 25 May 2018, companies are obliged to implement all necessary organizational and technical measures regarding the protection of natural persons from the European Union. In this research report, the researcher tries to explain how qualitatively ISO- and non-ISO certified companies have implemented the GDPR regulation. The problem therefore lies in finding the differences in the implementation quality of the GDPR at non-ISO certified companies compared to organizations that are ISO certified. Regarding ISO certified companies; the ISO 9001, ISO 27001 and ISO 14001-certified companies are examined specifically because they have already gained experience in taking the necessary organizational and technical measures to achieve and maintain this ISO certification.

The objective of this research is to analyse the quality of the GDPR implementation at Dutch organizations with a field service. The following research question has been formulated: "*Have ISO certified organizations implemented a more substantive GDPR implementation strategy than non-ISO certified organizations?*" Hereto the researcher will investigate how the differences in implementation quality of the GDPR can be determined and can be categorized in symbolic and substantive implementation quality. Contemporaneously, it is also examined to what extent the company size influences the implementation quality.

In order to answer the research question, an extensive literature study was carried out into the implementation quality of ISO standards and quality management as a base for the quantitative study. For this study, the privacy statements of more than 80 organisations were thoroughly read through their public sources and their certifications were sought. The investigated organisations vary from 20 to 10,000 employees. The privacy statements are compared with 25 selected clauses out of 13 of a total of 99 articles of the GDPR. The results showed that there is no significance between complying with ISO certification and the GDPR implementation strategy of companies, there is no relation between the size of an organization and the ISO certification on the implementation strategy and there is no multicollinearity between the two independent variables, as a result of which it can be concluded that there is no relationship between organisations with at least one ISO certificate and without an ISO certificate with the degree of GDPR implementation. The Dutch data protection authority; “Autoriteit Persoonsgegevens” or an accredited ISO certification body can therefore not assume that ISO certified organizations have implemented the GDPR more substantive than non ISO certified organizations. Based on the literature and the findings from this research report, three recommendations for practice and four recommendations for further research are proposed. In the Netherlands, the GDPR is also known under the name of the “Algemene Verordening Gegevensbescherming” (AVG).

Inhoudsopgave

1. Introductie

In dit hoofdstuk wordt de achtergrond en de gebiedsverkenning van het onderzoek behandeld. Aansluitend wordt de probleemstelling gekarakteriseerd gevolgd door de opdrachtformulering en een uiteenzetting op de relevantie van het onderzoek. Ter afsluiting wordt de aanpak van het onderzoek in hoofdlijnen beschreven.

1.1. Achtergrond

Privacy is een begrip met impact op de bedrijfsvoering van alle ondernemingen, instellingen en overheden geworden die persoonsgegevens bijhouden en verwerken van natuurlijke personen binnen de Europese Unie. Door de Europese verordening; General Data Protection Regulation (GDPR) zijn bedrijven verplicht alle benodigde organisatorische en technische maatregelen rondom de bescherming van natuurlijke personen uit de Europese Unie te implementeren. Het niet voldoen aan deze verordening kan resulteren in een boete. Het implementeren van deze privacy-verordening is voor elke onderneming, instelling of overheid een project op zichzelf echter is de vraag hoe kwalitatief de GDPR verordening is geïmplementeerd. In dit onderzoeksrapport wordt onderzocht hoe kwalitatief ondernemingen de GDPR verordening hebben geïmplementeerd met enerzijds de focus op niet-ISO-gecertificeerde ondernemingen en anderzijds op ISO-gecertificeerde ondernemingen waarbij gericht wordt gekeken naar ISO 9001 , ISO 27001 en/of ISO 14001 gecertificeerde ondernemingen. Zij hebben namelijk al ervaring opgedaan in het nemen van de benodigde organisatorische en technische maatregelen om deze ISO-certificering te realiseren. Het onderzoeksrapport beschrijft de gebiedsherkenning, de achterliggende probleemstelling, de doelstelling van het onderzoek met haar onderzoeksvraag en de maatschappelijke en wetenschappelijke relevantie van het onderzoek.

1.2. Gebiedsverkenning

Het onderzoek vindt plaats binnen het gebied van de implementatiekwaliteit van de GDPR verordening bij Nederlandse ISO- en niet-ISO-gecertificeerde ondernemingen waarbij implementatiekwaliteit wordt onderscheiden in symbolisch (symbolic) en grondig (substantive). Symbolische (symbolic) implementatie wordt gezien waarbij de maatregelen niet worden geïntegreerd in de dagelijkse bedrijfsvoering en waarbij het management minimaal betrokken is. Dit in tegenstelling tot de definitie van grondige (substantive) implementatie waarbij de maatregelen zijn geïntegreerd in de dagelijkse bedrijfsvoering en het management betrokken is. De ISO 9001, ISO 27001 en ISO 14001 begrippen zijn internationale kwaliteitsstandaarden die respectievelijk gericht zijn op kwaliteits-, informatiebeveiligings-, en milieu-managementsystemen en zijn door de “International Organization for Standardization” ontwikkeld. De GDPR staat voor General Data Protection Regulation en is in Nederland bekend onder de naam Algemene Verordening Gegevensbescherming (AVG). De GDPR is in mei 2016 in werking getreden en vanaf 25 Mei 2018 van toepassing.

1.3. Probleemstelling

Het verschil tussen het voldoen aan de ISO standaard en aan de GDPR regulering is dat de GDPR een verordening is en een ISO standaard niet. Het is aan elke onderneming of zij aan een ISO standaard wil voldoen want ISO-certificatie wordt niet door een overheidsinstantie opgelegd. Een overeenkomst tussen het voldoen aan de ISO standaard en aan de GDPR regulering is dat zowel ISO als GDPR een organisatie vertelt wat te doen echter niet hoe de bepalingen moeten worden uitgevoerd. Daarom is het aannemelijk af te vragen of ISO-gecertificeerde bedrijven alle benodigde organisatorische en technische maatregelen grondig hebben geïmplementeerd om aan deze privacy wetgeving te voldoen. De uitdaging is om de juiste verschillen te vinden in de implementatiekwaliteit van GDPR bij ISO-gecertificeerde en niet-ISO-gecertificeerde ondernemingen. Hierin schuilt de probleemstelling.

1.4. Opdrachtformulering

Het doel van dit onderzoek is om de kwaliteit van de GDPR implementatie te analyseren bij Nederlandse organisaties die ISO 9001, ISO 27001 en/of ISO 14001 gecertificeerd zijn en dus ervaring hebben in het implementeren van een bepaald kwaliteitssysteem ten opzichte van Nederlandse organisaties die niet-ISO gecertificeerd zijn. Met dit onderzoek wil de onderzoeker bereiken hoe de verschillen in implementatiekwaliteit van de GDPR bepaald en gecategoriseerd kunnen worden in symbolische- en grondige implementatiekwaliteit. De hoofdonderzoeksvraag van dit onderzoek is: "*Hebben ISO-gecertificeerde organisaties een grondige GDPR-implementatiestrategie dan niet-ISO-gecertificeerde organisaties?*" en met de deelvragen*; "Wat wordt onder kwaliteit verstaan?*", "*Welke determinanten bepalen een grondig kwaliteitsmanagement implementatieproject?*", "*Wat zijn de verschillen tussen een symbolische en een grondige implementatie van ISO?*" en "*Wat zijn de minimale eisen voor het implementeren van de GDPR?*" kan gerichter literatuur worden onderzocht.

1.5. Motivatie/ relevantie

Diverse literatuur die haar licht kan laten schijnen over de implementatiekwaliteit van de GDPR verordening; symbolische (symbolic)- versus grondige (substantive) GDPR implementatie is onderzocht. Op het moment (2019) van het literatuuronderzoek zijn zeer weinig bronnen over dit onderwerp gevonden. Het is ook niet verwonderlijk dat over de kwaliteit van een GDPR implementatie weinig bekend is omdat de verordening pas vanaf 25 mei 2018 van toepassing is. In tegenstelling tot literatuur over de implementatiekwaliteit van de GDPR verordening is over de implementatiekwaliteit van kwaliteitsmanagement en van ISO standaarden relevante onderzoeksliteratuur aanwezig echter is er geen literatuur gevonden over de relatie van ISO-gecertificeerde bedrijven met de implementatiekwaliteit van de GDPR verordening; een gemotiveerde reden om een exploratief onderzoek uit te voeren. Daarnaast is het onderzoek een aanvulling op de onderzoeken van Pershad, Lopes et al. en Tzolov waarbij respectievelijk de relatie tussen ISO 27001 en het voldoen aan de GDPR wordt gelegd (Pershad, 2018), hoe ISO 27001 kan zorgen voor GDPR compliance (Lopes, Guarda, & Pedro, 2019) en hoe ISO 9001 als raamwerk kan worden toegepast voor een GDPR implementatie (Tzolov, 2018). In tegenstelling tot hun onderzoeken wordt in dit onderzoek onderzocht of organisaties met minimaal één ISO-certificering de GDPR "grondiger" hebben geïmplementeerd dan niet-ISO-gecertificeerde organisaties. Verder is vanuit de valorisatie optiek dit onderzoek relevant omdat het ondersteuning aan auditeurs en stakeholders biedt die zich willen verdiepen in de implementatiekwaliteit van de GDPR verordening bij niet-ISO- en ISO-gecertificeerde organisaties. Deze belanghebbenden krijgen een betere inzage in het detecteren van de determinanten die de basis vormen voor een grondige GDPR implementatiekwaliteit ten opzichte van soortgelijke organisaties.

1.6. Aanpak in hoofdlijnen

Vanwege de hoofdonderzoeksvraag van dit onderzoek: "*Hebben ISO-gecertificeerde organisaties een grondige GDPR-implementatiestrategie dan niet-ISO-gecertificeerde organisaties?*" en het feit dat er weinig literatuur over dit onderwerp aanwezig is, is gekozen voor een kwantitatief exploratief onderzoek. Het onderzoeksrapport is als volgt opgesteld; hoofdstuk 2 beschrijft de onderzoeksaanpak met het theoretisch kader waarbij de theoretische antwoorden per deelvraag uit de literatuur worden gefundeerd. In hoofdstuk 3 wordt de onderzoeksmethode beschreven waarbij dataverzameling, data-analyse en betrouwbaarheid en validiteit de hoofdonderwerpen zijn. Vervolgens wordt in hoofdstuk 4 de resultaten vanuit verschillende perspectieven geïnterpreteerd om een gefundeerde conclusie op te kunnen stellen. Ten slotte wordt in hoofdstuk 5 de conclusie beschreven, een reflectie op het onderzoek uitgevoerd, worden aanbevelingen voor verder onderzoek en voor de praktijk voorgesteld en wordt bij de discussie de empirische bevindingen vergeleken met de literatuur.

2. Theoretisch kader

Hoofdstuk 2 beschrijft de onderzoeksaanpak en uitvoering voor het theoretisch kader waarbij vervolgens in paragraaf “Resultaten” de onderzoeker probeert de theoretische antwoorden van de deelvragen te onderbouwen en de sleutelbegrippen te definiëren en de verschillen te verduidelijken aan de hand van wetenschappelijke literatuur. Ten slotte worden de conclusies van het theoretisch kader vastgelegd en het doel voor het vervolgonderzoek bepaald.

2.1. Onderzoeksaanpak

In het onderzoek naar de implementatiekwaliteit van de GDPR is literatuur geraadpleegd naar de implementatiekwaliteit van ISO standaarden en kwaliteitsmanagement. Het doel van dit onderzoek is om de kwaliteit van de GDPR implementatie te analyseren bij Nederlandse organisaties die ervaring hebben in het implementeren van ISO 9001, ISO 27001 en/ of ISO 14001 en bij Nederlandse organisaties die niet-ISO gecertificeerd zijn. De basisartikelen “What Drives Substantive Versus Symbolic Implementation of ISO 14001 in a Time of Economic Crisis? Insights from Greek Manufacturing Companies” (Iatridis & Kesidou, 2018), “Stakeholder Pressures as Determinants of CSR Strategic Choice: Why do Firms Choose Symbolic Versus Substantive Self-Regulatory Codes of Conduct?” (Perez-Batres, Doh, Miller, & Pisani, 2012) en “Firm Self-Regulation through International Certifiable Standards: Determinants of Symbolic versus Substantive Implementation” (Christman & Taylor, 2006) hebben mij meer inzicht gegeven in het definiëren van de hoofdonderzoeksvraag; “*Hebben ISO-gecertificeerde organisaties een grondige GDPR-implementatiestrategie dan niet-ISO-gecertificeerde organisaties?*”

Aan de hoofdonderzoeksvraag zijn de volgende deelvragen bepaald*;* “*Wat wordt onder kwaliteit verstaan?*”, “*Welke determinanten bepalen een grondig kwaliteitsmanagement implementatieproject?*”, “*Wat zijn de verschillen tussen een symbolische en een grondige implementatie van ISO?*” en “*Wat zijn de minimale eisen voor het implementeren van de GDPR?*”.

Aan de hand van de deelvragen is diverse literatuur met behulp van de “building block”-, “forward snowball”- en “backward snowball”-methode via de zoekmachines Ebsco en Google Scholar gevonden en onderzocht. Een uitvoerig overzicht van gekozen queries per bron wordt in tabel 1 van bijlage 1 weergegeven.

2.2. Uitvoering

Vanuit de hoofdonderzoeksvraag is binnen de zoekmachine EBSCO host gezocht op de zoekwoorden “GDPR” en “ISO”. Via EBSCO werd m.b.v. Google Scholar het artikel “A model for implementation GDPR based on ISO standards” van Tzolov gevonden. Dit artikel gaf mij een gedegen beeld rondom ISO en het implementeren van GDPR om de zoektocht naar meer literatuur te vervolgen. Daarnaast gaf het aantal EBSCO zoekresultaten; 11 resultaten waarvan 1 chinees academisch artikel, duidelijk aan dat nog weinig onderzoek gedaan is in de relatie tussen ISO en GDPR. De query “Substantive AND symbolic AND implementation AND privacy regulation” en de query “Substantive AND symbolic AND implementation AND GDPR” hebben in EBSCO geen artikelen opgeleverd. Google Scholar geeft met de zoekwoorden ISO en GDPR in de periode vanaf 2018 1580 zoekresultaten weer. Alleen het zoekwoord ISO levert 46.900 resultaten op en het zoekwoord GDPR levert 15.200 resultaten op in dezelfde periode. In verhouding is er nog weinig literatuur aanwezig rondom ISO en GDPR. Het artikel “A model for implementation GDPR based on ISO standards” was het zesde resultaat op pagina 1 van Google Scholar. Op pagina 2 werd het artikel “Static Analyse for GDPR Compliance” doorgelezen en de 5 citerende artikelen. Hiervan is het artikel “Integrating Access Control and Business Process for GDPR Compliance: A Preliminary Study” van Calabro et al. aan de literatuurlijst toegevoegd.

Om aanvullende literatuur, naast het basisartikel “Stakeholder Pressures as Determinants of CSR Strategic Choice: Why do Firms Choose Symbolic Versus Substantive Self-Regulatory Codes of

Conduct?" van Perez-Batres et al. te verkrijgen rondom het bepalen van determinanten op een succesvolle implementatie is deelvraag 2 opgesteld: "*Welke determinanten bepalen een grondig kwaliteitsmanagement implementatieproject?*". Om literatuur te kunnen doornemen die op deelvraag 2 betrekking heeft is de volgende query in EBSCO opgesteld; "Substantive AND symbolic AND implementation AND regulation" en dit heeft geresulteerd in 6 artikelen. Hieronder is het basisartikel "Firm self-regulation through international certifiable standards: determinants of symbolic versus substantive implementation" van Christman en Taylor naar voren gekomen als de meest relevantste. Eveneens kwam dit artikel naar voren met de query "determinants AND substantive implementation" en vanuit dit basisartikel is de snowball-methode toegepast. Indirect is naar aanleiding van deelvraag 2 de kernvraag rondom kwaliteit opgesteld: "*Wat wordt onder kwaliteit verstaan?*". Een verdere toelichting op de uitvoering van het literatuuronderzoek wordt in bijlage 1 weer gegeven.

2.3. Resultaten

In de volgende vier sub paragrafen worden de antwoorden op de deelvragen; "*Wat wordt onder kwaliteit verstaan?*", "*Welke determinanten bepalen een grondig kwaliteitsmanagement implementatieproject?*", "*Wat zijn de verschillen tussen een symbolische en een grondige implementatie van ISO?*" en "*Wat zijn de minimale eisen voor het implementeren van de GDPR?*", uitvoerig beschreven.

2.3.1. Wat wordt onder kwaliteit verstaan?

Er zijn vele definities van kwaliteit. Van Dale definieert kwaliteit als; 'de mate waarin iets goed of slecht is' (Verburg, et al., 2009). Bekende westerse grondleggers van kwaliteitszorg zijn Juran, Crosby en Deming (Chase & Aquilano, 1995, p. 15). Juran definieerde kwaliteit als 'fitness for use' (Straker). Philip Crosby definieerde kwaliteit als 'Conformance to requirements' met het principe om het de eerste keer direct goed te doen; breng goede managementprincipes rondom kwaliteit tot stand zodat de besparingen hoger zijn dan de kosten van het kwaliteitssysteem (Baars, Hintzbergen, Hintzbergen, & Smulders, 2015). William Edwards Deming definieerde kwaliteit dat het gericht moet zijn op de behoeften van de consument; in het heden en in de toekomst. Kwaliteit is dynamisch omdat klantbehoeften en verwachtingen altijd veranderen waardoor de definitie van kwaliteit ook veranderd. Het managementteam dient in staat te zijn om zich aan de veranderingen in verwachtingen en behoeften van haar klanten aan te passen (Deming). De ISO-8402 norm definieert de basistermen die betrekking hebben op kwaliteitsbegrippen, zoals deze van toepassing zijn voor producten en diensten, bij de voorbereiding en het gebruik van kwaliteitsnormen, alsmede voor wederzijds begrip bij internationale communicatie. Volgens deze norm is de definitie van kwaliteit: 'Het geheel van eigenschappen en kenmerken van een product of dienst dat van belang is voor het voldoen aan vastgestelde of vanzelfsprekende behoeften. In verband hiermee staan taakvelden waarvan de wijze van uitvoering van belang is voor het voldoen aan vastgestelde of vanzelfsprekende eisen en randvoorwaarden met betrekking tot onder mee beschikbaarheid, betrouwbaarheid, beveiliging en standaardisatie' (Looijen, 1995).

2.3.2. Welke determinanten bepalen een grondig kwaliteitsmanagement implementatieproject?

De kwaliteitsdefinities zijn de basis voor kwaliteitsaspecten zoals beschreven in ISO 9000, ISO 27001, ISO 14001 en in Total Quality Management (TQM). ISO 9000 is een verzamelnaam voor een reeks internationale normen op het gebied van kwaliteitsborging. De TQM-aanpak en de ISO 9000-normen hangen met elkaar samen. Een organisatie die ISO 9000-normen toepast in basisprocedures kan de TQM-filosofie in de volgende fase implementeren (Waks & Frank, 1999). Bij Total Quality Management (TQM) is het van belang om het volgende met betrekking tot kwaliteit te onderkennen: Er zijn verschillende partijen in het spel bij kwaliteit; kwaliteit is niet alleen produktkwaliteit maar eveneens proceskwaliteit en kwaliteit is niet absoluut maar relatief

(Bemelmans, 1994). In deze paragraaf wordt dieper ingegaan op de determinanten bij het implementeren van TQM en bij ISO.

De determinanten voor een succesvolle TQM implementatie

TQM is een holistische kwaliteitsmanagement benadering die de gehele waardeketen bekijkt en die de menselijke factoren benadrukt (Hietschold, Reinhardt, & Gurtner, 2014, p. 6254) .TQM is een managementfilosofie gericht op voortdurende procesverbetering door het voorkomen van problemen en fouten; het continu monitoren en controleren van processen-prestaties en kwaliteit; het centraal stellen van de klant en het creëren van bewustzijn en betrokkenheid van het management, van alle werknemers, de klanten en leveranciers. De basis voor de TQM-aanpak kan worden weergegeven als een driehoek met kwaliteit, kosten en tijd als zijden. Dit betekent dat het doel is om te zorgen voor een kwaliteitsproces om het meest efficiënte product tegen minimale kosten en binnen de meest geschikte tijd te leveren. Één van de slogans van het systeem spoort aan om het juiste te doen, de eerste keer, altijd en in elk proces. Waar in het verleden kwaliteitsborging gericht was op de inspectie van conformiteit van specificaties, ligt de nadruk tegenwoordig ook op productgeschiktheid voor gebruik en totale klanttevredenheid, niet alleen de eindproductkwaliteit maar ook met veldondersteuning, gedurende de levensduur van het product. Deming, beschouwd als een van de belangrijkste goeroes van de TQM-methode, formuleerde 14 principes die sindsdien het klassieke fundament van het systeem zijn geworden waarvan de PDCA kwaliteitscirkel onderdeel is van deze principes (Waks & Frank, 1999). Bij het toepassen van deze 14 principes is leiderschap de sleutel, het creëren van een omgeving met Deming principes kan niet door het personeel worden gestuurd (Jankowski, 2006). TQM werd door vele bedrijven in de jaren ’80 toegepast echter het drong pas echt door bij bedrijven in de jaren ’90 (Chase & Aquilano, 1995). Volgens TQM, specificeren, meten en verbeteren kwaliteitsprofessionals de processen en indien nodig herontwerpen de processen om ervoor te zorgen dat organisaties bereiken wat zij willen (Baars, Hintzbergen, Hintzbergen, & Smulders, 2015, p. 2). Deming beweert dat effectief management gebouwd dient te worden op basis van respect en vertrouwen in de mens. Medewerkers dienen aangemoedigd te worden aan de hand van een proces van continue training en leiderschap en het opzetten van een organisatiecultuur die gebaseerd is op samenwerking, toewijding tot continue verbetering en erkenning in de vaardigheden van medewerkers. De verantwoordelijkheid van deze transformatie volgens Deming begint bij de eigenaar en op managementniveau. Organisaties die continu hun medewerkers betrekken bij de implementatie van een kwaliteitsmanagementsysteem zijn meer productief en winstgevend dan organisaties die dit nalaten. De output van medewerkers zijn het hoogst indien betrokkenheid van de medewerkers plaats vindt voordat met een totaal kwaliteitsmanagementsysteem wordt gestart (Braughton, 1999).
Hietschold et al. geeft aan dat het succes van elk kwaliteitsmanagementconcept afhangt van een succesvolle implementatie binnen een organisatie. In de praktijk echter is de implementatie van een totaal kwaliteitsmanagementsysteem een complex en moeilijk proces en de voordelen worden niet makkelijk behaald. Hierdoor is het onderzoeken van kritieke factoren die een succesvolle TQM implementatie bepalen in het bijzonder belangrijk. Onderzoeken geven weer dat deze factoren een positieve invloed hebben op de prestaties van een organisatie. Het meten van kritieke succes factoren is een belangrijke voorwaarde om het implementatieproces te controleren en om de kansen op succes te verhogen. Kwaliteitsmanagement evolueerde van een resultaat georiënteerde kwaliteitscontrole tot een integraal bedrijfsbrede aanpak; TQM. Het TQM concept bestaat uit drie componenten. Ten eerste, de term “total” veronderstelt dat alle individuen betrokken bij een bedrijf (medewerkers, klanten en leveranciers) bijdragen aan kwaliteitsmanagement. Ten tweede, ‘quality’ is het integrale deel van de bedrijfsfilosofie. En als laatste refereert de term ‘management’ naar de bestuurlijke verantwoordelijkheid en relevantie van de betrokkenheid van de leidinggevenden (Hietschold, Reinhardt, & Gurtner, 2014, p. 6255). Medewerkersparticipatie is tevens een kritieke succesfactor. Door actieve betrokkenheid verkrijgen medewerkers nieuwe kennis, herkennen sneller fouten en lossen problemen efficiënter op. Het daaruit voortvloeiende besef van het belang van kwaliteit leidt tot een versterkte betrokkenheid van TQM. Deze verandering in houding zorgt ervoor dat medewerkers zich als een onderdeel van de organisatie voelen en zorgt voor het creëren van een bedrijfsbrede kwaliteitscultuur. Participatie zorgt er mede

voor dat medewerkers worden aangemoedigd om ideeën voor continue kwaliteitsverbeteringen aan te leveren (Hietschold, Reinhardt, & Gurtner, 2014, p. 6258). TQM is een proces die geleid wordt door het senior management om de betrokkenheid van alle medewerkers te verkrijgen op de weg naar de continue verbetering van de prestaties van alle activiteiten (Kumar & Sharma, 2017, p. 1530).

De determinanten voor een succesvolle ISO implementatie

ISO (International Organization for Standardization) is een wereldwijde federatie van nationale normalisatie instituten (de ISO-leden) die in Oktober 1946 in Londen is opgericht met als doel uniformiteit en duidelijkheid te krijgen tussen alle landelijke normen. (ISO Central Secretariat, 1997) Het voorbereidingswerk voor internationale normen wordt doorgaans uitgevoerd door de technische commissies van ISO. Elk lid dat interesse heeft in een onderwerp waarvoor een technische commissie is samengesteld, heeft recht op vertegenwoordiging in deze commissie. Ook internationale organisaties, zowel overheidsinstanties als niet overheidsinstanties, nemen in samenwerking met ISO deel aan deze werkzaamheden. ISO werkt nauw samen met de International Electrotechnical Commission (IEC) inzake alle elektrotechnische normalisatie (Normalisatie-instituut, NEN-EN-ISO 9001, 2015). Het acroniem ISO refereert aan het Griekse woord ISOS wat betekent: Welke is gelijk of identiek aan een referentie model. In dit geval de normen ontwikkeld door het Internationale Organisatie voor Standaardisatie. (Boiral, 2007)

Met betrekking tot de implementatiekwaliteit van ISO is voornamelijk literatuur geraadpleegd over implementaties bij organisaties die ISO 9001 (Normalisatie-instituut, NEN-EN-ISO 9001, 2015), ISO 27001 (Normalisatie-instituut, NEN-ISO/IEC 27001, 2015) en/of ISO 14001 (Briggs, 2017) zijn gecertificeerd. De internationale standaard ISO 9001 is gebaseerd op de principes van kwaliteitsmanagement die worden beschreven in ISO 9000. De beschreven kwaliteitsmanagementprincipes zijn: klantgerichtheid, leiderschap, betrokkenheid van medewerkers, procesbenadering, verbetering, op bewijs gebaseerde besluitvorming en relatiemanagement (Normalisatie-instituut, NEN-EN-ISO 9001, 2015). ISO 27001 focust zich op managementsystemen voor informatiebeveiliging en ISO 14001 is een processtandaard die een raamwerk levert met als doel om milieu gerelateerde managementmethoden te integreren binnen de dagelijkse werkzaamheden van organisaties (Aravind & Christman, 2017). Internationale normeringen zoals ISO 9001, ISO 27001 en ISO 14001 vereisen van gecertificeerde firma's om specifieke managementprocessen te implementeren. Ook minder bekende ISO normen zoals ISO 20000 en ISO 55001 beschrijven onder andere de managementverantwoordelijkheden en de processen met betrekking tot respectievelijk de eisen rondom een service management - en een asset management systeem. Aravind beredeneert dat implementatie van ISO standaarden een middel is van strikte zelfregulering in het nakomen van de overeenkomstige ISO richtlijnen omdat van organisaties vereist wordt dat zij werkwijzen overnemen die verder gaan dan de eisen die de overheid hen oplegt (Aravind & Christmann, 2007). Vin beschrijft dat het inbeddingsproces van een integraal ISO managementsysteem in de organisatie gepaard gaat met significante organisatorische veranderingen, waarbij een gedegen planning en betrokkenheid in alle lagen kritische succesfactoren zijn. Weerstand kan zorgen voor het uitblijven van een optimale doorvoer van de nodige organisatorische veranderingen. (Vin, 2018)

2.3.3. Wat zijn de verschillen tussen een symbolische en een grondige implementatie van ISO?

Om deze derde deelvraag te beantwoorden wordt hieronder de kenmerken een van symbolische- en grondige implementatie van ISO, de redenen voor een grondige- of symbolische implementatie van ISO in het algemeen en specifiek bij het midden- en kleinbedrijf beschreven. De paragraaf wordt afgesloten met een toelichting op de institutionele theorie.

Symbolische implementatie van ISO

De definitie van symbolisch is volgens van Dale; 'iets dat symbolisch is, heeft een andere betekenis dan de gewone betekenis' (Verburg, et al., 2009)**.** In de literatuur wordt voor de term 'symbolisch' ook synoniemen gebruikt als ceremonieel, ritueel (Boiral, 2007) , retorisch en hypocriet (Heras-Saizarbitoria & Boiral, 2015). Bij een symbolische implementatie falen firma's om de werkwijze/ methoden volgens een gecertificeerde standaard in de dagelijkse operaties toe te passen (Christman & Taylor, 2006). Volgens Chowdhury et al. wordt symbolische implementatie van ISO 14001 gedefinieerd wanneer firma's de voorgeschreven basiseisen van de ISO 14001 standaard implementeren (Chowdhury, Prajogo, & Jayaram, 2018). Firma's die organisatorische methoden voor legitimiteitsredenen overnemen in tegenstelling tot efficiencyredenen ontkoppelen vaak de implementatie van adoptie door deze uitgebreide methoden niet in te bedden. (Aravind & Christman, 2011) (Christman & Taylor, 2006) (Iatridis & Kesidou, 2018). Boiral geeft ook in zijn onderzoek aan dat de formele structuur van het ISO 14001 systeem en de organisatorische dagelijkse werkzaamheden losjes aan elkaar zijn gekoppeld en in sommige casussen zelfs geheel zijn ontkoppeld. Symbolische implementatie is ook wanneer ISO 14001 standaarden een onderdeel wordt van het projectmanagementgedrag van een organisatie. Dit soort gedrag uit zich in een vorm dat de desbetreffende organisaties alleen die documentatie die betrekking heeft op het milieubeleid en op de procedures onderhouden en updaten en deze aan alle medewerkers mededelen (Boiral, 2007). Ook Aravind et al. onderschrijft dit; symbolische implementatie is dat sommige organisaties alleen de formele elementen van het ISO systeem onderhouden zoals de vereiste documentatie om de certificatie te verkrijgen terwijl de actuele werkwijze enorm afwijkt van de gedocumenteerde werkwijze (Aravind & Christman, 2017) of dat organisaties tijdens ISO 14001 implementatie geen milieumanagementsysteem bij hun dagelijkse werkzaamheden toepassen of dat zij alleen voldoen aan bepaalde componenten van Deming's PDCA cirkel en trachten om op het laatste moment implementatiebewijs te verzamelen met als enig doel het slagen voor de jaarlijkse certificatie-audit. In zo'n geval zal een organisatie niet echt proberen om aan de ISO 14001 eisen te voldoen en om haar milieuprestaties te verbeteren (Iatridis & Kesidou, 2018).

Redenen voor een symbolische implementatie

Bedrijven hebben een motief voor een symbolische implementatie van ISO 14001 omdat een grondige implementatie aanzienlijke inzet van tijd en middelen vergt (Aravind & Christman, 2017). De strategische implementatiebenadering van gecertificeerde standaarden door firma's is afhankelijk van de implementatiekwaliteit ten opzichte van de waargenomen kosten en voordelen. Aannemende dat een grondige implementatie meer kosten voor firma's met zich mee brengt dan een symbolische implementatie zullen firma's kiezen voor de symbolische implementatie totdat zij het beeld krijgen van de voordelen die verder gaan dan de symbolische waarde van certificatie. De hoge kosten die gepaard gaan met het continu verbeteren principe van management systeem standaarden zijn de hoofdreden waarom ISO-gecertificeerde firma's in China de standaarden niet volledig hebben geïmplementeerd (Christman & Taylor, 2006, p. 864).

Grondige implementatie van ISO

Van Dale geeft als definitie voor grondig; 'iets wat grondig gebeurt, gebeurt degelijk en zorgvuldig' (Verburg, et al., 2009)**.** Het operatieve model die ten grondslag ligt aan een grondige implementatie van ISO 14001 is de kwaliteitscirkel van Deming. Kern van deze visie is gebaseerd op het concept van continue verbetering en het blijven zoeken naar nieuwe kennis. Verbeteringsinspanningen in elke organisatie vereist kennis. Deming's theorie over kennis suggereert dat kennis, in vergelijking met informatie, van theorie komt en dat theorie leidt naar voorspellingen. Het doel van het onderzoeken van systemen en hun variabiliteit is om organisaties in staat te stellen correcte beslissingen over verbetering te ontwikkelen en systeemdoelen te bereiken (Horine, Yvarra, & Lindgren, 1994). Gebaseerd op deze benadering kan een organisatie die volledig is toegewijd aan milieugericht werken, ISO 14001 grondig implementeren als het een milieumanagementsysteem ontwerpt, ontwikkeld en implementeert die effectief alle vier componenten van de PDCA cirkel bevat. Organisaties als deze zullen hun dagelijkse werkzaamheden niet van ISO 14001 ontkoppelen maar zullen continu de ISO 14001 procedures en

methoden toepassen en hun milieumanagementsysteem integreren binnen hun dagelijkse werkzaamheden. Op deze manier zal een organisatie grondige werkprocedures overnemen die significant hun bedrijfsmodel, doelstellingen en processen beïnvloeden. Dit is wat de literatuur omschrijft als 'grondige implementatie' (Iatridis & Kesidou, 2018). Volgens Iatridis et al. kenmerkt een grondige implementatie van ISO 14001 door; het opstellen van beleid met het identificeren van de belangrijkste aspecten (de fase Plan); het invoeren van een gedocumenteerd managementsysteem om de ISO richtlijnen te integreren in de dagelijkse activiteiten (de fase Do); het monitoren en meten van de dagelijkse prestaties met behulp van het managementsysteem (de fase Check) en als laatste het onderhouden van procedures voor het bepalen van verantwoordelijkheden om in te kunnen grijpen bij gebreken, om potentiële problemen te voorkomen zodat correctieve maatregelen moeten worden geïmplementeerd (Iatridis & Kesidou, 2018). Net als bij ISO 14001 kenmerkt een ISO 9001 en ISO 27001 kwaliteitsmanagementsysteem zich ook aan het 'continu verbeteren' door de Plan, Do, Check en Act kwaliteitsverbeteringsstappen van Deming. Alhoewel de Deming cirkel in de laatste versie van ISO 27001 niet meer expliciet staat beschreven is er nog steeds een duidelijke link met deze verbeterstappen (Normalisatie-instituut, NEN-ISO/IEC 27001, 2015).

Redenen voor een grondige implementatie

Een ISO 14001 implementatie wordt als grondig gezien wanneer firma's consistent de werkwijze hanteren zoals voorgeschreven door de ISO 14001 standaard om hun milieu strategie af te stemmen op hun organisatiestrategie (Chowdhury, Prajogo, & Jayaram, 2018, p. 340). Een grondige implementatie laat zien dat firma's consistent de gecertificeerde standaard toepassen (Christman & Taylor, 2006). Iatridis et al. benoemt concurrentie als beweegreden om aan ISO 14001 certificering te voldoen. Concurrerende beweegredenen komen voort uit de verwachtingen van efficiency verbeteringen zoals het vooruitzicht in verbeteringen van productiviteit, prestaties en winstgevendheid (Iatridis & Kesidou, 2018).

Redenen voor een grondige- of symbolische implementatie bij Midden-Klein Bedrijven

Iatridis et al. beargumenteert dat de adoptiemotivatie van Midden- Klein Bedrijven (MKB's); ondernemingen met maximaal 250 medewerkers, voor het implementeren van een gecertificeerd management systeem ten behoeve van het nemen van de sociale verantwoordelijkheid van een onderneming duidelijk verschillend zijn tussen vroege - en late adopters. De vroege adopters zijn vooral gedreven door de te behalen interne efficiency zoals de mate waarbij de verandering de financiële en operationele prestaties van de organisatie verbeterd. Om die reden is betoogd dat vroege adopters geneigd zijn om zich volledig te houden aan de eisen van de standaard en in die zin de standaard dus grondig uitvoert. Daarentegen zijn de late adopters meer gedreven door coercieve- en nabootsende motieven om hun legitimiteit te behouden of te vergroten met als resultaat een symbolische implementatie; de organisatie probeert niet echt de vereisten van de standaard binnen hun operationele processen te integreren. Het midden- en klein bedrijf heeft de neiging op dezelfde manier als grote ondernemingen te reageren als het gaat om het nemen van de sociale verantwoordelijkheid en de gerelateerde gecertificeerde managementsystemen. Verder geeft de analyse van dit onderzoek weer dat de persoonlijke normen en waarden van de mensen die het midden- en klein bedrijf leidt, voorstanders zijn in het uitvoeren van activiteiten rondom sociale verantwoordelijkheid. Veelal zijn dit de eigenaren die waarschijnlijk tot de vroege adopters van de standaard behoren (Iatridis, Kuznetsov, & Whyman, 2016). In het algemeen neigt ISO 9000 te worden overgenomen op een manier die eerder past bij de verschillende behoeften en interne onvoorziene omstandigheden van een organisatie dan door de institutionele druk. Volgens de observaties in de casussen bij de MKB bedrijven schijnt dat retoriek en woorden meer gewicht in de schaal leggen dan concrete acties rondom ISO 9000 implementatie en vindt zelfs plaats bij MKB bedrijven waar de standaard grondig is overgenomen. De hypocriete of symbolische integratie kan niet alleen door de institutionele druk worden uitgelegd omdat organisaties met veelal dezelfde druk de standaard grondig of symbolisch hebben overgenomen. De mate van ontkoppeling van ISO 9000 met de organisatieprocessen is laag bij die organisaties, waarbij het

management leiderschap en betrokkenheid toont en gebruikersvriendelijke documentatie wordt benut alsmede innovatieve ondersteunende software en enige ondersteuning van consultants. Indien de betrokkenheid van de medewerkers bij de implementatie laag is en de uitvoering voornamelijk wordt gedaan onder verantwoordelijkheid van het middelmanagement en hoe meer consultants actief betrokken zijn bij de implementatie van ISO 9000, de meer de standaard neigt om oppervlakkig te worden geïmplementeerd en van de interne procedures wordt losgekoppeld (Heras-Saizarbitoria & Boiral, 2015).

Institutionele theorie

Organisaties strijden niet alleen om middelen en klanten, maar ook om politieke macht en institutionele legitimiteit om te voldoen aan de sociale als economische normen. Het concept van institutioneel isomorfisme is een nuttig hulpmiddel om de politiek en de plechtigheden te begrijpen die doordringen tot het moderne organisatieleven. Isomorfisme is een dwingend proces dat één eenheid in een populatie dwingt te lijken op andere eenheden die met dezelfde set omgevingsomstandigheden te maken hebben (DiMaggio & Powell, 1983). De institutionele theorie beargumenteert dat om te overleven organisaties aan de institutionele druk van de omgeving moeten voldoen zoals die van overheidsorganen, leidende organisaties en andere belanghebbenden zelfs als het voldoen aan die druk weinig te maken heeft met technische verbeteringen. Het voldoen aan deze institutionele druk levert een versterkte legitimiteit, verhoogde prestige, sociale ondersteuning en toegang tot middelen (Aravind & Christman, 2017). In het onderzoek van DiMaggio & Powell worden de drie soorten externe institutionele druk beschreven, namelijk:

1) Dwingende isomorfisme; voortkomend uit politieke invloeden en het legitimiteitsprobleem,
2) Imiterende isomorfisme; als gevolg van standaardreacties op onzekerheid en
3) Normatieve isomorfisme die met professionalisering wordt geassocieerd.

Dwingende isomorfisme omvat de druk van overheden, instanties en andere stakeholders op een organisatie om structuren en systemen over te nemen of aan te passen. Met betrekking tot ISO-certificatie wordt deze druk voornamelijk opgelegd door stakeholders zoals klanten omdat zij de voorkeur hebben om producten bij gecertificeerde ondernemingen af te nemen. Certificatie is de primaire reden als het antwoord op druk van klanten (Christman & Taylor, 2006), daarentegen wordt het voldoen aan de GDPR verordening door de overheid afgedwongen.

Imiterende isomorfisme wordt uitgevoerd door organisaties die zich willen modelleren aan soortgelijke organisaties in hetzelfde organisatieveld die als legitiem worden gezien. Iatridis et al. beargumenteert dat de late adopters meer vatbaar zijn voor imiterende motieven en zich minder willen committeren aan gecertificeerde managementstandaarden. Het is de vraag of organisaties die de GDPR verordening hebben geïmplementeerd kijken naar soortgelijke organisaties in hoeverre zij de GDPR kwalitatief hebben geïmplementeerd en deze implementatiekwaliteit imiteren maar dit is geen onderdeel van het huidige onderzoek.

De normatieve vergelijkbaarheid omvat de manier waarop van een organisatie wordt geëist om systemen en technieken over te nemen en zich hieraan te conformeren. Deze systemen en technieken worden door relevante professionele groepen als legitiem beschouwd. Heras et al. beschrijft in relatie met ISO-certificatie dat het die legitieme organisaties betreffen die de ISO richtlijnen zoveel mogelijk aan hun organisatieprocessen hebben gekoppeld, waarbij het management leiderschap en betrokkenheid toont en de organisatie innovatieve ondersteunende systemen toepast.

2.3.4. Wat zijn de minimale eisen voor het implementeren van de GDPR?

Voor een antwoord op de laatste deelvraag wordt in deze paragraaf een nadere toelichting gegeven op de GDPR, ISO 9001 en ISO 27001 als basis voor een GDPR implementatie en de factoren voor een succesvolle GDPR implementatie.

GDPR

GDPR is de afkorting van General Data Protection Regulation en is de nieuwe Europese privacywet die met ingang van 25 Mei 2018 van toepassing is. De GDPR is in Nederland ook bekend onder de naam Algemene Verordening Gegevensbescherming (AVG) en vervangt de Wet bescherming persoonsgegevens. Een verordening is een Europese wet die rechtstreekse werking heeft in de hele Europese Unie. De Verordening is dan ook gelijk voor alle lidstaten van de Europese Unie en heeft als wetgevend instrument voorrang op ons nationale recht. De Verordening regelt de rechtmatige en zorgvuldige omgang met persoonsgegevens binnen de Europese Unie. De Verordening bestaat uit 99 artikelen en 173 overwegingen bij deze artikelen. De toezichthouder in Nederland op de GDPR is de Autoriteit Persoonsgegevens (AP) (Schermer, Hagenauw, & Falot).

De 99 artikelen van de GDPR zijn onderverdeeld in 607 bepalingen/ sub artikelen (Verordening (EU) 2016/679 van het Europese parlement en de raad, 2016). De GDPR beschrijft de bescherming van natuurlijke personen uit de EU bij de verwerking van persoonsgegevens en beschrijft de beginselen en regels hiervoor. Tevens beoogt de GDPR de verwerkingsactiviteiten te harmoniseren en beoogt ook bij te dragen aan economische en sociale vooruitgang. Het is geen uitdagend probleem om aan de GDPR eisen te voldoen en dit beeld te demonstreren. Vanuit een praktisch oogpunt kan dit probleem worden opgelost door een bepaald data management systeem (DMS) toe te passen die voldoet aan de GDPR eisen en door het leveren van de benodigde informatie en bewijsstukken zodat een bevoegde auditorganisatie dit als bewijs van nakoming kan accepteren (Calabro, Daoudagh, & Marchetti, 2019). De EU-wetgever heeft certificering in de GDPR onderschreven door middel van twee speciale artikelen; artikelen 42 en 43 die het ontwerp en de werking van certificeringsregelingen rondom de bescherming van data beschrijven. Binnen de GDPR richtlijnen kan elke derde partij een certificatieregeling opstellen (Lachaud, 2020). Een officiële GDPR certificering is geen eis waardoor een symbolische implementatie al snel uitgevoerd kan worden.

ISO 9001 als basis voor een GDPR implementatie

De Internationale Standaard ISO 9001 beschrijft dat het invoeren van een kwaliteitsmanagementsysteem een strategische beslissing voor een organisatie is die kan bijdragen aan het verbeteren van de algehele prestaties en een goede basis kan bieden voor duurzame ontwikkelinitiatieven. De mogelijke voordelen die het kan bieden zijn onder andere om consequent te voorzien in producten en diensten die voldoen aan de eisen van de klant en van toepassing zijnde wet- en regelgeving, het oppakken van risico's en kansen in verband met haar context en doelstellingen en het vermogen om het voldoen aan gespecificeerde eisen voor een kwaliteitsmanagementsysteem aan te tonen. Het consequent voldoen aan eisen en ingaan op toekomstige behoeften en verwachtingen levert een uitdaging op voor organisaties die zich in een steeds meer dynamische en complexe omgeving bevinden (Normalisatie-instituut, NEN-EN-ISO 9001, 2015). Het conferentierapport van Tzolov kenschetst een model voor GDPR implementatie op basis van de ISO 9000 standaard. De 2015 versie van ISO 9001 beschrijft een raamwerk voor de ontwikkeling van een geïntegreerd management systeem gebaseerd op verscheidene gestructureerde homogene bepalingen. ISO 9001:2015 is gebaseerd op de procesbenadering en risicomanagement welke ook de onderbouwing is van de GDPR. De procesbenadering eist van organisaties dat zij o.a. continu hun processen verbeteren, haar processen managen om zo de geplande resultaten te behalen die in lijn liggen met de strategische organisatiedoelen. Met behulp van de PDCA-cyclus kan een organisatie bewerkstelligen dat haar processen over afdoende middelen beschikken en op toereikende wijze gemanaged worden, en dat verbeterkansen vastgesteld worden en dat er iets mee wordt gedaan. Een andere gedefinieerde methodologische eis is risico gebaseerd denken. Risico gebaseerd denken stelt een organisatie in staat de factoren te bepalen die ertoe zouden kunnen leiden dat haar processen en haar kwaliteitsmanagementsysteem afwijken van de geplande resultaten,
preventieve beheersmaatregelen in te zetten om negatieve effecten te minimaliseren en maximaal gebruik te maken van kansen op het moment dat die zich voordoen (Normalisatie-instituut, NEN-EN-ISO 9001, 2015). Organisaties dienen het risico gebaseerd denken te toetsen en te managen door planning en door het implementeren van de juiste maatregelen (Tzolov, 2018). De GDPR

verordening beschrijft in artikel 32 beveiliging van verwerking dat een organisatie om een op het risico afgestemd beveiligingsniveau te waarborgen een procedure hanteert voor het op gezette tijden testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking. Artikel 40 beschrijft het stimuleren van het opstellen van gedragscodes (Europese Unie, 2016, p. 51) en komt overeen met de kwaliteitsmanagementprincipes van ISO 9001 zoals leiderschap, betrokkenheid van medewerkers en verbetering. De procedure van artikel 32 komt overeen met de stappen van de PDCA cirkel van Deming. De proces- en risicomanagement benadering van ISO 9001:2015 is een goede link om de implementatiekwaliteit van GDPR door ISO 9001 gecertificeerde firma's te onderzoeken.

ISO 27001 als basis voor een GDPR implementatie

De Internationale Standaard ISO 27001 is opgesteld om te voorzien in eisen voor het vaststellen, implementeren, bijhouden en continu verbeteren van een managementsysteem voor informatiebeveiliging. De ISO 27001 standaard beschrijft dat het invoeren van een managementsysteem voor informatiebeveiliging voor een organisatie een strategische beslissing is. Het vaststellen en implementeren van een managementsysteem voor informatiebeveiliging wordt beïnvloed door de behoeften en doelstellingen van de organisatie, de beveiligingseisen, de procedures die de organisatie toepast en de omvang en structuur van de organisatie. Er wordt van uitgegaan dat al deze beïnvloedende factoren mettertijd wijzigen.
Het managementsysteem voor informatiebeveiliging beschermt de vertrouwelijkheid, de integriteit en de beschikbaarheid van informatie door een risicobeheerproces toe te passen, en geeft belanghebbenden het vertrouwen dat risico's adequaat worden beheerd (Normalisatie-instituut, NEN-ISO/IEC 27001, 2015). Ook Baars et al. legt uit dat de significantste principes in een informatiebeveiligingsprogramma te herleiden zijn naar beschikbaarheid, integriteit en exclusiviteit. Deze basisprincipes worden ook wel aangeduid met de BEI-driehoek. Beschikbaarheid waarborgt de betrouwbare en tijdige toegang tot data of computercapaciteit voor de medewerkers. Voor de beveiligingsverantwoordelijke betekent het dat de beveiligingsmaatregelen die op computersystemen genomen zijn ook daadwerkelijk naar behoren functioneren. Integriteit gaat over de bescherming tegen ongeautoriseerde modificatie van (data in) software en hardware en kan gebeuren door geautoriseerde en ongeautoriseerde medewerkers. Bij integriteit gaat het erom dat data betrouwbaar is. Exclusiviteit of te wel vertrouwelijkheid betreft de mate waarin de toegang tot informatie wordt beperkt tot een bepaalde groep gerechtigden, die inzage mag hebben in de data (Baars, Hintzbergen, Hintzbergen, & Smulders, 2015, p. 18).
Het is belangrijk dat het managementsysteem voor informatiebeveiliging deel uitmaakt van en geïntegreerd is met de procedures van de organisatie en met de algehele managementstructuur, en dat informatiebeveiliging in aanmerking wordt genomen bij het ontwerpen van processen, informatiesystemen en beheersmaatregelen. Er wordt van uitgegaan dat de implementatie van een managementsysteem voor informatiebeveiliging in omvang wordt afgestemd op de behoeften van de organisatie. (Normalisatie-instituut, NEN-ISO/IEC 27001, 2015) De GDPR verordening beschrijft het continu verbeteren in artikel 31, lid 1d en in lid 1b van hetzelfde artikel wordt beschreven dat de maatregelen om het beveiligingsniveau te waarborgen ook het vermogen om de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen omvat (Europese Unie, 2016). De beschreven technische en organisatorische maatregelen in de GDPR verordening kunnen bij een ISO 27001 gecertificeerde organisatie samen worden gevoegd in het managementsysteem voor informatiebeveiliging. De uitgangspunten van de ISO 27001 standaard komen overeen met enkele gewichtige bepalingen uit de GDPR verordening. Met ISO 27001 certificatie voldoet een organisatie al voor een zeer groot deel aan de GDPR bepalingen. Artikel 42 van de GDPR beschrijft dat een organisatie door het aantonen van een "data beschermingscertificaat" aan de GDPR wordt voldaan. Het voldoen aan het op de juiste wijze verwerken en bewaren van gevoelige en vertrouwelijke data hebben ISO 27001 en de GDPR in de kern gemeenschappelijk. Echter zijn er ook verschillen tussen beide standaarden. De GDPR is een wereldwijde standaard met een strategische visie hoe organisaties met data privacy moeten omgaan. ISO 27001 bestaat uit een reeks van beste praktijkervaringen

rondom informatiebeveiliging. Anders dan de GDPR dekt het niet de aspecten geassocieerd met dataprivacy zoals; het geven van toestemming; dataportabiliteit; recht van vergetelheid; het recht om verwerking te beperken; het recht om te reclameren en internationaal overdracht van persoonlijke data (Lopes, Guarda, & Pedro, 2019).

GDPR factoren voor een succesvol implementatieproject

Voor een succesvol dataprivacyproject is het noodzakelijke voorwaarde dat de juiste technische procedures binnen het budget worden geïmplementeerd, echter indien de verwerkersverantwoordelijke geen juist beeld van de projectuitkomsten heeft omdat deze afdeling wordt beïnvloed door een concurrent of omdat sommige procedures illegaal zijn dan kan het project wellicht worden beschouwd als een mislukking. De perceptie van de betrokken partijen is een belangrijk deel van project succes. Projectsucces kan niet alleen worden gemeten over de drie conventionele aspecten; tijd, budget en scope (vanuit de binnenkant bezien) maar ook door het behalen van de organisatie doelstellingen en de voordelen die het over verschillende periodes zal brengen voor de stakeholders (vanuit de buitenkant bezien). Organisaties moeten zich aanpassen om rekening te houden met de vereiste verandering. Zij moeten zich versterken en hun structuur verbeteren om zo de GDPR eisen te integreren. De redenen als wel projectsucces als ook de relatie van de redenen met projectsucces moeten worden gedefinieerd. Een succesvol project moet vanuit de binnenkant als vanuit de buitenkant van een organisatie worden bekeken. (Costa, Silva, Moehring, & de Almeida, 2018) Vanwege de toenemende druk van externe stakeholders hebben organisaties diverse verschillende standaarden overgenomen en voor elke standaard een apart management systeem geïmplementeerd. In de toekomst is het bijna zeker dat stakeholders eisen dat additionele standaarden worden overgenomen en dat de bestaande standaarden worden ge-update. Vanwege het groeiend aantal managementsysteemstandaarden is de enige manier om voordeel te halen is door het integreren van alle standaarden binnen één geïntegreerd managementsysteem (IMS) (Hoy & Foley, 2015). Indirect beschrijft lid 1 en 2 van artikel 24 van de GDPR dit ook: De passende technische en organisatorische maatregelen moeten door de verwerkingsverantwoordelijke worden geëvalueerd en indien nodig worden geactualiseerd" en "er dient een passend gegevensbeschermingsbeleid door de verwerkingsverantwoordelijke te worden uitgevoerd" (Europese Unie, 2016, p. 47). Niet alle artikelen van de GDPR verordening scheppen duidelijkheid. Volgens het onderzoek van Prestus et al. hebben vele Noorse bedrijven aangegeven dat zij moeite hebben in het begrijpen van de bepalingen rondom financiële sancties (Prestus, Sorum, & Andersen, 2018). Dit komt ook in het onderzoek van Koops naar voren. Hoe dient bijvoorbeeld artikel 23 geïnterpreteerd te worden zodat het voor dataverwerkersverantwoordelijken toegepast en uitvoerbaar kan worden? In plaats van het richten op het naleven van de regels bij het integraal invoeren van data beschermingseisen tijdens de systeemontwikkeling is het waardevoller om te focussen op een grondige naleving. Het verkrijgen van de juiste mindset bij de verantwoordelijken voor de ontwikkeling en beheer van de dataverwerkingssystemen is productiever dan het naleven van de regels aan de hand van technische maatregelen. Artikel 23 van de GDPR; beperkingen dient dan ook niet gelezen te worden als een procedurele eis om databeschermingsregels zoveel mogelijk in het systeemontwerp te integreren maar als een grondige eis richting databeheerders om privacy consistent in hun gedachten mee te nemen bij het definiëren van systeemeisen. Het creëren van een verschuiving in de gedachtengoed van organisaties die op grote schaal persoonsgegevens verwerken is niet iets dat kan worden gerealiseerd door een bepaling in een Europese verordening. Artikel 40 van de GDPR; gedragscodes is in lijn met deze gedachtengoed. Om gegevensbescherming door ontwerp ("Privacy by Design; PbD") in de praktijk te krijgen dienen de wettelijke verordeningsorganen zich niet zoveel te focussen om technische specificaties op te stellen maar te focussen in het bedenken van andere soorten van regelgeving die de gedachten van de institutionele betrokkenen, in plaats van computers, bereiken (Koops & Leenes, 2014). Volgens de GDPR is het toegestaan dat een informatiesysteem toegang heeft tot gevoelige data en zo nodig mag beheren om de functionaliteiten van het systeem uit te kunnen oefenen met gegevensbescherming door ontwerpprincipes. Tools die helpen om te checken hoe sensitieve data wordt verwerkt door een softwaresysteem kan een belangrijk middel worden voor de nakoming van GDPR. Statische analyse als "privacy enhancing technology" (PET) kan worden toegepast in de

gegevensbescherming door ontwerp benadering om aan de GDPR te voldoen. Statische analyse programma's worden al jaren toegepast. Met het oog of organisaties GDPR grondig of symbolisch hebben geïmplementeerd is het toepassen van statische analyse tooling een determinant binnen het onderzoek (Ferrara & Spoto, 2018). Prestus et al. beargumenteert dat er 11 primaire artikelen zijn die invloed hebben op de IT systemen van een organisatie en haar datamanagement. Deze 11 artikelen worden in tabel 4 weergegeven.

Artikel nummer	Artikelnaam	Artikelbeschrijving
5	Beginselen inzake verwerking van persoonsgegevens	Persoonsgegevens moeten rechtmatig, behoorlijk en transparant worden verwerkt en alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld.
7	Voorwaarden voor toestemming	U kunt te allen tijde uw toestemming eenvoudig intrekken.
15	Recht van inzage van de betrokkene	U kunt een bevestiging vragen of uw persoonlijke dat wel of niet zal worden verwerkt.
17	Recht op gegevenswissing („recht op vergetelheid")	U heeft het recht dat uw persoonsgegevens uit de organisatie wordt verwijderd.
20	Recht op overdraagbaarheid van gegevens	U heeft het recht om uw persoonlijke data te ontvangen en deze voor uw eigen doeleinden te gebruiken. Het stelt u in staat om uw persoonlijke data te verplaatsen, te kopiëren of over te hevelen van de ene naar de andere IT omgeving op een veilige manier.
22	Geautomatiseerde individuele besluitvorming, waaronder profilering	U heeft het recht om niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking gebaseerd besluit. (zonder tussenkomst van de mens).
25	Gegevensbescherming door ontwerp en door standaardinstellingen	De verwerkingsverantwoordelijke moet ervoor zorgen dat alleen persoonsgegevens worden verwerkt die noodzakelijk zijn voor elk specifiek doel van de verwerking.
30	Register van de verwerkingsactiviteiten	De verwerkingsverantwoordelijke moet een register van de verwerkingsactiviteiten bijhouden die onder zijn verantwoordelijkheid plaatsvindt zoals de naam en contactgegevens van de verwerkingsverantwoordelijke, eventuele gezamenlijke verwerkingsverantwoordelijke en van de functionaris voor gegevensbescherming.
32	Beveiliging van de verwerking	De verwerkingsverantwoordelijke moet de omvang van de beveiligingsmaatregelen beoordelen en een risicobeoordeling uitvoeren.
33	Melding van een inbreuk in verband met persoonsgegevens aan de toezichthoudende autoriteit	De verwerkingsverantwoordelijke meldt een breuk in verband met persoonsgegevens binnen 72 uur aan de toezichthoudende autoriteit.
37	Aanwijzing van de functionaris voor gegevensbescherming	De verwerkingsverantwoordelijke moeten een functionaris voor gegevensbescherming aanwijzen indien de verwerking wordt verricht door een overheidsinstantie of in de commerciële sector indien stelselmatig op grote schaal persoonsgegevens worden verwerkt.

Tabel 4
Overzicht 11 artikelen Prestus et al.

Voorbeelden van aanpassingen op systemen zijn websites zoals het weergeven van gedetailleerde informatie over cookies en de opt-out mogelijkheid. De GDPR brengt niet alleen uitdagingen voor een organisatie maar ook voordelen. Uitdagingen bijvoorbeeld rondom het verkrijgen van budget, het verkrijgen van de vereiste technologie, het begrijpen van alle GDPR artikelen, het inzetten van de juiste middelen en de hoeveelheid werk die GDPR met zich meebrengt. Maar ook voordelen zoals het opschonen van data; het verwijderen van data en data consistent maken. Andere voordelen om te voldoen aan de GDPR verordening dat het leidt tot tevreden klanten en concurrentievoordeel. Prestus et al. geeft aan dat bij het toepassen van GDPR elke organisatie haar processen en routines dient aan te passen en velen dienen hun systemen aan te passen of systemen aan te schaffen (Prestus, Sorum, & Andersen, 2018).

2.4. Conclusies van het theoretisch kader

Gedurende het wetenschappelijke literatuuronderzoek in 2019 is er geen informatie gevonden over de implementatiekwaliteit van de GDPR. Er zijn geen officiële richtlijnen beschikbaar die bepalen of een organisatie de GDPR grondig heeft geïmplementeerd.

2.4.1. Wat wordt onder kwaliteit verstaan?

Kwaliteit is een maat voor overeenkomst tussen prestatie en verwachting, met andere woorden komen de eigenschappen van een product of dienst overeen met wat ervan verwacht wordt. Op de eenvoudigste manier dient kwaliteit twee vragen te beantwoorden: ‘wat wordt er gevraagd?’ en ‘hoe doen we het?’ (Straker).

2.4.2. Determinanten die een grondig kwaliteitsmanagement implementatieproject bepalen

De 14 principes van Deming is het fundament voor het TQM systeem die op hun beurt de basis vormen voor de ISO richtlijnen zoals het voortdurend meten en verbeteren. Vin beschrijft dat een gedegen planning en betrokkenheid in alle lagen kritische succesfactoren zijn voor het inbeddingsproces van een integraal ISO managementsysteem. Het moet zichtbaar zijn dat de maatregelen in de organisatieprocessen zijn geïntegreerd en dat het management bij de implementatie betrokken is. Volgens de principes van Deming is leiderschap de sleutel tot het creëren van een kwaliteitsomgeving.
Voor een grondige implementatie is het waardevoller en productiever om eerst te focussen op de juiste mindset bij de verantwoordelijken voor de ontwikkeling en beheer van dataverwerkingssystemen dan het naleven van de regels aan de hand van maatregelen volgens Koops et al. Ook Braughton geeft aan dat de output van medewerkers het hoogst is indien betrokkenheid van de medewerkers plaats vindt voordat met een totaal kwaliteitsmanagementsysteem wordt gestart.

2.4.3. Verschillen tussen een grondige en symbolische ISO implementatie

Volgens de institutionele theorie wordt een grondige implementatie gerealiseerd door normatieve vergelijkbaarheid. Bij grondige implementaties van ISO systemen zorgen bedrijven ervoor dat zij beter hun doelstellingen zoals productiviteitsverbetering, concurrentieverbetering en winstgevendheid realiseren. De hoofdredenen voor een symbolische ISO implementatie komen voort uit een dwingende en nabootsende institutionele druk. Organisaties falen in het integreren van werkwijzen in de dagelijkse operaties en gaan voor legitimiteitsredenen in tegenstelling tot efficiencyredenen. De bevindingen van Iatridis et al. geven aan dat er geen verschil is tussen midden- en kleine organisaties ten opzichte van grote organisaties als het gaat om het nemen van de sociale verantwoordelijkheid en het implementeren van de gerelateerde gecertificeerde managementsystemen.

2.4.4. Minimale eisen voor het implementeren van de GDPR

Aan het voldoen aan de GDPR eisen kan simpel worden voldaan beschrijft Calabro et al. door een bepaald data management systeem aan te schaffen die aan de GDPR eisen voldoet en door het leveren van de benodigde informatie en bewijsstukken. Een bevoegde auditorganisatie kan dit als bewijs van nakoming accepteren. Dit is een voorbeeld van een symbolische implementatie door een dwingende institutionele druk.

2.4.5. Het beantwoorden van de hoofdonderzoeksvraag

Door het extracteren van de antwoorden op de vier deelvragen verkrijgt de onderzoeker op basis van het theoretisch kader een basisantwoord op de hoofdonderzoeksvraag:

"*Hebben ISO-gecertificeerde organisaties een grondige GDPR-implementatiestrategie dan niet-ISO-gecertificeerde organisaties?*"

Met de impact van GDPR op de bestaande systemen en processen zoals Prestus et al. aangeeft is het aannemelijk dat ook een GDPR implementatie te vergelijken is met de implementatie van een kwaliteitssysteem echter in hoeverre het een complex en moeilijk proces is zoals Hietschold et al. het beschrijft bij het implementeren van een TQM kwaliteitsmanagementsysteem is niet bekend. In ieder geval kunnen de bevindingen van Hietschold et al. om kritieke succes factoren te bepalen en te meten meegenomen worden als belangrijke voorwaarde om het GDPR implementatieproces te controleren en de kansen op een grondige GDPR implementatie te verhogen. De voornaamste determinanten die als verband kunnen dienen of de GDPR grondig is geïmplementeerd zijn; medewerkersparticipatie, betrokkenheid van het seniormanagement en integratie met de operationele processen met kwaliteitsverbeteringstappen zoals bijvoorbeeld het toepassen van de Deming-cirkel om de processen die de GDPR bepalingen raken continu te verbeteren. Hiervoor is het toepassen van een geïntegreerd managementsysteem voor het beheren van processen, maatregelen en voor het behalen van organisatiedoelstellingen essentieel. Verder is een duidelijke aantoonbaarheid in het voldoen aan de bepalingen van de GDPR verordening belangrijk; bijvoorbeeld het tonen hoe de organisatie het gedrag van haar medewerkers en management beïnvloedt om de GDPR verordening na te leven, een gedetailleerde beschrijving van de professionele kwaliteiten en deskundigheid op het gebied van de wetgeving en de praktijk inzake gegevensbescherming door de functionaris voor gegevensbescherming, de genomen maatregelen zoals het beheren van websites met gedetailleerde en duidelijke informatie over cookies, privacy beleid en opt-out regelingen.

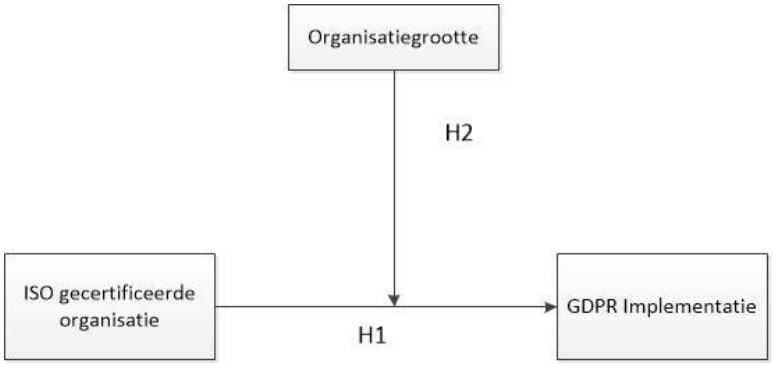
2.5. Doel van het vervolgonderzoek

Het doel van het vervolgonderzoek is minimaal het selecteren van die GDPR bepalingen die overeenkomen met de determinanten voor een grondige GDPR implementatie en de privacy statements van de geselecteerde organisaties hierop toetsen. De basis van de geselecteerde determinanten betreffen de primaire artikelen van Prestus et al. en artikel 40 die door Koops et al. als belangrijkste determinant wordt beschreven. Eveneens bevatten de artikelen van Prestus et al. ook enkele GDPR bepalingen die door Lopes et al. zijn aangeduid die door ISO 27001 niet worden ondervangen. Verder dienen de openbare bronnen te worden onderzocht of en welk ISO certificaat de organisatie bezit. Daarnaast moet de bedrijfsgrootte worden onderzocht om in het vervolgonderzoek te bepalen of de kwaliteit van de GDPR implementatie hieraan is gerelateerd. Tijdens het vervolgonderzoek dient er vergelijkend naar de implementatiekwaliteit tussen ISO- en niet-ISO-gecertificeerde organisaties te worden gekeken en niet op een abstracte manier.

2.5.1. Conceptueel model

Voor het beantwoorden van de vraagstelling is alle publieke informatie over de GDPR van een organisatie, de eventuele ISO-certificeringen en de organisatiegrootte nodig. Het kwaliteitsniveau van de GDPR implementatie wordt op basis van meetbare factoren gerelateerd aan de GDPR richtlijnen gemeten. Een organisatie voldoet wel of niet aan een GDPR bepaling, idem voor het bepalen van ISO-certificatie; een organisatie heeft wel of geen ISO-certificering. De organisatiegrootte wordt aan de hand van het aantal medewerkers gemeten. In hoofdstuk 3 wordt de methodiek verder toegelicht.

Aan de hand van de hoofdonderzoeksvraag en het theoretische kader is het conceptueel model opgesteld.



Figuur 1 Conceptueel model

2.5.2. Hypotheses

Op basis van het conceptueel model worden twee hypotheses gedefinieerd:

1. Hypothese 1: ISO-gecertificeerde organisaties hebben een grondige GDPR implementatie gerealiseerd dan niet-ISO-gecertificeerde organisaties.
2. Hypothese 2: Grote ISO-gecertificeerde organisaties hebben een grondiger GDPR implementatie gerealiseerd dan kleine ISO-gecertificeerde organisaties.

3. Methodologie

In dit hoofdstuk wordt de conclusie van het theoretische kader verwoord naar de onderzoeksmethode. Het type onderzoek, de stappen tijdens als het doel van het onderzoek wordt nader toegelicht. De hoofdonderzoeksvraag, uitgedrukt in een conceptueel model dient als basis voor het technisch ontwerp. In het technisch ontwerp wordt de operationalisatie van de variabelen verduidelijkt. Als laatste wordt gereflecteerd op validiteit, betrouwbaarheid en ethiek.

3.1. De onderzoeksmethode

3.1.1. Kwantitatief versus kwalitatief onderzoek

In het selecteren van onderzoeksmethoden zijn er twee keuzes; kwantitatief of kwalitatief. Kwantitatief onderzoek heeft betrekking op deductie (hypothesetoetsing) waarbij een omvangrijke hoeveelheid numerieke data verzameld wordt om statistisch verbanden aan te tonen. Hiermee kan in een kort tijdbestek data verzameld worden van vele organisaties. Bij kwalitatief onderzoek ligt de nadruk op inductie (hypothesevorming) en dient de data verzameld te worden door het uitvoeren van (semi) gestructureerde interviews, observaties en het analyseren van verwante documenten. Privacy en Security vraagstukken zijn delicate onderwerpen en het is de vraag in hoeverre medewerkers openheid gaan geven over dit onderwerp. Zijn de antwoorden dan wel betrouwbaar en valide, rekening houdend met het aantal medewerkers per bedrijf en hun beschikbaarheid tijdens de beknopte tijd van het empirisch onderzoek en worden wel alle verwante documenten beschikbaar gesteld?

Rekening houdend met de beschikbare tijd van 4 maanden (September 2019 t/m December 2019) om valide en betrouwbare data te kunnen verzamelen en te analyseren en de mogelijkheid om ervaringen tijdens het onderzoek met andere studiegenoten te delen is voor een kwantitatief onderzoek gekozen.

3.1.2. De stappen tijdens het onderzoek

De volgende stappen zijn gemaakt tijdens het onderzoek:

1) Pilotfase
    a. Enkele websites en aanverwante bronnen zoals LinkedIn pagina's analyseren om te bepalen welke bronnen de meeste en juiste informatie kan verstrekken
2) Het selecteren van Nederlandse bedrijven
3) Het verzamelen van de volgende gegevens, voornamelijk via de website van de organisatie:
    a. ISO-certificatie type.
    b. Privacy-bepalingen.
4) Het voornamelijk via de website, de LinkedIn pagina van de organisatie of via de Kamer van Koophandel verzamelen van:
    a. De bedrijfsgrootte uitgedrukt in aantal medewerkers.
5) Naar aanleiding van het theoretisch onderzoek het selecteren van:
    a. De juiste AVG bepalingen en aantal AVG bepalingen voor een betrouwbaar onderzoek om de grondigheid van de GDPR implementatie te kunnen beoordelen (zie tabel 5 in bijlage 2).
6) Het transformeren van de AVG bepalingen naar dummy variabelen
7) Het analyseren en vastleggen van de ISO-certificeringen.
8) Het transformeren van de ISO-certificeringen naar dummy variabelen.
9) Het analyseren van de privacy statements en deze toetsen met de geselecteerde AVG bepalingen.
10) Het via de website en de LinkedIn pagina van de organisatie verzamelen van:
    a. Aanwezigheid van een functionaris gegevensbescherming binnen een organisatie.

b. De competenties van de functionaris gegevensbescherming van de organisatie.
11) Het vastleggen van het voldoen aan de individuele AVG bepalingen per organisatie.
12) Het totaliseren van het aantal ISO-certificeringen per organisatie.
13) Het vastleggen aan de hand van een dummy variabele of de organisatie wel of niet ISO gecertificeerd is.
14) Het totaliseren van het aantal AVG bepalingen per organisatie waaraan wordt voldaan.
15) Het analyseren van de populatie of er een juiste verhouding is tussen wel en niet ISO-gecertificeerde organisaties.
16) Initiële statistische analyse, beschrijvende statistiek, uitvoeren m.b.v. SPSS software
17) Het aanpassen van de populatie om aan de hand van de mediaan een beter evenwicht te krijgen in het aantal organisaties met verschillende bedrijfsgroottes.
18) Aanvullende literatuuronderzoek.
19) Vervolg statistische analyse m.b.v. SPSS software.
20) Conclusies trekken.

De onafhankelijke variabelen ISO en niet-ISO gecertificeerd en bedrijfsgrootte zijn op nagenoeg alle bedrijfswebsites zichtbaar. De afhankelijk variabele over de GDPR implementatiekwaliteit dient op elke organisatiewebsite en openbare documenten zoals privacy statements ook zichtbaar te zijn. Artikel 7 van de GDPR verordening; voorwaarden voor toestemming beschrijft dat voor het verwerken van persoonsgegevens het verzoek tot toestemming in een begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal gepresenteerd moet worden.

Type organisatie

Het type organisatie die onderzocht zijn betreffen Nederlandse organisaties. Deze organisaties hebben een werknemersaantal die varieert van midden-klein (=<250 medewerkers) tot groot (= 10.000 medewerkers).

Populatiegrootte casus

Om een valide en betrouwbaar onderzoek uit te voeren zijn minimaal 80 te onderzoeken bedrijven als doelstelling voor de populatiegrootte gedefinieerd, waarvan ongeveer de helft van de organisaties minimaal een ISO certificaat bezitten. De populatiegrootte van Nederlandse ISO-gecertificeerde bedrijven is met de aanwezige openbare bronnen en de beschikbare tijd niet te achterhalen.

Iteratief proces

Het onderzoek is een iteratief proces; van literatuuronderzoek naar onderzoeksmethode en weer naar literatuuronderzoek om de onderzoeksmethode met het literatuuronderzoek te onderbouwen. Tijdens een pilotfase zijn organisaties onderzocht hoe zij de GDPR bepalingen via hun openbare bronnen naar hun stakeholders communiceren. Op basis van de uitkomsten zijn het aantal organisaties bepaald die in het onderzoek worden meegenomen en dat voornamelijk de privacy statements als primaire bron is geselecteerd Na de eerste analyse van de data en het feit dat het onderzoek een jaar verder is, heeft de onderzoeker via Google Scholar en EBSCO verder gezocht naar recente literatuur met de zoekwoorden; ISO 27001 AND GDPR compliance en met de zoekwoorden; GDPR AND Certification om aanvullende informatie te verkrijgen op het beantwoorden van de deelonderzoeksvragen "*Wat zijn de verschillen tussen een symbolische en een grondige implementatie van ISO?*" en "*Wat zijn de minimale eisen voor het implementeren van de GDPR?*" Voornamelijk de documenten "What GDPR Tells About Certification" van Lachaud en "Implementation of ISO 27001 Standards as GDPR Compliance Facilitator" geven aanvullende informatie en zijn als bron toegevoegd. Zie bijlage 1; tabel 3 voor een overzicht van aanvullende documenten.

3.1.3. Doel onderzoek

Het doel van dit deel van het onderzoek is om op basis van de literatuurstudie over de implementatiekwaliteit van aanverwante standaarden aan de GDPR (zie tabel 5) meer

duidelijkheid te krijgen over de implementatiekwaliteit van de GDPR bij Nederlandse organisaties. Door het verzamelen van data tijdens het empirisch onderzoek bij voornamelijk ISO 9001, ISO 27001 en/ of ISO 14001 gecertificeerde organisaties en niet-ISO-gecertificeerde organisaties in verschillende bedrijfsgroottes en het statistisch analyseren van deze data vanuit verschillende invalshoeken wordt inzicht verkregen in de implementatiekwaliteit van GDPR tussen ISO- en niet-ISO-gecertificeerde organisaties.

3.2. Technisch ontwerp

Met het meenemen van organisaties die minimaal één ISO certificaat bezitten probeert de onderzoeker de twee hypothesen te onderbouwen. Als kapstok voor de geselecteerde GDPR bepalingen worden de artikelen van Prestus et al. in de basis, met de bevindingen van Koops toegepast. Om het doel te bereiken dienen de kwalitatieve afhankelijke- en onafhankelijke variabelen geoperationaliseerd te worden. De operationalisatie wordt aan de hand van dummy variabelen (0 of 1) uitgevoerd.

3.2.1. Afhankelijke variabele Voldoet_aan_AVG

Om de GDPR implementatiekwaliteit te bepalen dienen er voldoende organisaties en voldoende AVG gerelateerde variabelen per organisatie te worden verzameld. Hiervoor zijn er 25 stellingen geselecteerd. Deze 25 stellingen zijn gerelateerd aan 25 van totaal 607 bepalingen uit 13 van totaal 99 artikelen van de GDPR verordening. Elke stelling met het gerelateerde artikel wordt in tabel 5 (zie bijlage 2) weergegeven. Komt de beschrijving van een AVG bepaling overeen met de beschrijving in het privacy statement van de organisatie dan scoort deze organisatie op deze AVG bepaling een JA, de organisatie voldoet aan de AVG op deze specifieke bepaling en de overeenkomstige dummy variabele krijgt de waarde “1”.

Per organisatie wordt de totale score van de 25 AVG bepalingen berekent en wordt de score van de bepalingen per artikel berekent (zie tabel 6) zodat uit twee invalshoeken de relatie kan worden onderzocht tussen ISO- en niet-ISO-gecertificeerde organisatie met de GDPR implementatiekwaliteit.

Variabele Naam	Variabele definitie	Variabele waarde Voldoet_aan_AVG	Max. te behalen score
Voldoet aan AVG	Totaal van de 25 AVG bepalingen	Aantal JA's	25
Voldoet aan Artikel 5	Totaal van de bepalingen van AVG artikel 5 waaraan wordt voldaan	Aantal JA's	3
Voldoet aan Artikel 7	Totaal van de bepalingen van AVG artikel 7 waaraan wordt voldaan	Aantal JA's	2
Voldoet aan Artikel 12	Totaal van de bepalingen van AVG artikel 12 waaraan wordt voldaan	Aantal JA's	2
Voldoet aan Artikel 13	Totaal van de bepalingen van AVG artikel 13 waaraan wordt voldaan	Aantal JA's	2
Voldoet aan Artikel 15	Totaal van de bepalingen van AVG artikel 15 waaraan wordt voldaan	Aantal JA's	2
Voldoet aan Artikel 17	Totaal van de bepalingen van AVG artikel 17 waaraan wordt voldaan	Aantal JA's	2
Voldoet aan Artikel 20	Totaal van de bepalingen van AVG artikel 20 waaraan wordt voldaan	Aantal JA's	1
Voldoet aan Artikel 25	Totaal van de bepalingen van AVG artikel 25 waaraan wordt voldaan	Aantal JA's	1
Voldoet aan Artikel 30	Totaal van de bepalingen van AVG artikel 30 waaraan wordt voldaan	Aantal JA's	2
Voldoet aan Artikel 32	Totaal van de bepalingen van AVG artikel 32 waaraan wordt voldaan	Aantal JA's	2
Voldoet aan Artikel 33	Totaal van de bepalingen van AVG artikel 33 waaraan wordt voldaan	Aantal JA's	1
Voldoet aan Artikel 37	Totaal van de bepalingen van AVG artikel 37 waaraan wordt voldaan	Aantal JA's	2
Voldoet aan Artikel 40	Totaal van de bepalingen van AVG artikel 40 waaraan wordt voldaan	Aantal JA's	3

Tabel 6
Overzicht te behalen score per variabele als basis voor het onderzoek

Per onderzochte organisatie wordt het aantal JA's en NEE's per bepaling geteld. Hoe hoger het aantal JA's bij het totaal van de 25 AVG bepalingen hoe grondiger de GDPR implementatie is uitgevoerd, hoe meer de organisatie voldoet aan de AVG

Voorbeeld: Een organisatie die 17 scoort op de 25 AVG bepalingen heeft een grondiger GDPR implementatie uitgevoerd dan een organisatie die een score van 14 haalt.

Om een bevestiging te krijgen van de GDPR implementatiekwaliteit over 25 AVG bepalingen wordt ook een vergelijk gemaakt hoe ISO en niet-ISO-gecertificeerde organisaties scoren per AVG artikel.

Voorbeeld: Indien dezelfde organisatie een 3 scoort op het AVG artikel 40 doordat deze organisatie voldoet aan alle drie geselecteerde AVG bepalingen van dit artikel en de andere organisatie scoort hier 0 dan heeft de onderzoeker de bevestiging dat deze organisatie op dit specifieke artikel deze bepalingen grondiger heeft geïmplementeerd. Indien deze verschillen de verhouding weergeeft tussen ISO-gecertificeerde organisaties en niet-ISO-gecertificeerde organisaties dan kan worden geconcludeerd dat ISO-gecertificeerde organisaties dit specifieke artikel grondiger hebben geïmplementeerd.

3.2.2. Onafhankelijke variabele ISO-certificatie

Om te achterhalen of een organisatie ISO gecertificeerd is moet de website van de organisatie onderzocht worden op hun ISO certificaten. De organisatielegitimiteit door ISO-certificering wordt veelal via logo's en keurmerken van de auditor op de website van de gecertificeerde organisatie kenbaar gemaakt. Een ISO-gecertificeerde organisatie wordt in het dataoverzicht gekenmerkt door de variabele-naam ISO_JA. De variabele ISO_JA krijgt de waarde "1" indien de organisatie één of meerdere ISO certificaten bezit, de dummy variabele krijgt de waarde "0" indien de organisatie geen ISO-certificatie bezit. Zie tabel 7 voor verdere uitleg.

Variabele definitie	**Variabele-waarde**
De organisatie is ISO gecertificeerd	ISO_JA = 1
De organisatie is NIET gecertificeerd	ISO_JA = 0

Tabel 7
Overzicht definitie ISO variabelen

3.2.3. Onafhankelijke variabele bedrijfsgrootte

Het bepalen van de bedrijfsgrootte wordt gedaan op basis van aantal werknemers en kan worden verkregen door het kamer van koophandel register of de website van de organisatie te raadplegen.

3.2.4. Gegevensanalyse

Het conceptueel model wordt getest met behulp van een lineare regressie. Lineaire regressie wordt toegepast om met de variabelen "ISO_JA" en "Bedrijfsgrootte" de GDPR implementatiekwaliteit te verklaren via een lineair verband. De GDPR implementatiekwaliteit wordt met de variabele "Voldoen_aan_AVG" weergegeven. De te verzamelen gegevens worden aan de hand van de statistische analyse software SPSS geanalyseerd.

De regressievergelijking

De regressievergelijking is: Voldoen aan AVG = C + B1 * ISO_JA + B2 * Bedrijfsgrootte + B3 * (ISO_JA * Bedrijfsgrootte)

"Voldoen aan AVG" is de afhankelijke variabele , ISO_JA en Bedrijfsgrootte zijn de onafhankelijke variabelen. C is hierbij een constante en de B's zijn de regressiecoëfficiënten.

Minimale uitgangspunten regressieberekening

Bij het berekenen van de regressie dienen aan diverse punten voldaan te worden waarvan (multi-) collineariteit wel de belangrijkste is. Indien twee of meer onafhankelijke (verklarende) variabelen in een regressiemodel sterk gecorreleerd zijn dan is de invloed van beide variabelen op de afhankelijke variabele dusdanig dat de berekening van de regressie coëfficiënten van de variabelen niet meer stabiel is (Saunders, Lewis, & Thornhil, 2016, p. 548). Indien collineariteit wordt aangetroffen dan is er aanvullende analyse nodig om de impact van de onafhankelijke variabelen te verklaren.

3.3. Reflectie t.a.v. validiteit, betrouwbaarheid en ethische aspecten

De literatuur van Saunders en de premaster managementwetenschappen zijn de basis voor de methodologische reflectie. Het onderzoek is een combinatie van verklarend en beoordelend. Een verklarend onderzoek is een waardevol middel om de relatie tussen variabelen te verklaren. In dit onderzoek is het verklaren van de relatie van de onafhankelijke variabele “ISO-gecertificeerde organisatie” met de verklarende variabele “implementatiekwaliteit van de GDPR” en de modererende variabele “organisatiegrootte” essentieel. Een beoordelend onderzoek binnen bedrijven en management heeft meer betrekking op het onderzoeken van de effectiviteit van een bedrijfsstrategie, beleid, programma, initiatieven of processen. In dit onderzoek is het onderzoeken naar de effectiviteit van het privacy-beleid en de gerelateerde processen belangrijk. Door deze beoordelende studie wordt niet alleen de nadruk gelegd op ‘hoe effectief’ iets is maar ook ‘waarom’ zodat de uitleg vergelijken kan worden met de bestaande theorie (Saunders, Lewis, & Thornhil, pp. 175, 176). Door het raadplegen van de openbare bronnen zoals de website van elke organisatie, hun privacyverklaring, de LinkedIn pagina van de organisatie en van de medewerkers van de organisatie en jaarverslagen, indien beschikbaar wordt veel kwantitatieve onderzoek data verkregen. In de volgende paragrafen wordt beschreven wat sterk en wat zwak is aan deze reflectie en in welke categorie de validiteitsprincipes van Yin (2009) vallen. Validiteit is volgens Yin te onderscheiden in vier criteria; constructvaliditeit, interne validiteit, externe validiteit en betrouwbaarheid (Gelderman, 2013, p. 12).

3.3.1. Interne betrouwbaarheid

Interne betrouwbaarheid refereert aan het zorgen van consistentie gedurende het onderzoeksproject. Dit kan worden gerealiseerd door meer dan één onderzoeker op het onderzoeksproject te zetten om de data te analyseren, deze data samen te evalueren en consensus over de data-analyse te verkrijgen. Daarnaast kan consistentie verder worden verkregen door regelmatig notities te maken om de stabiliteit aan te tonen bij het coderen van de data, het analyseren van de data en het interpreteren hiervan.

Betrouwbaarheid wordt ook verkregen door het toepassen van triangulatie. Triangulatie omvat dat meer dan één databron en methoden van verzamelen worden toegepast om de validiteit/kredietwaardigheid/authenticiteit van de onderzoeksdata, analyses en de invulling te bevestigen (Saunders, Lewis, & Thornhil, 2016, p. 207).

Sterk

Door bij elke te onderzoeken organisatie dezelfde kenmerken over de minimale eisen voor een grondige GDPR implementatie en dezelfde type bronnen te analyseren wordt voldaan aan het interne betrouwbaarheidsprincipe. Dezelfde aanpak zal zorgen voor consistente waarnemingen indien deze aanpak door dezelfde onderzoekers herhaald worden of door andere onderzoekers worden toegepast; externe betrouwbaarheidsprincipe (Saunders, Lewis, & Thornhil, 2016, p. 202)

Zwak

Het toetsen van de gevonden antwoorden uit één openbare bron draagt niet bij aan het triangulatieprincipe waardoor de interne betrouwbaarheid zwak is.

3.3.2. Externe betrouwbaarheid

Externe betrouwbaarheid refereert aan replicatie. Indien de aanpak door dezelfde onderzoekers herhaald worden of door andere onderzoekers worden uitgevoerd dan dienen de waarnemingen consistent te zijn; Er wordt voldaan aan de externe betrouwbaarheidsprincipe (Saunders, Lewis, & Thornhil, 2016, p. 202)

Sterk

Door bij elke te onderzoeken organisatie dezelfde kenmerken over de minimale eisen voor een grondige GDPR implementatie en dezelfde type bronnen te analyseren zal de aanpak zorgen voor consistente waarnemingen indien deze aanpak door dezelfde onderzoeker herhaald worden of door andere onderzoekers worden toegepast.

Zwak

Doordat één persoon het onderzoek uitvoert is de kans op vooringenomenheid groot. De mate van objectiviteit kan groter worden bij het nauwkeurig analyseren van de data en het operationaliseren van deze data. Daarnaast is de totale populatie van het onderzoek niet bekend waardoor de sample van de te onderzoeken bedrijven niet representatief is.

3.3.3. Planning

Sterk

In de periode van September 2019 t/m December 2019 is het empirisch onderzoek uitgevoerd. Er is een duidelijke scope van de termijn waarin het empirisch onderzoek moet plaats vinden en waar tijd voor het onderzoek kan worden gereserveerd.

Zwak

Rekening houdend met de dagelijkse werkzaamheden en de verantwoordelijkheden vanuit mijn functie wordt de planning soms door de waanzin van de dag achterhaald. Om dit risico te minimaliseren zal er voldoende speling in de planning gehouden worden.

3.3.4. Interne validiteit

Interne validiteit wordt verkregen indien het onderzoek een causale relatie tussen twee variabelen duidelijk weergeeft. Er dienen geen andere verklaringen mogelijk te zijn. (Saunders, Lewis, & Thornhil, 2016, p. 203). Interne validiteit refereert ook aan het vermogen van het onderzoek om te meten wat de onderzoeker als intentie heeft om te meten (Saunders, Lewis, & Thornhil, 2016, p. 450).

Sterk

De interne validiteit is sterk als de onderzoeker elke gedefinieerde variabele die per organisatie wordt geuit via de openbare bronnen op dezelfde manier wordt geïnterpreteerd. (Saunders, Lewis, & Thornhil, 2016, p. 451)

Zwak

In de oorzaak-gevolg relatie tussen de variabelen “ISO-gecertificeerde organisaties” en “GDPR implementatiekwaliteit” is het aannemelijk dat de GDPR implementatiekwaliteit ook afhankelijk kan zijn van een andere variabele. Tijdens het onderzoek is er geen tijd om het tegendeel te bewijzen.

3.3.5. Externe validiteit

Bij de externe validiteit gaat het om de generaliseerbaarheid van de onderzoeksresultaten (Gelderman, 2013, p. 13). Externe validiteit wordt omgeven door de vraag: Kunnen de bevindingen van het onderzoek worden gegeneraliseerd naar andere relevante omgevingen of groepen (Saunders, Lewis, & Thornhil, 2016, p. 204)?

Sterk

Door het uitvoeren van het onderzoek bij een groot aantal organisaties en door de geselecteerde organisaties te classificeren wordt voldaan aan de externe validiteit. Indien tijdens een soortgelijk

onderzoek de bovenstaande punten worden meegenomen bij andere organisaties dan zal de conclusie van het onderzoek nagenoeg dezelfde uitkomsten vertonen.

Zwak

Een soortgelijk onderzoek uitvoeren in een ander land of in een andere branche met andere externe invloeden kan ervoor zorgen dat de bevindingen niet generaliseerbaar zijn.

3.3.6. Ethiek

Ethiek verwijst naar gedragsstandaarden die zorgen voor de houding van de onderzoeker in relatie met de rechten van diegene die onderdeel van het onderzoekwerk uitmaakt of die wordt beïnvloed door het onderzoek. De toepasselijkheid van het gedrag van de onderzoeker wordt beïnvloed door een breed perspectief van sociale gedragsnormen (Saunders, Lewis, & Thornhil, 2016, pp. 239-240). De onderzoeker heeft integriteit en zorgvuldigheid hoog in zijn vaandel. De grote verscheidenheid aan originele bronnen, de tijd die wordt genomen om de analysetechnieken van het statistische software programma SPSS te doorgronden, het verfijnen van het onderzoeksrapport door aanvullende relevante literatuur na de initiële data-analyse te lezen en als bron toe te voegen aan het onderzoeksrapport bewijzen dit.

4. Resultaten

Gesteund door de gehanteerde methodiek wordt in dit hoofdstuk de geanalyseerde data weergegeven aan de hand van de beschrijvende statistiek en regressievergelijkingen. De onderzoeksdata is met behulp van het statistische computerprogramma SPSS geanalyseerd en de belangrijkste bevindingen worden in dit hoofdstuk aangestipt. Informatie over de data uit het SPSS programma wordt in bijlage 2 verduidelijkt.

4.1. Beschrijvende statistiek

De paragraaf beschrijvende statistiek geeft een overzicht van de populatie, met toelichting op de data-analyse van deze populatie vanuit verschillende invalshoeken. Eveneens wordt de betrouwbaarheid aan de hand van de univariate analyse getoetst alsmede de correlatie tussen de twee onafhankelijke variabelen.

4.1.1. Populatie

Initieel is de onderzoeker gestart met het analyseren van 87 organisaties. Binnen deze populatie hebben de meeste organisaties honderden tot enkele duizenden medewerkers echter enkele organisaties hebben meer dan tienduizend medewerkers; oplopend tot 375.000 waardoor deze organisaties invloed hebben op de standaard afwijking (Zie tabel 8 in bijlage 2).

In tabel 9 zijn de organisaties (6 totaal) met een bedrijfsgrootte van meer dan 10.000 medewerkers verwijderd waardoor de standaard deviatie nu evenwichtiger is geworden. Met deze populatie wordt de analyse vervolgt.

N = 81	ISO 9001	ISO 27001	ISO 14001	ISO 20000	ISO 55001	ISO_JA	Bedrijfsgrootte *
Minimum	0	0	0	0	0	0	20
Maximum	1	1	1	1	1	1	10.000
Gemiddelde	0,51	0,10	0,30	0,00	0,01	0,59	952,07
Mediaan	1	0	0	0	0	1	275,00
Std. Afwijking	0,503	0,300	0,459	0,000	0,111	0,494	1.770,21
Som	41	8	24	0	1	48	77.118

Tabel 9
Kenmerken van de onderzoekspopulatie (N = 81)
Opmerking: * Bedrijfsgrootte is uitgedrukt in aantal medewerkers

Van de 81 onderzochte organisaties is de helft ISO 9001 gecertificeerd. Procentueel gezien zijn er weinig verschillen met de populatie van 87. 48 organisaties hebben minimaal een ISO certificaat. De kleinste organisatie heeft 20 medewerkers en de grootste organisatie heeft 10.000 medewerkers. Voor de hypothese is uit gegaan dat een organisatie minimaal één ISO certificaat bezit; dit betreft de variabele ISO_JA. Een ISO 9001, ISO 27001, ISO 14001, ISO 55001 en/of ISO 20000 gecertificeerde organisatie wordt in het dataoverzicht ook gekenmerkt door de variabele ISO_JA. Binnen de populatie van 81 bedrijven is er één organisatie die ISO 55001 gecertificeerd is en geen organisatie met het ISO 20000 certificaat echter zijn beide organisaties wel ISO 9001 gecertificeerd.

25 van totaal 607 bepalingen uit 13 van totaal 99 artikelen van de GDPR verordening zijn geanalyseerd. In tabel 10 wordt het aantal organisaties die voldoen aan een bepaald aantal AVG bepalingen weergegeven. Het minimum aantal AVG bepalingen waar één of meerdere organisatie aan voldoen bedraagt 3; twee organisaties voldoen hieraan. Het maximum aantal AVG bepalingen waar één of meerdere organisaties aan voldoen bedraagt 19 (van de 25); één organisatie voldoet hieraan. De meeste organisaties voldoen aan 8 tot 15 AVG bepalingen Het gemiddelde aan AVG bepalingen waaraan organisaties voldoen ligt net onder de 11 AVG bepalingen.

Aantal vooraf geselecteerde AVG bepalingen waaraan wordt voldaan door één of meerdere organisaties	Aantal organisaties die voldoen aan het aantal vooraf geselecteerde AVG bepalingen
3	2
4	5
5	3
6	2
7	2
8	7
9	9
10	6
11	8
12	15
13	8
14	8
15	3
16	1
17	1
19	1

Tabel 10
Onderzoekspopulatie uitgedrukt in aantal organisaties die voldoen aan een bepaald aantal vooraf geselecteerde AVG artikelen

Grafiek 1 in bijlage 2 geeft de verdeling weer tussen bedrijfsgrootte en het aantal ISO-certificeringen per bedrijfsgrootte. Hier valt op dat vier, voornamelijk grote bedrijven, 3 ISO certificaten bezitten. Grafiek 2 in bijlage 2 toont de verdeling tussen bedrijfsgrootte en wel of geen ISO-certificering per bedrijfsgrootte. De verdeling bij de midden- en klein bedrijven tussen wel en niet ISO gecertificeerd is nagenoeg gelijk. Dit geldt ook bij grafiek 3 waar de bedrijfsgrootte wordt afgezet tegen wel of niet ISO 9001 gecertificeerde bedrijven omdat het overgrote deel van de ISO-gecertificeerde organisaties ISO 9001 zijn gecertificeerd.

Tabel 11 geeft een overzicht van het aantal ISO-certificatie 's van organisaties die minimaal ISO 27001 zijn gecertificeerd. Vier organisaties bezitten zowel het ISO 27001 als ISO 9001 certificaat. Vanuit het perspectief van ISO 27001 gecertificeerde organisaties; ongeveer 10% van de onderzochte organisaties, blijkt dat de maximum score met betrekking tot het voldoen aan AVG artikelen 15 is. Daarnaast valt op dat organisaties met een ISO 27001 certificaat en met meer ISO certificaten nog minder scoren. Vanwege de kleine populatie aan ISO 27001 gecertificeerde organisaties kunnen geen conclusies worden getrokken ten aanzien van de mate van de GDPR implementatie bij ISO 27001 gecertificeerde organisaties.

ISO 27001 gecertificeerd	ISO 9001 gecertificeerd	ISO 14001 gecertificeerd	Totaal aantal ISO certificaten	Aantal AVG bepalingen waaraan wordt voldaan
JA	JA	JA	3	5
JA	JA	JA	3	11
JA	JA	JA	3	12
JA	NEE	NEE	1	12
JA	NEE	NEE	1	12
JA	NEE	NEE	1	13
JA	JA	NEE	2	14
JA	NEE	NEE	1	15

Tabel 11
Onderzoekspopulatie uitgedrukt in aantal ISO-gecertificeerde organisaties die minimaal ISO 27001 zijn gecertificeerd

In tabel 12 wordt het aantal organisaties weergegeven die de functie functionaris voor gegevensbescherming in hun privacy statement beschrijven. Dit is het geval bij ongeveer 40% van de onderzochte organisaties. Indien specifiek wordt beoordeeld of de professionele kwaliteiten van de functionaris voor gegevensbescherming zijn beschreven dan blijkt dat geen enkele organisatie dit in haar privacy statement benoemd (zie tabel 13).

Beschrijving: De functie functionaris voor gegevensbescherming wordt duidelijk weergegeven	**Aantal**
voldoet niet aan AVG	50
voldoet aan AVG	31

Tabel 12
Voldoet aan artikel 37 van de GDPR: Aanwijzing van de functionaris voor gegevensbescherming

Beschrijving: De professionele kwaliteiten van de functionaris voor gegevensbescherming zoals het bezitten van kennis, kunde en ervaring in wetgeving en/of, persoonsgegevens bescherming wordt duidelijk weergegeven	**Aantal**
voldoet niet aan AVG	81
voldoet aan AVG	0

Tabel 13
Voldoet aan artikel 37 , lid 5 van de GDPR: Aanwijzing van de functionaris voor gegevensbescherming - De professionele kwaliteiten van de functionaris voor gegevensbescherming zoals het bezitten van kennis, kunde en ervaring in wetgeving en/of, persoonsgegevens bescherming wordt duidelijk weergegeven.

4.1.2. Univariate analyse

Met de univariate toets; onafhankelijke t-toets voor gelijkheid van gemiddelden wordt de betrouwbaarheid getoetst tussen een afhankelijke en onafhankelijke variabele. Tabel 14 in bijlage 2 geeft per individuele afhankelijke AVG variabele de betrouwbaarheid weer met de onafhankelijke variabele ISO_JA.

Niet alleen wordt het verband over betrouwbaarheid geanalyseerd tussen de afhankelijke variabele "Voldaan aan de AVG" met de onafhankelijk variabele "ISO_JA". Ook wordt geanalyseerd op de 13 afzonderlijke AVG bepalingen om het verband aan te tonen tussen het bezitten van minimaal één ISO certificaat en de GDPR-implementatiestrategie van organisaties. Bij een score van Sig (2-tailed) hoger dan 0,05 is er geen significant verband tussen elke individuele afhankelijke variabele met de onafhankelijk variabele ISO_JA. Elke Sig (2-tailed) waarde geeft aan dat er geen significant verband is tussen het bezitten van minimaal één ISO-certificering en er geen significant verband is tussen het bezitten van minimaal één ISO-certificering en het voldoen aan de 13 individuele AVG bepalingen. Om te bepalen of er een significant verband is tussen de bedrijfsgrootte en ISO-certificering op de implementatiestrategie van de GDPR wordt met de Pearson correlatie dit verband bepaald (Tabel 15)

Correlatie (N = 81)		**ISO_JA**	**Bedrijfsgrootte**
ISO_JA	Pearson Correlatie	1	,044
	Sig. (2-tailed)		,696
Bedrijfsgrootte	Pearson Correlatie	,044	1
	Sig. (2-tailed)	,696	

Tabel 15
Het verband tussen de grootte van een organisatie en ISO-certificering op de implementatiestrategie (N = 81)

Opmerking: ** De correlatie is significant op het niveau van 0,05 (2-tailed)

De uitkomst is: n = 81, r = ,044; p = ,696; n = 81.
De correlatie is voor 81 organisaties berekend. Deze groep is groot genoeg. De Pearson correlatie is 0,044 en is een zwakke, positieve correlatie. Uit de toets blijkt dat deze correlatie niet significant is, want de p-waarde (.696) is groter dan α (.05).

4.2. Regressievergelijkingen

de paragraaf regressievergelijkingen beschrijft de multicollineariteit en de regressievergelijkingen vanuit verschillende invalshoeken; met en zonder de onafhankelijke variabelen ISO 9001, ISO 27001, ISO_JA, Bedrijfsgrootte en met en zonder de modererende variabele ISO_JA en Bedrijfsgrootte. Op basis van het conceptueel model wordt in deze paragraaf vanuit verschillende invalshoeken de significantie tussen de onafhankelijk en afhankelijke variabelen nogmaals bepaald en worden de analyses van vijf verschillende lineaire regressievergelijkingen weergegeven en de toelichting beschreven.

4.2.1. Regressievergelijking met onafhankelijke variabele ISO_JA

Tabel 16 geeft de waarden weer indien de onafhankelijke variabele ISO_JA in het onderzoek wordt meegenomen. 48 Organisaties hebben minimaal één ISO-certificering.

Coëfficiënten [a]					
	Niet gestandaardiseerde coëfficiënten		**Gestandaardiseerde coëfficiënten**		
	B	**Std. fout**	**Bèta**	**t**	**Sig.**
(Constante)	9,946	,570		17,439	,000
ISO_JA	,819	,749	,117	1,093	,278
a. Afhankelijke variabele: Voldaan aan AVG artikel					

Tabel 16
Regressievergelijking met onafhankelijke variabele ISO_JA

De regressiecoëfficiënt ISO_JA = 0,819 en geeft de gemiddelde toename in het voldoen aan AVG aan wanneer ISO_JA met 1 toeneemt.

De regressievergelijking is:

Voldoen aan AVG = 9,946 + 0,819 * ISO-JA

De uitkomst komt overeen met de waarden gegeven in tabel 10 bij “Voldoet aan AVG”; respectievelijk ISO_JA = 10,77 en ISO_NEE = 9,94.

Bij ISO_JA = 1 wordt de waarde Voldoen aan AVG van de regressievergelijking gelijk aan 10,765. Bij ISO_JA = 0 wordt de waarde van de regressievergelijking gelijk aan 9,946 (waarde in tabel 10 bij ISO_NEE is gelijk aan 9,94).

Het significante cijfer Sig = 0,278 en is hoger dan 0,05. Er is geen significante relatie tussen de onafhankelijke variabele ISO_JA met de afhankelijke variabele.

4.2.2. Regressievergelijking met onafhankelijke variabele ISO 9001

Tabel 17 geeft de waarden weer indien de onafhankelijke variabele ISO_9001 in het onderzoek wordt meegenomen. 48 Organisaties hebben minimaal één ISO-certificering waarvan 41 organisaties ISO 9001 gecertificeerd zijn.

Coëfficiënten [a]					
	Niet gestandaardiseerde coëfficiënten		Gestandaardiseerde coëfficiënten		
	B	Std. fout	Bèta	t	Sig.
(Constante)	10,450	,544		19,223	,000
ISO 9001	-,035	,764	-,005	-,046	,963
a. Afhankelijke variabele: Voldaan aan AVG artikel					

Tabel 17
Regressievergelijking met onafhankelijke variabele ISO 9001

De regressiecoëfficiënt ISO 9001 = -,035 en geeft de gemiddelde afname in het voldoen aan AVG aan wanneer ISO 9001 met 1 toeneemt.

De regressievergelijking is:

Voldoen aan AVG = 10,450 - 0,035 * ISO 9001

Het significante cijfer Sig = 0,963 en is hoger dan 0,05. Er is geen significante relatie tussen de onafhankelijke variabele ISO 9001 met de afhankelijke variabele.

4.2.3. Regressievergelijking met onafhankelijke variabele ISO 27001

Tabel 18 geeft de waarden weer indien de onafhankelijke variabele ISO_27001 in het onderzoek wordt meegenomen. 48 Organisaties hebben minimaal één ISO-certificering waarvan 8 organisaties ISO 27001 gecertificeerd zijn.

Coëfficiënten [a]					
	Niet gestandaardiseerde coëfficiënten		Gestandaardiseerde coëfficiënten		
	B	Std. fout	Bèta	t	Sig.
(Constante)	10,288	,399		25,779	,000
ISO 27001	1,462	1,270	0,128	1,152	,253
a. Afhankelijke variabele: Voldaan aan AVG artikel					

Tabel 18
Regressievergelijking met onafhankelijke variabele ISO 27001

De regressiecoëfficiënt ISO 27001 = 1,462 en geeft de gemiddelde toename in het voldoen aan AVG aan wanneer ISO 27001 met 1 toeneemt.

De regressievergelijking is:

Voldoen aan AVG = 10,288 + 1,462 * ISO 27001

Het significante cijfer Sig = 0,253 en is hoger dan 0,05. Er is geen significante relatie tussen de onafhankelijke variabele ISO 27001 met de afhankelijke variabele.

4.2.4. Regressievergelijking met de onafhankelijke variabelen ISO_JA en bedrijfsgrootte en zonder de modererende variabele

In tabel 19 worden de waarden weergegeven indien de onafhankelijke variabele ISO_JA en bedrijfsgrootte maar zonder de modererende variabele in het onderzoek worden meegenomen.

Coëfficiënten [a]					
	Niet gestandaardiseerde coëfficiënten		**Gestandaardiseerde coëfficiënten**		
	B	**Std. fout**	**Bèta**	**t**	**Sig.**
(Constante)	9,907	,626		15,820	,000
ISO_JA	,825	,777	0,119	1,062	,292
Bedrijfsgrootte	3,807E-5	,000	0,020	,175	,861
a. Afhankelijke variabele: Voldaan aan AVG artikel					

Tabel 19
Regressie vergelijking met onafhankelijke variabele ISO_JA , Bedrijfsgrootte en zonder de modererende variabele

De regressiecoëfficiënt ISO_JA = 0,825 en geeft de gemiddelde toename in het voldoen aan AVG aan wanneer ISO_JA met 1 toeneemt.

De regressiecoëfficiënt Bedrijfsgrootte = 3,807 E-5 en geeft de gemiddelde toename in het voldoen aan AVG aan wanneer Bedrijfsgrootte met 1 toeneemt.

De regressievergelijking is:

Voldoen aan AVG = 9,907 + 0,825 * ISO_JA + 3,807 E-5 * Bedrijfsgrootte

De grootte van het effect van de bedrijfsgrootte is beduidend kleiner dan de grootte van het effect van ISO_JA op de afhankelijke variabele.

Het significante cijfer Sig = 0,292 en is hoger dan 0,05. Er is geen significante relatie tussen de onafhankelijke variabelen met de afhankelijke variabele.

4.2.5. Regressie vergelijking met de modererende variabele

In tabel 20 worden de waarden weergegeven indien de onafhankelijke variabele ISO_JA en Bedrijfsgrootte en de modererende variabele in het onderzoek worden meegenomen.

Coëfficiënten [a]					
	Niet gestandaardiseerde coëfficiënten		Gestandaardiseerde coëfficiënten		
	B	Std. fout	Bèta	t	Sig.
(Constante)	9,876	,705		14,000	,000
ISO_JA	,879	,957	0,127	,918	,362
Bedrijfsgrootte	3,602E-5	,000	0,019	,164	,870
Moderator	,112	1,161	,013	,096	,923
a. Afhankelijke variabele: Voldaan aan AVG artikel					

Tabel 20
Regressie vergelijking met de modererende variabele

De regressiecoëfficiënt ISO_JA = 0,879 en geeft de gemiddelde toename in het voldoen aan AVG aan wanneer ISO_JA met 1 toeneemt.

De regressiecoëfficiënt Bedrijfsgrootte = 3,602 E-5 en geeft de gemiddelde toename in het voldoen aan AVG aan wanneer Bedrijfsgrootte met 1 toeneemt.

De regressiecoëfficiënt Moderator = 0,112 en geeft de gemiddelde toename in het voldoen aan AVG aan wanneer de Moderator met 1 toeneemt.

De moderator = ISO_JA * Bedrijfsgrootte

De regressievergelijking is:

Voldoen aan AVG = 9,876 + 0,879 * ISO_JA + 3,602 E-5 * Bedrijfsgrootte + 0,112 * Moderator

De grootte van het effect van de bedrijfsgrootte is beduidend kleiner dan de grootte van het effect van de Moderator alsook van ISO_JA op de afhankelijke variabele.

Het significante cijfer Sig = 0,362 en is hoger dan 0,05. Er is geen significante relatie tussen de onafhankelijke variabelen met de afhankelijke variabele.

4.2.6. Multicollineariteit

Om te bepalen of onafhankelijke variabelen een dusdanige collineariteit op elkaar uitoefenen dat deze collineariteit effect heeft op de afhankelijke variabele dient een multicollineariteitstoets uitgevoerd te worden. De resultaten van de multicollineariteitstoets wordt in tabel 21 weergegeven.

Coëfficiënten [a]							
	Niet gestandaardiseerde coëfficiënten		**Gestandaar-diseerde coëfficiënten**			**Collineaire statistieken**	
	B	**Std. fout**	**Bèta**	**t**	**Sig.**	**Tolerantie**	**VIF**
(Constante)	9,907	,626		15,820	,000		
ISO_JA	,825	,777	0,119	1,62	,292	,998	1,002
Bedrijfsgrootte	3,807E-5	,000	0,020	,175	,861	,998	1,002
a. Afhankelijke variabele: Voldaan aan AVG artikel, N = 81							

Tabel 21
Multicollineariteit ISO_JA op Bedrijfsgrootte

Indien de VIF score lager is dan 10 dan is er geen samenhang. Tabel 21 geeft een VIF score weer lager dan 10, tussen de onafhankelijke variabelen ISO_JA en bedrijfsgrootte is geen samenhang; Er is geen multicollineariteit tussen deze twee onafhankelijke variabelen.

5. Conclusie, discussie, reflectie en aanbevelingen

De geanalyseerde data van het vorige hoofdstuk is de basis om conclusies te trekken, een discussie op gang te brengen, naast het literatuuronderzoek en de gehanteerde methodiek hierop te reflecteren en aanbevelingen te kunnen doen voor de praktijk en voor verder onderzoek. Hier wordt in het laatste hoofdstuk uitvoerig op ingegaan.

5.1. Conclusies

Op de hoofdonderzoeksvraag; "*Hebben ISO-gecertificeerde organisaties een grondige GDPR-implementatiestrategie dan niet-ISO-gecertificeerde organisaties?*" kan na het analyseren van de resultaten worden geconcludeerd dat er geen verband is tussen een grondige GDPR implementatie en organisaties met en zonder ISO-certificering. Zowel hypothese 1; "ISO-gecertificeerde organisaties hebben een grondige GDPR-implementatiestrategie dan niet-ISO-gecertificeerde organisaties" als hypothese 2; "Grote ISO-gecertificeerde organisaties hebben een grondiger GDPR implementatie dan kleine ISO-gecertificeerde organisaties"; op basis van het conceptueel model kunnen met de bevindingen niet onderbouwd worden. Op basis van de gemiddelde score op het voldoen aan de GDPR bepalingen kan worden geconcludeerd dat de meeste organisaties de GDPR symbolisch hebben geïmplementeerd. Naast het analyseren van het verband tussen de organisaties met minimaal één ISO-certificering en het voldoen aan de 25 geselecteerde AVG bepalingen is ook een analyse uitgevoerd tussen organisaties met minimaal één ISO certificaat en elk van de dertien afzonderlijke AVG artikelen. Ook hier worden de beide hypothesen niet onderbouwd. De modererende variabele bedrijfsgrootte heeft verder geen invloed op het voldoen aan de AVG. Van de 48 organisaties die minimaal één ISO certificaat bezitten zijn er 41 organisaties die ISO 9001 gecertificeerd zijn. Verder is er een analyse uitgevoerd op het verband tussen minimaal ISO 27001 gecertificeerde organisaties en het voldoen aan de AVG. Zowel voor ISO 9001 als ISO 27001 gecertificeerde organisaties is er geen onderbouwing van beide hypothesen gevonden. De conclusie komt overeen met het onderzoek van Persha; De toegevoegde waarde van ISO27001 op GDPR compliance (Pershad, 2018). Op de onderzoeksvraag "*Inzichtelijk krijgen wat de overeenkomsten zijn tussen de ISO/IEC 27001 normenkader en AVG.*" kan worden vastgesteld dat het simpelweg gecertificeerd zijn of op basis van ISO27001 niet voldoende is om compliant te zijn met de GDPR eisen.

5.2. Discussie

Voor het versterken van de interne validiteit zijn de privacy statements van de verschillende organisaties op de 25 GDPR bepalingen door één persoon; de analist en niet de onderzoeker geanalyseerd. De data is samen met de onderzoeker geëvalueerd zodat consensus en consistentie over de data-analyse is verkregen. Om te voldoen aan de externe validiteit is de toegepaste methode; het raadplegen van diverse bronnen en bij het analyseren het leggen van relaties vanuit verschillende invalshoeken tussen het voldoen aan de GDPR en/of op basis van individuele GDPR bepalingen met minimaal één of meerdere ISO-gecertificeerde ondernemingen om tot deze éénduidige conclusie te komen betrouwbaar en generaliseerbaar. Een soortgelijk onderzoek kan worden uitgevoerd bij andere organisaties en/of bij andere organisaties in andere landen wordt voldaan een de externe validiteit. De resultaten komen op basis van mijn verwachtingen en het literatuuronderzoek niet overeen. De verwachting was dat bedrijven met een mimimaal een ISO-certificering een grondige GDPR implementatie hadden uitgevoerd dan bedrijven zonder ISO-certificering omdat het gros van de bedrijven minimaal ISO 9001 gecertificeerd zijn en volgens het conferentierapport van Tzolov is het ISO 9001:2015 raamwerk een basis voor een GDPR implementatie. Een verklaring van een symbolische GDPR implementatie kan zijn dat de ISO-gecertificeerde ondernemingen hun GDPR implementatie door bijvoorbeeld geen betrokkenheid en leiderschap van het management hebben uitgevoerd zoals Heras et al. hebben aangetoond bij ISO 9000 implementaties en deze organisaties soortgelijk de GDPR hebben geïmplementeerd. De resultaten impliceren dat het geen verschil maakt of een organisatie ISO gecertificeerd is en één of

meerdere ISO certificaten bezit als het gaat om de kwaliteit van de GDPR implementatie. De Nederlandse gegevensbeschermingsautoriteit Autoriteit Persoonsgegevens of een geaccrediteerde ISO-certificatie-instelling kan er niet van uitgaan dat een ISO 9001 en een organisatie met minimaal een ISO certificaat de GDPR grondig heeft geïmplementeerd.

5.3. Reflectie

In deze paragraaf wordt gereflecteerd op het literatuuronderzoek, op de gehanteerde onderzoeksmethodologie en op de onderzoeksuitkomsten. Om de juiste richtlijnen te verkrijgen voor een grondige GDPR implementatie was vanuit de literatuur de informatie rondom grondige en symbolische implementaties bij ISO 14001 gecertificeerde ondernemingen en de kritische succesfactoren om TQM grondig te implementeren het meest bruikbaar, de informatie van Prestus et al. gaf de onderzoeker een houvast om de juiste GDPR bepalingen te selecteren. Al met al is er voldoende literatuur geraadpleegd echter is er te weinig literatuur beschikbaar over het grondig implementeren van de GDPR. Kijkend naar de beschikbare tijd en het feit dat een kwantitatief onderzoek naar de kwaliteit van GDPR implementatie nog niet was uitgevoerd heeft het kwantitatieve onderzoek met de gehanteerde analysemethodiek de juiste inzichten verschaft in de GDPR implementatiekwaliteit. Het meenemen van meer ISO 27001 gecertificeerde ondernemingen had het onderzoek nog betrouwbaarder gemaakt. De onderzoeksuitkomsten bieden voldoende inzichten om met relevante aanbevelingen te komen. Voor de totstandkoming van de uitkomsten is na de initiële analyse van de data wederom literatuur geraadpleegd waarna vanuit meerdere invalshoeken gekeken is naar de relatie van GDPR implementatiekwaliteit en de mate van ISO-certificatie waardoor op de juiste manier gebruik is gemaakt van de theorie en de onderzoeksmethoden. Voor de onderzoeker persoonlijk heeft het onderzoek voldoende inzichten verschaft rondom het grondig implementeren van kwaliteitssystemen en specifiek het implementeren en managen van een grondige GDPR.

5.4. Aanbevelingen voor de praktijk

De onderzoeker karakteriseert drie praktijkaanbevelingen evenwel geldt voor alle drie aanbevelingen dat het management focus blijft houden op het gedrag van alle betrokkenen zoals Koops et al. in zijn onderzoek heeft waargenomen. Het integreren van de GDPR binnen een innovatief ondersteunend IMS systeem bij een ISO 9001 of ISO 27001 gecertificeerde organisatie is de eerste aanbeveling voor een grondige GDPR implementatie. Zowel ISO 9001 als ISO 27001 kan volgens respectievelijk Tzolov en Lopes et al. als een goede basis worden toegepast om te voldoen aan de GDPR. Beide certificeringen vereisen het toepassen van een Informatie Management Systeem (IMS). Hoy et al. geeft aan dat vanwege het groeiend aantal managementsysteemstandaarden de enige manier om voordeel te halen is door het integreren van alle standaarden binnen één geïntegreerd informatie managementsysteem (IMS). Met behulp van een geïntegreerd IMS, het meten van kritieke succes factoren en medewerkersparticipatie volgens Hietschold et al. wordt het beleid ISO 9001 en/ of ISO 27001 continu verbeterd. Het GDPR beleid lift hierop mee waardoor de GDPR implementatie hetzelfde niveau van kwaliteit verkrijgt als dat van een ISO 9001 of ISO 27001 implementatie; synergie voordelen. De tweede praktijkaanbeveling voor een grondige GDPR implementatie betreft het toekennen van een GDPR certificatieregeling op een geïmplementeerd GDPR IMS systeem door een certificatie-instelling die geaccrediteerd is door de Raad voor Accreditatie (Accreditatie, 2018) bij organisaties die geen ISO 9001 en/ of ISO 27001 certificering bezitten. Calabro et al. geeft aan dat het toepassen van een bepaald data management systeem (DMS) die voldoet aan de GDPR eisen en door het leveren van de benodigde informatie en bewijsstukken aan een bevoegde auditorganisatie, deze auditorganisatie dit als bewijs van nakomen van de GDPR kan accepteren echter voor een grondig inbeddingsproces dient het management door de certificatie-instelling worden gewezen op een gedegen planning en betrokkenheid van alle lagen voor een zoals Vin in haar bevindingen heeft beschreven. De laatste aanbeveling voor de praktijk slaat op het privacy statement. Het openbare privacy statement dient zo beschreven te worden dat expliciet door de stakeholders kan worden gelezen aan welke GDPR bepalingen wordt voldaan, hoe hieraan wordt voldaan en hoe grondig de GDPR is

geïmplementeerd. Het privacy statement dient expliciet die determinanten te beschrijven die staan voor een grondige GDPR implementatie. Een voorbeeld is het beschrijven van de competenties die de functionaris gegevensbescherming bezit en wie deze functie vervuld. Ook dient gedetailleerd beschreven te worden welke organisatorische- en technische maatregelen door de organisatie zijn genomen, dat de organisatie expliciet beschrijft wat men onder kwaliteit verstaat en dat de organisatie haar GDPR beleid en de maatregelen continu verbeterd volgens PDCA. Dit sluit aan bij de informatie over TQM beleid en over het implementeren van TQM en ISO kwaliteitsmanagementsystemen; waarbij het een continu verbeterproces betreft. In dit perspectief past een quote van één van de respondenten in het onderzoek van Prestus et al.: "***Complying with GDPR is not a goal to be reached, it is the start of a journey***".

5.5. Aanbevelingen voor verder onderzoek

Door de beperkte tijd en resources heeft de onderzoeker niet voldoende organisaties kunnen selecteren die ISO 27001 gecertificeerd zodat de relatie van specifiek ISO 27001 gecertificeerde ondernemingen op het voldoen aan de GDPR bepalingen niet kon worden onderzocht. Een overzicht in aantallen van Nederlandse gecertificeerde ISO organisaties was via openbare bronnen niet te achterhalen en dus ook niet de verhouding tussen ISO 27001 gecertificeerde organisaties. Daarnaast zijn er meerdere factoren die invloed hebben op implementatiekwaliteit van de GDPR en niet onderzocht konden worden. Op basis van de literatuur en dit onderzoek met als doel dat de GDPR grondig wordt geïmplementeerd worden vier aanbevelingen voorgesteld. Een vervolgonderzoek zou zich kunnen focussen op het kwantitatief onderzoeken van ISO 27001 gecertificeerde organisaties op de implementatiekwaliteit van de GDPR omdat volgens Lopes et al. een ISO 27001 gecertificeerde organisatie al voor een zeer groot deel voldoet aan de GDPR bepalingen. De tweede aanbeveling betreft het verbeteren van de interne validiteit van dit onderzoek. In de oorzaak-gevolg relatie tussen de variabelen "ISO-gecertificeerde organisaties" en "GDPR implementatiekwaliteit" is het aannemelijk dat de GDPR implementatiekwaliteit ook afhankelijk kan zijn van andere variabelen. Een vervolgonderzoek naar andere variabelen die impact uitoefenen op de GDPR implementatiekwaliteit wordt aanbevolen. Het derde advies raakt de artikelen 42 en 43 van de GDPR. Hoe moet een databeschermingscertificering worden opgesteld zodat derde partijen die geaccrediteerd zijn door de Raad voor Accreditatie volgens de EN-ISO/IEC 17065 (Accreditatie, 2018) een audit kunnen uitvoeren en een overeenkomstig certificaat mogen uitgeven. In dit verdere onderzoek kan ook rekening worden gehouden met de specifieke behoeften van kleine, middelgrote en micro-ondernemingen zoals in sub 1 van artikel 42 van de GDPR wordt aangegeven. Met de bevindingen uit dit onderzoek en de bevindingen van Tzolov en Lopes et al. met betrekking tot het feit dat respectievelijk ISO 9001 en ISO 27001 een basisraamwerk bevatten voor het voldoen aan de GDPR is de vierde en laatste aanbeveling om te onderzoeken welk concept opgesteld moet worden om de ISO 9001 en ISO 27001 gecertificeerde IMS systemen en managementprocessen dusdanig te transformeren dat het voldoen aan de GDPR richtlijnen dezelfde implementatiekwaliteit kan bereiken als de implementatiekwaliteit van ISO 9001 en ISO 27001 en hierbij rekening houdend met het veranderingsproces van de betrokken actoren en de beschikbare middelen in tijd en geld.

6. Referenties

Accreditatie, R. v. (2018, Juni 28). *AVG-certificatie*. Opgehaald van Raad voor Accreditatie: https://www.rva.nl/nieuws/2018/avg-certificatie

Aravind, D., & Christman, P. (2011). *Declouping of standard implementation from certification: Does quality of ISO 14001 implementation affect facilities environmental environment performance?* New York: CUNY Academic Works.

Aravind, D., & Christman, P. (2017). *Institutional and resource baed determinants of substantive implementation of ISO 14001*. Academy of Management.

Aravind, D., & Christmann, P. (2007, November 30). Substantive versus symbolic implementation of ISO 14001: The role of corporate headquarters. *Academy of Management*, 9.

Baars, H., Hintzbergen, J., Hintzbergen, K., & Smulders, A. (2015). *Basiskennis informatiebeveiliging op basis van ISO27001 en ISO27002*. Amersfoort: Van Haren Publishing.

Bemelmans, T. (1994). *Bestuurlijke informatiesystemen en automatisering* (Zesde herziene druk, tweede oplage ed.). Deventer: KLuwer Bedrijfswetenschappen.

Boiral, O. (2007). Corporate greening through ISO 14001: a rational myth? *Organization Science*, 127-146.

Braughton, W. (1999). Edwards Demings Profound Knowledge and Individual Psychology. *Journal of Individual Psycholgy*, p. 449.

Briggs, S. L. (2017). ISO 14001:2015 Environmental Management Systems. *A practical guide for SMEs*. Genevè, Zwitserland: ISO. Opgehaald van https://www.iso.org/files/live/sites/isoorg/files/store/en/iso_14001_guide_preview.pdf

Calabro, A., Daoudagh, S., & Marchetti, E. (2019). Integrating Access Control and Business Process for GDPR Compliance: A Preliminary Study. *Proceedings of the Third Italian Conference on Cyber Security* (pp. 1-14). Pisa: CEUR. Opgehaald van http://ceur-ws.org/Vol-2315/paper07.pdf

Chase, R. B., & Aquilano, N. J. (1995). *Production and Operations Management Manufacturing and Services* (7 ed.). USA: Irwin.

Chowdhury, M., Prajogo, D., & Jayaram, J. (2018, April 18). Comparing symbolic and substantive implementation of international standards – the case of ISO 14001 certification. *Australasian Journal of Environmental Management*, 339-361. Opgehaald van https://doi.org/10.1080/14486563.2018.1451402

Christman, P., & Taylor, G. (2006, 11). Firm self-regulation through international certifiable standards: determinants of symbolic versus substantive implementation. *Journal of International Business Studies*, 863-878. Opgehaald van http://www.jstor.org/stable/4540389

Costa, N. A., Silva, J., Moehring, M. M., & de Almeida, I. D. (2018). Definition of key drivers for project success regarding the General Data Protection Regulation (GDPR). *ResearchGate*, (p. 10).

Deming, W. E. (2000). *Out of the Crisis*. Cambridge, Massachusetts, USA: Massachusetts Institute of Technology, Center for Advanced Educational Services.

DiMaggio, P. J., & Powell, W. W. (1983, April). The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields. *American Sociological Review*, 147-160. Opgehaald van http://www.jstor.com/stable/2095101

Europese Unie. (2016). Verordening (EU) 2016/679 van het Europese parlement en de raad. Brussel: Europese Unie.

Ferrara, P., & Spoto, F. (2018). Static Analysis for GDPR Compliance. *Italian Conference on Cyber Security* (pp. 1-10). Milaan: CEUR. Opgehaald van http://ceur-ws.org/Vol-2058/paper-10.pdf

Gelderman, C. (2013). Wetenschappelijk onderzoek en de afstudeerscriptie. In *Premaster managementwetenschappen* (pp. 7-17). Heerlen: Open Universiteit.

Heras-Saizarbitoria, I., & Boiral, O. (2015). Symbolic adoption of ISO 9000 in small and medium-sized enterprises: The role of internal contingencies. *International Small Business Journal*, 22.

Hietschold, N., Reinhardt, R., & Gurtner, S. (2014, April 14). Measuring critical success factors of TQM implementation succesfully-a systematic literature review. *International Journal of Production Research*, 6254-6272.

Horine, J. E., Yvarra, P., & Lindgren, C. (1994). A philosophical and educational view of the theory contained in demings profound knowledge. (Eduction, Red.) *Education*(Vol 115, Issue 2), 290. Opgeroepen op Augustus 1, 2020

Hoy, Z., & Foley, A. (2015). A structured approach to integrating audits to create organisational efficiencies ISO 9001 and ISO 27001 audits. *Total Quality Management & Business Excellence*. Portsmouth, United Kingdom.

Iatridis, K., & Kesidou, E. (2018). What Drives Substantive Versus Symbolic Implementation of ISO 14001 in a Time of Economic Crisis? Insights from Greek Manufacturing Companies. *Journal of Business Ethics*, 859-877.

Iatridis, K., Kuznetsov, A., & Whyman, P. B. (2016). SMEs and Certified Management Standards: The Effect of Motives and Timing on Implementation and Commitment. *Business Ethics Quarterly*, 67-94. doi:10.1017/beq.2016.9

ISO Central Secretariat. (1997). *Friendship among equals.* Genève, Switzerland: ISO. Opgehaald van https://www.iso.org/files/live/sites/isoorg/files/about%20ISO/docs/en/Friendship_among_equals.pdf

Jankowski, D. (2006, Augustus). What can we learn from Deming>. *Mortgage Banking*, 94-99.

Koops, B.-J., & Leenes, R. (2014). Privacy regulation cannot be hardcoded. A critical comment on the privacy by design provision in data-protection law. *International Review of Law, Computers & Technologie*, 159-171.

Kumar, V., & Sharma, R. (2017, Januari 17). An empirical investigation of critical success factors influencing the successful TQM implementation for firms with different strategic orientation. *International Journal of Quality & Reliability Management*, 1530-1550. Opgehaald van https://doi.org/10.1108/IJQRM-09-2016-0157

Lachaud, E. (2020). *What GDPR Tells About Certification*. Tilburg Institute, Law, Technology, and Society. Tilburg: Home of Tilburg Institute for Law, Technology, and Society. Opgehaald van https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3557167

Looijen, M. (1995). *Beheer van informatiesystemen* (1e druk ed.). Deventer: Kluwer Bedrijfswetenschappen.

Lopes, I. M., Guarda, T., & Pedro, O. (2019, Augustus 22). Implementation of ISO 27001 Standards as GDPR Compliance Facilitator. *Journal of Information Systems Engineering & Management*.

Normalisatie-instituut, N. (2015, Oktober). NEN-EN-ISO 9001. *Kwaliteitsmanagementsystemen*. Delft: Nederlands Normalisatie-instituut.

Normalisatie-instituut, N. (2015, December). NEN-ISO/IEC 27001. *Informatietechnologie - Beveiligingstechnieken -Managementsystemen voor informatiebeveiliging*. Delft: Nederlands Normalisatie-instituut.

Perez-Batres, L. A., Doh, J. P., Miller, V. V., & Pisani, M. J. (2012, 8 21). Stakeholder Pressures as Determinants of CSR Strategic Choice: Why do Firms Choose Symbolic Versus Substantive Self-Regulatory Codes of Conduct? *J Bus Ethics*, 16.

Pershad, A. (2018). *The added value of ISO 27001 on GDPR compliance/De toegevoegde waarde van ISO27001 op GDPR compliance*. Heerlen: Open Universiteit.

Prestus, W., Sorum, H., & Andersen, L. R. (2018). GDPR compliance in Norwegian companies. *Proceedings from the annual NOKOBIT conference* (p. 15). Svalbard: Nokobit.

Saunders, M., Lewis, P., & Thornhil, A. (2016). *Research Methods for Business Students*. Harlow: Pearson.

Schermer, B. W., Hagenauw, D., & Falot, N. (sd). *Handleiding Algemene verordening gegevensbescherming en Uitvoeringswet Algemene verordening gegevensbescherming*. Ministerie van Justitie en Veiligheid.

Straker, D. (sd). What is Quality? *Quality World*. Opgehaald van http://syque.com/articles/what_is_quality/what_is_quality_1.htm

Tzolov, T. (2018). A model for implementation GDPR based on ISO standards. *Proceedings of the International Conference on Information Technologies (InfoTech-2018)*, (p. 6). Bulgaria.

Verburg, M., Stumpel, R., Aalbrecht, H., Bol, A., Parqui, J., Vollering, M., & de Smit, M. (Red.). (2009). *Van Dale Nederlands als tweede taal (NT2)*. Opgeroepen op Augustus 1, 2020, van Van Dale op school: https://www.vandale.nl/zoeken/opschool.do

Verordening (EU) 2016/679 van het Europese parlement en de raad. (2016, April 27). Brussel.

Vin, S. (2018). *Decoupling & Loose coupling bij het ISO certificeren*. Heerlen: Open Universiteit Nederland.

Waks, S., & Frank, M. (1999, September). Application of the Total Quality Management Approach Principles and the ISO 9000 Standards in Engineering Education. *Europea Journal of Engineering Education*, 249. doi:10.1080/03043799908923560

Bijlage 1

Deel vraag	NR	Zoekmethodes	Databronnen	Zoekwoorden	Resultaten	Uitleg
1	1	Er is gezocht binnen alle bronnen, document typen en alle talen tussen de gepubliceerde datum van 01-01-2018 tot/met 31-12-2019	Ebsco. Via Ebsco doorverwezen naar Google scholar	gdpr AND iso	11 (**Ebsco)**	Om informatie te verzamelen die betrekking heeft op deelvraag 2.
1	2	Er is gezocht op artikelen sinds 2018, gesorteerd op relevantie en in elke taal	Google scholar (geen resultaten bij EBSCO)	gdpr implementation drivers	1790	Om informatie te verzamelen die betrekking heeft op deelvraag 2. Artikel 3 op pagina 1 is geselecteerd; "Definition of key drivers for project success regarding the General Data Protection Regulation"
1	3	Er is gezocht op artikelen sinds 2018, gesorteerd op relevantie en in elke taal	Google scholar	GDPR implementation stakeholders	2800	Om informatie te verzamelen die betrekking heeft op deelvraag 2. In het artikel "Implementation of the General Data Protection Regulation: A Survey in Health Clinics" wordt een implementatiemethodiek beschreven. Dit artikel had plaats 7 op pagina 1 en werd door 5 anderen geciteerd
1	4	Er is gezocht binnen alle artikelen, document typen en alle talen tussen de gepubliceerde datum van 01-01-2016 tot/met 31-12-2018	Ebsco	determinants AND substantive implementation	2 waarvan 1 basisartikel ; "Firm self-regulation through international certifiable standards determinants of symbolic versus substantive implementation"	Om informatie te verzamelen die betrekking heeft op deelvraag 2. Beide artikelen zijn toegepast waarbij met het relevantste artikel; "Firm self-regulation through international certifiable standards determinants of symbolic versus substantive implementation" de forward snowball methode is toegepast
1	5	Er is gezocht binnen peer reviewed artikelen,	Ebsco	Symbolic AND adoption AND ISO	6	Om informatie te verzamelen die betrekking heeft op deelvraag 2

		document typen en alle talen tussen de gepubliceerde datum van 01-01-2015 tot/met 31-12-2018				
1	6	Er is gezocht op relevantie binnen peer reviewed artikelen, document typen en alle talen tussen de gepubliceerde datum van 01-01-2012 tot/met 31-12-2018	Ebsco	total quality management AND implementation AND critical success factors	51	Om informatie te verzamelen over deelvraag 2. 2 artikelen: "Measuring critical success factors of TQM implementation succesfully-a systematic literature review" en "An empirical investigation of critical success factors influencing the successful TQM implementation for firms with different strategic orientation" zijn geselecteerd
1	7	Er is gezocht op artikelen sinds 2018, gesorteerd op relevantie en in de Nederlandse taal	Google scholar	NEN-EN-ISO 9001:2015 ISO decoupling	31 Levert 4 artikelen op	Om informatie te verzamelen die betrekking heeft op deelvraag 2. Artikel van Vin is geselecteerd omdat hier expliciet nog onderzoek wordt gedaan naar decoupling bij ISO-certificering. decoupling" word in diverse literatuur in verband gebracht met symbolische implementatie en zodoende geeft dit artikel ook informatie over deelvraag 2
2	0	Er is gezocht binnen alle artikelen, document typen en alle talen tussen de gepubliceerde datum van 01-01-2016 tot/met 31-12-2018	Ebsco	Symbolic AND substantive implementation AND ISO	4 waar van 3 peer reviewed journals inclusief 1 basisartikel	Om informatie te verzamelen die betrekking heeft op deelvraag 3.
2	1	Er is gezocht binnen peer reviewed artikelen, document typen en alle talen tussen de gepubliceerde	Ebsco	Compliance AND privacy regulation AND Netherlands OR dutch OR holland	3	Om informatie te verzamelen die betrekking heeft op deelvraag 3.

		datum van 01-01-2014 tot/met 31-12-2018				
2	2	Er is gezocht binnen peer reviewed artikelen, document typen en alle talen tussen de gepubliceerde datum van 01-01-2013 tot/met 31-12-2018	Ebsco	Total quality management AND implementation AND process AND iso AND sme	4	Om informatie te verzamelen die betrekking heeft op deelvraag 3.
2	3	Er is gezocht binnen peer reviewed artikelen, document typen en alle talen tussen de gepubliceerde datum van 01-01-2012 tot/met 31-12-2018	Ebsco	Critical success factors AND implementing change	2	Om informatie te verzamelen die betrekking heeft op deelvraag 3.
3	1	Niet gezocht				Om informatie te verzamelen die betrekking heeft op deelvraag 4. De verordening EU 2016 is hiervoor gebruikt en was al in bezit van de onderzoeker. Engelse versie door de heer L. Bollen aangeleverd als basisartikel
3	2	Er is gezocht op artikelen sinds 2018, gesorteerd op relevantie en in elke taal	Google scholar	GDPR compliance	12600	Om informatie te verzamelen die betrekking heeft op deelvraag 4. Nummer 2 en nummer 6 van de eerste pagina zijn geselecteerd, respectievelijk “GDPR compliance in Norwegian Companies” en “Static Analysis for GDPR Compliance”. Met forward snowball methodiek is het artikel “Integrating Access control Business Process for GDPR Compliance A preliminary study” ook geselecteerd
3	2	Er is gezocht binnen alle artikelen,	Ebsco	GDPR AND compliance	414	Om informatie te verzamelen die betrekking heeft op

		document typen, relevantie en alle talen tussen de gepubliceerde datum van 01-01-2018 tot/met 31-12-2018				deelvraag 4. Voornamelijk artikelen uit tijdschriften. 2 zijn er geselecteerd
4	1	Er is gezocht binnen peer reviewed artikelen, document typen, relevantie en alle talen tussen de gepubliceerde datum van 01-01-2012 tot/met 31-12-2018	Ebsco	quality management AND change management AND business processes	55	Om informatie te verzamelen die betrekking heeft op deelvraag 1 en vanwege het feit dat implementatie van kwaliteit invloed heeft op de bedrijfsprocessen en zorgt voor veranderingen
4	2	Er is gezocht binnen peer reviewed artikelen, document typen, relevantie en alle talen tussen de gepubliceerde datum van 01-01-1999 tot/met 31-12-2018	Ebsco	Total quality management AND deming	123	Om informatie te verzamelen die betrekking heeft op deelvraag 1 en aanvullende informatie over de visie van Deming te verkrijgen over kwaliteit
4	3	Er is gezocht binnen peer reviewed artikelen, document typen, relevantie en alle talen tussen de gepubliceerde datum van 01-01-2015 tot/met 31-12-2018		Quality management AND iso 9001 AND iso 27001	6	Om informatie te verzamelen die betrekking heeft op deelvraag 1 en relaties tissen kwaliteit en meerdere iso systemen te analyseren

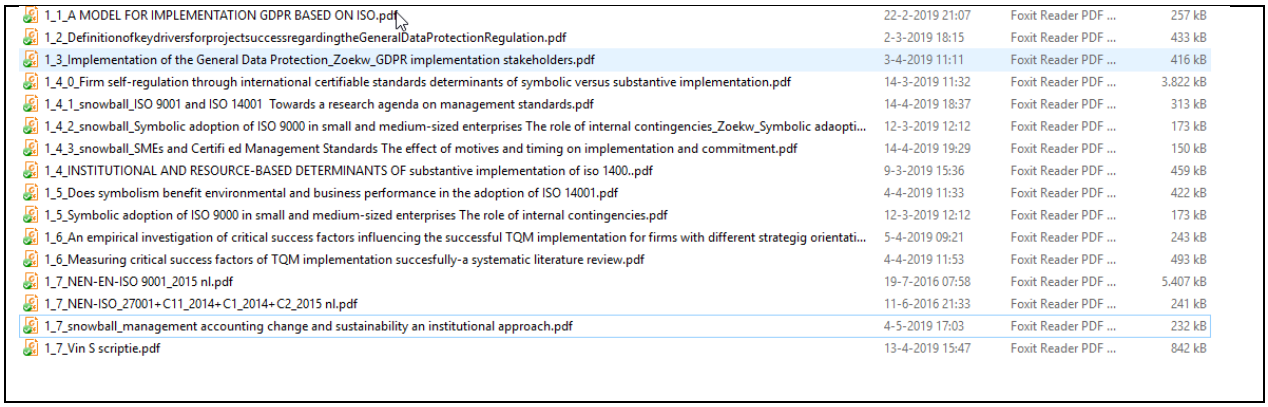
Tabel 1
Query overzicht

Door het toepassen van de snowball-methode op het basisartikel “Firm self-regulation through international certifiable standards: determinants of symbolic versus substantive implementation” van Christman en Taylor gaf Google Scholar 518 citaties weer. Hieruit is op de eerste pagina het artikel “ISO 9001 and ISO 14001: towards a research agenda on management system standards” van Heras doorgenomen. Met 301 citaten relevant. Via de link citaten zijn de eerste 2 pagina’s doorgenomen waarbij het artikel van Heras; “Symbolic adoption of ISO 9000 in small and medium-sized enterprises: The role of internal contingencies” opviel. Enerzijds door “Symbolic adoption” en anderzijds door het feit dat door het “building blocks” zoeken in EBSCO dit artikel met behulp van de zoekwoorden Symbolic AND adoption AND ISO ook naar voren kwam. Dit artikel werd 47 maal geciteerd en het artikel “SMEs and Certified Management Standards: The Effect of Motives and Timing on Implementation and Commitment” van Iatris werd verder doorgenomen. Dit artikel heeft ook citaten toegepast van het basisartikel “What Drives Substantive Versus Symbolic Implementation of ISO 14001 in a Time of Economic Crisis? Insights from Greek Manufacturing Companies” van Iatridis. Door het volledig doorlezen van bovenstaande relevante artikelen zijn meer zoekwoorden geselecteerd en queries opgesteld waardoor de literatuurlijst verder is uitgebreid. Voorbeelden van deze zoekwoorden zijn ‘total quality management’, ‘processen’ , ‘decoupling’ en ‘deming’ die veelal terugkomen in literatuur rondom ISO implementatie. Met behulp van deze zoekmethodiek zijn initieel ongeveer 30 artikelen (zie tabel 3) gebruikt voor het onderzoek waarvan voornamelijk de peer reviewed artikelen de relevantste artikelen zijn.

		Er is gezocht op artikelen sinds 2018, gesorteerd op relevantie en in elke taal	Google scholar Aan de hand van artikel “Static Analysis for GDPR compliance” zijn de geciteerde artikelen door genomen. Artikel “Integrating Access Control and Business Process for GDPR Compliance: A Preliminary Study” is nav het abstract verder doorgelzen	Gdpr Iso compliance	761 en 5 nadat gefilterd is op geciteerde artikelen.	Om aanknopingspunten te vinden in het nakomen van iso eisen en gdpr eisen.

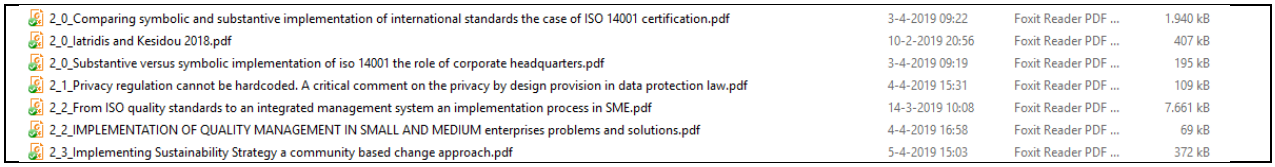
Tabel 2
Snowball overzicht

Overzicht van artikelen behorende bij deelvraag 1



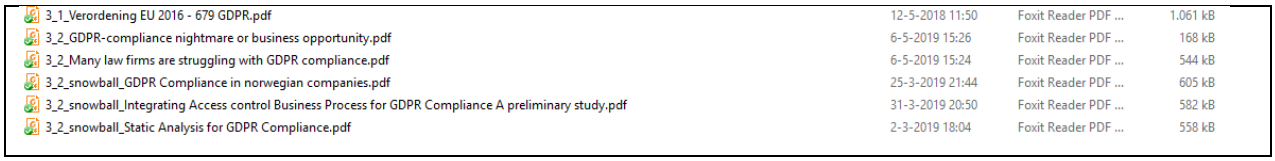
1_1_A MODEL FOR IMPLEMENTATION GDPR BASED ON ISO.pdf	22-2-2019 21:07	Foxit Reader PDF ...	257 kB
1_2_DefinitionofkeydriversforprojectsuccessregardingtheGeneralDataProtectionRegulation.pdf	2-3-2019 18:15	Foxit Reader PDF ...	433 kB
1_3_Implementation of the General Data Protection_Zoekw_GDPR implementation stakeholders.pdf	3-4-2019 11:11	Foxit Reader PDF ...	416 kB
1_4_0_Firm self-regulation through international certifiable standards determinants of symbolic versus substantive implementation.pdf	14-3-2019 11:32	Foxit Reader PDF ...	3.822 kB
1_4_1_snowball_ISO 9001 and ISO 14001 Towards a research agenda on management standards.pdf	14-4-2019 18:37	Foxit Reader PDF ...	313 kB
1_4_2_snowball_Symbolic adoption of ISO 9000 in small and medium-sized enterprises The role of internal contingencies_Zoekw_Symbolic adaopti...	12-3-2019 12:12	Foxit Reader PDF ...	173 kB
1_4_3_snowball_SMEs and Certifi ed Management Standards The effect of motives and timing on implementation and commitment.pdf	14-4-2019 19:29	Foxit Reader PDF ...	150 kB
1_4_INSTITUTIONAL AND RESOURCE-BASED DETERMINANTS OF substantive implementation of iso 1400..pdf	9-3-2019 15:36	Foxit Reader PDF ...	459 kB
1_5_Does symbolism benefit environmental and business performance in the adoption of ISO 14001.pdf	4-4-2019 11:33	Foxit Reader PDF ...	422 kB
1_5_Symbolic adoption of ISO 9000 in small and medium-sized enterprises The role of internal contingencies.pdf	12-3-2019 12:12	Foxit Reader PDF ...	173 kB
1_6_An empirical investigation of critical success factors influencing the successful TQM implementation for firms with different strategig orientati...	5-4-2019 09:21	Foxit Reader PDF ...	243 kB
1_6_Measuring critical success factors of TQM implementation succesfully-a systematic literature review.pdf	4-4-2019 11:53	Foxit Reader PDF ...	493 kB
1_7_NEN-EN-ISO 9001_2015 nl.pdf	19-7-2016 07:58	Foxit Reader PDF ...	5.407 kB
1_7_NEN-ISO_27001+C11_2014+C1_2014+C2_2015 nl.pdf	11-6-2016 21:33	Foxit Reader PDF ...	241 kB
1_7_snowball_management accounting change and sustainability an institutional approach.pdf	4-5-2019 17:03	Foxit Reader PDF ...	232 kB
1_7_Vin S scriptie.pdf	13-4-2019 15:47	Foxit Reader PDF ...	842 kB

Overzicht van artikelen behorende bij deelvraag 2



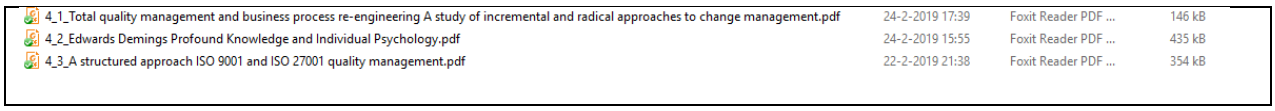
2_0_Comparing symbolic and substantive implementation of international standards the case of ISO 14001 certification.pdf	3-4-2019 09:22	Foxit Reader PDF ...	1.940 kB
2_0_Iatridis and Kesidou 2018.pdf	10-2-2019 20:56	Foxit Reader PDF ...	407 kB
2_0_Substantive versus symbolic implementation of iso 14001 the role of corporate headquarters.pdf	3-4-2019 09:19	Foxit Reader PDF ...	195 kB
2_1_Privacy regulation cannot be hardcoded. A critical comment on the privacy by design provision in data protection law.pdf	4-4-2019 15:31	Foxit Reader PDF ...	109 kB
2_2_From ISO quality standards to an integrated management system an implementation process in SME.pdf	14-3-2019 10:08	Foxit Reader PDF ...	7.661 kB
2_2_IMPLEMENTATION OF QUALITY MANAGEMENT IN SMALL AND MEDIUM enterprises problems and solutions.pdf	4-4-2019 16:58	Foxit Reader PDF ...	69 kB
2_3_Implementing Sustainability Strategy a community based change approach.pdf	5-4-2019 15:03	Foxit Reader PDF ...	372 kB

Overzicht van artikelen behorende bij deelvraag 3



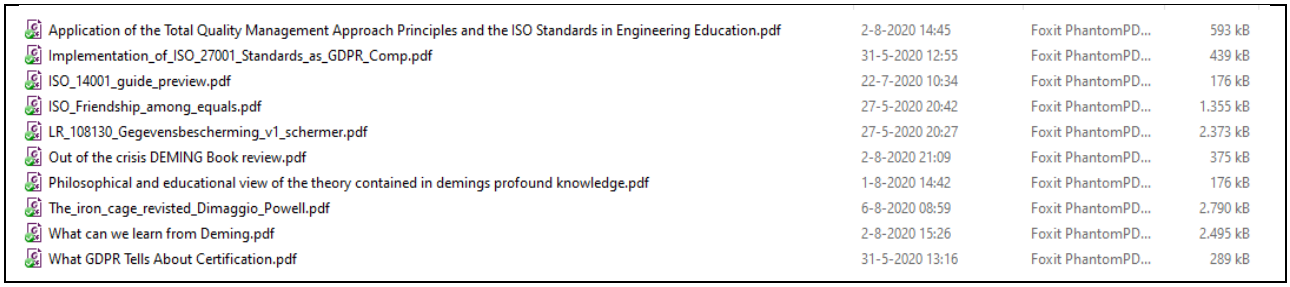
3_1_Verordening EU 2016 - 679 GDPR.pdf	12-5-2018 11:50	Foxit Reader PDF ...	1.061 kB
3_2_GDPR-compliance nightmare or business opportunity.pdf	6-5-2019 15:26	Foxit Reader PDF ...	168 kB
3_2_Many law firms are struggling with GDPR compliance.pdf	6-5-2019 15:24	Foxit Reader PDF ...	544 kB
3_2_snowball_GDPR Compliance in norwegian companies.pdf	25-3-2019 21:44	Foxit Reader PDF ...	605 kB
3_2_snowball_Integrating Access control Business Process for GDPR Compliance A preliminary study.pdf	31-3-2019 20:50	Foxit Reader PDF ...	582 kB
3_2_snowball_Static Analysis for GDPR Compliance.pdf	2-3-2019 18:04	Foxit Reader PDF ...	558 kB

Overzicht van artikelen behorende bij deelvraag 4



4_1_Total quality management and business process re-engineering A study of incremental and radical approaches to change management.pdf	24-2-2019 17:39	Foxit Reader PDF ...	146 kB
4_2_Edwards Demings Profound Knowledge and Individual Psychology.pdf	24-2-2019 15:55	Foxit Reader PDF ...	435 kB
4_3_A structured approach ISO 9001 and ISO 27001 quality management.pdf	22-2-2019 21:38	Foxit Reader PDF ...	354 kB

Overzicht van artikelen die na de analyse van de data zijn toegevoegd



Application of the Total Quality Management Approach Principles and the ISO Standards in Engineering Education.pdf	2-8-2020 14:45	Foxit PhantomPD...	593 kB
Implementation_of_ISO_27001_Standards_as_GDPR_Comp.pdf	31-5-2020 12:55	Foxit PhantomPD...	439 kB
ISO_14001_guide_preview.pdf	22-7-2020 10:34	Foxit PhantomPD...	176 kB
ISO_Friendship_among_equals.pdf	27-5-2020 20:42	Foxit PhantomPD...	1.355 kB
LR_108130_Gegevensbescherming_v1_schermer.pdf	27-5-2020 20:27	Foxit PhantomPD...	2.373 kB
Out of the crisis DEMING Book review.pdf	2-8-2020 21:09	Foxit PhantomPD...	375 kB
Philosophical and educational view of the theory contained in demings profound knowledge.pdf	1-8-2020 14:42	Foxit PhantomPD...	176 kB
The_iron_cage_revisted_Dimaggio_Powell.pdf	6-8-2020 08:59	Foxit PhantomPD...	2.790 kB
What can we learn from Deming.pdf	2-8-2020 15:26	Foxit PhantomPD...	2.495 kB
What GDPR Tells About Certification.pdf	31-5-2020 13:16	Foxit PhantomPD...	289 kB

Tabel 3
Overzicht artikelen

Bijlage 2

Variabele Naam	Artikel	Variabele definitie	Variabele waarde
1_5	5_Beginselen inzake verwerking van persoonsgegevens	De informatie dat persoonsgegevens die rechtmatig, behoorlijk en transparant moeten worden verwerkt wordt duidelijk weergegeven	JA = '1' NEE = 'o'
2_5	5_Beginselen inzake verwerking van persoonsgegevens	De informatie dat persoonsgegevens alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld wordt duidelijk weergegeven	JA = '1' NEE = 'o'
3_5	5_Beginselen inzake verwerking van persoonsgegevens	De informatie dat persoonsgegevens ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt ('minimale gegevensverwerking') wordt duidelijk weergegeven	JA = '1' NEE = 'o'
4_7	7_Voorwaarden voor toestemming	De organisatie kan duidelijk aantonen dat de betrokkene toestemming heeft gegeven voor de verwerking van zijn persoonsgegevens.	JA = '1' NEE = 'o'
5_7	7_Voorwaarden voor toestemming	Het intrekken van toestemming wordt in een duidelijke en eenvoudige taal gepresenteerd	JA = '1' NEE = 'o'
6_12	12_Transparante informatie, communicatie en nadere regels voor de uitoefening van de rechten van de betrokkene	In verband met de verwerking wordt de communicatie beknopt, transparant, begrijpelijk en in toegankelijke vorm weergegeven	JA = '1' NEE = 'o'
7_12	12_Transparante informatie, communicatie en nadere regels voor de uitoefening van de rechten van de betrokkene	In verband met de verwerking wordt de communicatie in duidelijke en eenvoudige taal weergegeven	JA = '1' NEE = 'o'
8_13	13_Te verstrekken informatie wanneer persoonsgegevens bij de betrokkene worden verzameld	De identiteit en de contactgegevens van de verwerkingsverantwoordelijk wordt duidelijk weergegeven	JA = '1' NEE = 'o'
9_13	13_Te verstrekken informatie wanneer persoonsgegevens bij de betrokkene worden verzameld	De contactgegevens van de functionaris voor gegevensbescherming wordt duidelijk weergegeven	JA = '1' NEE = 'o'
10_15	15_Recht van inzage van de betrokkene	De verwerkingsdoeleinden van de persoonsgegevens worden duidelijk weergegeven	JA = '1' NEE = 'o'
11_15	15_Recht van inzage van de betrokkene	De betrokken categorieën van de persoonsgegevens worden duidelijk weergegeven	JA = '1' NEE = 'o'
12_17	17_Recht op gegevenswissing	Het recht dat persoonsgegevens mogen worden gewist zodra dat deze gegevens niet langer	JA = '1'

	(„recht op vergetelheid")	nodig zijn voor de doeleinden waarvoor zij zijn verzameld wordt duidelijk weergegeven	NEE = '0'
13_17	17_Recht op gegevenswissing („recht op vergetelheid")	De organisatie duidelijk contactgegevens en een procedure beschrijft zodat betrokkene de toestemming van het verwerken van persoonsgegevens zoals beschreven in lid 1b van artikel 17 intrekt	JA = '1' NEE = '0'
14_20	20_Recht op overdraagbaarheid van gegevens	Het recht om persoonsgegevens te overdragen wordt duidelijk weergegeven	JA = '1' NEE = '0'
15_25	25_Gegevensbescherming door ontwerp en door standaardinstellingen	Het verwerken van persoonsgegevens die alleen noodzakelijk zijn voor een specifiek doel van de verwerking wordt duidelijk weergegeven	JA = '1' NEE = '0'
16_30	30_Register van de verwerkingsactiviteiten	Het bijhouden van een register van de verwerkingsactiviteiten met naam en contactgegevens van de verwerkingsverantwoordelijke wordt duidelijk weergegeven	JA = '1' NEE = '0'
17_30	30_Register van de verwerkingsactiviteiten	Het bijhouden van een register van de verwerkingsactiviteiten met contactgegevens van de functionaris voor gegevensbescherming wordt duidelijk weergegeven	JA = '1' NEE = '0'
18_32	32_Beveiliging van de verwerking	De maatregel pseudonimisering van persoonsgegevens als gegevensbeschermingsbeginsel of versleuteling wordt duidelijk weergegeven	JA = '1' NEE = '0'
19_32	32_Beveiliging van de verwerking	Een procedure voor het regelmatig testen, beoordelen en evalueren van de maatregelen wordt duidelijk weergegeven	JA = '1' NEE = '0'
20_33	33_Melding van een inbreuk in verband met persoonsgegevens aan de toezichthoudende autoriteit	Het melden van een breuk in verband met persoonsgegevens binnen 72 uur aan de toezichthoudende autoriteit wordt duidelijk weergegeven.	JA = '1' NEE = '0'
21_37	37_Aanwijzing van de functionaris voor gegevensbescherming	De functie functionaris voor gegevensbescherming wordt duidelijk weergegeven	JA = '1' NEE = '0'
22_37	37_Aanwijzing van de functionaris voor gegevensbescherming	De professionele kwaliteiten van de functionaris voor gegevensbescherming zoals het bezitten van kennis, kunde en ervaring in wetgeving en/of, persoonsgegevens bescherming wordt duidelijk weergegeven	JA = '1' NEE = '0'
23_40	40_Gedragscodes	Gedragscodes zijn duidelijk beschreven omtrent transparante verwerking, verzameling of pseudonimisering van persoonsgegevens	JA = '1' NEE = '0'
24_40	40_Gedragscodes	Gedragscodes zijn duidelijk beschreven omtrent de informatie verstrekt aan en de bescherming van kinderen	JA = '1' NEE = '0'
25_40	40_Gedragscodes	Gedragscodes zijn duidelijk beschreven omtrent de doorgifte van persoonsgegevens aan derde landen of internationale organisaties	JA = '1' NEE = '0'

Tabel 5
Overzicht 25 AVG bepalingen van 13 artikelen als basis voor het onderzoek

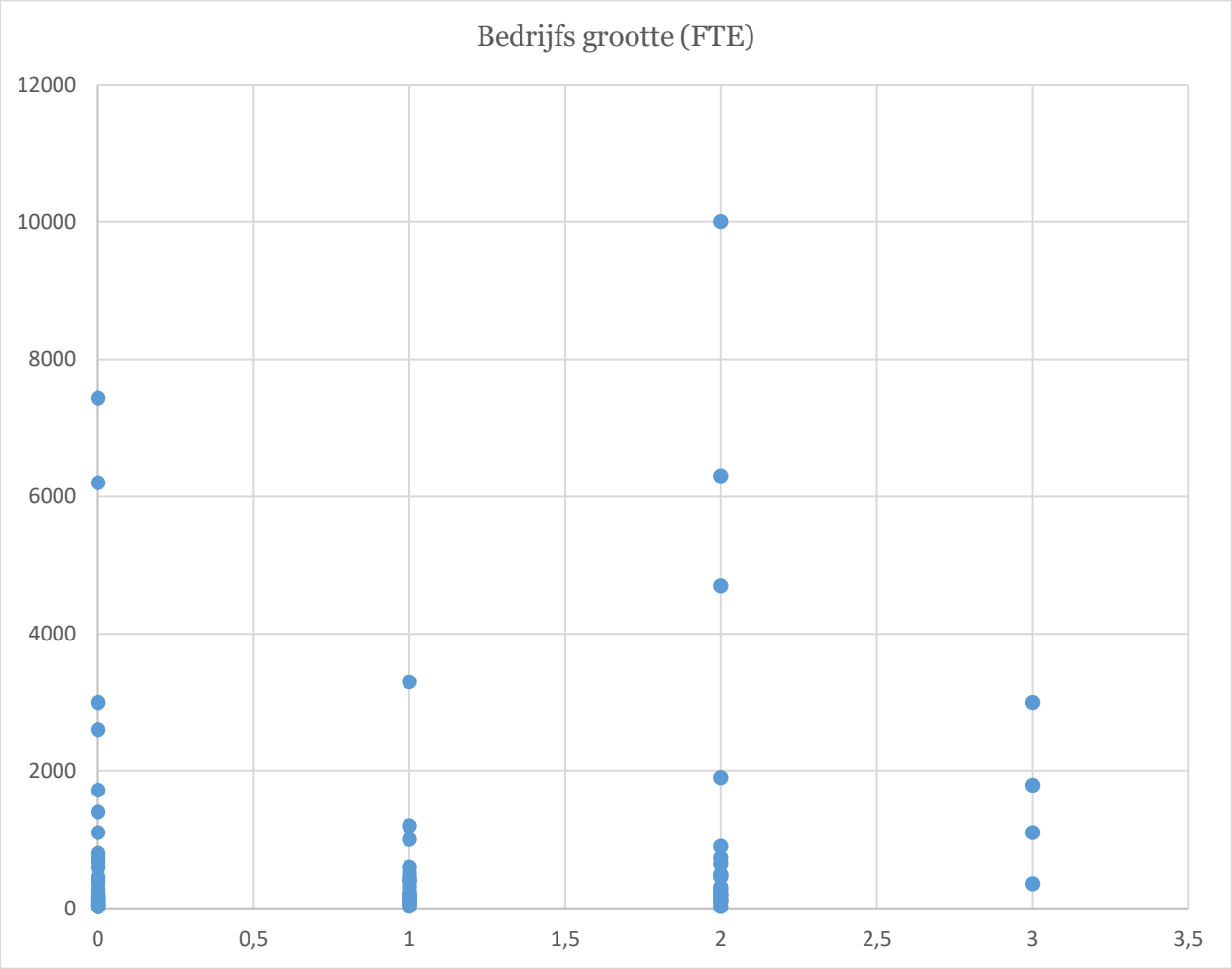
N = 87	ISO 9001	ISO 27001	ISO 14001	ISO 20000	ISO 55001	ISO_JA	Bedrijfsgrootte *
Minimum	0	0	0	0	0	0	20
Maximum	1	1	1	1	1	1	34.500
Gemiddelde	0,51	0,11	0,29	0,01	0,01	0,59	2.163,08
Mediaan	1	0	0	0	0	1	350,00
Std. Afwijking	0,503	0,321	0,455	0,107	0,107	0,495	5.201,59
Som	44	10	25	1	1	51	188.188

Tabel 8
Kenmerken van de onderzoekspopulatie (N = 87)
Opmerking: * Bedrijfsgrootte is uitgedrukt in aantal medewerkers

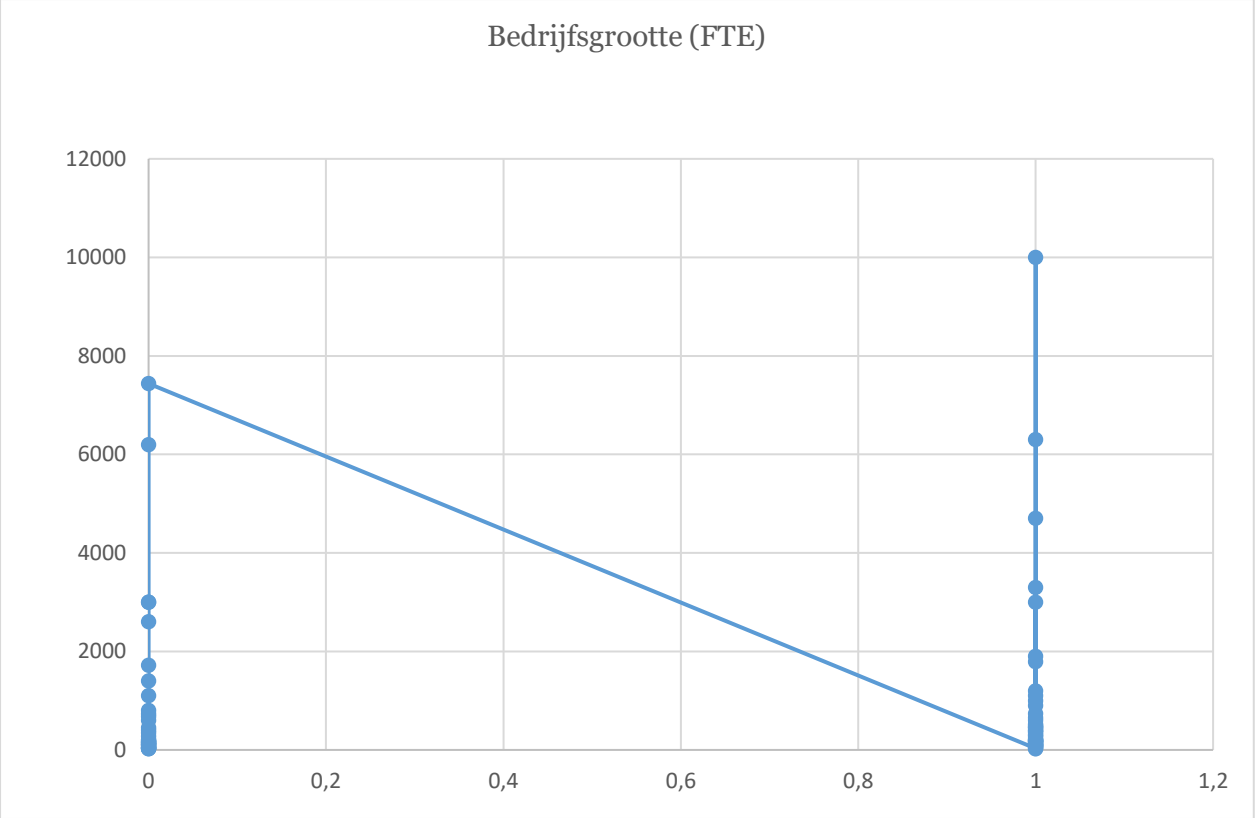
	ISO_JA = 1 (n = 48)	ISO_JA = 0 (n = 33)	t-test voor gelijkheid van gemiddelden	
	Gemiddelde	Gemiddelde	t	Sig. (2-tailed)
Voldoet aan AVG	10,77	9,94	-1,077	,285
Voldoet aan artikel 5 , beginselen inzake verwerking persoonsgegevens	1,33	1,09	-1,329	,188
Voldoet aan artikel 7 , voorwaarden voor toestemming	1,19	1,03	-,871	,386
Voldoet aan artikel 12 , transparantie, communicatie en nadere regels voor de uitoefening van de rechten van de betrokkenen	2,00	1,94	-1,738	,086
Voldoet aan artikel 13 , te verstrekken informatie wanneer persoonsgegevens bij de betrokkene worden verzameld	1,17	1,24	,478	,634
Voldoet aan artikel 15 , recht van inzage van de betrokkene	1,00	1,03	,249	,804
Voldoet aan artikel 17 , recht op vergetelheid	1,38	1,18	-1,299	,198
Voldoet aan artikel 20 , recht op overdraagbaarheid van gegevens	0,56	0,52	-,416	,679
Voldoet aan artikel 25 , gegevensbescherming door ontwerp en door standaardinstellingen	0,83	0,73	-1,147	,255
Voldoet aan artikel 30 , register van de verwerkingsactiviteiten	0,04	0,03	-,263	,793
Voldoet aan artikel 32 , beveiliging van de verwerking	0,38	0,30	-,552	,582

Voldoet aan artikel 33 , melding van een inbreuk in verband met persoonsgegevens aan de toezichthoudende autoriteit	0,04	0,00	-1,183	,240
Voldoet aan artikel 37 , aanwijzing van de functionaris voorgegevensbescherming	0,35	0,42	,631	,530
Voldoet aan artikel 40 , gedragscodes	0,50	0,39	-,790	,432

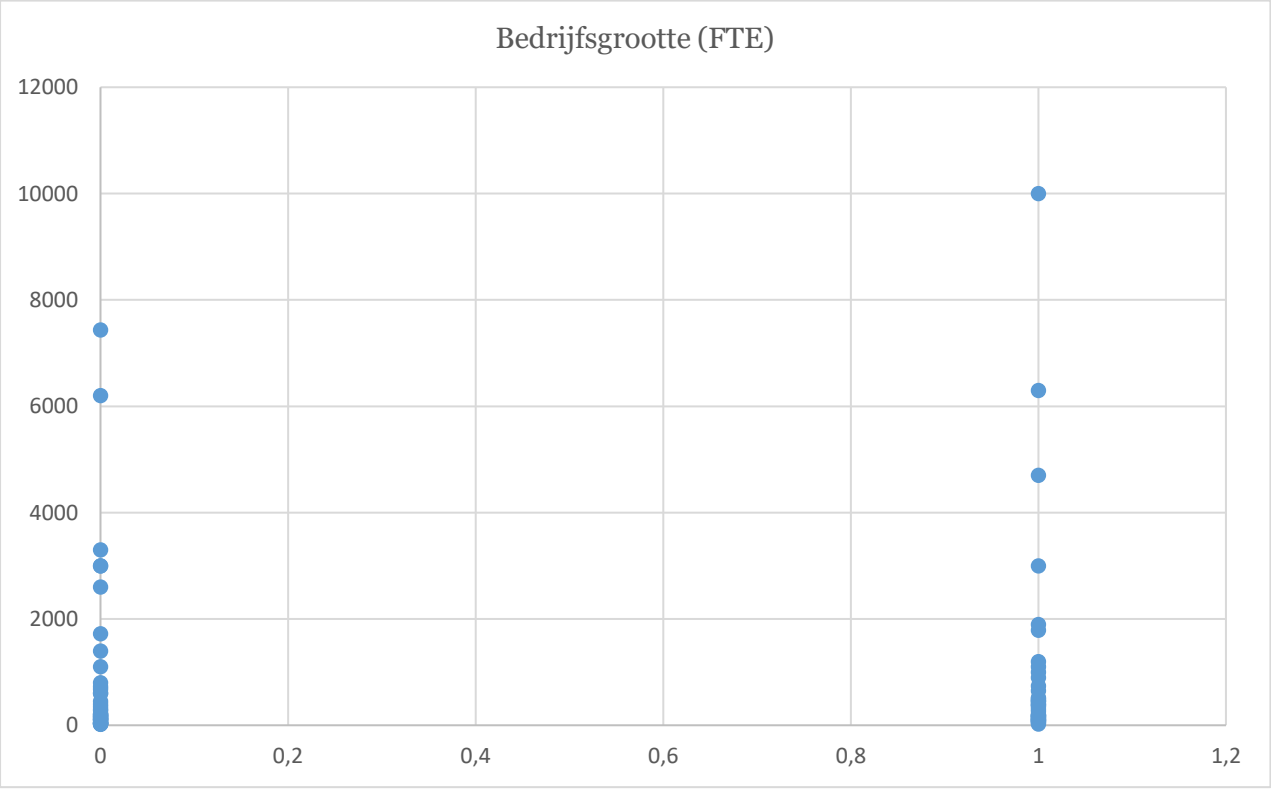
Tabel 14
Het verband tussen het voldoen aan ISO-certificatie en de GDPR-implementatiestrategie van bedrijven.



Grafiek 1
De verdeling tussen bedrijfsgrootte en het aantal ISO certificaten per bedrijfsgrootte.



Grafiek 2
Het verband tussen bedrijfsgrootte en ISO_JA



Grafiek 3
Het verband tussen bedrijfsgrootte en ISO-9001

Bijlage 3

Het dataset bestand; *.sav en de geanalyseerde databestanden; *.spv zijn opvraagbaar.