MASTER'S THESIS

Ontwikkeling van een AVG-volwassenheidsmodel

Gerritse, P. (Pieter)

Award date:
2019

Ontwikkeling van een AVG-volwassenheidsmodel

Opleiding:	Open Universiteit, faculteit Management, Science & Technology Masteropleiding Business Process Management & IT
Programme:	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:	Pieter Gerritse
Datum:	27 juni 2019
Afstudeerbegeleider	Ben Roelens
Meelezer	Laury Bollen
Derde beoordelaar	-
Versie nummer:	1.0
Status:	definitieve versie

Versie	Datum	Aanpassing	Auteur
0.10	2018-09-23	Introductie eerste opzet	PG
0.15	2018-10-14	Introductie verwerken feedback	PG
0.20	2018-10-19	Introductie deels verwerken tweede feedback	PG
0.25	2018-11-06	Theoretisch kader eerste opzet	PG
0.30	2018-11-27	Theoretisch kader feedback verwerkt en uitgebreid	PG
0.35	2018-12-17	Theoretisch kader feedback verwerkt	PG
0.40	2018-12-27	Methodologie eerste opzet	PG
0.42	2019-01-10	Aanpassen Theoretische kader	PG
0.44	2019-01-17	Aanpassen TK	PG
0.46	2019-01-19	Verwerken feedback	PG
0.47	2019-01-20	Verwerken feedback	PG
0.48	2019-01-29	Verwerken feedback op concept	PG
0.49	2019-02-08	Verwerken feedback	PG
0.50	2019-02-08	Ingeleverd VAF	PG
0.52	2019-03-10	Opstellen vragen demonstratie	PG
0.54	2019-03-19	Opstellen vragen demonstratie en evaluatie	PG
0.56	2019-04-16	Verrijken model met vanuit aspecten privacy mm Consistent maken dimensies in model	PG
0.6	2019-05-28	Verwerken resultaten op basis van interviews	PG
0.7	2019-06-06	Verder uitwerken resultaten en discussie	PG
0.8	2019-06-08	Samenvatting	PG
0.85	2019-06-15	Feedback verwerken	PG
0.87	2019-06-22	Samenvatting vertalen, abstract	PG
0.9	2019-06-26	Layout, opmaak, laatste bijstellingen	PG

Abstract

Sinds 25 mei 2018 is in alle Europese lidstaten de Algemene Verordening Gegevensbescherming (AVG) van toepassing met als belangrijkste doel om natuurlijke personen te beschermen met betrekking tot de verwerking van hun persoonsgegevens. Organisaties die in de verwerking van persoonsgegevens niet voldoen aan de verordening kunnen boetes tot vier procent van de jaaromzet krijgen. Inmiddels zijn in Europa enkele organisaties in overtreding bevonden en daarvoor beboet.

Een manier om vast te stellen in welke mate organisaties aan AVG voldoen is een volwassenheidsmodel, maar deze is niet beschikbaar voor AVG. Organisaties staan daarmee voor het probleem dat zij geen objectief meetinstrument hebben om hun AVG-implementatie te toetsen. In dit onderzoek is dit probleem het hoofd geboden door een AVG-volwassenheidsmodel te ontwikkelen gebaseerd op de zes AVG-basisprincipes en bestaande modellen voor Enterprise Architectuur en Data Management.

Na ontwikkeling is het model gedemonstreerd en geëvalueerd in twee organisaties. Dit heeft geleid tot een aantal aanpassingen, waardoor het model relevanter, minder datatechnisch en consistenter is geworden. Hierdoor is de algemene tevredenheid van respondenten toegenomen.

Het resultaat is een AVG-volwassenheidsmodel genaamd AVGMM, waarmee organisaties hun AVG-volwassenheid kunnen meten en advies kunnen formuleren voor de verbetering van hun AVG-implementatie.

Sleutelbegrippen

Algemene Verordening Gegevensbescherming, volwassenheidsmodel, Enterprise Architecture, Data Management, Design Science Research

Samenvatting

Sinds 25 mei 2018 is in alle Europese lidstaten de Algemene Verordening Gegevensbescherming (AVG) van toepassing. Deze verordening heeft als belangrijkste doel om natuurlijke personen te beschermen met betrekking tot de verwerking van hun persoonsgegevens. Organisaties die in de verwerking van persoonsgegevens niet voldoen aan de normen in de verordening kunnen rekenen op hoge boetes tot vier procent van de jaaromzet. Inmiddels zijn in Europa enkele organisaties door de wettelijke toezichthouder in overtreding bevonden en daarvoor beboet.

Daarom zoeken organisaties naar manieren om vast te stellen in welke mate hun verwerking van persoonsgegevens aan AVG voldoet. Een van die manieren kan een volwassenheidsmodel zijn, een beproefd concept in het vakgebied ICT voor het meten van de volwassenheid van bepaalde ICT-disciplines binnen een organisatie. Er zijn veel volwassenheidsmodellen, bijvoorbeeld voor Enterprise Architectuur (EA) of Data Management (DM), maar niet voor AVG. Organisaties staan daarmee voor het probleem dat zij geen objectief meetinstrument hebben om hun AVG-implementatie te toetsen.

Dit probleem is in dit onderzoek het hoofd geboden door een AVG-volwassenheidsmodel te ontwikkelen volgens de Design Science Research-methode voor de ontwikkeling van ICT-volwassenheidsmodellen. Het AVG-volwassenheidsmodel is gebaseerd op bestaande modellen binnen EA en DM en gaat uit van de zes basisprincipes van AVG, i.e. ‘rechtmatigheid, behoorlijkheid en transparantie’, ‘doelbinding’, ‘minimale gegevensverwerking’, ‘juistheid’, ‘opslagbeperking’ en ‘integriteit en vertrouwelijkheid’. Het model kent voor ieder basisprincipe vijf volwassenheidsniveaus, i.e. ‘performed’, ‘managed’, ‘defined’, ‘measured’ en ‘optimized’.

Na ontwikkeling is het model gedemonstreerd en geëvalueerd in twee organisaties. De evaluaties hebben geleid tot een aantal aanpassingen. In het oorspronkelijke model was voor de invulling van het AVG-basisprincipe “minimale gegevensverwerking” geen consensus over de relevantie. Die consensus is bereikt door het model op basis van kwalitatieve feedback aan te passen met specifieke AVG-aspecten. Daarnaast zijn de gebruikte termen in het gehele model bijgesteld naar termen die gebruikelijk zijn in het kader van AVG, omdat het oorspronkelijke model door de basis vanuit EA en DM te datatechnisch geformuleerd was. Ook is het model over de aspecten en niveaus consistenter en daarmee beter toepasbaar gemaakt. Door deze aanpassingen is de algemene tevredenheid van respondenten toegenomen.

Na twee evaluaties is het resultaat een AVG-volwassenheidsmodel genaamd AVGMM (AVG-maturiteitsmodel). Het kan de implementatie van zes AVG-basisprincipes op vijf volwassenheidsniveaus meten. Aan de hand van een set multiplechoicevragen kunnen organisaties in korte tijd hun algemene volwassenheid vaststellen en vanuit deze vaststelling advies formuleren voor de verbetering van de AVG-implementatie.

Summary

On May 25th, 2018 the General Date Protection Regulation (GDPR) became enforceable in all member states of the European Union. The main purpose of this regulation is to protect natural persons regarding the processing of their personal data. Organizations that process personal data in a way that is not compliant with the standards in the regulation can expect high fines of up to four percent of annual turnover. In the meantime, supervisory authorities have fined several organizations in Europe for infringing the regulation.

That is why organizations are looking for ways to determine the extent to which their processing of personal data complies with GDPR. One of these ways can be a maturity model, a tried and tested concept in the IT field for measuring the maturity of certain IT disciplines within an organization. There are many maturity models, for example for Enterprise Architecture (EA) or Data Management (DM), but not for GDPR. Organizations are thus faced with the problem that they do not have an objective measuring instrument to test their GDPR implementation.

This study has addressed this problem by developing a GDPR maturity model according to the Design Science Research method for development of IT maturity models. The GDPR model is based on existing models within EA and DM as well as on the six basic principles of GDPR: 'lawfulness, fairness and transparency', 'purpose limitation', 'data minimization', 'accuracy', 'storage limitation' and 'integrity and confidentiality'. The model has five maturity levels for each basic principle: 'performed', 'managed', 'defined', 'measured' and 'optimized'.

Once the model was developed, it was demonstrated and evaluated in two organizations. Evaluations led to several adjustments. In the original model there was no consensus on relevance for the implementation of the GDPR basic principle 'data minimization'. This consensus was reached by adapting the model through adding specific GDPR aspects based on qualitative feedback. In addition, the terminology used in the entire model was adjusted to be more appropriate in the context of GDPR because the original model, being based on EA and DM, was too data-technical. The model was also made more consistent across GDPR-aspects and maturity levels and therefore more applicable. These adjustments have increased the overall satisfaction of respondents.

After two evaluations the result is a GDPR maturity model named AVGMM. It can measure the implementation of the six GDPR basic principles at five maturity levels. Using a set of multiple-choice questions, organizations can quickly determine their general maturity and formulate advice for improving the GDPR implementation based on this assessment.

Inhoudsopgave

1. Introductie

1.1. Achtergrond

In alle lidstaten van de Europese Unie is met ingang van 25 mei 2018 de Algemene Verordening Gegevensbescherming (AVG) van toepassing (Schermer, 2018). De essentie van deze verordening laat zich verduidelijken door de doelen, de rechtspersonen en de basisbeginselen te beschrijven.

De AVG dient twee doelen. Het eerste doel is de bescherming van natuurlijke personen met betrekking tot de verwerking van hun gegevens. Tegelijkertijd moet de verordening vrij verkeer van persoonsgegevens binnen de Europese Unie waarborgen.

De AVG maakt daarbij onderscheid tussen drie soorten rechtspersonen:

- "De verwerkingsverantwoordelijke is degene die het doel en de middelen voor de verwerking vaststelt op basis van feitelijke invloed, specifieke juridische en/of impliciete bevoegdheid" (Schermer, 2018, p. 12).
- "De verwerker is degene die de gegevens verwerkt binnen een hiërarchische verhouding met de verwerkingsverantwoordelijke" (Schermer, 2018, p. 12).
- "De betrokkene is degene wiens persoonsgegevens verwerkt worden" (Schermer, 2018, p. 14).

Bij deze automatische gegevensverwerking moeten verantwoordelijke organisaties voldoen aan de zes beginselen van de AVG:

- "Rechtmatigheid, behoorlijkheid en transparantie; de verwerking van persoonsgegevens moet rechtmatig, behoorlijk en transparant zijn" (Schermer, 2018, p. 15).
- "Doelbinding; de verwerking moet gebonden zijn aan specifieke verzameldoelen" (Schermer, 2018, p. 15).
- "Minimale gegevensverwerking; de persoonsgegevens moeten toereikend zijn, ter zake dienend, en beperkt tot wat noodzakelijk is" (Schermer, 2018, p. 15).
- "Juistheid; de gegevens moeten juist zijn" (Schermer, 2018, p. 15).
- "Opslagbeperking; de gegevens mogen niet langer bewaard worden dan nodig" (Schermer, 2018, p. 15).
- "Integriteit en vertrouwelijkheid; gegevens moeten goed beveiligd zijn en vertrouwelijk blijven" (Schermer, 2018, p. 15).

Naast de AVG, is ook sprake van de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG). De AVG is de harmonisering van gegevensbescherming binnen Europa, terwijl de UAVG de ruimte is die een lidstaat heeft om verdere invulling te geven aan de bepalingen (Schermer, 2018).

1.2. Gebiedsverkenning

Geautomatiseerde gegevensverwerking binnen organisaties vindt plaats in een interne datastructuur die samenhangt met bedrijfsprocessen, informatiesystemen en onderliggende technologische infrastructuren. De implementatie van AVG vereist grote veranderingen aan de interne datastructuur en heeft daarmee impact op die samenhang. Het is dus belangrijk om vast te stellen of de implementatie van AVG effectief is uitgevoerd zonder nadelige gevolgen voor de samenhang in de organisatie.

Enterprise Architecture (EA) en *Data Management* (DM) zijn twee onderzoeksgebieden die nagaan hoe data efficiënt gebruikt kan worden binnen een organisatie.

De definitie van EA is “een samenhangend geheel van principes, methodes en modellen die richting geven aan ontwerp en realisatie van organisatiestructuren, bedrijfsprocessen, informatiesystemen en infrastructuur in een organisatie” (Lankhorst, 2009, p. 3). Vanuit die samenhang kan de impact van veranderingen worden bepaald en daarmee is EA een belangrijk instrument om veranderingen aan de interne datastructuren, ook in het kader van AVG, vorm te geven. *The Open Group Architecture Framework* (TOGAF) is een standaardmethode die een aanpak biedt voor het opstellen en toepassen van EA (Lankhorst, 2009).

DM beschrijft “de processen voor het plannen, specificeren, activeren, creëren, verkrijgen, onderhouden, gebruiken, archiveren, terugvinden, beheersen en vernietigen van data”. (The Data Management Assocation, 2014, p. 5). Deze beschrijvingen zijn als *best practices* relevant bij het vaststellen van de effectieve implementatie van de AVG. Over DM bestaan verschillende interpretaties en visies. De *DAMA-DMBOK2 Guide* (The Data Management Assocation, 2014) zet een industriestandaard van kennisgebieden, terminologie en *best practices*.

1.3. Probleemstelling

In Nederland, is de verwerkingsverantwoordelijke verplicht om verantwoording af te leggen aan de Autoriteit Persoonsgegevens (AP) over de mate waarin AVG effectief is geïmplementeerd. Het probleem hierbij is dat de verwerkingsverantwoordelijke zelf een beeld geeft over de eigenlijke implementatie, wat subjectiviteit in de hand werkt. Er is dus behoefte aan een objectief instrument, dat momenteel echter niet beschikbaar is.

De probleemstelling luidt dan ook: “Verwerkingsverantwoordelijken in organisaties met een geautomatiseerde verwerking van persoonsgegevens hebben geen instrument om een objectief beeld te geven van de AVG-implementatie binnen de eigen organisatie”.

1.4. Opdrachtformulering

Onderdeel van de EA-methode TOGAF is het *Architecture Capability Maturity Model* (ACMM), waarmee de volwassenheid van EA in een organisatie objectief gemeten kan worden (The Open Group, 2018). In dat volwassenheidsmodel worden *key capabilities* van EA afgezet tegen *maturity levels* om zo een beeld te krijgen van de mate waarin een organisatie effectief EA toepast.

Door de sterke relatie tussen EA en de interne datastructuren van organisaties, en de impact van AVG op diezelfde interne datastructuren, kan een AVG-volwassenheidsmodel ontwikkeld worden op basis van het EA-volwassenheidsmodel. Dit volwassenheidsmodel kan er dan voor zorgen dat er een objectief beeld gevormd wordt van de mate waarin de AVG effectief wordt toegepast binnen de organisatie. Vanwege de sterke impact van AVG op bedrijfsdata, kan het te ontwikkelen AVG-volwassenheidsmodel verder verfijnd worden op basis van volwassenheidsmodellen binnen Data Management.

Het doel van dit onderzoek is dus om een model te ontwikkelen waarmee organisaties de volwassenheid van hun implementatie van AVG-basiswetgeving objectief kunnen vaststellen. Daarmee wordt bereikt dat organisaties kunnen voldoen aan de verantwoordingsplicht van de Autoriteit Persoonsgegevens.

Het onderscheid tussen de basiswetgeving en de uitvoeringswet, en de verschillende rechtspersonen zijn aanleiding voor de verdere afbakening van dit onderzoek. Om de resultaten van dit onderzoek niet alleen in Nederland, maar in de gehele EU relevant te laten zijn, beperkt dit onderzoek zich tot de invoering van de basiswetgeving en richt het zich niet op de specifieke Nederlandse uitvoeringswet. Daarnaast focust dit onderzoek op de verplichtingen van de verwerkingsverantwoordelijke, omdat de verwerkingsverantwoordelijke de plicht heeft om te rapporteren over de gegevensverwerking.

Dit leidt tot de volgende opzet van onderzoeksvragen en deelonderzoeksvragen:

<u>Onderzoeksvraag:</u>

Hoe kan een AVG-volwassenheidsmodel ontwikkeld worden op basis van volwassenheidsmodellen binnen Enterprise Architectuur en Data Management?

<u>Deelonderzoeksvragen:</u>

- Welke volwassenheidsmodellen binnen EA kunnen de basis vormen voor een AVG-volwassenheidsmodel?
- Welke volwassenheidsmodellen binnen DM kunnen de basis vormen voor een AVG-volwassenheidsmodel?
- Hoe kan een AVG-volwassenheidsmodel worden samengesteld op basis van de geïdentificeerde volwassenheidsmodellen binnen EA en DM?
- Is het ontwikkelde AVG-volwassenheidsmodel toepasbaar binnen organisaties?

Antwoorden op deze vragen resulteren in een AVG-volwassenheidsmodel dat door organisaties in de praktijk gebruikt kan worden om hun eigen AVG-implementatie objectief te meten, te verbeteren en hierover verantwoording af te leggen aan de Autoriteit Persoonsgegevens.

Het ontwerp van het volwassenheidsmodel zal gebeuren aan de hand van de *Design Science Research (DSR) Methodology.* Deze methode is bij uitstek geschikt omdat zij uitgaat van een cyclus van rigoureus ontwerp (i.e., *rigor*) en praktische evaluatie. In dit onderzoek zullen twee Design Science artefacten ontwikkeld worden (Hevner & al, 2004): het te ontwikkelen volwassenheidsmodel (i.e., een model) en het toegepaste model in de organisatie (i.e., een instantie). Binnen DSR gebruiken we de specifiekere methode van Becker et al (2009), die bijzonder geschikt is omdat ze specifiek bedoeld is voor de ontwikkeling van volwassenheidsmodellen. Deze methode kent het volgende stappenplan: *(1) problem definition, (2) comparison of existing maturity models, (3) determination of the design strategy, (4) iterative maturity model development, (5) conception of transfer and evaluation, (6) implementation of the transfer media, en (7) evaluation*.

In de introductie (zie paragraaf 1.3) is het probleem gedefinieerd (*problem definition*) als het ontbreken van een objectief meetinstrument om de implementatie van AVG in een organisatie vast te kunnen stellen. In het theoretisch kader worden verschillende volwassenheidsmodellen voor EA en DM vergeleken (i.e., *comparison of existing maturity models*) als input voor het AVG-volwassenheidsmodel. Op basis van deze vergelijking is de ontwerpstrategie bepaald (i.e., *determination of the design strategy*); het combineren van verschillende modellen voor EA/DM-volwassenheid in een nieuw model voor AVG-volwassenheid.
De aanpak is iteratief (i.e., *iterative maturity model development*) en binnen dit onderzoek wordt gekozen voor twee cycli op basis van inhoudelijke evaluatie. “In *conception of transfer and evaluation* worden de verschillende vormen van overdracht voor de wetenschap en de gebruikers bepaald” (Becker & al, 2009, p. 218). De *implementation of the transfer media* is het AVG-volwassenheidsmodel dat effectief gecommuniceerd zal worden tijdens de demonstratie in de casestudy in hoofdstuk 4. Tijdens de evaluatie (i.e., *evaluation*) wordt vastgesteld of het AVG-volwassenheidsmodel toereikend is om het probleem op te lossen (zie hoofdstuk 4). Dit zal voorstellen opleveren om het initiële ontwerp aan te passen in de volgende ontwerpcyclus.

1.5. Motivatie en relevantie

Organisaties verwerken steeds vaker en steeds meer persoonsgegevens. De bescherming van die persoonsgegevens is een grondrecht, vastgelegd in het Handvest van de Grondrechten van de EU (Schermer, 2018). Dit grondrecht moet bescherming bieden aan de betrokkene, de natuurlijke persoon om wiens persoonsgegevens het gaat. Daarnaast heeft het grondrecht impact op de verwerkingsverantwoordelijke die moet voldoen aan de AVG-wet die het grondrecht regelt. Overtreding van de AVG kan voor organisaties leiden tot een boete van maximaal 20 miljoen euro of 4% van de wereldwijde jaaromzet (Schermer, 2018). Zo heeft het Portugese ziekenhuis Centro Hospitalar Barreiro Montijo een boete gekregen van 400.000 euro voor grove schendingen van de AVG. De Portugese toezichthouder stelde in een onderzoek vast dat de beveiliging van systemen ondermaats was en dat bijna 1.000 personen toegang hadden tot medische gegevens van patiënten terwijl er maar 296 artsen werkzaam waren (ICTRecht, 2018).

Het is daarom maatschappelijk relevant dat een objectief AVG-volwassenheidsmodel onderzocht wordt, om bedrijven te helpen in het naleven van AVG en daarmee de gegevens van natuurlijke personen te beschermen. Deze maatschappelijke relevantie wordt verder onderstreept in een sector als de zorg omdat zorgverleners privacygevoelige informatie van patiënten digitaal verwerken

(Autoriteit Persoonsgegevens, 2019), maar ook in het onderwijs neemt de automatische gegevensverwerking van persoonsgegevens van leerlingen toe in digitale toetsingsprogramma's, leerlingvolgsystemen, sociale media en apps (Autoriteit Persoonsgegevens, 2019).

Dit onderzoek is wetenschappelijk relevant omdat er geen modellen zijn voor het objectief vaststellen van AVG-volwassenheid binnen organisaties, terwijl er wel volwassenheidsmodellen zijn voor gerelateerde onderzoeksgebieden als Enterprise Architectuur (EA) en Data Management (DM). Er is dus momenteel sprake van een kennishiaat in het AVG-onderzoeksgebied, dat door dit onderzoek ingevuld zal worden. Omdat bij de ontwikkeling van een AVG-volwassenheidsmodel een literatuuronderzoek naar relevante EA- en DM-volwassenheidsmodellen wordt uitgevoerd, is er ook wetenschappelijke relevantie binnen de onderzoeksgebieden EA en DM.

1.6. Aanpak in hoofdlijnen

In de introductie (zie hoofdstuk 1) wordt de achtergrond geschetst als de invoering van de AVG en de basisprincipes van deze verordening (zie paragraaf 1.1). Daarna wordt het onderzoeksgebied in relatie tot AVG verkend en worden EA en DM onderkend als twee onderzoeksgebieden die een sterke relatie hebben met AVG (zie paragraaf 1.2). Volgens wordt de probleemstelling geformuleerd (zie paragaaf 1.3). Hieruit volgt de opdrachtformulering (zie paragraaf 1.4) met de vraagstelling: Hoe kan een AVG-volwassenheidsmodel ontwikkeld worden op basis van volwassenheidsmodellen binnen Enterprise Architectuur en Data Management? In motivatie en relevantie wordt toegelicht waarom dit onderzoek maatschappelijk en wetenschappelijk relevant is (zie paragraaf 1.5).

In de methodologie (zie hoofdstuk 2) wordt de DSR-methode (Hevner & al, 2004) (zie paragraaf 2.1) gekozen. Daarbinnen wordt gekozen voor de methode van Becker et al (2009), die specifiek gericht is op de ontwikkeling van volwassenheidsmodellen. Conform de stappen in deze methode wordt de aanpak ontworpen voor de ontwikkeling van een AVG-volwassenheidsmodel (zie paragraaf 2.2). In de gegevensanalyse wordt de aanpak in lijn met de casestudy-researchmethode (Yin, 2003) verder ontworpen voor demonstratie en evaluatie. In evaluatie worden *perceived usefulness*, *intention to use*, *perceived ease of use* (Moody, 2003), relevantie en algemene tevredenheid gemeten, waarbij kwalitatieve feedback wordt gevraagd (zie paragraaf 2.3). In een reflectie worden de validiteit, betrouwbaarheid en ethische aspecten van dit onderzoek beschreven (zie paragraaf 2.4).

In het theoretisch kader (zie hoofdstuk 3) wordt de onderzoeksaanpak beschreven voor het vinden van relevante EA- en DM-volwassenheidsmodellen beschreven (zie paragraaf 3.1) en uitgevoerd (zie paragraaf 3.2). Vervolgens worden de AVG-basisprincipes, de volwassenheidsniveaus en -aspecten geïntegreerd tot een nieuw AVG-volwassenheidsmodel (zie paragraaf 3.3).

In de resultaten (zie hoofdstuk 4) wordt het ontwikkelde model in een casestudy gedemonstreerd (zie paragraaf 4.1.) en geëvalueerd (zie paragrafen 4.2. en 4.3.) in de praktijk. In iteraties wordt het model na evaluatie aangepast op basis van kwalitatieve feedback.

In "Conclusies, discussie en aanbevelingen" (zie hoofdstuk 5) wordt de conclusie geformuleerd (zie paragraaf 5.1.) en de discussie en reflectie (zie paragraaf 5.2.) beschreven, alsmede de aanbevelingen voor de praktijk en verder onderzoek (zie paragrafen 5.3. en 5.4.).

2. Methodologie

2.1. Conceptueel ontwerp: keuze van onderzoeksmethode(n)

In dit onderzoek wordt een AVG-volwassenheidsmodel ontwikkeld om de implementatie van de wetgeving in een organisatie op een objectieve manier te kunnen meten. Hierbij is de volgende informatie nodig: (i) welke volwassenheidsmodellen binnen EA/DM kunnen de basis vormen voor een AVG-volwassenheidsmodel en (ii) welke AVG-aspecten, -volwassenheidsniveaus, en -criteria kunnen worden afgeleid uit volwassenheidsmodellen uit EA en DM. Vervolgens wordt onderzocht hoe het ontwikkelde AVG-volwassenheidsmodel gevalideerd kan worden in een praktische bedrijfscontext. De informatie, die hiervoor nodig is, kan gevonden worden in relevante literatuur over AVG, EA, DM en literatuur die aangeeft hoe volwassenheidsmodellen ontworpen en in een praktische bedrijfscontext gevalideerd kunnen worden.

Hierbij wordt de *DSR* (Hevner & al, 2004) methodologie toegepast. Deze methode is geschikt omdat ze gericht is op het ontwerp van *IT artifacts* door middel van iteratieve cycli van ontwikkeling en evaluatie. Hierbij wordt het ontwerp van het artifact onderbouwd door relevante wetenschappelijke literatuur en vervolgens wordt het artifact geëvalueerd in een praktische bedrijfscontext. *DSR* is een overkoepelende methode, waarbinnen voor ontwerp en evaluatie meer specifieke methodes gevolgd kunnen worden.

2.2. Technisch ontwerp: uitwerking van de methode

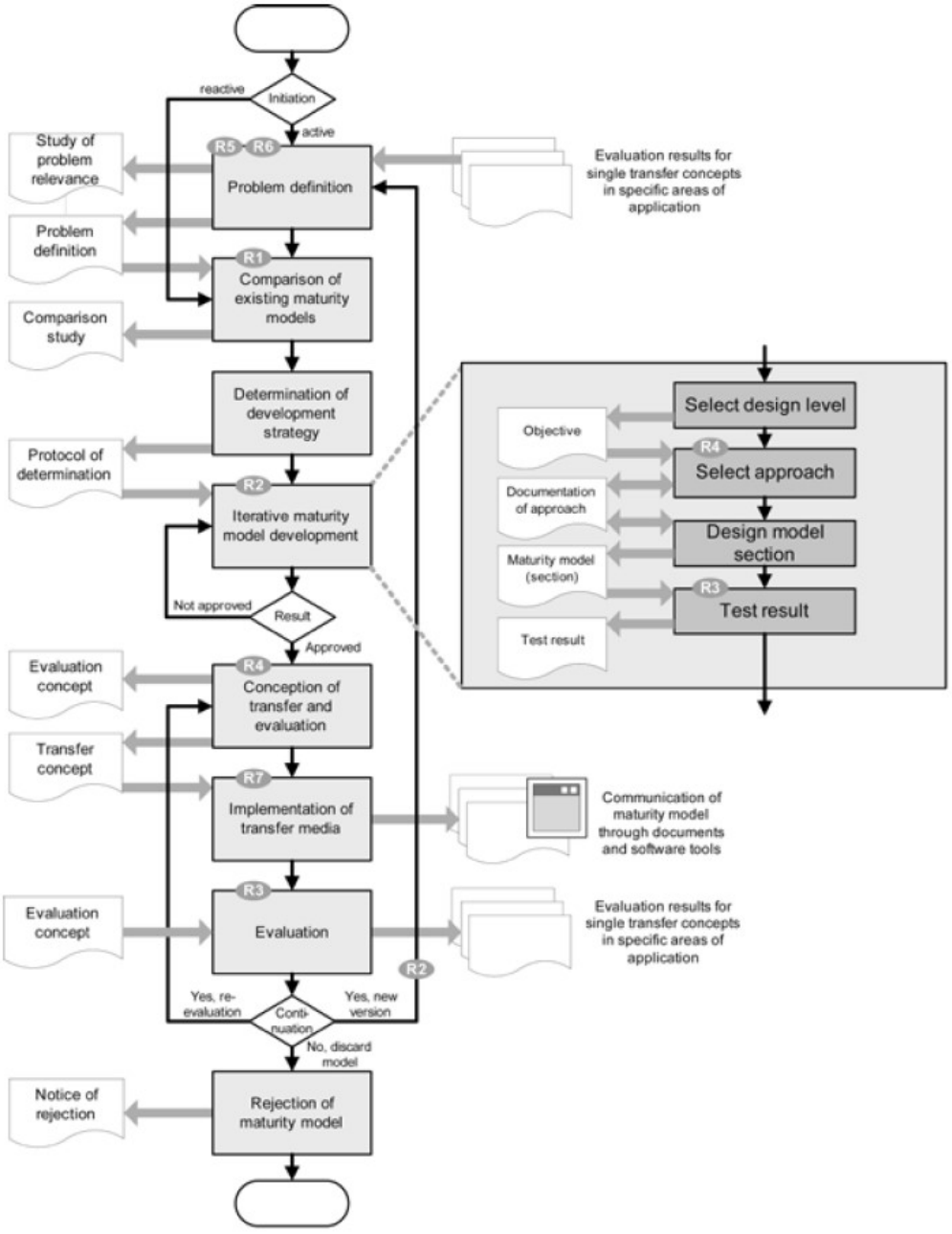
Binnen de DSR-methode wordt specifiek de methode van Becker et al (2009) toegepast voor de ontwikkeling van het AVG-volwassenheidsmodel. Deze methode is bijzonder geschikt omdat ze specifiek bedoeld is voor de ontwikkeling van volwassenheidsmodellen. De methode is specifiek ontworpen binnen de ontwerprichtlijnen van Hevner et al (2004) die de basis vormen voor een achttal requirements waaraan de ontwikkeling van volwassenheidmodellen volgens Becker et al (2009) moet voldoen.

- R1: “Vergelijken met bestaande volwassenheidsmodellen; de noodzaak voor de ontwikkeling van een nieuw volwassenheidsmodel moet onderbouwd worden door een vergelijking met bestaande modellen” (Becker & al, 2009, p. 214).
- R2: “Iteratieve procedure; volwassenheidsmodellen moeten iteratief ontwikkeld worden, en stap voor stap” (Becker & al, 2009, p. 214).
- R3: “Evaluatie; alle principes en voorwaarden voor de ontwikkeling van een volwassenheidsmodel, alsmede de bruikbaarheid, kwaliteit en effectiviteit van het artifact, moet iteratief geëvalueerd worden” (Becker & al, 2009, p. 214).
- R4: “Multi-methodologische procedure; de ontwikkeling van volwassenheidsmodellen past een diversiteit van onderzoeksmethoden toe die gefundeerd gekozen en op elkaar afgestemd zijn” (Becker & al, 2009, p. 214).
- R5: “Identificatie van de relevantie van het probleem; de relevantie van de probleemoplossing (i.e., het volwassenheidsmodel) voor onderzoekers en vakmensen moet worden gedemonstreerd” (Becker & al, 2009, p. 214).

- R6: “Probleemdefinitie; het beoogde toepassingsgebied van het volwassenheidsmodel, alsmede de voorwaarden voor toepassing en de beoogde baten moeten bepaald worden voorafgaand aan het ontwerp” (Becker & al, 2009, p. 214).
- R7: “Gerichte presentatie van resultaten; de presentatie van het volwassenheidsmodel moet gekaderd worden binnen de toepassingsvoorwaarden en de behoefte van de gebruikers” (Becker & al, 2009, p. 216).
- R8: “Wetenschappelijke documentatie; het ontwerpproces van het volwassenheidsmodel moet gedetailleerd gedocumenteerd worden, waarbij iedere processtap, de betrokken partijen, de toegepaste methoden en de resultaten overwogen worden” (Becker & al, 2009, p. 216).

De methode van Becker et al (2009) omvat de volgende stappen (zie figuur 1), die in dit onderzoek worden doorlopen.

Figuur 1 Proceduremodel voor de ontwikkeling van volwassenheidsmodellen (Becker & al, 2009)



In de introductie (zie paragraaf 1.3) is het probleem gedefinieerd *(problem definition*) als het ontbreken van een objectief meetinstrument om de implementatie van AVG in een organisatie vast te kunnen stellen. De relevantie van dit probleem is maatschappelijk, omdat de privacy van betrokkenen in het geding is en organisaties verantwoording moeten kunnen afleggen aan de Autoriteit Persoonsgegevens, en wetenschappelijk omdat er in de wetenschap op dit moment geen AVG-volwassenheidsmodellen bestaan. Het *target domain* (Becker & al, 2009) is ICT, omdat binnen dit domein veel persoonsgegevens verwerkt worden. AVG is binnen ICT is de specifieke discipline die zich richt op de bescherming van persoonsgegevens. Het IT-management van organisaties vormen de *internal target group* en de *external target group* zijn de betrokkenen wiens persoongegevens verwerkt worden.

In het theoretisch kader zijn verschillende volwassenheidsmodellen voor EA (i.e., IT-CMF, EAMM) en DM (i.e., MD3M, DMM) vergeleken (i.e., *comparison of existing maturity models)* als input voor het AVG-volwassenheidsmodel. Op basis van deze vergelijking is de ontwerpstrategie bepaald (i.e., *determination of the design strategy);* het combineren van verschillende modellen voor EA/DM-volwassenheid in een nieuw model voor AVG-volwassenheid (zie paragraaf 1.4).

De aanpak is iteratief (i.e., *iterative maturity model development)* en binnen dit onderzoek is gekozen voor twee ontwerpcycli (zie Delphi study-techniek in paragraaf 2.3). Binnen deze cyclus is het *designlevel* vastgesteld op een model bestaand uit AVG-principes en volwassenheidsniveaus (zie paragraaf 3.3.3). Hierbij is de *approach* als volgt. Allereerst zijn volwassenheidsniveaus in de vier EA/DM-volwassenheidsmodellen vergeleken, en bij overlappende inhoud geïntegreerd in volwassenheidsniveaus voor het AVG-volwassenheidsmodel. Daarna zijn relevante volwassenheidsaspecten uit de vier EA/DM-modellen per volwassenheidsniveau bijeengebracht in een tabel. Vervolgens is deze tabel herschreven naar een AVG-volwassenheidsmodel waarbij overlappende inhoud is geïntegreerd. Dit leidt tot het *design*, het eigenlijke ontwerp van het AVG-volwassenheidsmodel (zie 3.3.3).

In *conception of transfer and evaluation* worden de verschillende vormen van *overdracht* voor de wetenschap en de gebruikers bepaald (Becker & al, 2009) opgenomen. In het ontwerp van de *transfer* wordt gekozen om het AVG-volwassenheidsmodel toe te passen in interviews met betrokken respondenten op basis van een schriftelijke vragenlijst. Vervolgens wordt het volwassenheidsmodel geëvalueerd tijdens een casestudy door middel van kwantitatieve vragen en kwalitatieve feedback, waarbij de respondenten voorstellen voor inhoudelijke aanpassingen kunnen meegeven. De *implementation of the transfer media* is het AVG-volwassenheidsmodel (zie beschrijving van het model in paragraaf 3.3.3) dat effectief gebruikt wordt tijdens de demonstratie in de casestudy in hoofdstuk 4. Tijdens de evaluatie (i.e., *evaluation*) wordt vastgesteld of het AVG-volwassenheidsmodel toereikend is om het probleem op te lossen (zie hoofdstuk 4). Dit levert voorstellen op om het initiële ontwerp aan te passen.

2.3. Gegevensanalyse

In de casestudy research methode (Yin, 2003) is sprake van demonstratie en evaluatie. Daarbij komen tijdens de gegevensanalyse de volgende onderzoeksvragen naar voren:

- Voor demonstratie:
  Is de methode in staat om de AVG-volwassenheid binnen de organisatie te meten?
- Voor evaluatie:
  Zijn er aanpassingen nodig aan initiële ontwerp (aspecten, volwassenheidsniveaus, criteria)

De stelling hierbij is dat het ontwerp van het voorgestelde volwassenheidsmodel geschikt is om de implementatie van de AVG-wetgeving binnen de organisatie op een objectieve wijze te meten. De *analyse unit* binnen het *target domain* ICT is de AVG-volwassenheid binnen de organisatie. Het model wordt gedemonstreerd in twee organisaties in een gezamenlijk interview van anderhalf uur met de functionaris gegevensbescherming (FG) en de informatiearchitect (IA). Aan de hand van vragen wordt vastgesteld hoe de organisaties scoren in het AVG-volwassenheidsmodel.

Daarna wordt in interviews van één uur met de vier respondenten afzonderlijk het model geëvalueerd. De mate waarin het AVG-volwassenheidsmodel effectief het probleem oplost, wordt daarbij getoetst met vragen uit het Technology Acceptance Model (Moody, 2003) omtrent *perceived usefulness* ofwel waargenomen toepasbaarheid*,* i.e. de mate aan waarin een persoon gelooft dat een systeem de kwaliteit en prestaties van zijn of haar werk verbeterd. Daarnaast wordt het waargenomen gebruiksgemak van het model getoetst met vragen omtrent *perceived ease of use,* i.e. de mate waarin een persoon gelooft dat een systeem gemakkelijk te gebruiken. De *intention to* use, i.e. de intentie om het AVG-volwassenheidsmodel gaan gebruiken hangt sterk samen met de waargenomen toepasbaarheid en gebruiksgemak.
In de analyse van de inhoudelijke evaluatie wordt de iteratieve Delphi-casestudytechniek (Bruin & Rosemann, 2007) toegepast. In die techniek moet consensus of stabiliteit zijn voor de beslissing of een demonstratievraag definitief in het model opgenomen of geschrapt moet worden. De consensus (Looy & al, 2013) wordt gecontroleerd aan de hand van vier criteria:

- 50% van de respondenten zijn het minstens eens om een vraag te schrappen (score 1-2) of in de set op te nemen (score 6-7),
- 75% van de respondenten scoren 1-2-3 of 5-6-7,
- geen tegenstrijdige extreme scores (bv 1 ingeval van houden, of 7 ingeval van schrappen),
- interkwartielbereik is kleiner dan 1,5.

Er is consensus als aan alle criteria is voldaan. Wanneer voor het opnemen of schrappen van een vraag geen consensus vastgesteld is, wordt stabiliteit van de evaluatiescores bepaald door de free-marginal kappa (Randolph, 2005) te berekenen. Bij een free-marginal kappa groter dan 0,4 (Randolph, 2005) is er sprake van stabiliteit. Op deze wijze wordt de relevantie van iedere demonstratievraag door de respondenten geanalyseerd. Voor het interpreteren van de resultaten wordt rekening gehouden met het feit dat het onmogelijk is om statistische testen uit te voeren op de resultaten van multiple-casestudy in twee organisaties. Om een beter inzicht te krijgen, zullen we de data daarom aanvullen met kwalitatieve feedback van de respondenten. Tot slot wordt de algemene tevredenheid over de inhoud van het model door respondenten geëvalueerd. Nadat alle respondenten bevraagd zijn, worden demonstratievragen waarvoor geen consensus of stabiliteit kan worden vastgesteld, aangepast op basis van de kwalitatieve feedback. De aangepaste

demonstratievragen worden vervolgens voor een tweede evaluatie (i.e. de tweede ontwerpcyclus) voorgelegd aan de respondenten om nogmaals de relevantie per demonstratievraag en de algemene tevredenheid te evalueren. Het aantal iteraties in de casestudy wordt gestopt als voor alle vragen consensus of stabiliteit is bereikt en/of door stopcriteria voor de algemene tevredenheid, gemeten op een 11-punts Likertschaal in cijfers van 0 tot 10. Er wordt gestopt met evalueren en aanpassen wanneer aan de volgende stopcriteria (Bruin & Rosemann, 2007) wordt voldaan:

- de minimale algemene tevredenheid van de vier respondenten is groter of gelijk aan 5,
- de gemiddelde algemene tevredenheid is groter of gelijk aan 7.5,
- de spreiding in de scores voor algemene tevredenheid, i.e. de standaarddeviatie, is kleiner dan 1.5.

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

De constructvaliditeit (Yin, 2003) geeft aan of het instrument, het AVG-volwassenheidsmodel, meet wat het zou moeten meten, namelijk de volwassenheid van de AVG-implementatie in een organisatie. In dit onderzoek is dit niet te garanderen, zonder de toetsing op veel bredere schaal uit te voeren en de resultaten statistisch te analyseren. Voor de evaluatie gebruiken we kwantitatieve evaluatiemethodes van het Technology Acceptance Model (Moody, 2003) en de condities voor consensus, stabiliteit (Looy & al, 2013) en de stopcriteria voor algemene tevredenheid binnen de Delphi casestudytechniek (Bruin & Rosemann, 2007). Deze methodes worden letterlijk overgenomen en daarmee is de constructvaliditeit van deze methodes is wel te garanderen omdat deze in eerder onderzoek is aangetoond.

De mate waarin het veronderstelde causaal verband optreedt tussen de geschiktheid van het model en de uitkomsten van de evaluatie, bepaalt de interne validiteit (Yin, 2003). Daartoe proberen we verstorende (derde) factoren zoveel mogelijk uit te sluiten door gelijke omstandigheden te creëren bij het toepassen en evalueren van het AVG-volwassenheidsmodel. In twee organisaties wordt het model toegepast en geëvalueerd door personen die over de informatie beschikken om de AVG-volwassenheid te kunnen beoordelen, te weten de functionaris gegevensbescherming en de informatiearchitect. Daarnaast worden interviews in dezelfde tijdsduur afgenomen. Omdat we onmogelijk statistische testen kunnen uitvoeren worden de kwantitatieve TAM-data ondersteund door een semi-gestructureerd interview.

Het onderzoek wordt uitgevoerd in twee organisaties in verschillende sectoren, onderwijs en zorg. Voor de externe validiteit (Yin, 2003) van dit onderzoek (i.e., de veralgemeenbaarheid van de resultaten), houdt een inherente beperking van multiple-casestudy onderzoek bij twee organisaties in dat een beperkte hoeveelheid onderzoeksdata opgeleverd wordt. Om te komen tot veralgemeenbare resultaten zijn verdere veldstudies en/of grootschalige experimenten nodig.

De betrouwbaarheid (Yin, 2003) wordt bepaald door de mate waarin de resultaten reproduceerbaar zijn. Dit wordt bereikt door: alle (interview)materialen beschikbaar te stellen in een databank, in beide bedrijven meerdere mensen te interviewen, te weten de functionaris gegevensbescherming en de informatie architect, om uitkomsten te dubbelchecken en door de interviews voor te leggen aan respondenten na transcriptie.

Dit onderzoek houdt rekening met een aantal algemene ethische aspecten (Saunders & al, 2015). Voor respondenten geldt een vrijwillige deelname en zij hebben steeds het recht om zich geheel of gedeeltelijk terug te trekken uit het onderzoek. De privacy van respondenten wordt geborgd door niet de naam, maar de rol en/of functie van de respondenten te noemen. Ook worden met de bedrijf afspraken gemaakt omtrent geheimhouding en worden bedrijven niet bij naam genoemd maar als een bedrijf uit de sectoren onderwijs en zorg.

3. Theoretisch kader

3.1. Onderzoeksaanpak

In de introductie is vanuit de probleemstelling de overkoepelende onderzoeksvraag naar voren gekomen. In dit theoretisch kader moeten de volgende deelvragen beantwoord worden door literatuuronderzoek:

- Welke volwassenheidsmodellen binnen EA kunnen de basis vormen voor een AVG-volwassenheidsmodel?
- Welke volwassenheidsmodellen binnen DM kunnen de basis vormen voor een AVG-volwassenheidsmodel?
- Hoe kan een AVG-volwassenheidsmodel worden samengesteld op basis van de geïdentificeerde volwassenheidsmodellen binnen EA en DM?

3.1.1. Aanpak voor EA-volwassenheidsmodellen

Welke volwassenheidsmodellen binnen EA kunnen de basis vormen voor een AVG-volwassenheidsmodel? Om deze deelonderzoeksvraag te kunnen beantwoorden zijn allereerst de zoektermen bepaald. Met de “Building Blocks”-methode (Westerkamp & Veen, 2008) wordt de vraagstelling ontleedt, wat leidt tot de identificatie van volgende Engelstalige zoektermen: *maturity model* en *enterprise architecture*. Vervolgens is de zoekterm *maturity framework* toegevoegd, omdat dit binnen de academische literatuur een veelgebruikt synoniem is voor *maturity model*. Omdat *maturity models* meestal ontwikkeld zijn door privé-organisaties, is gezocht naar wetenschappelijke artikelen die een verzameling EA-volwassenheidsmodellen analyseren. Daartoe zijn de zoektermen *analysis* en *review* toegevoegd, alsmede afgeleide werkwoorden en Brits- en Amerikaans-Engelse varianten, zoals *analyse, analyze, analysing, analyzing, reviewing*. Met alle genoemde zoektermen is de volgende query opgesteld:

(“maturity model” OR “maturity framework”) AND (“enterprise architecture”) AND (“analysis” OR “analyse” OR “analyze” OR “analysing” OR “analysing” OR “review” OR “reviewing”)

Om de kwaliteit van de gevonden reviews te garanderen is de query uitgevoerd op Web of Science. Om actuele resultaten te vinden is in Web of Science de zoekoptie “na 1/1/2008” ingesteld. De gevonden artikelen worden in volgorde getoetst aan vier handmatige selectiecriteria:

- Engelstalig, omdat dit tegenwoordig de standaardtaal is voor wetenschappelijke publicaties.
- EA-volwassenheidsmodel; het artikel dient te verwijzen naar een (meerdere) specifiek(e) EA-volwassenheidsmodel(len).
- Review; het artikel is een review en geen ontwerp van (een) EA-volwassenheidsmodel(len).
- Volledige tekst beschikbaar; dit is een pragmatisch criterium i.v.m. de beschikbare OU-licenties.

Wanneer een artikel niet aan een bepaald criterium voldoet, worden de volgende criteria niet meer expliciet getoetst. Op de gevonden artikelen wordt *backward snowballing* toegepast om het oorspronkelijk bronmateriaal van de modellen te vinden, waarnaar in de gevonden review artikelen wordt verwezen.

3.1.2. Aanpak voor DM-volwassenheidsmodellen

Welke volwassenheidsmodellen binnen DM kunnen de basis vormen voor een AVG-volwassenheidsmodel? Om deze deelvraag te kunnen beantwoorden zijn allereerst de relevante zoektermen bepaald. Met de "Building Blocks"-methode (Westerkamp & Veen, 2008) wordt de vraagstelling ontleedt, wat leidt tot de volgende Engelstalige zoektermen: *maturity model* en *data management*. De zoekterm *maturity framework* is toegevoegd, omdat dit binnen de academische literatuur een veelgebruikt synoniem is voor *maturity model*. *Data governance* is als zoekterm toegevoegd omdat het sterk gerelateerd is aan *data management*; *data governance* is immers de basis , waarbinnen de spelregels voor *data management* worden bepaald. Er is gezocht naar wetenschappelijke artikelen die het ontwerp van een DM-volwassenheidsmodel beschrijven of analyseren. Daartoe zijn de zoektermen *analysis* en *design* toegevoegd, alsmede afgeleide werkwoorden en Brits- en Amerikaans-Engelse varianten, zoals analyse, analyze, analysing, analyzing, designing. Met alle genoemde zoektermen is de volgende query opgesteld:
("maturity model" OR "maturity framework") AND ("data management" OR "data governance") AND ("analysis" OR "analyse" OR "analyze" OR "analysing" OR "analysing" OR "design" OR "designing")

Met deze query wordt exploratief gezocht op Google Scholar, waarbij de zoekoptie "na 1/1/2008" meegegeven is om actuele artikelen te vinden. De gevonden artikelen worden in volgorde getoetst aan vier selectiecriteria:

- Engelstalig; omdat dit tegenwoordig de standaardtaal is voor wetenschappelijke publicaties
- DM-volwassenheidsmodel; het artikel dient te verwijzen naar een of meerdere specifiek(e) DM-volwassenheidsmodel(len).
- Ontwerp; het artikel beschrijft of analyseert het ontwerp van een relevant DM-volwassenheidsmodel.
- Volledige tekst beschikbaar; dit is een pragmatisch criterium i.v.m. de beschikbare OU-licenties.

Wanneer een artikel niet aan een bepaald criterium voldoet, worden de volgende criteria niet meer expliciet getoetst. Daarnaast is een stopcriterium toegepast. Er is gestopt met analyseren na het tiende artikel op rij dat niet voldoet aan de vier criteria. Op de gevonden artikelen wordt *backward snowballing* toegepast om het oorspronkelijk bronmateriaal van de modellen te vinden, waarnaar in de gevonden review artikelen wordt verwezen.

3.2. Uitvoering

3.2.1. Uitvoering voor EA-volwassenheidsmodellen

In Web of Science zijn vijftien artikelen gevonden na 1/1/2008 (zie tabel 17 in bijlage 1). Hierop zijn achtereenvolgens vier selectiecriteria toegepast. Dit bracht het aantal relevante artikelen terug naar twee:

- Analysing enterprise architecture maturity models: a learning perspective (Vallerand, 2017)
- An Analysis of Enterprise Architecture Frameworks (Meyer & al, 2011)

Op deze artikelen is “backward snowballing” toegepast op en dat heeft geleid tot elf EA-volwassenheidsmodellen:

- Gartner’s ITScore for EA
- Forrester’s EA maturity assessment tool
- IVI IT-Capability Maturity Framework
- NASCIO Enterprise Architecture Maturity Model
- SEI Capability Maturity Model Integration
- USDoC Enterprise Architecture Capability Maturity Model
- USGAO Enterprise Architecture Management Maturity Framework
- USOMB Enterprise Architecture Assessment Framework
- COBIT/ValIT
- Luftmann’s SAMM
- The MIT Center for Information Systems Research Enterprise Architecture Maturity Model

Vanuit het onderzoeksteam zijn een tweetal EA-volwassenheidsmodellen toegekend aan dit onderzoek:

- IT-Capability Maturity Framework (Curley, 2016)
- Enterprise Architecture Maturity Model (NASCIO, 2003)

3.2.2. Uitvoering voor DM-volwassenheidsmodellen

Met de query en de zoekopties zijn in Google Scholar in eerste instantie 5380 artikelen gevonden. Google Scholar sorteert deze artikelen op relevantie en in deze volgorde zijn de resultaten geanalyseerd op basis van titel en abstract, waarbij een stopcriterium is toegepast. Er is gestopt met analyseren na het tiende artikel op rij dat niet voldoet aan de selectiecriteria (zie tabel 18 in bijlage 2). Dit heeft geleid tot de volgende artikelen over DM-volwassenheid:

- MD3M: The master data management maturity model (Spruit & Pietzka, 2015)
- Research and application of data management based on Data Management Maturity Model (Baolong & al, 2018)

Het artikel over MD3M bevat het MD3M-model in de bijlage. Op het artikel over DMM is *backward snowballing* toegepast. Zo zijn de volgende DM-volwassenheidsmodellen gevonden:

- Master data management maturity model (MD3M) (Spruit & Pietzka, 2015)
- Data Management Maturity Model (DMM) (CMMI Institute, 2018)

3.3. Resultaten en conclusies

3.3.1. Gevonden modellen voor EA-volwassenheid

IT-CMF

De 2e editie van het IT-Capability Maturity Framework (IT-CMF) werd ontwikkeld door het Innovation Value Institute in juni 2016. Dit model kan maturiteit toetsen op een hoog abstractieniveau, maar ook in voldoende detail. De focus van dit maturity model is immers breder dan EA, aangezien het niet alleen de traditionele EA-lagen aftoetst (i.e., business, application, en technology) maar ook strategie

(i.e., planning, finance en governance) en operatie (i.e., projectmanagement, servicemanagement en quality-management). IT-CMF is process-based, omdat het de activiteiten van verschillende stakeholders toetst binnen EA in termen van input, output en doelen, maar ook characteristics-based, want het toetst de karakteristieken, criteria, categorieën van EA (Meyer & al, 2011). Het model is eerder descriptief dan prescriptief omdat het wil vermijden om te prescriptief te zijn, wat moeilijk is aangezien iedere organisatie anders is (Curley, 2016). De volwassenheidsniveaus van IT-CMF zijn te vinden in tabel 19 in bijlage 3. IT-CMF toetst de volwassenheid van aspecten in vier perspectieven:

- *managing IT like a business*: verandering van focus op technologie naar focus op klanten en bedrijfsprocessen
- *managing the IT budget*: duurzame bekostiging van IT diensten
- *managing IT for business value*: bedrijfswaarde als motivatie voor IT-investeringen
- *managing the IT capability*: systematische aanpak voor onderhoud en ontwikkeling van IT-diensten

Omdat het vierde perspectief een sterke relatie heeft met AVG zijn relevante aspecten in dat perspectief in relatie gebracht met de basisbeginselen van AVG (zie tabel 1 voor de relevante aspecten, zie volledige tabel 23 in bijlage 4).

Tabel 1 IT-CMF: Managing the IT capability aspecten (IVI, 2018) in relatie met AVG-basisbeginselen

IT-CMF: managing the IT capability	**Omschrijving**	**Gerelateerd AVG-beginsel**	**Argumentatie**
Information Security Management	Managen van beleid en controle voor integriteit, vertrouwelijkheid, verantwoordelijkheid, bruikbaarheid en beschikbaarheid van informatie (IVI, 2018).	Integriteit en vertrouwelijkheid	Door het managen van beleid en controle voor informatiebeveiliging wordt integriteit en vertrouwelijkheid van persoonlijke data verhoogd.
Personal Data Protection	Ontwerpen en toepassen van beleid, systemen en controle voor het verwerken van persoonlijke en privacygevoelige data m.b.t. levende personen in alle digitale, geautomatiseerde en handmatige verwerking. Dit garandeert de privacy van betrokkenen en het feit dat de organisatie persoonlijke data alleen gebruikt voor het specifieke doel afgestemd met de betrokkenen (IVI, 2018).	Rechtmatigheid, behoorlijkheid en transparantie. Doelbinding	Het afstemmen van het gebruik van persoonlijke data met betrokkenen maakt het opslaan en verwerken van persoonlijke data transparant. Het specifieke doel van de verwerking leidt tot de doelbinding.

EAMM

Het Enterprise Architecture Maturity Model (EAMM) werd ontwikkeld door de organisatie NASCIO (Meyer & al, 2011). De meest recente versie is versie 1.3 van december 2003. Het model is *characteristics-based*, want het toetst de karakteristieken, criteria en categorieën van EA. EAMM focust op strategie (en dan met name *governance*) en op architectuur en heeft weinig focus op *operations*. De volwassenheidsniveaus van EAMM zijn te vinden in tabel 20 in bijlage 3. EAMM toetst op een achttal aspecten (zie volledige tabel 24 in bijlage 4) en deze zijn, indien relevant, in relatie gebracht met AVG-beginselen (zie tabel 2).

Tabel 2 EAMM-aspecten (NASCIO, 2003, p. 6) in relatie met AVG-basisbeginselen

EAMM-aspect (NASCIO, 2003)	**Omschrijving**	**Gerelateerd AVG-beginsel**	**Argumentatie**
EA Blueprint	Verzameling van standaarden en specificaties (NASCIO, 2003, p. 6)	Doelbinding	De EA-standaarden en -specificaties beschrijven de alignment tussen bedrijfsprocessen, informatie en technologie. Deze alignment versterkt de doelbinding van de verwerking van persoonlijke data, omdat bedrijfsprocessen aan benodigde informatie gekoppeld worden.

3.3.2. Gevonden modellen voor DM-volwassenheid

MD3M

Het MD3M-model is ontwikkeld door Spruit en Pietzka (Spruit & Pietzka, 2015). Het model is *characteristics-based*, want het beschrijft de karakteristieken van effectief datamanagement. Het is niet *process-based* omdat het model toepasbaar moet zijn in verschillende organisaties, die verschillende processen kennen (Spruit & Pietzka, 2015, p. 1070). De volwassenheidsniveaus van MD3M zijn te vinden in in tabel 21 in bijlage 3. MD3M toetst op een vijftal hoofdaspecten (zie volledige tabel 25 in bijlage 4) en deze zijn, indien relevant, in relatie gebracht met AVG-beginselen (zie tabel 3).

Tabel 3 MD3M-aspecten (Spruit & Pietzka, 2015, p. 1072) in relatie met AVG-basisbeginselen

MD3M-aspect (Spruit & Pietzka, 2015, p. 1072)	**Omschrijving**	**Gerelateerd AVG-beginsel**	**Argumentatie**
Data Quality	Assessment of Data Quality, Impact on Business, Awareness of Quality Gaps, Improvement	Juistheid	Analyseren en verbeteren van datakwaliteit verbetert de juistheid van persoonlijke data.
Usage & Ownership	Data Usage, Data Ownership, Data Access	Rechtmatigheid, behoorlijkheid en transparantie	Beschrijving van gebruik en eigenaarschap van en toegang tot data binnen de organisatie dragen bij aan de rechtmatigheid, behoorlijkheid en transparantie van persoonlijke data.
Data Protection	Data Protection	Integriteit en vertrouwelijkheid	Bescherming van data verbetert de integriteit en vertrouwelijkheid van persoonlijke data.
Maintenance	Storage, Data Lifecycle	Opslagbeperking	Opslag en data lifecycle dragen bij aan opslagbeperking van persoonlijke data.

DMM

Het Data Management Maturity model werd ontwikkeld door het CMMI-instituut (CMMI Institute, 2018). De laatste versie van het model is versie 1.1. Het model is process-based, d.w.z. het is erop gericht om processen en activiteiten voor *datamanagement* te verbeteren. DMM definieert de eisen en activiteiten voor effectief data Management op een descriptieve manier. DMM schrijft dus niet voor hoe een organisatie de verbeteringen moet doorvoeren. De volwassenheidsniveaus van DMM zijn te vinden in tabel 22 in bijlage 3. DMM toetst op een zestal hoofdaspecten (zie volledige tabel 26 in bijlage 4) en deze zijn, indien relevant in relatie gebracht met AVG-beginselen (zie tabel 4).

Tabel 4 DMM-aspecten (CMMI Institute, 2018, pp. 11-138) in relatie met AVG-beginselen.

DMM-aspect (CMMI Institute, 2018)	**Omschrijving**	**Gerelateerd AVG-beginsel**	**Argumentatie**
Data Governance Governance Management, Business Glossary, Metadata Management	Best practices voor een breed draagvlak in de praktijk en senior-level toezicht in de effectiviteit van datamanagement (CMMI Institute, 2018, p. 41)	Rechtmatigheid, behoorlijkheid en transparantie	Het toezicht op datamanagement van persoonsdata op senior level draagt bij aan het garanderen van de rechtmatigheid, behoorlijkheid en transparantie van de verwerking van persoonlijke data.
Data Quality Data Quality Strategy, Data Profiling, Data Quality Assessment, Data Cleansing	Best practices voor het definiëren van een aanpak voor het detecteren en corrigeren van foutieve data om te borgen dat de juiste data beschikbaar is voor gebruik in bedrijfsprocessen, beslissingen en planning. (CMMI Institute, 2018, p. 64)	Juistheid	Detectie en correctie van foutieve persoonsdata draagt bij aan de juistheid van persoonlijke data.
Data Operations Data Requirements Definition, Data Lifecycle Management, Provider Management	Best practices voor het specificeren van data requirements en het managen van geïmplementeerde data door de gehele organisatie (CMMI Institute, 2018, p. 89)	Doelbinding	De afstemming van data requirements op bedrijfsdoelen draagt bij aan de doelbinding van de verwerking van persoonlijke data.
Platform & Architecture Architectural Approach, Architectural Standards, Data Management Platform, Data Integration, Historical Data & Archiving	Best practices voor het bepalen van methoden en standaarden die borgen dat het datamanagement platform de bedrijfsdata integreert, vasthoudt en archiveert om bedrijfsdoelen te ondersteunen. (CMMI Institute, 2018, p. 108)	Opslagbeperking Minimale gegevensverwerking.	Het platform dat bedrijfsdata vasthoudt om bedrijfsdoelen te ondersteunen realiseert de opslagbeperking van persoonlijke data. De architectuur van het platform stemt de verwerking van persoonlijke data af op de bedrijfsdoelen zodat niet meer verwerkt wordt dan noodzakelijk is.

3.3.3. Opstellen model AVG-volwassenheid

In de voorgaande paragrafen zijn twee EA-volwassenheidsmodellen en twee DM-volwassenheidsmodellen beschreven. De volwassenheidsniveaus uit die vier modellen worden geïntegreerd tot volwassenheidsniveaus voor het AVG-volwassenheidsmodel. Van de EA-modellen heeft EAMM zes niveaus, waarbij het 0-niveau dat aangeeft dat er geen EA is. De beide DM-modellen gaan uit van vijf niveaus. Omdat de aspecten van de DM-modellen sterker gerelateerd zijn met AVG, leveren ze meer input en daarom kiezen we voor het AVG-volwassenheidsmodel ook voor vijf niveaus. Bij de integratie van statements worden overlappingen verwijderd en aanvullingen geïntegreerd, zoals te zien is in tabel 5.

Tabel 5 Volwassenheidsniveaus van vier modellen en integratie naar volwassenheidsniveaus van het AVG-model

Model	0	1	2	3	4	5
ITCMF		**Initial:** Inadequate benadering en gefragmenteerde scope, zelden herhaalbare uitkomsten.	**Basic:** Benadering gedefinieerd met inconsistenties, gelimiteerde scope met hiaten, soms herhaalbare uitkomsten.	**Intermediate:** Standaard benaderingen, inconsistenties worden aangepakt. Scope in lijn met een afdeling (bij IT). Vaak herhaalbare uitkomsten.	**Advanced:** Benadering is aanpasbaar voor innovatie. Scope dekt de hele organisatie. Zeer vaak herhaalbare uitkomsten.	**Optimizing:** Benadering is van wereldklasse. Scope voorbij de eigen organisatie. Praktisch altijd herhaalbare uitkomsten.
EAMM	**No program** Geen gedocumenteerd architectuur raamwerk.	**Informal Program** Basis architectuur en standaarden gedefinieerd, maar informeel uitgevoerd.	**Repeatable Program** Basisarchitectuur en standaarden gedefinieerd. Getraceerde en geverifieerde uitvoering.	**Well-Defined Program** Goed gedefinieerde EA met gebruik van standaard of aangepaste templates.	**Managed Program** Prestatie wordt gemeten en geanalyseerd. Op de uitkomst wordt geacteerd. De meting wordt gebruikt voor voorspellingen.	**Continuously Improving Vital Program** Volwassen processen. Doelen voor effectiviteit zijn gericht op bedrijfsdoelen. Voortdurende verbeteringen.
MD3M		**Initial:** Besef van issues mbt MDM op operationeel level. Initiele stappen zijn gezet.	**Repeatable:** Maatregelen door individuen voor individuele problemen. Geen samenwerking. Operationeel.	**Defined process**: Samenwerking op tactisch niveau. Besef van verschillende initiatieven.	**Managed and measurable:** Best practices voor MDM. Gedefinieerde processen op tactisch niveau.	**Optimized:** Geoptimaliseerde MDM. Verbeterde efficientie van de organisatie. Tactische benadering op het onderwerp.
DMM		**Performed:** Processen zijn ad-hoc, reactief en worden niet toegepast over verschillende domeinen.	**Managed:** Processen worden gepland en uitgevoerd conform beleid door getrainde werknemers in samenspraak met relevante stakeholders.	**Defined:** Een set van standaard processen is vastgelegd en wordt gevolgd. Specifieke behoeftes worden vervuld door processen conform beleid te baseren op de standaard processen.	**Measured:** Metrics van processen zijn vastgelegd en worden gebruikt voor data management. Dit houdt in: management van afwijkingen, voorspellingen en analyse. Processen worden gemanaged tijdens de uitvoering.	**Optimized:** Processen worden geoptimaliseerd door het toepassen van niveau 4 analyse voor verbetermogelijkheden. Best practices worden gedeeld met andere bedrijven.
Integratie naar AVG-volwassenheids model.		**Performed** Processen voor AVG zijn adhoc, informeel en worden toegepast op gefragmenteerde scope	**Managed** Processen voor AVG worden gepland en uitgevoerd in gelimiteerde scope.	**Defined** Standaard processen zijn gedefinieerd en worden gevolgd. Specifieke behoeften worden vervuld door processen afgeleid van standaard processen.	**Measured** AVG-processen worden gemeten en geanalyseerd om afwijkingen vast te stellen en voorspellingen te doen. AVG-processen worden gemanaged tijdens uitvoering.	**Optimized** Processen worden geoptimaliseerd op basis van analyse. Effectiviteit wordt getoetst aan bedrijfsdoelen. Best practices worden gedeeld met andere bedrijven.

De relevante aspecten per volwassenheidsniveau (zie tabel 27 in bijlage 5) uit de vier volwassenheidsmodellen worden hieronder geïntegreerd in een AVG-volwassenheidsmodel. Voor de relevante aspecten uit IT-CMF-model zijn geen statements per niveau beschikbaar, maar de algemene aspectbeschrijving wordt meegenomen in de statements van het nieuwe AVG-model. De volwassenheidsaspecten uit de vier modellen worden per volwassenheidsaspect en per volwassenheidsniveau geïntegreerd. Bij het eerste ontwerp zijn de statements tevens minder datatechnisch gemaakt door statements uit het Privacy Volwassenheidsmodel (Koers & al, 2017) te integreren. Ook zijn de statements over de dimensies heen consistent gemaakt. Dit heeft geleid tot de eerste versie van het AVG-volwassenheidsmodel. (zie onderstaande tabel 6).

Tabel 6 AVG-beginselen gerelateerd aan geïntegreerde volwassenheidsaspecten uit IT-CMF/EAMM/MD3M/DMM/Privacy volwassenheidsmodel

AVG-volwassenheidsmodel					
	1 - Performed	2 - Managed	3 - Defined	4 - Measured	5 - Optimized
"Rechtmatigheid, behoorlijkheid en transparantie; de verwerking van persoonsgegevens moet rechtmatig, behoorlijk en transparant zijn.	Eigenaarschap en verantwoordelijkheid voor persoonsdata worden soms in projecten toegewezen (CMMI Institute, 2018, p. 44) (Spruit & Pietzka, 2015, p. 1075). Gebruik van persoonsdata is bij sommige diensten afgestemd met betrokkenen (IVI, 2018).	Logisch consistente rollen en verantwoordelijkheden zijn vastgelegd voor persoonsdata op prioriteit voor de organisatie (CMMI Institute, 2018, p. 44). (Spruit & Pietzka, 2015, p. 1075). Beleid en processen managen de afstemming van gebruik van persoonsdata met betrokkenen (IVI, 2018).	Organisatiebrede governance van persoonsdata met alle bedrijfsonderdelen die persoonsdata met hoge prioriteit gebruiken en/of leveren (CMMI Institute, 2018, p. 45) (Spruit & Pietzka, 2015, p. 1075). Gedefinieerde afstemming van gebruik van persoonsdata met betrokkenen (IVI, 2018).	Governance van persoonsdata wordt statistisch geëvalueerd of deze de organisatie op geschikte wijze bijstuurt. Op basis van deze analyse wordt governance van persoonsdata bijgesteld (CMMI Institute, 2018, p. 46). De afstemming met betrokkenen over gebruik van persoonsdata wordt gemeten (IVI, 2018).	Eigen best practices voor governance van persoonsdata worden gedeeld. Governance voor persoonsdata wordt continue verfijnd en verbeterd (CMMI Institute, 2018, p. 46). De afstemming met betrokkenen over het gebruik van persoonsdata wordt continue verbeterd (IVI, 2018).
Doelbinding; de verwerking moet gebonden zijn aan specifieke verzameldoelen.	Stakeholders, beleid en controle doen informeel en inconsistent review en goedkeuring van requirements van persoonsdata en garanderen daarmee soms dat de organisatie persoonlijke data alleen gebruikt voor het specifieke doel (CMMI Institute, 2018, p. 93) (NASCIO, 2003, p. 8) (IVI, 2018).	Requirements voor persoonsdata t.a.v. bedrijfsdoelen worden gevolgd en beheersen zo het feit dat de organisatie persoonsdata alleen gebruikt voor het specifieke doel (CMMI Institute, 2018, p. 94) (IVI, 2018).	Voor bedrijfsprocessen die persoonsdata produceren zijn requirements voor persoonsdata gedefinieerd, gevalideerd op bedrijfsprioriteit en geïntegreerd in een standaard raamwerk. Beleid en controle garanderen altijd het feit dat de organisatie persoonsdata alleen gebruikt voor het specifieke doel. bedrijfsdoelen (CMMI Institute, 2018, p. 94) (IVI, 2018).	Gedefinieerde meetwaarden borgen dat requirements voor persoonsdata invulling geven aan bedrijfsdoelen, en eventuele correcties worden uitgevoerd. (CMMI Institute, 2018, pp. 96-97) (NASCIO, 2003, p. 11). Beleid en controle garanderen op meetbare wijze het feit dat de organisatie persoonsdata alleen gebruikt voor het specifieke doel. (IVI, 2018)	Best practices voor requirements voor persoonsdata t.a.v. doelbinding worden binnen de sector gedeeld (CMMI Institute, 2018, p. 97) (NASCIO, 2003, p. 13). Beleid en controle worden continue verbeterd en garanderen dat de organisatie persoonsdata alleen gebruikt voor het specifieke doel. (IVI, 2018)
Minimale gegevensverwerking; de persoonsgegevens moeten toereikend zijn, ter zake dienend, en beperkt tot wat noodzakelijk is.	Benodigde persoonsdata wordt in data-architectuur vastgelegd op informele en inconsistente wijze (CMMI Institute, 2018, p. 110).	Met persoonsdata-architectuur worden issues als dubbele opslag, uitzonderingen op standaardgebruik gemanaged. Creatie en gebruik van persoonsdata is traceerbaar in alle bronnen (CMMI Institute, 2018, p. 111).	Een gedefinieerd datarationalisatieproces borgt de minimale gegevensverwerking: persoonsdata wordt gecheckt op dubbele opslag, de noodzaak voor business-doelen. (CMMI Institute, 2018, p. 113).	Op basis van statistische analyse van het datarationalisatieproces worden correcties op persoonsdata-architectuur uitgevoerd en gebruikt als input voor design. (CMMI Institute, 2018, p. 113).	Voorspellingen worden geëvalueerd in relatie tot een continu proces van verbetering van persoonsdata-architectuur. Best practices over persoonsdata-architectuur worden gedeeld binnen de sector (CMMI Institute, 2018, p. 115).
Juistheid; de gegevens moeten juist zijn.	Juistheid van persoonsdata wordt ad hoc getoetst en resultaten worden vastgelegd (CMMI Institute, 2018, p. 78) (Spruit & Pietzka, 2015, p. 1074).	Doelen en standaarden voor de toetsing van juistheid van persoonsdata zijn vastgelegd, gebruikt en onderhouden met standaard technieken en processen (CMMI Institute, 2018, p. 78) (Spruit & Pietzka, 2015, p. 1074).	Juistheid van persoonsdata door gedefinieerd beleid en controls, i.e. preventieve en correctieve maatregelen, zoals periodieke toetsing volgens schema en na specifieke triggers, en mogelijkheden voor correctie door betrokkenen. (CMMI Institute, 2018, p. 80) (Spruit & Pietzka, 2015, p. 1074) (Koers & al, 2017)	Meting van processen voor juistheid op kritische attributen van alle persoonsdata wordt systematisch vastgelegd in rapporten (CMMI Institute, 2018, p. 81). (Spruit & Pietzka, 2015, p. 1074).	Best practices voor de juistheid van persoonsdata worden in de sector gedeeld. Juistheid van persoonsdata en de toetsing daarvan wordt continue en geautomatiseerd verbeterd. (CMMI Institute, 2018, p. 81) (Spruit & Pietzka, 2015, p. 1074).

Opslagbeperking; de gegevens mogen niet langer bewaard worden dan nodig.	Historische persoonsdata ondersteunt soms bedrijfsdoelen, datastores worden geback-upt en data wordt gearchiveerd (CMMI Institute, 2018, pp. 133-134) (Spruit & Pietzka, 2015, p. 1075).	Logica, toegang, aanpassing, opslag, vernietiging en auditing van persoonsdata worden gecontroleerd door beleid en processen (CMMI Institute, 2018, p. 134) (Spruit & Pietzka, 2015, p. 1075).	Gedefinieerde processen voor audit en feedback met stakeholders en regelgevers versterken opslag en archiveringsbeleid m.b.t historische persoonsdata (CMMI Institute, 2018, p. 135). Automatische tools checken regelmatig op dubbele opslag. Richtlijnen zijn opgesteld voor persoonsdata lifecycle (Spruit & Pietzka, 2015, p. 1075).	Metingen worden gebruikt om beleid m.b.t. opslag en -archivering van persoonsdata te evalueren en verbeteren (CMMI Institute, 2018, p. 136). Datalogica wordt regelmatig gecheckt op persistentie, prestatie en efficiëntie. Voor ieder persoonsdata-item is één bron vastgesteld (Spruit & Pietzka, 2015, p. 1075).	De organisatie deelt beleid en best practices over historische persoonsdata en archivering in haar sector (CMMI Institute, 2018, p. 136). Continu procesverbetering voor de opslag van persoonsdata met mogelijkheden voor analyse en voorspellingen (Spruit & Pietzka, 2015, p. 1075).
Integriteit en vertrouwelijkheid; gegevens moeten goed beveiligd zijn en vertrouwelijk blijven".	Integriteit en vertrouwelijkheid van persoonsdata zijn informeel en inconsistent beschreven en gemanaged. (IVI, 2018). Informeel en inconsistent, de technische eisen voor bescherming van persoonsdata zijn vervuld (Spruit & Pietzka, 2015, p. 1075).	Integriteit en vertrouwelijkheid van persoonsdata zijn beschreven en gemanaged (IVI, 2018). Toegang tot data wordt alleen geactiveerd op verzoek (Spruit & Pietzka, 2015, p. 1075).	Beleid en controls zijn gedefinieerd borgen integriteit en vertrouwelijkheid van persoonsdata (IVI, 2018). Richtlijnen bepalen welke rollen datatoegang krijgen (Spruit & Pietzka, 2015, p. 1075).	Effectiviteit van beleid en controls voor integriteit, vertrouwelijkheid wordt gemeten (IVI, 2018). Voor systemen met toegang tot persoonsdata bestaan wachtwoorden die voldoen aan algemene security standaarden en die regelmatig aangepast worden (Spruit & Pietzka, 2015, p. 1075).	Beleid en controls voor integriteit en vertrouwelijkheid van persoonsdata worden continue gemeten en verfijnd (IVI, 2018). Best practices voor gegevensbescherming worden gedeeld in de sector. Security awareness voor bescherming van persoonsdata wordt verhoogd onder personeel (Spruit & Pietzka, 2015, p. 1075).

3.3.4. Doel van het vervolgonderzoek

In voorgaande paragrafen is een AVG-volwassenheidsmodel ontwikkeld op basis van bestaande EA- en DM-volwassenheidsmodellen. Het doel van het vervolgonderzoek is om dit model te evalueren en verbeteren zodat het geschikt wordt voor toepassing in de praktijk. Conform de methode van Becker et al (2009) wordt het model gedemonstreerd en geëvalueerd in de praktijk. Dit gebeurt in iteraties, waarbij voor iedere iteratie bepaald wordt of het model is verbeterd. Daarmee wordt antwoord gegeven op de vraag: “Is het ontwikkelde AVG-volwassenheidsmodel toepasbaar binnen organisaties?” Hiervoor zijn interviews nodig met personen die vanuit hun functie de kennis en ervaring hebben om de AVG-volwassenheid van de organisatie te scoren in de demonstratie. Met deze personen, de functionaris gegevensbescherming en de informatiearchitect, moet vervolgens geëvalueerd worden hoe het gedemonstreerde model toepasbaar is en hoe het verbeterd kan worden.

4. Resultaten

Het AVG-volwassenheidsmodel is gedemonstreerd en geëvalueerd worden in twee organisaties, een organisatie in het hoger onderwijs en een organisatie in de zorg.

4.1. Demonstratie

In beide organisaties is het model gedemonstreerd in een gezamenlijk interview met twee respondenten, i.e. de functionaris gegevensbescherming (FG) en de informatiearchitect (IA). Op basis van de antwoorden op demonstratievragen (zie tabellen 28 en 29 in bijlage 6) hebben de organisaties als volgt gescoord in het AVG-volwassenheidsmodel (zie tabel 7).

Tabel 7 Demonstratiescores organisaties

	Educatieve organisatie	Zorgorganisatie
Rechtmatigheid, behoorlijkheid en transparantie	3 - Defined	3 - Defined
Doelbinding	2 - Managed	3 - Defined
Minimale gegevensverwerking	2 - Managed	3 - Defined
Juistheid	3 - Defined	5 - Optimized
Opslagbeperking	2 - Managed	2 - Managed
Integriteit en vertrouwelijkheid	4 - Measured	3 - Defined

De educatieve organisatie scoorde bovengemiddeld (‘4-measured’) op ‘Integriteit en vertrouwelijkheid’ door gedegen beleid, ingerichte correctieve en preventieve maatregelen, structurele audits en security awareness-trainingen. Op het gebied van ‘doelbinding’, ‘minimale gegevensverwerking’ en ‘opslagbeperking’ scoorde de organisatie ‘2-managed’, omdat beleid en controls nog niet standaard gedefinieerd waren, al waren de projecten hiervoor al wel gestart.

De zorgorganisatie scoorde zeer goed (‘5-optmized’) op ‘Juistheid’, doordat in ieder contact met patiënten en door automatische systemen de juistheid van persoonsgegevens continu verbeterd wordt. Op het gebied van opslagbeperking scoorde de zorgorganisatie ‘2-managed’, omdat beleid en controls hiervoor nog niet voor alle informatievoorziening gedefinieerd was.

4.2. Eerste evaluatie

Na demonstratie van het model zijn de waargenomen bruikbaarheid, waargenomen gebruiksgemak, intentie voor gebruik, de relevantie per vraag en de algemene tevredenheid geëvalueerd met de vier respondenten.

Met vragen gebaseerd op het Technology Acceptance Model (Moody, 2003) zijn eerst de waargenomen toepasbaarheid, het waargenomen gebruiksgemak en de intentie voor gebruik gemeten (zie tabel 30 in bijlage 7). Per respondent zijn gemiddelde scores berekend, waarbij scores op negaties gespiegeld zijn in de 7-punts Likertschaal. In onderstaande tabel 8 zijn de gemiddelde scores per gebruiker en in totaal weergegeven.

Tabel 8 TAM: waargenomen bruikbaarheid, gebruiksgemak en intentie voor gebruik in eerste evaluatie

	Respondent 1	Respondent 2	Respondent 3	Respondent 4	Gemiddeld
Waargenomen bruikbaarheid	4,4/7	5,4/7	5,5/7	5,8/7	5,3/7
Waargenomen gebruiksgemak	2,7/7	4,3/7	4,7/7	4,3/7	4/7
Intentie voor gebruik	5/7	4,5/7	6/7	6/7	5,4/7

Uit de evaluatie blijkt dat respondent 1 kritisch tegenover het model staat, maar wel de intentie heeft om het te gebruiken. Gemiddeld zijn de respondenten het enigszins eens tot eens met de waargenomen bruikbaarheid (5,3/7) en hun intentie om het model te gaan gebruiken (5,4/7). Gemiddeld is men neutraal (4/7) over het waargenomen gebruiksgemak, vanwege de datatechnische termen, de inconsistente dimensies en het ontbreken van specifieke AVG-aspecten Daarin dient het model nog verbeterd te worden.

Vervolgens is voor iedere demonstratievraag bepaald (zie tabellen 31-34 in bijlage 7) wat de relevantie van de vraag is voor het toetsen van de AVG-volwassenheid binnen de specifieke dimensie, i.e. het AVG-basisprincipe. In onderstaande tabel 9 wordt het aantal respondenten per vraag en per score weergegeven.

Tabel 9 Relevantie vragen in eerste evaluatie: aantal respondenten per score

	Zeer oneens	Oneens	Enigszins oneens	Niet oneens, niet eens	Enigszins eens	Eens	Zeer eens
	1	2	3	4	5	6	7
Relevantie vragen voor de toetsing van AVG-volwassenheid							
Vraag RBT1 is relevant om de AVG-volwassenheid binnen de dimensie “Rechtmatigheid, behoorlijkheid en transparantie” te toetsen.					1	1	2
Vraag RBT2 is relevant om de AVG-volwassenheid binnen de dimensie “Rechtmatigheid, behoorlijkheid en transparantie” te toetsen.						3	1
Vraag D1 is relevant om de AVG-volwassenheid binnen de dimensie “Doelbinding” te toetsen.					1	3	
Vraag MG1 is relevant om de AVG-volwassenheid binnen de dimensie “Minimale gegevensverwerking” te toetsen.		1			3		
Vraag J1 is relevant om de AVG-volwassenheid binnen de dimensie “Juistheid” te toetsen.					1	3	
Vraag O1 is relevant om de AVG-volwassenheid binnen de dimensie “Opslagbeperking” te toetsen.					4		
Vraag IV1 is relevant om de AVG-volwassenheid binnen de dimensie “Integriteit en vertrouwelijkheid” te toetsen.					1	3	
Vraag IV2 is relevant om de AVG-volwassenheid binnen de dimensie “Integriteit en vertrouwelijkheid” te toetsen.					3	1	

Voor de relevantie van de demonstratievragen is vervolgens conform de Delphi-casestudytechniek (Bruin & Rosemann, 2007) berekend over er consensus of stabiliteit vast te stellen in de antwoorden van de respondenten (zie tabel 10).

Tabel 10 Consensus voor relevantie in eerste evaluatie

	Minstens 50% scoort 1-2 of 6-7	Minstens 75% van de respondenten scoort 1,2,3,5,6 of 7	Geen strijdige extremen (geen 1 en 7)	Interkwartielbereik < 1,5	Consensus
Vraag RBT1	X	X	X	X	X
Vraag RBT2	X	X	X	X	X
Vraag D1	X	X	X	X	X
Vraag MG1		X	X		
Vraag J1	X	X	X	X	X
Vraag O1		X	X	X	
Vraag IV1	X	X	X	X	X
Vraag IV2		X	X	X	

Over de vragen MG1, O1 en IV2 blijkt uit de scores van de respondenten volgens de criteria geen consensus. Voor deze vragen is de stabiliteit van de scores bepaald door de free-marginal kappa (Randolph, 2005) te berekenen.

Tabel 11 Stabiliteit voor relevantie in eerste evaluatie

	Free-marginal kappa	Stabiliteit
Vraag MG1	0.25	
Vraag O1	1.00	X
Vraag IV2	1.00	X

Bij een free-marginal kappa groter dan 0,4 (Randolph, 2005) is er sprake van stabiliteit. Voor vraag MG1 over minimale gegevensverwerking is geen consensus of stabiliteit vastgesteld en deze vraag is aangepast in het model op basis van de kwalitatieve feedback (zie tabellen 31-34 in bijlage 7) voor minimale gegevensverwerking. De aangedragen AVG-aspecten over proportionaliteit, subsidiariteit en anonimisatie, alsmede het verwijderen van de termen dubbele dataopslag en data-architectuur, zijn in vraag MG1 verwerkt.

Omdat het gebruiksgemak (score 4/7) verbeterd moest worden, zijn er toch extra aanpassingen (zie tabel 12) gedaan aan de andere vragen op basis van de kwalitatieve feedback (zie tabellen 31-34 in bijlage 7). Dit was mogelijk omdat de gegeven feedback concreet genoeg was om verdere verbeteringen aan te brengen in het model. Deze (niet-verplichte) aanpassingen zijn meegenomen in de tweede evaluatie via email.

Tabel 12 Extra aanpassingen aan demonstratievragen na eerste evaluatie

Vraag	Aanpassing
RBT1	• AVG-term verwerkingsregister opgenomen
D1	• doelbinding tweeledig gemaakt, enerzijds doel vastleggen en anderzijds alleen voor dat doel gebruiken • term requirements voor persoonsdata verwijdert omdat deze te datatechnisch is
J1	• juistheid term toegelicht
O1	• datalogica, aanpassing, toegang verwijderd • bewaartermijn toegevoegd • automatische tools bij N3 verwijderd • term vernietiging van data opgenomen
IV1	• specifieke maatregelen opgenomen: multifactor-authenticatie, encryptie, checksum en termen toegelicht • security awareness uit IV2 naar IV1 verplaatst, omdat security awareness in brede zin over integriteit en vertrouwelijkheid gaat
Alle vragen	• niveaus over dimensies consistenter gemaakt in bewoordingen • alle antwoordopties laten beginnen met niveau-aanduiding: performed, managed, defined, measured, optimized

Tot slot is in deze eerste evaluatie de algemene tevredenheid (zie tabel 35 in bijlage 7) over het model geëvalueerd door de vier respondenten te laten scoren op een 11-punts Likertschaal (0-10).

De algemene tevredenheid is minimaal 5, gemiddeld 6,5 met een standaarddeviatie van 0,87. Omdat het stopcriterium “gemiddeld ≥ 7,5” nog niet gehaald is, wordt conform de methode nog een iteratie van evaluatie gedaan.

4.3. Tweede evaluatie

De aangepaste modelvragen zijn via e-mail voorgelegd aan de respondenten en deze hebben nogmaals de relevantie per vraag gescoord (zie tabel 13).

Tabel 13 Relevantie vragen in tweede evaluatie: aantal respondenten per score

	Zeer oneens	Oneens	Enigszins oneens	Niet oneens, niet eens	Enigszins eens	Eens	Zeer eens
Tweede Evaluatie	1	2	3	4	5	6	7
Relevantie vragen voor de toetsing van AVG-volwassenheid							
Vraag RBT1 is relevant om de AVG-volwassenheid binnen de dimensie “Rechtmatigheid, behoorlijkheid en transparantie” te toetsen.						1	3
Vraag RBT2 is relevant om de AVG-volwassenheid binnen de dimensie “Rechtmatigheid, behoorlijkheid en transparantie” te toetsen.						1	3
Vraag D1 is relevant om de AVG-volwassenheid binnen de dimensie “Doelbinding” te toetsen.						1	3
Vraag MG1 is relevant om de AVG-volwassenheid binnen de dimensie “Minimale gegevensverwerking” te toetsen.						4	
Vraag J1 is relevant om de AVG-volwassenheid binnen de dimensie “Juistheid” te toetsen.						3	1
Vraag O1 is relevant om de AVG-volwassenheid binnen de dimensie “Opslagbeperking” te toetsen.						1	3
Vraag IV1 is relevant om de AVG-volwassenheid binnen de dimensie “Integriteit en vertrouwelijkheid” te toetsen.						1	3
Vraag IV2 is relevant om de AVG-volwassenheid binnen de dimensie “Integriteit en vertrouwelijkheid” te toetsen.						2	2

Vervolgens is voor de relevantie van de demonstratievragen consensus bepaald. Voor alle vragen was consensus (zie tabel 14) en daarom is er geen stabiliteit berekend.

Tabel 14 Consensus over relevantie in tweede evaluatie

	Minstens 50% scoort 1-2 of 6-7	Minstens 75% van de respondenten scoort 1,2,3,5,6 of 7	Geen strijdige extremen (geen 1 en 7)	Interkwartielbereik < 1,5	Consensus
Vraag RBT1	X	X	X	X	X
Vraag RBT2	X	X	X	X	X
Vraag D1	X	X	X	X	X
Vraag MG1	X	X	X	X	X
Vraag J1	X	X	X	X	X
Vraag O1	X	X	X	X	X
Vraag IV1	X	X	X	X	X
Vraag IV2	x	X	X	X	X

In de tweede evaluatie is ook de algemene tevredenheid door respondenten gescoord. Daarover zijn het minimum, het gemiddelde en de standaarddeviatie berekend. In tabel 15 is de toename van de algemene tevredenheid af te lezen.

Tabel 15 Toegenomen algemene tevredenheid in twee iteraties

Algemene tevredenheid	1e iteratie	2e iteratie	Verbetering
Minimum	5	7	+2
Gemiddelde	6,5	8	+1,5
Standaarddeviatie	0.87	0,71	-0,16

Op basis van de statistische analyse is na de tweede evaluatie bepaald dat er consensus en stabiliteit is voor de relevantie van de demonstratievragen en voldoende algemene tevredenheid over het model. Binnen dit onderzoek is het model daarom niet meer fundamenteel veranderd. Wel zijn een aantal gebruikte termen aangescherpt op basis van de kwalitatieve feedback bij de tweede evaluatie:

- De term persoonsdata is vervangen door persoonsgegevens.
- De term anonimisatie is vervangen door anonimisering en toegelicht.
- De toelichtingen voor proportionaliteit en subsidiariteit zijn verbeterd.

Overige verkregen kwalitatieve feedback wordt meegenomen in aanbevelingen voor verder onderzoek. Na twee iteraties van evaluatie is het resultaat een AVG-volwassenheidsmodel dat de naam AVGMM (AVG-maturiteitsmodel) krijgt en is beschreven in tabel 16. Organisaties kunnen dit model toepassen door de vragen te beantwoorden in tabel 42 bijlage 9.

Tabel 16 AVG-volwassenheidsmodel na twee iteraties

AVG-maturiteitsmodel (AVGMM v1.0)					
	1 - Performed	**2 - Managed**	**3 - Defined**	**4 - Measured**	**5 - Optimized**
"Rechtmatigheid, behoorlijkheid en transparantie; de verwerking van persoonsgegevens moet rechtmatig, behoorlijk en transparant zijn.	Eigenaarschap en verantwoordelijkheid voor persoonsgegevens worden ad hoc, informeel en inconsistent geborgd. Betrokkenen worden ad hoc, inconsistent en informeel geïnformeerd over het gebruik van hun persoonsgegevens	Het toewijzen van eigenaarschap en verantwoordelijkheid voor persoonsgegevens en het vastleggen van verwerking van persoonsgegevens in een verwerkingsregister wordt gemanaged. Processen managen dat betrokkenen geïnformeerd worden over de verwerking van hun persoonsgegevens.	Rollen in eigenaarschap en verantwoordelijkheid worden gedefinieerd met alle afdelingen die persoonsgegevens gebruiken/leveren. Vastlegging in een verwerkingsregister is gedefinieerd en geborgd. Het informeren van betrokkenen is organisatiebreed gedefinieerd en wordt geborgd door beleid en processen.	Governance op eigenaarschap en verantwoordelijkheid wordt gemeten. Vastlegging in een verwerkingsregister wordt gemeten. Het informeren van betrokkenen over verwerking van hun persoonsgegevens en beleid en controle daarop worden gemeten.	Governance op eigenaarschap, vastlegging in een verwerkingsregister en het informeren van betrokkenen over worden continu verbeterd. De organisatie deelt best practices voor governance op eigenaarschap, verwerkingsregister en afstemming met betrokkenen in de sector.
Doelbinding; de verwerking moet gebonden zijn aan specifieke verzameldoelen.	Doelbinding wordt adhoc, informeel en inconsistent geborgd.	Het vastleggen van het doel van persoonsgegevensverwerking en de naleving van de doelbinding worden gemanaged.	Het vastleggen van het doel van persoonsgegevensverwerking en de naleving van de doelbinding zijn gedefinieerd in een standaardraamwerk en worden geborgd door beleid, preventieve en correctieve maatregelen.	Het vastleggen van het doel van persoonsgegevensverwerking en de naleving van de doelbinding worden gemeten.	Het vastleggen van het doel van persoonsgegevensverwerking en de naleving van de doelbinding wordt continu verbeterd. De organisatie deelt best practices voor doelbinding in de sector.
Minimale gegevensverwerking; de persoonsgegevens moeten toereikend zijn, ter zake dienend, en beperkt tot wat noodzakelijk is.	Minimale gegevensverwerking wordt ad hoc, informeel en inconsistent geborgd.	Dataminimalisatie door proportionaliteit, subsidiariteit en anonimisering wordt gemanaged.	Dataminimalisatie door proportionaliteit en subsidiariteit voor productie, alsmede anonimisering voor onderzoek en test zijn gedefinieerd in een standaard raamwerk en geborgd door beleid, preventieve en correctieve maatregelen.	Dataminimalisatie door proportionaliteit en subsidiariteit en anonimisering worden gemeten.	Dataminimalisatie door proportionaliteit, subsidiariteit en anonimisering worden continu verbeterd. De organisatie deelt best practices voor dataminimalisatie in de sector.
Juistheid; de gegevens moeten juist zijn.	Juistheid van persoonsgegevens wordt ad hoc, informeel en inconsistent geborgd.	Juistheid van persoonsgegevens wordt gemanaged door processen.	Doelen en criteria voor juistheid zijn gedefinieerd in een standaard raamwerk en worden geborgd door beleid, preventieve en correctieve maatregelen, zoals periodieke en trigger-gebaseerde toetsing. Betrokkenen kunnen de juistheid van eigen persoonsgegevens (laten) aanpassen.	Juistheid van persoonsgegevens op kritische attributen van wordt gemeten en systematisch vastgelegd in rapporten.	Juistheid van persoonsgegevens wordt continu verbeterd. De organisatie deelt best practices voor juistheid in de sector.
Opslagbeperking; de gegevens mogen niet langer bewaard worden dan nodig.	Opslagbeperking wordt ad hoc, informeel en inconsistent geborgd.	Opslag en vernietiging van persoonsgegevens worden gemanaged door processen.	Bewaartermijnen van persoonsgegevens en processen voor opslag en vernietiging zijn gedefinieerd in een standaard raamwerk en worden geborgd door beleid voor lifecycle van persoonsgegevens. Voor ieder persoonsgegevens-item is één bron vastgelegd.	Lifecycle, opslag en vernietiging van persoonsgegevens wordt gemeten door audits en feedback door stakeholders en regelgevers.	Lifecycle, opslag en vernietiging van persoonsgegevens wordt continue verbeterd. De organisatie deelt best practices voor opslagbeperking in de sector.
Integriteit en vertrouwelijkheid; gegevens moeten goed beveiligd zijn en vertrouwelijk blijven".	Integriteit, vertrouwelijkheid en de toegang tot persoonsgegevens worden ad hoc, informeel en inconsistent geborgd.	Integriteit en vertrouwelijkheid van persoonsgegevens worden gemanaged in beheer en processen. Toegang tot persoonsgegevens wordt alleen geactiveerd op verzoek.	Beleid, zoals BIV-classificatie, en technische maatregelen zoals multi-factor authenticatie, encryptie en checksum zijn gedefinieerd en borgen de integriteit en vertrouwelijkheid van persoonsgegevens. Toegang tot persoonsgegevens is gedefinieerd in een standaard raamwerk van rollen en richtlijnen en wordt geborgd door autorisatiebeleid, authenticatiebeleid en technische maatregelen.	Integriteit en vertrouwelijkheid van persoonsgegevens worden gemeten en geaudit. Security Awareness wordt gemeten onder personeel. Toegang tot persoonsgegevens wordt gemeten en geaudit.	Integriteit en vertrouwelijkheid van persoonsgegevens en security awareness van personeel worden continu verbeterd. Beveiliging van toegang tot persoonsgegevens wordt continu verbeterd. De organisatie deelt best practices voor integriteit, vertrouwelijkheid en toegang tot persoonsgegevens in de sector.

5. Conclusies, discussie en aanbevelingen

5.1. Conclusies

In dit onderzoek is antwoord gegeven op de vraag hoe een AVG-volwassenheidsmodel ontwikkeld kan worden op basis van volwassenheidsmodellen binnen Enterprise Architectuur en Data Management".

Het model is ontwikkeld aan de hand van de DSR-methode (Hevner & al, 2004) en de ontwikkelmethode voor volwassenheidsmodellen van Becker (2009). In literatuurstudie zijn zoekqueries opgesteld volgens de Building Blocks-methode (Westerkamp & Veen, 2008) en deze queries zijn ingevoerd in Web of Science en Google Scholar. Hiermee zijn modellen gevonden voor EA en DM, te weten IT-CMF (IVI, 2018), EAMM (NASCIO, 2003), M3DM (Spruit & Pietzka, 2015) en DMM (CMMI Institute, 2018). Een eerste AVG-volwassenheidsmodel is tot stand gekomen door het combineren van zes AVG-basisprincipes (Schermer, 2018) met statements en -niveaus uit de gevonden volwassenheidsmodellen voor EA en DM.

Het model gaat uit van zes AVG-basisprincipes:

- 'rechtmatigheid, behoorlijkheid en transparantie',
- 'doelbinding',
- 'minimale gegevensverwerking',
- 'juistheid',
- 'opslagbeperking',
- 'integriteit en vertrouwelijkheid'

Deze basisprincipes worden getoetst op vijf niveaus, i.e. 'performed', 'managed', 'defined', 'measured' en optimized'.

De statements uit EA- en DM-volwassenheidsmodellen leverden een datatechnisch model op, dat nog niet geschikt was voor toepassing in de praktijk. Daarnaast was het model nog niet genoeg consistent in statements over de verschillende dimensies en niveaus. Daarom is het model voor demonstratie bijgesteld op basis van het Privacy Volwassenheidsmodel (Koers & al, 2017) en over de dimensies heen consistenter gemaakt.

Vervolgens is het model gedemonstreerd bij twee organisaties in educatie en zorg. Daarna zijn in interviews met vier respondenten evaluaties gedaan op basis van het Technology Acceptance Model (Moody, 2003) en de Delphi-casestudytechniek (Bruin & Rosemann, 2007).

In de eerste iteratie was er geen consensus of stabiliteit in de antwoorden van respondenten over de relevantie van de demonstratievraag voor minimale gegevensverwerking. Ook was vooral het waargenomen gebruiksgemak, maar ook de waargenomen toepasbaarheid en intentie voor gebruik ((Moody, 2003) nog niet voldoende. Daarnaast was de gemiddelde algemene tevredenheid nog niet hoger of gelijk aan 7,5 op een schaal van 0-10 (Bruin & Rosemann, 2007). Om deze redenen is het model niet alleen m.b.t. minimale gegevensverwerking, maar ook in de andere dimensies met specifieke AVG-termen aangepast en nogmaals consistenter gemaakt op basis van kwalitatieve feedback.

In de tweede iteratie is het aangepaste model geëvalueerd met dezelfde vier respondenten via e-mail. In deze evaluatie zijn consensus over de relevantie en voldoende algemene tevredenheid gemeten (zie tabel x en x in paragraaf 4.3.). Tenslotte zijn de termen persoonsgegevens, anonimisering, proportionaliteit en subsidiariteit in de demonstratievragen nog beter toegelicht.

Het resultaat is een AVG-volwassenheidsmodel dat de naam AVGMM krijgt (zie tabel 16, paragraaf 4.4) en kan worden toepast aan de hand van de AVGMM-vragenlijst (zie tabel 42 in bijlage 9). Dit model is een eerste stap in de totstandkoming van een maatschappelijk relevant AVG-volwassenheidsmodel dat oplossing kan bieden voor het probleem dat er geen objectief meetinstrument is voor het meten van AVG-volwassenheid in organisaties. Daarnaast geeft dit wetenschappelijk onderbouwde model een eerste invulling van het kennishiaat met betrekking tot AVG-volwassenheid in de wetenschappelijke literatuur.

5.2. Discussie en reflectie

Het AVG-volwassenheidsmodel is ontwikkeld op basis van bestaande EA- en DM-volwassenheidsmodellen. In twee iteraties zijn verbeteringen aangebracht waarbij het model inhoudelijk verrijkt is met inzichten uit de praktijk. Ook hebben de oorspronkelijke datatechnische termen uit EA en DM plaatsgemaakt voor termen die in de context van de AVG gebruikelijk zijn. Hierdoor zijn oorspronkelijke EA- en DM-statements minder direct te herleiden in het model, maar is de relevantie van het model en de algemene tevredenheid van de vier respondenten verbeterd.

Door het verwerken van de kwalitatieve feedback is geprobeerd om het gebruiksgemak te verbeteren, maar dit is niet nogmaals geëvalueerd. Het model zal in verder onderzoek (zie aanbevelingen in paragraaf 5.4.) doorontwikkeld moeten worden, maar heeft ook nu al impact gehad. Tijdens het onderzoek gaven respondenten aan dat hun deelname aan de demonstratie en evaluatie van het model heeft geleid tot een beter inzicht en overzicht in AVG.

Inhoudelijk zal het model verbeterd kunnen worden door een aantal specifieke AVG-aspecten toe te voegen aan het model en de demonstratievragen. Vanuit de ervaringen in de organisaties kwam de kwalitatieve feedback dat de aspecten ‘privacy by design’, ‘uitwisseling persoonsgegevens met derden’ en ‘inzage en verwijdering van persoonsgegevens op aanvraag van betrokkene’ nog toegevoegd zouden kunnen worden aan het model. Onder het principe ‘Rechtmatigheid, behoorlijkheid en transparantie’ is het relevant dat betrokkenen toestemming moeten geven, voordat hun persoonsgegevens uitgewisseld worden met derden. Ook is het onder dit principe relevant dat betrokkenen altijd inzage hebben in hun verwerkte persoonsgegevens en daarbij tevens het recht om deze gegevens te laten verwijderen.

In evaluatie is ook gebleken dat de toepasbaarheid voor verschillende respondenten mede afhankelijk is van interpretatie van gebruikte termen. Zo kan in het principe ‘Rechtmatigheid, behoorlijkheid en transparantie’ nog kritisch gekeken worden naar de term ‘eigenaarschap en verantwoordelijkheid’, waarbij ’verantwoordelijkheid’ een verdieping is op ‘eigenaarschap’. Om verschillende interpretaties te voorkomen kan gekozen worden om te spreken van ‘eigenaarschap en daarmee verantwoordelijkheid’.

In de uitvoering van onderzoek zijn validiteit, betrouwbaarheid en ethische aspecten van groot belang. In validiteit maken we onderscheid tussen construct-, interne en externe validiteit.

De constructvaliditeit (Yin, 2003) geeft aan of het instrument, het AVG-volwassenheidsmodel, meet wat het zou moeten meten, namelijk de volwassenheid van de AVG-implementatie in een organisatie. Dit is nagestreefd door het model te baseren op bestaande generieke modellen en te verbeteren door toetsing in de praktijk. De constructvaliditeit is echter niet te garanderen, zonder de toetsing op veel bredere schaal uit te voeren en de resultaten statistisch te analyseren. De constructvaliditeit van de toegepaste ontwikkel- en evaluatiemethodes is wel te garanderen omdat deze is aangetoond in eerder onderzoek.

Om de interne validiteit van het onderzoek, i.e. het causale verband tussen de geschiktheid van het model en de uitkomst van de evaluaties, te verbeteren, zijn zoveel mogelijk (derde) verstorende factoren uitgesloten door gelijke omstandigheden te creëren bij de demonstraties en evaluaties. De twee demonstratiesessies hebben plaatsgevonden in anderhalf uur, waarbij in beide organisaties de functionaris gegevensbescherming (FG) en de informatiearchitect (IA) in een gezamenlijke sessie geïnterviewd zijn, omdat deze personen vanuit hun rol de AVG-volwassenheid in hun organisatie kunnen beoordelen. Daarna heeft de eerste evaluatie plaatsgevonden in afzonderlijke sessies met de vier respondenten. Deze sessies hadden in drie van vier gevallen de voorgenomen tijdsduur van één uur, de vierde sessie duurde anderhalf uur. Alle evaluaties zijn parallel verwerkt in een verbeterd model en deze is via e-mail aangeboden voor een tweede evaluatie door de respondenten.

Voor de externe validiteit van dit onderzoek, i.e. de veralgemeenbaarheid van de resultaten, houdt een inherente beperking van multiple-casestudy onderzoek bij twee organisaties in dat een beperkte hoeveelheid onderzoeksdata opgeleverd wordt. Om te komen tot veralgemeenbare resultaten zijn verdere veldstudies en/of grootschalige experimenten nodig.

De betrouwbaarheid is nagestreefd door de volgende maatregelen. Alle interview-materialen, i.e. opnames en ingevulde vragenlijsten, zijn beschikbaar gesteld. Bij iedere eerste evaluatie is de ingevulde demonstratie met de betrokken respondent gedeeld. Bij de tweede evaluatie via e-mail is de transcriptie van de eerste evaluatie met de betrokken respondent gedeeld.

Dit onderzoek heeft rekening gehouden met een aantal algemene ethische aspecten (Saunders & al, 2015). Voor respondenten gold een vrijwillige deelname en zij hadden steeds het recht om zich geheel of gedeeltelijk terug te trekken uit het onderzoek. De privacy van respondenten is geborgd door niet de naam, maar de rol en/of functie van de respondenten te noemen. Ook zijn met de organisatie afspraken gemaakt omtrent geheimhouding. Organisaties worden niet bij naam genoemd maar als een organisatie uit de sectoren onderwijs en zorg. De opnames van de interviews worden na beoordeling door de afstudeerbegeleider vernietigd.

5.3. Aanbevelingen voor de praktijk

Voor toepassing van dit model in de praktijk gelden een aantal aanbevelingen. Dit model gaat uit van zes basisprincipes van AVG op vijf volwassenheidsniveaus en geeft daarmee een algemeen beeld van de AVG-volwassenheid in een organisatie. Op basis van dit beeld kunnen adviezen worden geformuleerd die te onderbouwen zijn vanuit de AVG-basisprincipes. Bij de toepassing van het model is het verstandig om het vaststellen van volwassenheidsniveaus in de bijhorende toelichting

goed te onderbouwen met argumenten en bronnen. De onderbouwde toelichting en navolgbare bronnen geven een objectievere en herleidbare vaststelling van de AVG-volwassenheidsniveaus van de organisatie. Dit draagt bij aan de kwaliteit van de adviezen voor verbetering van de AVG-implementatie.

Doordat het model algemeen is, kan het bepalen van AVG-volwassenheid en het opstellen van adviezen in weinig tijd gedaan worden. De adviezen zijn dan op het algemene niveau van de zes AVG-basisprincipes. In verdieping daarop kunnen bij de daadwerkelijke implementatie van verbeteringen checklists gebruikt worden die in het werkveld bekend zijn, zoals de Checklist Privacy AVG (Berkvens & al, 2018). Hiermee kunnen organisaties aan de hand van 46 checklists een privacy policy implementeren die afgestemd is op AVG.

5.4. Aanbevelingen voor verder onderzoek

Uit dit onderzoek volgen aanbevelingen voor vervolgonderzoek.

Voor de demonstratievragen, waarmee het model wordt toegepast, is in de evaluaties gebleken dat de vragen meervoudig zijn over samengestelde AVG-deelaspecten. Het is een overweging om deze vragen op te knippen in vragen per deelaspect. Binnen het principe ‘Integriteit en vertrouwelijkheid’ wordt in het huidige model een algemene en een verdiepende vraag voor toegangsbeleid gesteld. Wellicht is het beter om aparte vragen te stellen voor integriteit en vertrouwelijkheid.

In volgende iteraties binnen de methode van Becker (Becker & al, 2009) zouden door demonstratie en evaluatie op grotere schaal verdere verbeteringen gedaan moeten worden om te komen tot een algemeen geaccepteerd en breder toepasbaar AVG-volwassenheidsmodel. De huidige aanpak van vragenlijsten en interviews is dan niet houdbaar door de vele interviews. Een betere optie voor transfer en evaluatie op grote schaal is het afnemen van een online survey onder respondenten in meerdere organisaties en in verschillende sectoren.

Referenties

Al-Ruithe, & al, e. (2016). A conceptual framework for designing data governance for cloud computing.

Al-Sharida. (2015). Data governance in electronic health records: A systematic review.

Autoriteit Persoonsgegevens. (2019, 06 22). *Checklist: houd grip op persoonsgegevens.* Retrieved from Autoriteit Persoonsgegevens: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/checklist_houd_grip_op_persoonsgegevens_def.pdf

Autoriteit Persoonsgegevens. (2019, 01 19). *Scholen & de AVG*. Retrieved from Autoriteit Persoonsgegevens: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/onderwijs/scholen-de-avg

Autoriteit Persoonsgegevens. (2019, 01 19). *Zorgverleners en de AVG*. Retrieved from Autoriteit Persoonsgegevens: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/gezondheid/zorgverleners-en-de-avg

Ball. (2012). Review of data management lifecycle models.

Baolong, & al, e. (2018). Research and application of data management based on Data Management Maturity Model.

Becker, & al, e. (2009). *Developing Maturity Models for IT Management – A Procedure Model and its Application.*

Berkvens, & al, e. (2018). *Checklist Privacy AVG: privacybeleid in 46 checklists.* Amsterdam: Berghauser Pont Publishing.

Bruin, & Rosemann. (2007). Using the Delphi technique to identify BPM capability areas.

Chuah, & al, e. (2012). Construct an enterprise business intelligence maturity model (EBI2M) using an integration approach: A conceptual framework.

Chuah, & Wong. (2012). A framework for accessing an enterprise business intelligence maturity model (EBI2M): Delphi study approach.

CMMI Institute. (2018). *Data Management Maturity Model v1.1.*

Cosic, & al, e. (2012). Towards a business analytics capability maturity model.

Crowston, & al, e. (2011). A capability maturity model for scientific data management: Evidence from the literature.

Cuenca, & al. (2010). Enterprise Architecture Framework with Early Business/ICT Alignment.

Cuenca, & al. (2011). Architecting Business and IS/IT Strategic Alignment for extended enterprises.

Curley, M. (2016). *An IT Value Based Capability Maturity Framework 2nd Edition.* Van Haren Publishing.

Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology.

Dinter. (2012). The maturing of a business intelligence maturity model.

Fernandez, & al. (2017). Analysis of enterprise architecture maturity models.

Franke, & al. (2014). An architecture framework for enterprise IT service availability analysis.

Gao, & Chen. (2012). Case study on enterprise architecture management based on TOGAF .

Gongora, & Bernal. (2016). Validation Architecture for information technology in smart cities.

Hevner, & al. (2004). Design Science in Information Systems Research.

ICTRecht. (2018, 11 1). *Boetes onder de AVG: de stand van zaken*. Retrieved from ICTRecht: https://ictrecht.nl/2018/11/01/boetes-onder-de-avg-de-stand-van-zaken/

IVI. (2018). *IT-CMF Critical Capabilities*. Retrieved from IVI: https://ivi.ie/critical-capabilities/

Jonker, & al, e. (2011). Effective master data management.

Koers, & al, e. (2017). Privacy volwassenheidsmodel.

Koznov, & al. (2015). Specifics of projects in the area of enterprise architecture development.

Lankhorst, e. a. (2009). *Enterprise Architecture at Work.* Dordrecht Heidelberg London New York: Springer-Verlag.

Llamosa-Villalba, & al. (2015). Enterprise Architecture of Colombian Higher Education.

Looy, A. v., & al. (2013). Choosing the right process maturity model. *Information & Management*.

Martinez, & al. (2015). Approach to Evaluation of Maturity Level in Enterprise Architecture.

Mathiesen, & al, e. (2011). A comparative analysis of business analysis (BA) and business process management (BPM) capabilities.

Meyer, & al. (2011). An Analysis of Enterprise Architecture Maturity.

Moody, D. (2003). *The Method Evaluation Model: A Theoretical Model for Validating Information Systems Design Methods.*

Morabito. (2015). Big data governance.

NASCIO. (2003). *NASCIO Enterprise Architecture Maturity Model Version 1.3.* Retrieved from Nascio: https://www.nascio.org/hotIssues/EA/EAMM.pdf

Niemi. (2011). Designing a Data Governance Framework.

Ong, & Siew. (2013). An empirical analysis on business intelligence maturity in Malaysian organizations.

Otto. (2013). On the evolution of data governance in firms: the case of Johnson & Johnson consumer products North America.

Otto, & al, e. (2011). A morphology of the organization of data governance.

Peffers, K., Tuunanen, T., Gengler, C. E., Rossi, M., Hui, W., Virtanen, V., & Bragge, J. (2008). The Design Science Research Process: A model for producing and presenting information systems research.

Proenca. (2016). Methods and Techniques for Maturity Assessment.

Proenca, & Borbinha. (2017). Enterprise Architecture A Maturity Model Based on TOGAF ADM.

Randolph, J. J. (2005). Free-marginal multirater kappa: An alternative to Fleiss´ fixed-marginal multirater kappa.

Rifaie, & al, e. (2009). Data governance strategy: A key issue in building enterprise data warehouse.

Rohloff. (2009). Case study and maturity model for business process management implementation.

Sallans, & Lake. (2014). Data management assessment and planning tools.

Saunders, & al, e. (2015). *Methoden en technieken van onderzoek.* Amsterdam: Pearson.

Schermer, e. a. (2018, 09 23). *Handleiding Algemene Verordening Gegevensbescherming en uitvoeringswet Algemene Verordening Gegevensbescherming.* Opgehaald van Autoriteit Persoonsgegevens: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/handleidingalgemeneverordeninggegevensbescherming.pdf

Schmidt, & al. (2014). Towards a framework for enterprise Architecture Analysis.

Spruit, M., & Pietzka, S. (2015). MD3M: The master data management maturity model. *Computers in Human Behavior*.

Stall, & al, e. (2016). The American Geophysical Union Data Management Maturity Program.

Steenbergen, V., & al. (2010). The Dynamic Architecture Maturity Matrix; Instrument Analysis and Refinement.

Sulaiman, & al, e. (2015). Big data maturity model for Malaysian zakat institutions to embark on big data initiatives.

Tan, & al, e. (2011). A maturity model of enterprise business intelligence.

The Data Management Assocation. (2014). *DAMA-DMBOK2 Framework.*

The Open Group. (2018). *TOGAF® 9.1 > Part VII: Architecture Capability Framework > Architecture Maturity Models*. Retrieved from The Open Group: http://pubs.opengroup.org/architecture/togaf91-doc/arch/chap51.html

Vallerand, e. a. (2017). Analysing enterprise architecture maturity models: a learning perspective.

Westerkamp, & Veen, v. (2008). *Deskresearch: Informatie selecteren, beoordelen en verwerken; .* Amsterdam: Pearson Prentice Hall.

Yin, R. K. (2003). Case Study Research Design and Methods.

Zhang, & al, e. (2013). A PLM components monitoring framework for SMEs based on a PLM maturity model and FAHP methodology.

Bijlage 1 Selectie artikelen Enterprise Architectuur

Tabel 17 Selectie EA-artikelen

Art.	Titel	Ref	Engels	EA-volwassenheids model	Review	Volledige tekst beschikbaar
#1	Analysis of enterprise architecture maturity models	(Fernandez & al, 2017)	0			
#2	Analysing enterprise architecture maturity models: a learning perspective	(Vallerand, 2017)	x	x	x	x
#3	Enterprise Architecture A Maturity Model Based on TOGAF ADM	(Proenca & Borbinha, 2017)	x	x	0	
#4	Validation Architecture for information technology in smart cities	(Gongora & Bernal, 2016)	0			
#5	Methods and Techniques for Maturity Assessment	(Proenca, 2016)	x	x	0	
#6	Approach to Evaluation of Maturity Level in Enterprise Architecture	(Martinez & al, 2015)	0			
#7	Enterprise Architecture of Colombian Higher Education	(Llamosa-Villalba & al, 2015)	x	0		
#8	Specifics of projects in the area of enterprise architecture development	(Koznov & al, 2015)	x	x	0	
#9	An architecture framework for enterprise IT service availability analysis	(Franke & al, 2014)	x	0		
#10	Towards a framework for enterprise Architecture Analysis	(Schmidt & al, 2014)	x	x	0	
#11	Case study on enterprise architecture management based on TOGAF	(Gao & Chen, 2012)	x	x	0	
#12	Architecting Business and IS/IT Strategic Alignment for extended enterprises	(Cuenca & al, 2011)	x	x	0	
#13	An Analysis of Enterprise Architecture Frameworks	(Meyer & al, 2011)	x	x	x	x
#14	Enterprise Architecture Framework with Early Business/ICT Alignment	(Cuenca & al, 2010)	x	x	0	
#15	The Dynamic Architecture Maturity Matrix; Instrument Analysis and Refinement	(Steenbergen & al, 2010)	x	x	0	

Bijlage 2 Selectie artikelen Data Management

Tabel 18 Selectie DM-artikelen

Art.	Titel	Ref	Engels	DM-volwassenheidsmodel	Ontwerp	Volledige tekst beschikbaar
#1	Review of data management lifecycle models	(Ball, 2012)	x	0		
#2	A capability maturity model for scientific data management: Evidence from the literature	(Crowston & al, 2011)	x	0		
#3	The maturing of a business intelligence maturity model	(Dinter, 2012)	x	0		
#4	A morphology of the organization of data governance.	(Otto & al, 2011)	x	0		
#5	MD3M: The master data management maturity model	(Spruit & Pietzka, 2015)	x	x	x	x
#6	Data governance strategy: A key issue in building enterprise data warehouse	(Rifaie & al, 2009)	x	0		
#7	On the evolution of data governance in firms: the case of Johnson & Johnson consumer products North America	(Otto, 2013)	x	0		
#8	An empirical analysis on business intelligence maturity in Malaysian organizations	(Ong & Siew, 2013)	x	0		
#9	A framework for accessing an enterprise business intelligence maturity model (EBI2M): Delphi study approach	(Chuah & Wong, 2012)	x	0		
#10	A maturity model of enterprise business intelligence	(Tan & al, 2011)	x	0		
#11	A capability maturity model for data acquisition and utilization	G Murphy, A Chang 2009	x	0		
#12	The American Geophysical Union Data Management Maturity Program	(Stall & al, 2016)	x	x	0	
#13	Data management assessment and planning tools	(Sallans & Lake, 2014)	x	x	0	
#14	Data governance in electronic health records: A systematic review	(Al-Sharida, 2015)	x	0		
#15	Research and application of data management based on Data Management Maturity Model (DMM)	(Baolong & al, 2018)	x	x	x	x
#16	Big data governance	(Morabito, 2015)	x	x	x	0
#17	Big data maturity model for Malaysian zakat institutions to embark on big data initiatives	(Sulaiman & al, 2015)	x	0		
#18	Construct an enterprise business intelligence maturity model (EBI2M) using an integration approach: A conceptual framework	(Chuah & al, 2012)	x	0		
#19	A PLM components monitoring framework for SMEs based on a PLM maturity model and FAHP methodology	(Zhang & al, 2013)	x	0		
#20	Designing a Data Governance Framework	(Niemi, 2011)	x	0		
#21	Case study and maturity model for business process management implementation	(Rohloff, 2009)	x	0		
#22	A comparative analysis of business analysis (BA) and business process management (BPM) capabilities	(Mathiesen & al, 2011)	x	0		
#23	Effective master data management	(Jonker & al, 2011)	x	0		
#24	Towards a business analytics capability maturity model	(Cosic & al, 2012)	x	0		
#25	A conceptual framework for designing data governance for cloud computing	(Al-Ruithe & al, 2016)	x	0		

Bijlage 3 Volwassenheidsniveaus uit EA en DM

Tabel 19 IT-CMF-volwassenheidsniveaus (Curley, 2016, p. 8)

Initial	Approaches are inadequate and unstable. Scope is fragmented and incoherent. Repeatable outcomes are rare
Basic	Approaches are defined, but inconsistencies remain. Scope is limited to a partial area of a business function or domain area, deficiencies remain. Repeatable outcomes are achieved occasionally
Intermediate	Approaches are standardized, inconsistencies are addressed. Scope expands to cover a business function (typically IT) or domain area. Repeatable outcomes are often achieved,
Advanced	Approaches can systematically flex for innovative adaptations. Scope cover end-to-end organization / neighbouring domain areas. Repeatable outcomes are very often achieved.
Optimizing	Approaches demonstrate world-class attributes. Scope extends beyond the borders of the organization / neighbouring domains. Repeatable outcomes are virtually always achieved.

Tabel 20 EAMM-volwassenheidsniveaus (NASCIO, 2003, pp. 7-12)

0 No program	There is not a documented architectural framework in place at this level of maturity.
1 Informal Program	The base architecture framework and standards have been defined and are typically performed informally.
2 Repeatable Program	The base architecture and standards have been identified and are being tracked and verified.
3 Well-Defined Program	The enterprise architecture framework is well defined; using approved standard and/or customized versions of the templates.
4 Managed Program	Performance metrics are collected, analyzed and acted upon. The metrics are used to predict performance and provide better understanding of the processes and capabilities.
5 Continuously Improving Vital Program	The processes are mature; targets have been set for effectiveness and efficiency based on business and technical goals. There are ongoing refinements and improvements based on the understanding of the impact changes have to these processes.

Tabel 21 MD3M-volwassenheidsniveaus (Spruit & Pietzka, 2015, p. 1070)

1: Initial	A first awareness for issues regarding the topic of MDM has been raised on an operational level. Initial steps are initialized.
2: Repeatable	Measures from individuals are conducted to solve individual problems. No connection to other units or projects. Still operational.
3: Defined process	First collaborations take place on a tactical level. Awareness was created for the existence of other initiatives
4: Managed and measurable	Best practices are in place for handling of MDM. There are defined processes on a tactical level
5: Optimized	Optimized handling of MDM. The organization's efficiency has been improved. Tactical approach on the topic.

Tabel 22 DMM-volwassenheidsniveaus (CMMI Institute, 2018, p. 7)

1: Performed	Processen zijn ad-hoc, reactief en worden niet toegepast over verschillende domeinen.
2: Managed	Processen worden gepland en uitgevoerd conform beleid door getrainde werknemers in samenspraak met relevante stakeholders
3: Defined	Een set van standaard processen is vastgelegd en wordt gevolgd. Specifieke behoeftes worden vervuld door processen conform beleid te baseren op de standaard processen,
4: Measured	Metrics van processen zijn vastgelegd en worden gebruikt voor datamanagement. Dit houdt in: management van afwijkingen, voorspellingen en analyse. Processen worden gemanaged tijdens de uitvoering.
5: Optimized	Processen worden geoptimaliseerd door het toepassen van niveau 4 analyse voor verbetermogelijkheden. Best practices worden gedeeld met andere bedrijven.

Bijlage 4 Volwassenheidsaspecten uit EA en DM.

Tabel 23 IT-CMF: Managing the IT capability aspecten (IVI, 2018) in relatie met AVG-basisbeginselen

IT-CMF: managing the IT capability	**Omschrijving**	**Gerelateerd AVG-beginsel**	**Argumentatie**
Capability Assessment Management	Evaluatie huidige status IT-mogelijkheden, plannen verbeteringen.	Nvt	
Enterprise Architecture Management	Visie en regie over, planning en ontwerp van processen in relatie tot IT-services, security, netwerk, data-opslag.	Nvt	
Information Security Management	Managen van beleid en controle voor integriteit, vertrouwelijkheid, verantwoordelijkheid, bruikbaarheid en beschikbaarheid van informatie.	Integriteit en vertrouwelijkheid	Door het managen van beleid en controle voor informatiebeveiliging wordt integriteit en vertrouwelijkheid van persoonlijke data verhoogd.
Knowledge Management	Identificeren, vastleggen, analyseren en toepassen van kennis om de prestaties van de organisatie te verbeteren.	Nvt	
People Asset Management	Managen van eisen van de organisatie in relatie tot effectieve IT-medewerkers.	Nvt	
Personal Data Protection	Ontwerpen en toepassen van beleid, systemen en controle voor het verwerken van persoonlijke en privacygevoelige data m.b.t. levende personen in alle digitale, geautomatiseerde en handmatige verwerking. Dit garandeert de privacy van betrokkenen en het feit dat de organisatie persoonlijke data alleen gebruikt voor het specifieke doel afgestemd met de betrokkenen.	Rechtmatigheid, behoorlijkheid en transparantie. Doelbinding	Het afstemmen van het gebruik van persoonlijke data met betrokkenen maakt het opslaan en verwerken van persoonlijke data transparant. Het specifieke doel van de verwerking leidt tot de doelbinding.
Programme Management	Samenstellen en toekennen van resources om waarde te identificeren, selecteren, goed te keuren, te overzien en te leveren vanuit programma-organisatie	Nvt	
Project Management	Toekennen van resources aan het initiëren, plannen, uitvoeren, monitoren, beheersen en afsluiten van projecten met afgestemde kosten, tijd, kwaliteit en inzet.	Nvt	
Relationship Management	Analyseren, plannen, onderhouden en verbeteren van relaties tussen IT en de rest van het bedrijf.	Nvt	
Research, Development Engineering	Onderzoeken en ontwikkelen van nieuwe technologieën en oplossingen en toepassingen die waarde kunnen geven voor de organisatie.	Nvt	
Service Provisioning	Managen van IT-diensten in afstemming met de *requirements* van de organisatie. Hierbij horen ook activiteiten gerelateerd aan de operatie, onderhoud, continue verbetering van dienstverlening en de overgang naar nieuwe diensten en het afstoten van diensten.	Nvt	
Solutions Delivery	Ontwerpen, valideren en aanbieden IT-oplossingen in afstemming met bedrijfsdoelen, -eisen en -kansen.	Nvt	
Technical Infrastructure Management	Managen van de IT-infrastructuur gedurende de gehele life-cycle. (inrichten, uitfaseren, en dagelijks onderhoud	Nvt	
User Experience Design	Proactief afwegen van de behoeften van gebruikers gedurende de life-cycle van IT-diensten en -oplossingen.	Nvt	

User Training Management	Aanbieden van trainingen om de vaardigheden van gebruikers te verbeteren in het gebruik van bedrijfsapplicaties en IT-diensten.	Nvt	

Tabel 24 EAMM-aspecten (NASCIO, 2003, p. 6) in relatie met AVG-basisbeginselen

EAMM-aspect (NASCIO, 2003)	**Omschrijving**	**Gerelateerd AVG-beginsel**	**Argumentatie**
EA Administration	Governance rollen en verantwoordelijkheden.	Nvt	
EA Planning	EA programma road map and implementatieplan.	Nvt	
EA Framework	Processen en templates voor Enterprise Architecture.	Nvt	
EA Blueprint	Verzameling van standaarden en specificaties.	Doelbinding	De EA-standaarden en -specificaties beschrijven de alignment tussen bedrijfsprocessen, informatie en technologie. Deze alignment is versterkt de doelbinding van de verwerking van persoonlijke data, omdat bedrijfsprocessen aan benodigde informatie gekoppeld worden.
EA Communication	Opleiding en verspreiding van EA en Blueprint details.	Nvt	
EA Compliance	Voldoen aan standaarden, processen en overige EA-elementen, en de processen om afwijkingen te traceren en vast te leggen.	Nvt	
EA Integration	Raakvlakken van managementprocessen en EA.	Nvt	
EA Involvement	Draagvlak voor het EA programma in de gehele organisatie.	Nvt	

Tabel 25 MD3M-aspecten (Spruit & Pietzka, 2015, p. 1072) in relatie met AVG-basisbeginselen

MD3M-aspect	**Omschrijving**	**Gerelateerd AVG-beginsel**	**Argumentatie**
Data Model	Definition of Master Data, Master Data Model, Data Landscape	Nvt	
Data Quality	Assessment of Data Quality, Impact on Business, Awareness of Quality Gaps, Improvement	Juistheid	Analyseren en verbeteren van datakwaliteit verbetert de juistheid van persoonlijke data.
Usage & Ownership	Data Usage, Data Ownership, Data Access	Rechtmatigheid, behoorlijkheid en transparantie	Beschrijving van gebruik en eigenaarschap van en toegang tot data binnen de organisatie dragen bij aan de rechtmatigheid, behoorlijkheid en transparantie van persoonlijke data.
Data Protection	Data Protection	Integriteit en vertrouwelijkheid	Bescherming van data verbetert de integriteit en vertrouwelijkheid van persoonlijke data.
Maintenance	Storage, Data Lifecycle	Opslagbeperking	Opslag en data lifecycle dragen bij aan opslagbeperking van persoonlijke data.

Tabel 26 DMM-aspecten (CMMI Institute, 2018, pp. 11-138) in relatie met AVG-beginselen.

DMM-aspect (CMMI Institute, 2018)	**Omschrijving**	**Gerelateerd AVG-beginsel**	**Argumentatie**
Data Strategy Data Management Strategy, Communications, Data Management Function, Business Case Funding	Best practices voor het vastleggen, communiceren en rechtvaardigen van een visie op data management (CMMI Institute, 2018, p. 11)	Nvt	
Data Governance Governance Management, Business Glossary, Metadata Management	Best practices voor een breed draagvlak in de praktijk en senior-level toezicht in de effectiviteit van data management (CMMI Institute, 2018, p. 41)	Rechtmatigheid, behoorlijkheid en transparantie	Het toezicht op datamanagement van persoonsdata op senior level draagt bij aan het garanderen van de rechtmatigheid, behoorlijkheid en transparantie van de verwerking van persoonlijke data.
Data Quality Data Quality Strategy, Data Profiling, Data Quality Assessment, Data Cleansing	Best practices voor het definiëren van een aanpak voor het detecteren en corrigeren van foutieve data om te borgen dat de juiste data beschikbaar is voor gebruik in bedrijfsprocessen, beslissingen en planning. (CMMI Institute, 2018, p. 64)	Juistheid	Detectie en correctie van foutieve persoonsdata draagt bij aan de juistheid van persoonlijke data.
Data Operations Data Requirements Definition, Data Lifecycle Management, Provider Management	Best practices voor het specificeren van data requirements en het managen van geïmplementeerde data door de gehele organisatie (CMMI Institute, 2018, p. 89)	Doelbinding	De afstemming van data requirements op bedrijfsdoelen draagt bij aan de doelbinding van de verwerking van persoonlijke data.
Platform & Architecture Architectural Approach, Architectural Standards, Data Management Platform, Data Integration, Historical Data & Archiving	Best practices voor het bepalen van methoden en standaarden die borgen dat het data management platform de bedrijfsdata integreert, vasthoudt en archiveert om bedrijfsdoelen te ondersteunen. (CMMI Institute, 2018, p. 108)	Opslagbeperking Minimale gegevensverwerking.	Het platform dat bedrijfsdata vasthoudt om bedrijfsdoelen te ondersteunen realiseert de opslagbeperking van persoonlijke data. De architectuur van het platform stemt de verwerking van persoonlijke data af op de bedrijfsdoelen zodat niet meer verwerkt wordt dan noodzakelijk is.
Supporting Processes Measurement and Analysis, Process Management, Process Quality Assurance, Risk Management, Configuration Management	Definitie van bedrijfsprocessen voor het beoordelen en implementeren van effectiviteit van data management in alle proces gebieden. (CMMI Institute, 2018, p. 138)	Nvt	

Bijlage 5 Relevante volwassenheidsaspecten uit EA en DM gerelateerd aan AVG-beginselen

Tabel 27 Relevante volwassenheidsaspecten uit IT-CMF/EAMM/MD3M/DMM gerelateerd aan AVG-beginselen

	1 - Performed	2 - Managed	3 - Defined	4 - Measured	5 - Optimized
"Rechtmatigheid, behoorlijkheid en transparantie; de verwerking van persoonsgegevens moet rechtmatig, behoorlijk en transparant zijn.	DMM: Eigenaarschap en verantwoordelijkheid voor data worden in projecten toegewezen. (CMMI Institute, 2018, p. 44) MD3M Het is bekend wie welke data gebruikt. Data-elementen zijn eigendom van individuen of afdelingen. Er is een proces om toegang tot data te krijgen (Spruit & Pietzka, 2015, p. 1075)	Rollen en verantwoordelijkheden zijn vastgelegd per data-gebied op prioriteit in lijn met het bedrijf. Er is een review proces om data governance te evalueren en verbeteren. (CMMI Institute, 2018, p. 44) MD3M Voor iedere medewerker is bekend of hij de data gebruikt die hij heeft. Data-elementen zijn eigendom van logisch consistente rollen en afdelingen. De eigenaar bepaalt het gebruik, het doel en de inhoud. Toegang tot data wordt geweigerd voor niet-geautoriseerd personeel. (Spruit & Pietzka, 2015, p. 1075)	Organisatiebrede data governance met vertegenwoordigers uit alle bedrijfsonderdelen die data met hoge prioriteit gebruiken en/of leveren. (CMMI Institute, 2018, p. 45) MD3M: Medewerkers worden op de hoogte gesteld van iedere databron die zij nodig hebben en er wordt toegang gegeven. Verantwoordelijke personen voor data zijn bekend binnen de gehele organisatie. De data-eigenaar heeft verantwoordelijkheden gedefinieerd voor de omgang met data. Iedere medewerker heeft toegang tot de data die hij nodig heeft voor zijn taak. (Spruit & Pietzka, 2015, p. 1075) <<IT-CMF>> Ontwerpen en toepassen van beleid, systemen en controle voor het verwerken van persoonlijke en privacygevoelige data m.b.t. levende personen in alle digitale, geautomatiseerde en handmatige verwerking Dit garandeert het feit dat de organisatie persoonlijke data alleen gebruikt wordt, zoals afgestemd met de betrokkenen. (IVI, 2018)	Statistische technieken worden toegepast om te evalueren of data governance de organisatie op geschikte wijze bijstuurt. Op basis van deze analyse wordt data governance bijgesteld. (CMMI Institute, 2018, p. 46) MD3M Data repositories worden met regelmaat onderhouden en raken niet verouderd of onbruikbaar. Data stewards zijn aangesteld voor data sets. Iedere werknemer heeft toegang tot data voor zijn taak en alleen die data. (Spruit & Pietzka, 2015, p. 1075)	Externe data governance structuren en casussen worden geëvalueerd om best practices en ideeën op te doen. De eigen structuur wordt gedeeld als best practice. Data governance wordt continue verfijnd en verbeterd. (CMMI Institute, 2018, p. 46) MD3M Medewerkers gebruiken de mogelijkheden die zij hebben en zijn niet terughoudend om bepaalde systemen te gebruiken om data uit te verkrijgen. Data stewardschap wordt gepromoot en opgenomen in functiebeschrijvingen. Iedere medewerker weet tot welke bronnen hij toegang heeft en wat hij daar kan vinden. (Spruit & Pietzka, 2015, p. 1075)

Doelbinding; de verwerking moet gebonden zijn aan specifieke verzameldoelen.	DMM: Stakeholders doen review en goedkeuring van data requirements, die worden vastgelegd en vastgelegd in een glossary (CMMI Institute, 2018, p. 93) EAMM Documentatie van bedrijfsdoelen en technologiestandaarden is informeel en inconsistent. (NASCIO, 2003, p. 8)	DMM: Definitie van data requirements is gedocumenteerd wordt gevolgd en is aantoonbaar in lijn met bedrijfsdoelen. (CMMI Institute, 2018, p. 94) EAMM Bedrijfsdoelen, strategische informatie en de behoefte om dit vast te leggen in een respository zijn geidentificeerd. (NASCIO, 2003, p. 9)	DMM: Data requirements zijn gedefinieerd, gevalideerd en geïntegreerd in het standaard raamwerk van de organisatie. Data requirements worden getoetst op basis van bedrijfsprioriteit. Bedrijfsprocessen die data produceren zijn vastgelegd en gelinkt aan data requirements die zijn geëvalueerd op implementeerbaarheid. (CMMI Institute, 2018, pp. 94-95) EAMM Bedrijfsdoelen, strategische informatie en technologie standaarden zijn consistent gedocumenteerd. (NASCIO, 2003, p. 10) <<IT-CMF>> Ontwerpen en toepassen van beleid, systemen en controle voor het verwerken van persoonlijke en privacygevoelige data m.b.t. levende personen in alle digitale, geautomatiseerde en handmatige verwerking Dit garandeert het feit dat de organisatie persoonlijke data alleen gebruikt voor het specifieke doel. (IVI, 2018)	DMM: Best practices uit de sector zijn geevalueerd voor toepassing op data requirements. Gedefinieerde meetwaarden borgen dat data requirements invulling geven aan bedrijfsdoelen. En eventuele correcties worden uitgevoerd. (CMMI Institute, 2018, pp. 96-97) EAMM Documentatie van bedrijfsdoelen, strategische informatie en classificatie van producten zijn een standaard gebruik. De organisatie meet het compliance proces om de documentatie te updaten. (NASCIO, 2003, p. 11)	DMM: Continue procesverbetering om consistente prioritering, selectie en verificatie van data requirements te borgen. Het delen van best practices voor data requirements binnen de sector. (CMMI Institute, 2018, p. 97) EAMM Informatie over bedrijfsdoelen en technologie worden gereviewd om de mogelijkheden van nieuwe technologie voor bedrijfsdoelen te verkennen. De organisatie werkt samen met andere organisaties om informatie te delen over business- en technologietrends (NASCIO, 2003, p. 13)
Minimale gegevensverwerking; de persoonsgegevens moeten toereikend zijn, ter zake dienend, en beperkt tot wat noodzakelijk is.	DMM: De datastore is door data-architectuur afgestemd op bedrijfsdoelen voor minstens 1 project. Business en IT zijn betrokken. Technische mogelijkheden en eisen zijn bepaald. (CMMI Institute, 2018, p. 110)	DMM: Governance stemt de data-architectuur af op bedrijfsdoelen. Data-architectuur adresseert issues als, conflicterende business-definities, dubbele opslag, uitzonderingen op standaard data gebruik. Data creatie en gebruik is traceerbaar in alle bronnen. (CMMI Institute, 2018, p. 111)	DMM: Datastore rationalisatieproces wordt uitgevoerd: data wordt gecheckt op dubbele opslag, de noodzaak voor business-doelen en de gebruikte technologie. Architectuur, requirements en technische infrastructuurmogelijkheden zijn in lijn. (CMMI Institute, 2018, p. 113)	DMM: Statistische analyse van performance en datakwaliteit wordt gebruikt als input voor design onder architectuur. (CMMI Institute, 2018, p. 114)	DMM: Voorspellingen worden geëvalueerd in relatie tot architectuuraanpassingen. Lessons-learned over architectuur en platform worden gedeeld in publicaties en conferenties. (CMMI Institute, 2018, p. 115)

Juistheid; de gegevens moeten juist zijn.	DMM: Toetsing van datakwaliteit wordt uitgevoerd en resultaten worden vastgelegd. (CMMI Institute, 2018, p. 78) MD3M Er is een beeld of data van goede of slechte kwaliteit is. Een gespecialiseerd team is op de hoogte van het feit dat er verschillende redenen zijn voor slechte datakwaliteit. De organisatie herkent gebieden waarin de datakwaliteit niet voldoende is. (Spruit & Pietzka, 2015, p. 1074)	DMM: Doelen en standaarden voor de toetsing van datakwaliteit zijn vastgelegd gebruikt en onderhouden met standaard technieken en processen. (CMMI Institute, 2018, p. 78) MD3M Het is duidelijk welke aspecten gemeten moeten worden voor datakwaliteit. Redenen in de organisatie voor slechte datakwaliteit kunnen door de organisatie benoemd worden. Het belang van hoge datakwaliteit voor efficiëntie en effectiviteit is bekend. (Spruit & Pietzka, 2015, p. 1074)	DMM: Periodieke toetsing van datakwaliteit conform beleid en volgens schema en specifieke triggers. (CMMI Institute, 2018, p. 80) MD3M Datakwaliteit is gedefinieerd conform requirements van verschillende stakeholders. Patronen van slechte datakwaliteit worden onderzocht. Er is een benchmark-systeem om de datakwaliteit te toetsen. (Spruit & Pietzka, 2015, p. 1074)	DMM: Meting van datakwaliteit op kritische data-attributen wordt systematisch vastgelegd in rapporten. (CMMI Institute, 2018, p. 81) MD3M Datakwaliteit wordt objectief gemeten en voor alle data is de kwaliteit bekend. Medewerker zijn bekend met de redenen en bronnen van slechte datakwaliteit in hun dagelijks werk en de consequenties daarvan. Maatregelen voor verbetering van datakwaliteit zijn geïnstalleerd. (Spruit & Pietzka, 2015, p. 1074)	DMM: Meerwaarde van voorgestelde data-aanpassingen wordt kwantitatief getoetst en prioriteiten van management worden verfijnd. Toetsing en rapportage wordt continue verbeterd. (CMMI Institute, 2018, p. 81) MD3M Toetsing van datakwaliteit wordt regelmatig gedaan voor iedere dataset. De organisatie kent de zwakke plekken in haar data en de redenen daarvan. De organisatie toetst datakwaliteit met een benchmark-systeem en borgt dat de datakwaliteit binnen de gedefinieerde kaders blijft (Spruit & Pietzka, 2015, p. 1074)
Opslagbeperking; de gegevens mogen niet langer bewaard worden dan nodig.	DMM: Historische data ondersteunt bedrijfsdoelen, datastores worden gebackupt en data wordt gearchiveerd conform beleid. (CMMI Institute, 2018, pp. 133-134) MD3M Data is opgeslagen op een persistente manier (Spruit & Pietzka, 2015, p. 1075).	DMM: Gedefinieerde methode zorgt dat historische data is beschikbaar voor bedrijfsprocessen. Toegang, aanpassing, retentie, vernietiging en auditing worden gecontroleerd door beleid en processen. (CMMI Institute, 2018, p. 134) MD3M Regelmatig wordt gecheckt of datalogica up-to-date is (Spruit & Pietzka, 2015, p. 1075).	DMM: Een data warehouse geeft toegang tot historische data voor analyses die bedrijfsprocessen ondersteunen. Een audit-programma en een feedbackproces met stakeholders en regelgevers versterken retentie en archiveringsbeleid. (CMMI Institute, 2018, p. 135) MD3M Automatische tools checken regelmatig op dubbele opslag en duplicaten. Richtlijnen zijn opgesteld voor data lifecycle (Spruit & Pietzka, 2015, p. 1075).	DMM: Modellen worden toegepast om compliance met wet- en regelgeving te voorspellen. Metingen en stakeholder feedback worden gebruikt om beleid m.b.t. dataretentie en -archivering te evalueren en verbeteren. (CMMI Institute, 2018, p. 136) MD3M Datalogica wordt regelmatig gecheckt op persistentie, prestatie en efficiëntie. Voor ieder data item is één bron vastgesteld (Spruit & Pietzka, 2015, p. 1075).	DMM: De organisatie deelt beleid en best practices over historische data en archivering in haar sector. (CMMI Institute, 2018, p. 136) MD3M Data is opgeslagen met mogelijkheden voor analyse en voorspellingen (Spruit & Pietzka, 2015, p. 1075).

Integriteit en vertrouwelijkheid; gegevens moeten goed beveiligd zijn en vertrouwelijk blijven".	MD3M De technische eisen voor databescherming zijn vervuld. (Spruit & Pietzka, 2015, p. 1075)	MD3M Toegang tot data wordt alleen geactiveerd op verzoek. (Spruit & Pietzka, 2015, p. 1075)	MD3M Richtlijnen bepalen welke rollen datatoegang krijgen. (Spruit & Pietzka, 2015, p. 1075) <<IT-CMF>> Managen van beleid en controls voor integriteit, vertrouwelijkheid, verantwoordelijkheid, bruikbaarheid en beschikbaarheid van informatie. (IVI, 2018)	MD3M Voor systemen met datatoegang bestaan wachtwoorden die voldoen aan algemene security standaarden en die regelmatig aangepast worden. (Spruit & Pietzka, 2015, p. 1075)	MD3M Security awareness in het kader van databescherming wordt verhoogd onder personeel. (Spruit & Pietzka, 2015, p. 1075)

Bijlage 6 Demonstratie in organisaties

Tabel 28 Demonstratie in educatieve organisatie a.d.h.v. eerste versie vragenlijst AVG-volwassenheidsmodel

Vragen voor rechtmatigheid, behoorlijkheid en transparantie	**Antwoord**
RBT1 Hoe is eigenaarschap en verantwoordelijkheid voor persoonsdata toegewezen? 1. Soms in projecten 2. In logisch consistente rollen en verantwoordelijkheden op prioriteit voor de organisatie 3. Door organisatiebrede governance met alle afdelingen die persoonsdata gebruiken/leveren. 4. Door governance op persoonsdata die gemeten en verbeterd wordt 5. Door governance op persoonsdata die continue verbeterd wordt waarbij best practices worden gedeeld in de sector.	3
RBT2 Hoe wordt gebruik van persoonsdata afgestemd met betrokkenen? 1. Soms, inconsistent bij sommige diensten wordt afgestemd 2. Processen managen deze afstemming. 3. Beleid en processen borgen de gedefinieerde afstemming. 4. De afstemming en beleid en controle daarop worden gemeten. 5. De afstemming alsmede beleid en controle daarop worden continu verbeterd.	3
Score	3
Vragen voor doelbinding	**Antwoord**
D1 Hoe wordt geborgd dat de organisatie persoonsdata alleen gebruikt voor het specifieke doel? 1. Informele en inconsistente review van requirements van persoonsdata t.a.v. organisatiedoelen. 2. Requirements voor persoonsdata t.a.v. organisatiedoelen worden gevolgd en gemanaged. 3. Requirements voor persoonsdata zijn gedefinieerd, gevalideerd op organisatieprioriteit en geïntegreerd in een standaard raamwerk. Beleid en controls, i.e. preventieve en correctieve maatregelen, borgen de doelbinding. 4. Requirements voor persoonsdata t.a.v. de organisatiedoelen worden geborgd door gedefinieerde meetwaarden. Beleid en controle voor doelbinding zijn meetbaar. 5. Best practices voor requirements voor persoonsdata t.a.v. organisatiedoelen worden gedeeld binnen de sector. Beleid en controle voor doelbinding worden continu verbeterd.	2
Score	2
Vragen voor minimale gegevensverwerking	**Antwoord**
MG1 Hoe wordt geborgd dat de organisatie voor persoonsdata minimale gegevensverwerking doet? 1. persoonsdata-architectuur is informeel en inconsistent. 2. Met persoonsdata-architectuur worden issues als dubbele opslag, uitzonderingen op standaardgebruik gemanaged. Creatie en gebruik van persoonsdata zijn traceerbaar in alle bronnen. 3. Een gedefinieerd datarationalisatieproces borgt de minimale gegevensverwerking: persoonsdata wordt gecheckt op dubbele opslag, noodzaak t.a.v. organisatiedoelen. 4. Op basis van statistische analyse van het datarationalisatieproces worden correcties op architectuur van persoonsdata uitgevoerd en gebruikt als input voor design. 5. Voorspellingen worden geëvalueerd in relatie tot een continu proces van verbetering van persoonsdata-architectuur. Best practices over persoonsdata-architectuur worden gedeeld binnen de sector.	2
Score	2
Vragen voor juistheid	**Antwoord**
J1 Hoe wordt de juistheid van persoonsdata geborgd? 1. Juistheid van persoonsdata wordt ad hoc getoetst en resultaten worden vastgelegd. 2. Doelen en standaarden voor de toetsing van juistheid van persoonsdata zijn vastgelegd, gebruikt en onderhouden met standaard technieken en processen. 3. Door gedefinieerd beleid en controls, i.e. preventieve en correctieve maatregelen, zoals periodieke toetsing volgens schema en na specifieke triggers, en mogelijkheden voor correctie door betrokkenen. 4. Meting van processen voor juistheid op kritische attributen van alle persoonsdata wordt systematisch vastgelegd in rapporten. 5. Best practices voor de juistheid van persoonsdata worden in de sector gedeeld. Juistheid van persoonsdata en de toetsing daarvan wordt continu en geautomatiseerd verbeterd.	3
Score	3

Vragen voor opslagbeperking	Antwoord
O1 Hoe wordt opslagbeperking van persoonsdata geborgd? 1. Historische persoonsdata ondersteunt soms bedrijfsdoelen, datastores worden geback-upt en data wordt gearchiveerd 2. Logica, toegang, aanpassing, opslag, vernietiging en auditing van persoonsdata worden gecontroleerd door beleid en processen 3. Gedefinieerde processen voor audit en feedback met stakeholders en regelgevers versterken opslag en archiveringsbeleid m.b.t historische persoonsdata. Automatische tools checken regelmatig op dubbele opslag. Richtlijnen zijn opgesteld voor persoonsdata lifecycle. 4. Metingen worden gebruikt om beleid m.b.t. opslag en -archivering van persoonsdata te evalueren en verbeteren. Datalogica wordt regelmatig gecheckt op persistentie efficiëntie. Voor ieder persoonsdata-item is één bron vastgesteld. 5. Best practices over historische persoonsdata en archivering worden gedeeld in de sector. Continue procesverbetering voor de opslag van persoonsdata met mogelijkheden voor analyse en voorspellingen.	2
Score	2
Vragen voor integriteit en vertrouwelijkheid	**Antwoord**
IV1 Hoe worden integriteit en vertrouwelijkheid van persoonsdata geborgd? 1. Integriteit en vertrouwelijkheid van persoonsdata zijn informeel en inconsistent beschreven en gemanaged 2. Integriteit en vertrouwelijkheid van persoonsdata zijn beschreven en gemanaged. 3. Beleid, zoals BIV-classificatie, en controls, i.e. preventieve en correctieve maatregelen, zijn gedefinieerd voor het borgen van integriteit en vertrouwelijkheid van persoonsdata. 4. Effectiviteit van beleid en controls voor integriteit en vertrouwelijkheid wordt gemeten. 5. Beleid en controls voor integriteit en vertrouwelijkheid worden continu gemeten en verfijnd. Best practices voor gegevensbescherming worden gedeeld in de sector.	4
IV2 Hoe wordt toegang tot persoonsdata geregeld? 1. Informeel en inconsistent, de technische eisen voor bescherming van persoonsdata zijn vervuld. 2. Toegang tot data wordt alleen geactiveerd op verzoek. 3. Richtlijnen bepalen welke rollen datatoegang krijgen. 4. Voor systemen met toegang tot persoonsdata bestaan wachtwoorden die voldoen aan algemene security standaarden en die regelmatig aangepast worden. 5. Security awareness, i.e. bewustzijn en verantwoordelijkheidsgevoel om beveiligingsincidenten met persoonsdata te voorkomen, wordt verhoogd onder personeel.	5
Score	4

Tabel 29 Demonstratie in zorgorganisatie

Vragen voor rechtmatigheid, behoorlijkheid en transparantie	Antwoord
RBT1 Hoe is eigenaarschap en verantwoordelijkheid voor persoonsdata toegewezen? 1. Soms in projecten 2. In logisch consistente rollen en verantwoordelijkheden op prioriteit voor de organisatie 3. Door organisatiebrede governance met alle afdelingen die persoonsdata gebruiken/leveren. 4. Door governance op persoonsdata die gemeten en verbeterd wordt 5. Door governance op persoonsdata die continue verbeterd wordt waarbij best practices worden gedeeld in de sector.	3
RBT2 Hoe wordt gebruik van persoonsdata afgestemd met betrokkenen? 1. Soms, inconsistent bij sommige diensten wordt afgestemd 2. Processen managen deze afstemming. 3. Beleid en processen borgen de gedefinieerde afstemming. 4. De afstemming en beleid en controle daarop worden gemeten. 5. De afstemming alsmede beleid en controle daarop worden continu verbeterd.	4
Score	3

Vragen voor doelbinding	**Antwoord**
D1 Hoe wordt geborgd dat de organisatie persoonsdata alleen gebruikt voor het specifieke doel? 1. Informele en inconsistente review van requirements van persoonsdata t.a.v. organisatiedoelen. 2. Requirements voor persoonsdata t.a.v. organisatiedoelen worden gevolgd en gemanaged. 3. Requirements voor persoonsdata zijn gedefinieerd, gevalideerd op organisatieprioriteit en geïntegreerd in een standaard raamwerk. Beleid en controls, i.e. preventieve en correctieve maatregelen, borgen de doelbinding. 4. Requirements voor persoonsdata t.a.v. de organisatiedoelen worden geborgd door gedefinieerde meetwaarden. Beleid en controle voor doelbinding zijn meetbaar. 5. Best practices voor requirements voor persoonsdata t.a.v. organisatiedoelen worden gedeeld binnen de sector. Beleid en controle voor doelbinding worden continu verbeterd.	3
Score	3
Vragen voor minimale gegevensverwerking	**Antwoord**
MG1 Hoe wordt geborgd dat de organisatie voor persoonsdata minimale gegevensverwerking doet? 1. persoonsdata-architectuur is informeel en inconsistent. 2. Met persoonsdata-architectuur worden issues als dubbele opslag, uitzonderingen op standaardgebruik gemanaged. Creatie en gebruik van persoonsdata zijn traceerbaar in alle bronnen. 3. Een gedefinieerd datarationalisatieproces borgt de minimale gegevensverwerking: persoonsdata wordt gecheckt op dubbele opslag, noodzaak t.a.v. organisatiedoelen. 4. Op basis van statistische analyse van het datarationalisatieproces worden correcties op architectuur van persoonsdata uitgevoerd en gebruikt als input voor design. 5. Voorspellingen worden geëvalueerd in relatie tot een continu proces van verbetering van persoonsdata-architectuur. Best practices over persoonsdata-architectuur worden gedeeld binnen de sector.	3
Score	3
Vragen voor juistheid	**Antwoord**
J1 Hoe wordt de juistheid van persoonsdata geborgd? 1. Juistheid van persoonsdata wordt ad hoc getoetst en resultaten worden vastgelegd. 2. Doelen en standaarden voor de toetsing van juistheid van persoonsdata zijn vastgelegd, gebruikt en onderhouden met standaard technieken en processen. 3. Door gedefinieerd beleid en controls, i.e. preventieve en correctieve maatregelen, zoals periodieke toetsing volgens schema en na specifieke triggers, en mogelijkheden voor correctie door betrokkenen. 4. Meting van processen voor juistheid op kritische attributen van alle persoonsdata wordt systematisch vastgelegd in rapporten. 5. Best practices voor de juistheid van persoonsdata worden in de sector gedeeld. Juistheid van persoonsdata en de toetsing daarvan wordt continu en geautomatiseerd verbeterd.	5
Score	5
Vragen voor opslagbeperking	**Antwoord**
O1 Hoe wordt opslagbeperking van persoonsdata geborgd? 1. Historische persoonsdata ondersteunt soms bedrijfsdoelen, datastores worden geback-upt en data wordt gearchiveerd 2. Logica, toegang, aanpassing, opslag, vernietiging en auditing van persoonsdata worden gecontroleerd door beleid en processen 3. Gedefinieerde processen voor audit en feedback met stakeholders en regelgevers versterken opslag en archiveringsbeleid m.b.t historische persoonsdata. Automatische tools checken regelmatig op dubbele opslag. Richtlijnen zijn opgesteld voor persoonsdata lifecycle. 4. Metingen worden gebruikt om beleid m.b.t. opslag en -archivering van persoonsdata te evalueren en verbeteren. Datalogica wordt regelmatig gecheckt op persistentie efficiëntie. Voor ieder persoonsdata-item is één bron vastgesteld. 5. Best practices over historische persoonsdata en archivering worden gedeeld in de sector. Continue procesverbetering voor de opslag van persoonsdata met mogelijkheden voor analyse en voorspellingen.	2
Score	2

Vragen voor integriteit en vertrouwelijkheid	Antwoord
IV1 Hoe worden integriteit en vertrouwelijkheid van persoonsdata geborgd? 1. Integriteit en vertrouwelijkheid van persoonsdata zijn informeel en inconsistent beschreven en gemanaged 2. Integriteit en vertrouwelijkheid van persoonsdata zijn beschreven en gemanaged. 3. Beleid, zoals BIV-classificatie, en controls, i.e. preventieve en correctieve maatregelen, zijn gedefinieerd voor het borgen van integriteit en vertrouwelijkheid van persoonsdata. 4. Effectiviteit van beleid en controls voor integriteit en vertrouwelijkheid wordt gemeten. 5. Beleid en controls voor integriteit en vertrouwelijkheid worden continu gemeten en verfijnd. Best practices voor gegevensbescherming worden gedeeld in de sector.	2
IV2 Hoe wordt toegang tot persoonsdata geregeld? 1. Informeel en inconsistent, de technische eisen voor bescherming van persoonsdata zijn vervuld. 2. Toegang tot data wordt alleen geactiveerd op verzoek. 3. Richtlijnen bepalen welke rollen datatoegang krijgen. 4. Voor systemen met toegang tot persoonsdata bestaan wachtwoorden die voldoen aan algemene security standaarden en die regelmatig aangepast worden. 5. Security awareness, i.e. bewustzijn en verantwoordelijkheidsgevoel om beveiligingsincidenten met persoonsdata te voorkomen, wordt verhoogd onder personeel.	4
Score	3

Bijlage 7 Eerste evaluatie

Tabel 30 Eerste evaluatie: vragenlijst AVG-volwassenheidsmodel, waargenomen toepasbaarheid, waargenomen gebruiksgemak, intentie voor gebruik, aantal respondenten per vraag per score.

	Zeer oneens	Oneens	Enigszins oneens	Niet oneens, niet eens	Enigszins eens	Eens	Zeer eens
Eerste evaluatie	1	2	3	4	5	6	7
waargenomen bruikbaarheid							
Ik geloof dat dit volwassenheidsmodel de inspanning zou verminderen die nodig is om de AVG-volwassenheid van de organisatie te meten.					1	3	
Het meten van de AVG-volwassenheid door middel van dit volwassenheidsmodel zou lastig zijn om te begrijpen door gebruikers.			3			1	
Met dit volwassenheidsmodel kunnen gebruikers gemakkelijker controleren of de AVG correct wordt toegepast.		1			1	2	
Over het algemeen vond ik het volwassenheidsmodel nuttig						4	
Het gebruik van dit volwassenheidsmodel zou het moeilijker maken om de AVG-volwassenheid te meten.		4					
Over het algemeen denk ik dat dit volwassenheidsmodel geen effectieve oplossing biedt om de AVG-volwassenheid van de organisatie in kaart te brengen.		2	2				
Over het algemeen denk ik dat dit volwassenheidsmodel een verbetering is voor de standaard implementatie van de AVG.		1			1	2	
Met behulp van dit volwassenheidsmodel zou het gemakkelijker zijn om de AVG volwassenheid te communiceren naar eindgebruikers.				1	1	2	
waargenomen gebruiksgemak							
Ik vond de procedure voor het toepassen van het volwassenheidsmodel complex en moeilijk te volgen		1		1	1	1	
Over het algemeen vond ik het volwassenheidsmodel moeilijk te gebruiken				2	1	1	
Ik vond het volwassenheidsmodel eenvoudig om aan te leren			1	1	2		
Ik vond het moeilijk om het volwassenheidsmodel toe te passen om de AVG-volwassenheid te meten binnen mijn eigen bedrijfscontext		1			2	1	
Ik vond de vragen van het volwassenheidsmodel duidelijk en gemakkelijk te begrijpen.		1			3		
Ik heb er geen vertrouwen in dat ik nu in staat ben om dit volwassenheidsmodel in de praktijk toe te passen.		1	1	2			
Intentie voor gebruik							
Ik zou dit volwassenheidsmodel zeker niet gebruiken om de AVG-volwassenheid van de organisatie te meten.		3	1				
Ik ben in de toekomst van plan om dit volwassenheidsmodel bij voorkeur te gebruiken bij het in kaart brengen van de AVG-volwassenheid in plaats van de standaard rapportages.				2		2	

Tabel 31 Eerste evaluatie, educatie FG, relevantie vragenlijst AVG-volwassenheidsmodel

	Zeer oneens	Oneens	Enigszins oneens	Niet oneens, niet eens	Enigszins eens	Eens	Zeer eens	Toelichting
	1	2	3	4	5	6	7	
Relevantie vragen voor de toetsing van AVG-volwassenheid								
Vraag RBT1 is relevant om de AVG-volwassenheid binnen de dimensie "Rechtmatigheid, behoorlijkheid en transparantie" te toetsen.							v	
Vraag RBT2 is relevant om de AVG-volwassenheid binnen de dimensie "Rechtmatigheid, behoorlijkheid en transparantie" te toetsen.							v	Uitbreiding: alle verwerkingen persoonsdata opgenomen in verwerkingsregister
Vraag D1 is relevant om de AVG-volwassenheid binnen de dimensie "Doelbinding" te toetsen.						v		Tweeledig maken: eerst doel vastleggen dan alleen voor dat doel gebruiken. Opties: requirements verwoording versimpelen, is te complex, te datatechnisch
Vraag MG1 is relevant om de AVG-volwassenheid binnen de dimensie "Minimale gegevensverwerking" te toetsen.		v						Opties minder relevant: Dubbele opslag minder relevant, data-architectuur ook minder relevant. Proportionaliteit en subsidiariteit opnemen, anonimiseren opnemen, verschillende minimalisaties in verschillende contexten
Vraag J1 is relevant om de AVG-volwassenheid binnen de dimensie "Juistheid" te toetsen.						v		
Vraag O1 is relevant om de AVG-volwassenheid binnen de dimensie "Opslagbeperking" te toetsen.					v			Logica aanpassing toegang weg, bewaartermijn toevoegen, wettig opslaan, doelbinding, en zet anonimisering in
Vraag IV1 is relevant om de AVG-volwassenheid binnen de dimensie "Integriteit en vertrouwelijkheid" te toetsen.						v		Specifieker: 2factor, versleuteling, kijk naar 'privacy by design', security awareness hier toevoegen
Vraag IV2 is relevant om de AVG-volwassenheid binnen de dimensie "Integriteit en vertrouwelijkheid" te toetsen.					v			Least privilege principle, continu updaten middels account autorisaties lifecycle,

Tabel 32 Eerste evaluatie, educatie IA, relevantie vragenlijst AVG-volwassenheidsmodel

	Zeer oneens	Oneens	Enigszins oneens	Niet oneens, niet eens	Enigszins eens	Eens	Zeer eens	Toelichting
	1	2	3	4	5	6	7	
Relevantie vragen voor de toetsing van AVG-volwassenheid								
Vraag RBT1 is relevant om de AVG-volwassenheid binnen de dimensie "Rechtmatigheid, behoorlijkheid en transparantie" te toetsen.						v		
Vraag RBT2 is relevant om de AVG-volwassenheid binnen de dimensie "Rechtmatigheid, behoorlijkheid en transparantie" te toetsen.						v		
Vraag D1 is relevant om de AVG-volwassenheid binnen de dimensie "Doelbinding" te toetsen.					v			Requirements-term anders formuleren
Vraag MG1 is relevant om de AVG-volwassenheid binnen de dimensie "Minimale gegevensverwerking" te toetsen.					v			Dubbele opslag n.v.t., niet meer verwerken dan nodig binnen ieder systeem, niet herhaaldelijk opvragen, eventueel extra vraag afsplitsen
Vraag J1 is relevant om de AVG-volwassenheid binnen de dimensie "Juistheid" te toetsen.						v		Wellicht juistheid scherp toelichten. Correctie mogelijkheden door betrokkenen anders verwoorden zodat het niet correctierecht is!
Vraag O1 is relevant om de AVG-volwassenheid binnen de dimensie "Opslagbeperking" te toetsen.					v			Opslagbeperking goed onderscheiden van minimale gegevensverwerking, woordkeus tussen juridisch en technisch jargon, moeten de wet nog dekken, maar goed te interpreteren zijn door verschillende gebruikers van het model, automatische tools hoeven nog niet bij 3, level 2 moet managed bevatten, aansluiten op definitie maturity model
Vraag IV1 is relevant om de AVG-volwassenheid binnen de dimensie "Integriteit en vertrouwelijkheid" te toetsen.						v		Managed niet in niveau 1, data vs gegevens consistent te gebruiken (verschil aangeven)
Vraag IV2 is relevant om de AVG-volwassenheid binnen de dimensie "Integriteit en vertrouwelijkheid" te toetsen.					v			De werkwijze is meer herkenbaar, concreter, maar opties zijn inconsistent met model.

Tabel 33 Eerste evaluatie, zorg FG, relevantie vragenlijst AVG-volwassenheidsmodel

	Zeer oneens	Oneens	Enigszins oneens	Niet oneens, niet eens	Enigszins eens	Eens	Zeer eens	Toelichting
	1	2	3	4	5	6	7	
Relevantie vragen voor de toetsing van AVG-volwassenheid								
Vraag RBT1 is relevant om de AVG-volwassenheid binnen de dimensie "Rechtmatigheid, behoorlijkheid en transparantie" te toetsen.							v	Verwerkingsregister benoemen
Vraag RBT2 is relevant om de AVG-volwassenheid binnen de dimensie "Rechtmatigheid, behoorlijkheid en transparantie" te toetsen.						v		
Vraag D1 is relevant om de AVG-volwassenheid binnen de dimensie "Doelbinding" te toetsen.						v		Vraag relevant, maar Woordkeus opties kan duidelijker
Vraag MG1 is relevant om de AVG-volwassenheid binnen de dimensie "Minimale gegevensverwerking" te toetsen.					v			Anonimisering, woordkeus minder datatechnisch, dubbele opslag is niet zo relevant, proportionaliteit
Vraag J1 is relevant om de AVG-volwassenheid binnen de dimensie "Juistheid" te toetsen.						v		N5, "deels automatisch" overwegen als aspect
Vraag O1 is relevant om de AVG-volwassenheid binnen de dimensie "Opslagbeperking" te toetsen.					v			Verwijderen moet prominenter terugkomen in model, opslagbeperking per onderdeel/item/datagebied
Vraag IV1 is relevant om de AVG-volwassenheid binnen de dimensie "Integriteit en vertrouwelijkheid" te toetsen.						v		Security awareness hoort bij deze vraag
Vraag IV2 is relevant om de AVG-volwassenheid binnen de dimensie "Integriteit en vertrouwelijkheid" te toetsen.						v		n5 verbeteren, continu verbetering, automatisering, delen in sector.

Tabel 34 Eerste evaluatie, zorg IA, relevantie vragenlijst AVG-volwassenheidsmodel

	Zeer oneens	Oneens	Enigszins oneens	Niet oneens, niet eens	Enigszins eens	Eens	Zeer eens	Toelichting
	1	2	3	4	5	6	7	
Relevantie vragen voor de toetsing van AVG-volwassenheid								
Vraag RBT1 is relevant om de AVG-volwassenheid binnen de dimensie "Rechtmatigheid, behoorlijkheid en transparantie" te toetsen.					v			Verschil tussen 4 en 5: verbeteren, is "best practices delen" een voorbeeld of een must?
Vraag RBT2 is relevant om de AVG-volwassenheid binnen de dimensie "Rechtmatigheid, behoorlijkheid en transparantie" te toetsen.						v		Wellicht vraag aanpassen: hoe wordt afstemming van gebruik persoonsdata geborgd? en dan verwerkingsregister onderdeel maken, RBT terug laten komen in vraagstelling!
Vraag D1 is relevant om de AVG-volwassenheid binnen de dimensie "Doelbinding" te toetsen.						v		leesbaarheid
Vraag MG1 is relevant om de AVG-volwassenheid binnen de dimensie "Minimale gegevensverwerking" te toetsen.					v			Alle niveaus in alle vragen wellicht beginnen met performed, managed, etc. Termen verbeteren: persoonsdata-architectuur, antwoorden beter relateren aan MG, opties meer ontwerpkant, bevatten, subsidiariteit en proportionaliteit terug laten komen
Vraag J1 is relevant om de AVG-volwassenheid binnen de dimensie "Juistheid" te toetsen.					v			automatisch signaleren van mogelijke onjuistheid vs automatisch verbeteren, verschuiving van juistheid meten naar processen meten oplossen
Vraag O1 is relevant om de AVG-volwassenheid binnen de dimensie "Opslagbeperking" te toetsen.					v			Datalifecycle in de vraagstelling prominenter, termen verduidelijken, scherper maken
Vraag IV1 is relevant om de AVG-volwassenheid binnen de dimensie "Integriteit en vertrouwelijkheid" te toetsen.					v			Voorbeelden van controls, daardoor concreter
Vraag IV2 is relevant om de AVG-volwassenheid binnen de dimensie "Integriteit en vertrouwelijkheid" te toetsen.					v			Model wijkt af tav consistentie in model, security awareness hoort bij vorige vraag. Afwegen of dit niet afgedekt wordt in de vraag.

Tabel 35 Eerste evaluatie: Algemene tevredenheid, aantal respondenten per score

	Zeer ontevreden					Noch ontevreden, noch tevreden					Zeer tevreden
	0	1	2	3	4	5	6	7	8	9	10
Algemene tevredenheid eerste evaluatie											
Hoe tevreden ben je in het algemeen met ontwerp en de toepasbaarheid van de vragen binnen het volwassenheidsmodel?						1		3			

Tabel 36 Na eerste evaluatie: Tweede versie vragenlijst AVG-volwassenheidsmodel

Rechtmatigheid, behoorlijkheid en transparantie Dit principe wordt getoetst door te bepalen hoe eigenaarschap en verantwoordelijkheid van persoonsdata in de organisatie toegewezen wordt en hoe het gebruik van persoonsdata wordt vastgelegd en afgestemd met betrokkenen.		
	Antwoord	**Toelichting**
RBT1 Hoe zijn eigenaarschap en verantwoordelijkheid voor persoonsdata in de organisatie geborgd? 1. Performed: Ad hoc, informeel en inconsistent 2. Managed: Het toewijzen van eigenaarschap en verantwoordelijkheid wordt gemanaged in processen. Het vastleggen van verwerking van persoonsdata in een verwerkingsregister wordt gemanaged. 3. Defined: Rollen in eigenaarschap en verantwoordelijkheid worden gedefinieerd met alle afdelingen die persoonsdata gebruiken/leveren. Vastlegging in een verwerkingsregister is gedefinieerd en geborgd. 4. Measured: Governance op eigenaarschap en verantwoordelijkheid wordt gemeten. Vastlegging in een verwerkingsregister wordt gemeten. 5. Optimized: Governance op eigenaarschap en vastlegging in een verwerkingsregister worden continu verbeterd. De organisatie deelt best practices voor governance op eigenaarschap en verwerkingsregister in de sector.		
RBT2 Hoe wordt gebruik van persoonsdata afgestemd met betrokkenen? 1. Performed: Ad hoc, informeel en inconsistent 2. Managed: Processen managen de afstemming, 3. Defined: De afstemming is organisatiebreed gedefinieerd en wordt geborgd door beleid en processen. 4. Measured: De afstemming en beleid en controle daarop worden gemeten. 5. Optimized: De afstemming alsmede beleid en controle daarop worden continu verbeterd. De organisatie deelt best practices voor afstemming met betrokkenen in de sector.		
Score		

Doelbinding Dit principe wordt getoetst door te bepalen hoe geborgd wordt dat de verwerking van persoonsdata in de organisatie alleen plaatsvindt voor specifieke en gerechtvaardigde doelen.		
	Antwoord	**Toelichting**
D1 Hoe wordt geborgd dat de organisatie persoonsdata alleen verwerkt voor het specifieke doel? 1. Performed: Ad hoc, Informeel en inconsistent 2. Managed: Het vastleggen van het doel van persoonsdataverwerking en de naleving van de doelbinding worden gemanaged. 3. Defined: Het vastleggen van het doel van persoonsdataverwerking en de naleving van de doelbinding zijn gedefinieerd in een standaardraamwerk en worden geborgd door beleid, preventieve en correctieve maatregelen. 4. Measured: Het vastleggen van het doel van persoonsdataverwerking en de naleving van de doelbinding worden gemeten. 5. Optimized: Het vastleggen van het doel van persoonsdataverwerking en de naleving van de doelbinding wordt continu verbeterd. De organisatie deelt best practices voor doelbinding in de sector.		
Score		

Minimale gegevensverwerking

Dit principe wordt getoetst door te bepalen hoe dataminimalisatie in de organisatie geborgd wordt door proportionaliteit, subsidiariteit en anonimisatie van persoonsdataverwerking. Toelichting:

- Proportionaliteit houdt in dat voor iedere verwerking persoonsdata niet specifieker dan strikt noodzakelijk verwerkt wordt, bijvoorbeeld: “cijfers van postcode i.p.v. volledige postcode” of “ouder dan 18 i.p.v. geboortedatum”.
- Subsidiariteit houdt in dat voor iedere verwerking bepaald wordt of het doel ook bereikt kan worden zonder verwerking van persoonsdata, bijvoorbeeld: “ontmoeting organiseren i.p.v. lijst e-mailadressen verstrekken”.

	Antwoord	**Toelichting**
MG1 Hoe wordt geborgd dat de organisatie voor persoonsdata minimale gegevensverwerking doet? 1. Performed: Ad hoc, informeel en inconsistent. 2. Managed: Dataminimalisatie door proportionaliteit, subsidiariteit en anonimisatie wordt gemanaged. 3. Defined: Dataminimalisatie door proportionaliteit en subsidiariteit voor productie, alsmede anonimisatie voor onderzoek en test zijn gedefinieerd in een standaard raamwerk en geborgd door beleid, preventieve en correctieve maatregelen. 4. Measured: Dataminimalisatie door proportionaliteit en subsidiariteit en anonimisatie worden gemeten. 5. Optimized: Dataminimalisatie door proportionaliteit, subsidiariteit en anonimisatie worden continu verbeterd. De organisatie deelt best practices voor dataminimalisatie in de sector.		
Score		

Juistheid

Dit principe wordt getoetst door te bepalen hoe de organisatie borgt dat persoonsdata juist is in overeenstemming met de werkelijkheid.

	Antwoord	**Toelichting**
J1 Hoe wordt de juistheid van persoonsdata geborgd? 1. Performed: Ad hoc, informeel en inconsistent. 2. Managed: Juistheid van persoonsdata wordt gemanaged door processen. 3. Defined: Doelen en criteria voor juistheid zijn gedefinieerd in een standaard raamwerk en worden geborgd door beleid, preventieve en correctieve maatregelen, zoals periodieke toetsing volgens schema en na specifieke triggers. Betrokkenen kunnen de juistheid van eigen persoonsdata laten aanpassen. 4. Measured: Juistheid van persoonsdata op kritische attributen van wordt gemeten en systematisch vastgelegd in rapporten. 5. Optimized: Juistheid van persoonsdata wordt continu verbeterd. De organisatie deelt best practices voor juistheid in de sector.		
Score		

Opslagbeperking

Dit principe wordt getoetst door te bepalen hoe de organisatie borgt dat persoonsdata niet langer bewaard wordt dan strikt noodzakelijk voor de verwerking.

	Antwoord	**Toelichting**
O1 Hoe wordt opslagbeperking van persoonsdata geborgd? 1. Performed: Ad hoc, informeel en inconsistent 2. Managed: Opslag en vernietiging van persoonsdata worden gemanaged door processen. 3. Defined: Bewaartermijnen voor persoonsdata en processen voor opslag en vernietiging zijn gedefinieerd in een standaard raamwerk en worden geborgd door beleid voor lifecycle van persoonsdata. Voor ieder persoonsdata-item is één bron vastgelegd. 4. Measured: Lifecycle, opslag en vernietiging van persoonsdata wordt gemeten door audits en feedback door stakeholders en regelgevers. 5. Optimized: Lifecycle, opslag en vernietiging van persoonsdata wordt continue verbeterd. De organisatie deelt best practices voor opslagbeperking in de sector.		
Score		

Integriteit en vertrouwelijkheid

Dit principe wordt getoetst door te bepalen hoe in de organisatie integriteit en vertrouwelijkheid geborgd worden en hoe de toegang tot persoonsdata beveiligd is.

Toelichting:

- Integriteit is de mate waarin persoonsdata in het systeem onterecht aangepast of vernietigd wordt.
- Vertrouwelijkheid is de mate waarin persoonsdata in het systeem niet toegankelijk is voor onbevoegden.
- BIV-classificatie is informatiebeveiligingsbeleid dat per dienst vastlegt wat de vereiste niveaus van (beschikbaarheid,) integriteit en vertrouwelijkheid zijn en welke (technische) maatregelen daarbij genomen moeten worden.
- Multifactor-authenticatie is het bewijzen van identiteit door verschillende factoren, bijvoorbeeld: “inloggen met een wachtwoord (iets wat men weet) en een vingerdruk (iets wat men heeft).
- Encryptie is een techniek waarmee persoonsdata versleuteld wordt, zodat deze niet gelezen kan worden door derden zonder sleutel.
- Checksum is een techniek waarmee de integriteit van (persoons)data tussen systemen gecontroleerd kan worden.
- Security Awareness is het bewustzijn en verantwoordelijkheidsgevoel om beveiligingsincidenten met (persoons)data te voorkomen.

	Antwoord	**Toelichting**
IV1 Hoe worden integriteit en vertrouwelijkheid van persoonsdata geborgd? 1. Performed: Adhoc, informeel en inconsistent. 2. Managed: Integriteit en vertrouwelijkheid van persoonsdata worden gemanaged in beheer en processen. 3. Defined: Beleid, zoals BIV-classificatie, en technische maatregelen zoals multi-factor authenticatie, encryptie en checksum zijn gedefinieerd en borgen de integriteit en vertrouwelijkheid van persoonsdata. 4. Measured: Integriteit en vertrouwelijkheid van persoonsdata worden gemeten en geaudit. Security Awareness wordt gemeten onder personeel. 5. Optimized: Integriteit en vertrouwelijkheid van persoonsdata en security awareness van personeel worden continu verbeterd. De organisatie deelt best practices voor integriteit en vertrouwelijkheid van persoonsdata worden in de sector.		
IV2 Hoe wordt toegang tot persoonsdata beveiligd? 1. Performed: Ad hoc, informeel en inconsistent. 2. Managed: Toegang tot data wordt alleen geactiveerd op verzoek. 3. Defined: Toegang tot persoonsdata is gedefinieerd in een standaard raamwerk van rollen en richtlijnen en wordt geborgd door autorisatiebeleid, wachtwoordbeleid en technische maatregelen. 4. Measured: Toegang tot persoonsdata wordt gemeten en geaudit. 5. Optimized: Beveiliging van toegang tot persoonsdata wordt continu verbeterd. De organisatie deelt best practices voor toegang tot persoonsdata worden in de sector.		
Score		

Bijlage 8 Tweede Evaluatie

Tabel 37 Tweede evaluatie, educatie FG, relevantie tweede versie vragenlijst AVG-volwassenheidsmodel

	Zeer oneens	Oneens	Enigszins oneens	Niet oneens, niet eens	Enigszins eens	Eens	Zeer eens	Feedback (niet verplicht)
	1	2	3	4	5	6	7	
Relevantie vragen voor de toetsing van AVG-volwassenheid								
Vraag RBT1 is relevant om de AVG-volwassenheid binnen de dimensie "Rechtmatigheid, behoorlijkheid en transparantie" te toetsen.							x	Mits je "verantwoording voor gebruik van persoonsgegevens" bedoelt en niet verantwoordelijk…
Vraag RBT2 is relevant om de AVG-volwassenheid binnen de dimensie "Rechtmatigheid, behoorlijkheid en transparantie" te toetsen.							x	Vraag die ik mis is hoe de rechten van betrokkenen geborgd zijn (inzage, correctie, etc)
Vraag D1 is relevant om de AVG-volwassenheid binnen de dimensie "Doelbinding" te toetsen.							x	
Vraag MG1 is relevant om de AVG-volwassenheid binnen de dimensie "Minimale gegevensverwerking" te toetsen.						x		
Vraag J1 is relevant om de AVG-volwassenheid binnen de dimensie "Juistheid" te toetsen.						x		
Vraag O1 is relevant om de AVG-volwassenheid binnen de dimensie "Opslagbeperking" te toetsen.						x		
Vraag IV1 is relevant om de AVG-volwassenheid binnen de dimensie "Integriteit en vertrouwelijkheid" te toetsen.						x		Misschien vraag IV1 en IV2 opdelen in een vraag naar integriteitsborging en een vraag naar vertrouwelijkheid/toegang
Vraag IV2 is relevant om de AVG-volwassenheid binnen de dimensie "Integriteit en vertrouwelijkheid" te toetsen.						x		

Tabel 38 Tweede evaluatie, educatie IA, relevantie tweede versie vragenlijst AVG-volwassenheidsmodel

	Zeer oneens	Oneens	Enigszins oneens	Niet oneens, niet eens	Enigszins eens	Eens	Zeer eens	Feedback (niet verplicht)
	1	2	3	4	5	6	7	
Relevantie vragen voor de toetsing van AVG-volwassenheid								
Vraag RBT1 is relevant om de AVG-volwassenheid binnen de dimensie "Rechtmatigheid, behoorlijkheid en transparantie" te toetsen.							x	
Vraag RBT2 is relevant om de AVG-volwassenheid binnen de dimensie "Rechtmatigheid, behoorlijkheid en transparantie" te toetsen.						x		
Vraag D1 is relevant om de AVG-volwassenheid binnen de dimensie "Doelbinding" te toetsen.						x		
Vraag MG1 is relevant om de AVG-volwassenheid binnen de dimensie "Minimale gegevensverwerking" te toetsen.						x		
Vraag J1 is relevant om de AVG-volwassenheid binnen de dimensie "Juistheid" te toetsen.						x		Ik zou correctierecht onder 2 opnemen (en/of onder 3 iets opnemen over kwalitatief goede verwerking).
Vraag O1 is relevant om de AVG-volwassenheid binnen de dimensie "Opslagbeperking" te toetsen.							x	
Vraag IV1 is relevant om de AVG-volwassenheid binnen de dimensie "Integriteit en vertrouwelijkheid" te toetsen.							x	
Vraag IV2 is relevant om de AVG-volwassenheid binnen de dimensie "Integriteit en vertrouwelijkheid" te toetsen.						x		

Tabel 39 Tweede evaluatie, zorg FG, relevantie tweede versie vragenlijst AVG-volwassenheidsmodel

	Zeer oneens	Oneens	Enigszins oneens	Niet oneens, niet eens	Enigszins eens	Eens	Zeer eens	Feedback (niet verplicht)
	1	2	3	4	5	6	7	
Relevantie vragen voor de toetsing van AVG-volwassenheid								
Vraag RBT1 is relevant om de AVG-volwassenheid binnen de dimensie "Rechtmatigheid, behoorlijkheid en transparantie" te toetsen.							x	
Vraag RBT2 is relevant om de AVG-volwassenheid binnen de dimensie "Rechtmatigheid, behoorlijkheid en transparantie" te toetsen.							x	
Vraag D1 is relevant om de AVG-volwassenheid binnen de dimensie "Doelbinding" te toetsen.							x	
Vraag MG1 is relevant om de AVG-volwassenheid binnen de dimensie "Minimale gegevensverwerking" te toetsen.						x		
Vraag J1 is relevant om de AVG-volwassenheid binnen de dimensie "Juistheid" te toetsen.						x		
Vraag O1 is relevant om de AVG-volwassenheid binnen de dimensie "Opslagbeperking" te toetsen.							x	
Vraag IV1 is relevant om de AVG-volwassenheid binnen de dimensie "Integriteit en vertrouwelijkheid" te toetsen.							x	
Vraag IV2 is relevant om de AVG-volwassenheid binnen de dimensie "Integriteit en vertrouwelijkheid" te toetsen.							x	

Tabel 40 Tweede evaluatie, zorg IA, relevantie tweede versie vragenlijst AVG-volwassenheidsmodel

	Zeer oneens	Oneens	Enigszins oneens	Niet oneens, niet eens	Enigszins eens	Eens	Zeer eens	Feedback (niet verplicht)
	1	2	3	4	5	6	7	
Relevantie vragen voor de toetsing van AVG-volwassenheid								
Vraag RBT1 is relevant om de AVG-volwassenheid binnen de dimensie "Rechtmatigheid, behoorlijkheid en transparantie" te toetsen.						v		Kan het verschil tussen 2 en 3 nog iets duidelijker?
Vraag RBT2 is relevant om de AVG-volwassenheid binnen de dimensie "Rechtmatigheid, behoorlijkheid en transparantie" te toetsen.							v	
Vraag D1 is relevant om de AVG-volwassenheid binnen de dimensie "Doelbinding" te toetsen.							v	
Vraag MG1 is relevant om de AVG-volwassenheid binnen de dimensie "Minimale gegevensverwerking" te toetsen.						v		Als je anonimisatie in de toelichting opneemt, is het helemaal compleet.
Vraag J1 is relevant om de AVG-volwassenheid binnen de dimensie "Juistheid" te toetsen.							v	
Vraag O1 is relevant om de AVG-volwassenheid binnen de dimensie "Opslagbeperking" te toetsen.							v	
Vraag IV1 is relevant om de AVG-volwassenheid binnen de dimensie "Integriteit en vertrouwelijkheid" te toetsen.							v	
Vraag IV2 is relevant om de AVG-volwassenheid binnen de dimensie "Integriteit en vertrouwelijkheid" te toetsen.							v	

Tabel 41 Tweede evaluatie: Algemene tevredenheid, aantal respondenten per score

	Zeer ontevreden					Noch ontevreden, noch tevreden					Zeer tevreden
	0	1	2	3	4	5	6	7	8	9	10
Algemene tevredenheid tweede evaluatie											
Hoe tevreden ben je in het algemeen met ontwerp en de toepasbaarheid van de vragen binnen het volwassenheidsmodel?								1	2	1	

Bijlage 9 Vragenlijst AVGMM

Het AVG-volwassenheidsmodel bestaat uit zes AVG-basisprincipes op vijf volwassenheidsniveaus. Per AVG-basisprincipe worden één tot twee multiplechoicevragen gesteld, om het volwassenheidsniveau, i.e. *performed, managed, defined, measured* of *optimized*, te meten. Hieronder zijn de vragen en de toelichting per vraag voor de toepassing van het model beschreven.

Tabel 42 AVGMM v1.0 Vragenlijst (na tweede evaluatie)

Rechtmatigheid, behoorlijkheid en transparantie Dit principe wordt getoetst door te bepalen hoe eigenaarschap en verantwoordelijkheid van persoonsgegevens in de organisatie toegewezen wordt en hoe het gebruik van persoonsgegevens wordt vastgelegd en afgestemd met betrokkenen.		
	Antwoord	**Toelichting**
RBT1 Hoe zijn eigenaarschap en verantwoordelijkheid voor persoonsgegevens in de organisatie geborgd? 1. Performed: Ad hoc, informeel en inconsistent 2. Managed: Het toewijzen van eigenaarschap en verantwoordelijkheid wordt gemanaged in processen. Het vastleggen van verwerking van persoonsgegevens in een verwerkingsregister wordt gemanaged. 3. Defined: Rollen in eigenaarschap en verantwoordelijkheid worden gedefinieerd met alle afdelingen die persoonsgegevens gebruiken/leveren. Vastlegging in een verwerkingsregister is gedefinieerd en geborgd. 4. Measured: Governance op eigenaarschap en verantwoordelijkheid wordt gemeten. Vastlegging in een verwerkingsregister wordt gemeten. 5. Optimized: Governance op eigenaarschap en vastlegging in een verwerkingsregister worden continu verbeterd. De organisatie deelt best practices voor governance op eigenaarschap en verwerkingsregister in de sector.		
RBT2 Hoe worden betrokkenen geïnformeerd over gebruik van hun persoonsgegevens? 1. Performed: Ad hoc, informeel en inconsistent 2. Managed: Processen managen deze afstemming met betrokkenen. 3. Defined: De afstemming met betrokkenen is organisatiebreed gedefinieerd en wordt geborgd door beleid en processen. 4. Measured: De afstemming en beleid en controle daarop worden gemeten. 5. Optimized: De afstemming alsmede beleid en controle daarop worden continu verbeterd. De organisatie deelt best practices voor afstemming met betrokkenen in de sector.		
Score		

Doelbinding

Dit principe wordt getoetst door te bepalen hoe geborgd wordt dat de verwerking van persoonsgegevens in de organisatie alleen plaatsvindt voor specifieke en gerechtvaardigde doelen.

	Antwoord	Toelichting
D1 Hoe wordt geborgd dat de organisatie persoonsgegevens alleen verwerkt voor het specifieke doel? 1. Performed: Ad hoc, Informeel en inconsistent 2. Managed: Het vastleggen van het doel van persoonsgegevensverwerking en de naleving van de doelbinding worden gemanaged. 3. Defined: Het vastleggen van het doel van persoonsgegevensverwerking en de naleving van de doelbinding zijn gedefinieerd in een standaardraamwerk en worden geborgd door beleid, preventieve en correctieve maatregelen. 4. Measured: Het vastleggen van het doel van persoonsgegevensverwerking en de naleving van de doelbinding worden gemeten. 5. Optimized: Het vastleggen van het doel van persoonsgegevensverwerking en de naleving van de doelbinding wordt continu verbeterd. De organisatie deelt best practices voor doelbinding in de sector.		
Score		

Minimale gegevensverwerking

Dit principe wordt getoetst door te bepalen hoe dataminimalisatie in de organisatie geborgd wordt door proportionaliteit, subsidiariteit en anonimisering van persoonsgegevensverwerking. Toelichting:

- Proportionaliteit houdt in dat de inbreuk op de belangen van de betrokkene niet onevenredig mag zijn in verhouding tot het met de verwerking te dienen doel, bijvoorbeeld: “cijfers van postcode i.p.v. volledige postcode” of “ouder dan 18 i.p.v. geboortedatum”.
- Subsidiariteit houdt in dat voor iedere verwerking bepaald wordt of het doel ook bereikt kan worden zonder verwerking van persoonsgegevens, bijvoorbeeld: “ontmoeting organiseren i.p.v. lijst e-mailadressen verstrekken”. Ingevolge het subsidiariteitsbeginsel mag het doel in redelijkheid niet op een andere, voor de betrokkene minder nadelige wijze kunnen worden verwerkelijkt.
- Anonimisering is de verwerkingshandeling die zorgt dat gegevens niet meer terug te voeren zijn op identificeerbare natuurlijke personen, ook niet door herleiding, koppeling of deductie.

	Antwoord	Toelichting
MG1 Hoe wordt geborgd dat de organisatie voor persoonsgegevens minimale gegevensverwerking doet? 1. Performed: Ad hoc, informeel en inconsistent. 2. Managed: Dataminimalisatie door proportionaliteit, subsidiariteit en anonimisering wordt gemanaged. 3. Defined: Dataminimalisatie door proportionaliteit en subsidiariteit voor productie, alsmede anonimisering voor onderzoek en test zijn gedefinieerd in een standaard raamwerk en geborgd door beleid, preventieve en correctieve maatregelen. 4. Measured: Dataminimalisatie door proportionaliteit en subsidiariteit en anonimisering worden gemeten. 5. Optimized: Dataminimalisatie door proportionaliteit, subsidiariteit en anonimisering worden continu verbeterd. De organisatie deelt best practices voor dataminimalisatie in de sector.		
Score		

Juistheid

Dit principe wordt getoetst door te bepalen hoe de organisatie borgt dat persoonsgegevens juist is in overeenstemming met de werkelijkheid.

	Antwoord	Toelichting
J1 Hoe wordt de juistheid van persoonsgegevens geborgd? 1. Performed: Ad hoc, informeel en inconsistent. 2. Managed: Juistheid van persoonsgegevens wordt gemanaged door processen. 3. Defined: Doelen en criteria voor juistheid zijn gedefinieerd in een standaard raamwerk en worden geborgd door beleid, preventieve en correctieve maatregelen, zoals periodieke toetsing volgens schema en na specifieke triggers. Betrokkenen kunnen de juistheid van eigen persoonsgegevens (laten) aanpassen. 4. Measured: Juistheid van persoonsgegevens op kritische attributen van wordt gemeten en systematisch vastgelegd in rapporten. 5. Optimized: Juistheid van persoonsgegevens wordt continu verbeterd. De organisatie deelt best practices voor juistheid in de sector.		
Score		

Opslagbeperking

Dit principe wordt getoetst door te bepalen hoe de organisatie borgt dat persoonsgegevens niet langer bewaard wordt dan strikt noodzakelijk voor de verwerking.

	Antwoord	Toelichting
O1 Hoe wordt opslagbeperking van persoonsgegevens geborgd? 1. Performed: Ad hoc, informeel en inconsistent 2. Managed: Opslag en vernietiging van persoonsgegevens worden gemanaged door processen. 3. Defined: Bewaartermijnen voor persoonsgegevens en processen voor opslag en vernietiging zijn gedefinieerd in een standaard raamwerk en worden geborgd door beleid voor lifecycle van persoonsgegevens. Voor ieder persoonsgegevens-item is één bron vastgelegd. 4. Measured: Lifecycle, opslag en vernietiging van persoonsgegevens wordt gemeten door audits en feedback door stakeholders en regelgevers. 5. Optimized: Lifecycle, opslag en vernietiging van persoonsgegevens wordt continue verbeterd. De organisatie deelt best practices voor opslagbeperking in de sector.		
Score		

Integriteit en vertrouwelijkheid

Dit principe wordt getoetst door te bepalen hoe in de organisatie integriteit en vertrouwelijkheid geborgd worden en hoe de toegang tot persoonsgegevens beveiligd is.

Toelichting:

- Integriteit is de mate waarin persoonsgegevens in het systeem onterecht aangepast of vernietigd wordt.
- Vertrouwelijkheid is de mate waarin persoonsgegevens in het systeem niet toegankelijk is voor onbevoegden.
- BIV-classificatie is informatiebeveiligingsbeleid dat per dienst vastlegt wat de vereiste niveaus van (beschikbaarheid,) integriteit en vertrouwelijkheid zijn en welke (technische) maatregelen daarbij genomen moeten worden.
- Multifactor-authenticatie is het bewijzen van identiteit door verschillende factoren, bijvoorbeeld: “inloggen met een wachtwoord (iets wat men weet) en een vingerdruk (iets wat men heeft).
- Encryptie is een techniek waarmee persoonsgegevens versleuteld wordt, zodat deze niet gelezen kan worden door derden zonder sleutel.
- Checksum is een techniek waarmee de integriteit van (persoons)data tussen systemen gecontroleerd kan worden.
- Security Awareness is het bewustzijn en verantwoordelijkheidsgevoel om beveiligingsincidenten met (persoons)data te voorkomen.

	Antwoord	**Toelichting**
IV1 Hoe worden integriteit en vertrouwelijkheid van persoonsgegevens geborgd? 1. Performed: Adhoc, informeel en inconsistent. 2. Managed: Integriteit en vertrouwelijkheid van persoonsgegevens worden gemanaged in beheer en processen. 3. Defined: Beleid, zoals BIV-classificatie, en technische maatregelen zoals multi-factor authenticatie, encryptie en checksum zijn gedefinieerd en borgen de integriteit en vertrouwelijkheid van persoonsgegevens. 4. Measured: Integriteit en vertrouwelijkheid van persoonsgegevens worden gemeten en geaudit. Security Awareness wordt gemeten onder personeel. 5. Optimized: Integriteit en vertrouwelijkheid van persoonsgegevens en security awareness van personeel worden continu verbeterd. De organisatie deelt best practices voor integriteit en vertrouwelijkheid van persoonsgegevens in de sector.		
IV2 Hoe wordt toegang tot persoonsgegevens beveiligd? 1. Performed: Ad hoc, informeel en inconsistent. 2. Managed: Toegang tot persoonsgegevens wordt alleen geactiveerd op verzoek. 3. Defined: Toegang tot persoonsgegevens is gedefinieerd in een standaard raamwerk van rollen en richtlijnen en wordt geborgd door autorisatiebeleid, authenticatiebeleid en technische maatregelen. 4. Measured: Toegang tot persoonsgegevens wordt gemeten en geaudit. 5. Optimized: Beveiliging van toegang tot persoonsgegevens wordt continu verbeterd. De organisatie deelt best practices voor toegang tot persoonsgegevens worden in de sector.		
Score		