Aantoonbaarheid van GDPR-compliance van Topicus met behulp van Enterprise Architecture

Auteur	Ruben Stam
Project	Afstudeerscriptie
Datum	21-1-2019
Versie	2.0.0

Versiehistorie

Versie	Datum	Beschrijving	Auteur
0.1.0	10-09-2018	Document aangemaakt.	Ruben Stam
0.2.0	29-09-2018	Probleemanalyse toegevoegd.	Ruben Stam
0.3.0	17-09-2018	Gedeelte contextanalyse toegevoegd.	Ruben Stam
0.4.0	20-10-2018	Contextanalyse afgemaakt en feedback verwerkt.	Ruben Stam
0.4.1	30-10-2018	Opmaak vernieuwd.	Ruben Stam
0.5.0	05-11-2018	Behoefteanalyse toegevoegd.	Ruben Stam
0.6.0	09-11-2018	Initiële requirements toegevoegd.	Ruben Stam
0.7.0	26-11-2018	Literatuuronderzoek toegevoegd.	Ruben Stam
0.8.0	03-12-2018	Architectuurplaat toegevoegd.	Ruben Stam
0.9.0	16-12-2018	Feedback verwerkt	Ruben Stam
0.10.0	25-12-2018	Analyse toegevoegd.	Ruben Stam
0.11.0	01-01-2018	Feedback literatuuronderzoek verwerkt en architectuurplaten toegevoegd.	Ruben Stam
0.11.1	03-01-2018	Contextanalyse herschreven.	Ruben Stam
1.0.0	07-01-2018	Officiële conceptversie .	Ruben Stam
1.1.0	16-01-2018	Feedback verwerkt.	Ruben Stam
2.0.0	21-01-2018	Definitieve versie	Ruben Stam

Tabel 1 Versiehistorie

Management samenvatting

Topicus is een softwarebedrijf dat software maakt voor zorg-, onderwijs-, overheids- en financiële instellingen. Voor het verwerken van hypotheekaanvragen ontwikkeld Topicus de applicatie FORCE. De organisatie wil aan kunnen tonen dat zij aan de General Data Protection Regulation (GDPR) regelgeving voldoet. Met behulp van Enterprise Architecture kunnen de relaties tussen bedrijfsprocessen, data, applicaties en infrastructuur in kaart worden gebracht en inzichtelijk worden gemaakt. Dit zorgt voor traceerbaarheid, wat mogelijk bij kan dragen aan het aantonen van GDPR-compliance. Deze toepassing van Enterprise Architecture is in deze scriptie onderzocht.

In het vooronderzoek is onder andere naar de inhoud van de GDPR gekeken en welke eisen het stelt aan Topicus. Daarnaast is er een Enterprise Architecture framework gekozen om componenten van FORCE in te modelleren.

Vervolgens zijn er Enterprise Archtiecture-modellen van de FORCE-componenten Morality, NHG Gateway, Proposals en Agreements opgesteld en zijn deze geanalyseerd. Voor de analyse zijn de user requirements naast de architectuurplaten gelegd om na te gaan wat er uit de architectuurmodellen afgeleid kan worden. Uit de analyse komen de volgende punten naar voren:

- Uit de architectuurplaten is af te leiden in welke *informatiesystemen* er data wordt verzameld.
- Uit de architectuurplaten is af te leiden in welke *businessprocessen* er data wordt verzameld.
- Uit de architectuurplaten is deels af te leiden *waar* data wordt opgeslagen: Databases zijn af te leiden, maar overige opslaglocaties zoals logbestanden niet.
- Uit de architectuurplaten is deels af te leiden *welke* data wordt opgeslagen: Het onderwerp waar data betrekking op heeft is inzichtelijk, bijvoorbeeld een hypotheekovereenkomst of een rentevoorstel, maar niet welke data er daadwerkelijk opgeslagen wordt zoals NAW-gegevens, onderpand, BSN, etc.

Dat maar deels af te leiden is welke data opgeslagen wordt en waar data opgeslagen wordt is te wijten aan de aard van Enterprise Architecture, de bijbehorende modelleertaal ArchiMate en de aard van dit onderzoek. Enterprise Architecture en ArchiMate zijn alleenstaand niet geschikt voor het gedetailleerd modelleren en inzichtelijk maken van software, hetgeen juist in dit onderzoek gewenst is. Het gevolg hiervan is dat er maar één maatregel geïdentificeerd kan worden om Topicus meer GDPR-compliant te maken, namelijk het uitbreiden van de Record Retention-functionaliteit naar alle databases. Wel bestaat het vermoeden dat Enterprise Architecture in combinatie met UML-diagrammen tot meer inzicht kan leiden.

Concluderend is Enterprise Architecture alleenstaand niet geschikt voor Topicus om toegepast te worden om GDPR-compliance aan te tonen. Om GDPR-compliance voor Topicus aan te tonen en te toetsen dient er te gedetailleerd ingegaan te worden op software. Enterprise Architecture is hier niet geschikt voor. Wel bestaat het vermoeden dat Enterprise Architecture in combinatie met UML het inzicht biedt dat Topicus zoekt. Daarom wordt aangeraden om dit verder te onderzoeken.

Inhoudsopgave

Versiehistorie 2
Management samenvatting 3
Inhoudsopgave 4
1 Inleiding 6
2 Begrippenlijst 7
3 Methodieken en onderzoeksopzet 8
3.1 Ontwerponderzoek 8
3.2 Deskresearch 9
3.3 Brainstormen 9
3.4 Perspectieven 9
3.5 Interview 9
3.6 Stakeholderanalyse 9
3.7 Aggregatiemodel en DESTEP 10
3.8 Oorzaak-gevolgdiagram 11
4 Probleemanalyse 12
4.1 Methodieken 12
4.2 Resultaten 14
4.3 Conclusie 16
4.4 Leeswijzer voor de deelvragen 17
5 Contextanalyse 18
5.1 Methodieken 18
5.2 Resultaten 19
5.3 Conclusie 26
6 Uitwerking General Data Protection Regulation (GDPR) 27
6.1 De GDPR in een notendop 28
6.2 De grondslag 29
6.3 Zorgvuldigheid 29
6.4 Verplichtingen 30
6.5 Rechten van de betrokkenen 31
6.6 Getroffen maatregelen 33
6.7 Scoping 33
7 Behoefteanalyse 34
7.1 Methodieken 34
7.2 Translatie van de requirements 36
7.3 Macht-belangdiagram 37
7.4 Resultaten van de stakeholderinterviews 38
7.5 Conclusie 40
8 Literatuuronderzoek 43
8.1 Methodieken 43
8.2 Resultaten 44
8.3 Conclusie 49
9 Architectuurplaat 50
9.1 Dataverzamelingsmethode 50
9.2 Keuze architectuurframework 50

9.3 Hoog-over architectuur 50
9.4 Detailarchitectuur per component 52
9.5 Volledige Architectuurplaat 58

10 Analyse 59
10.1 Wat kan er afgeleid worden? 59
10.2 Wat kan er niet afgeleid worden? 60
10.3 Oorzaken 60
10.4 Tekortkomingen 61

11 Conclusie 62
11.1 Antwoord op de deelvragen 62
11.2 Antwoord op de hoofdvraag 63
11.3 Discussie 63
11.4 Beperkingen en suggesties voor verder onderzoek 64

12 Reflectie 65

13 Bibliografie 67

14 Figurenlijst 70

15 Tabellenlijst 70

16 Bijlage 71
16.1 Bijlage A: Architectuurprincipes FORCE 71
16.2 Bijlage B: Interviewvragen Stefan Hessels 72
16.3 Bijlage C: Interviewvragen Wietze Spijkerman 72
16.4 Bijlage D: Vragen Maarten Schopman 73
16.5 Bijlage E: Uitwerking GDPR 74
16.6 Bijlage F: GDPR-standpunten Topicus 81
16.8 Bijlage G: FORCE Product Suite 2018 91

1 Inleiding

Topicus is een softwarebedrijf dat software maakt voor zorg-, onderwijs-, overheids- en financiële instellingen. De financiële tak van het bedrijf houdt zich onder andere bezig met het maken van hypotheekoplossingen en richt zich op het ondersteunen van de adviseur, de geldverstrekker en de consument. Met Topicus' hypotheekoplossingen worden er uitgebreide Front-, Mid- en Backofficesystemen aangeboden om financiële instellingen te ondersteunen bij het verwerken van hypotheekaanvragen.

Topicus wil aan kunnen tonen dat zij aan de General Data Protection Regulation (GDPR) regelgeving voldoet. Deze regelgeving heeft geleid tot meer focus en meer bewustwording bij ondernemingen dat er op een verantwoorde manier met persoonsgegevens omgegaan moet worden. Binnen het hypotheekproces is er sprake van veel en vooral ook zeer gevoelige persoonsinformatie wat maakt dat het bedrijf en haar klanten behoefte hebben aan inzicht in de huidige stand van zaken. Graag willen zij dan ook de mogelijkheden verkennen om tot een compleet dekkende oplossing te komen en daarbij onderzoeken of Enterprise Architecture hieraan bij kan dragen.

Met behulp van Enterprise Architecture kunnen de relaties tussen bedrijfsprocessen, data, applicaties en infrastructuur in kaart worden gebracht en inzichtelijk worden gemaakt. Door middel van Enterprise Architecture kan er traceerbaarheid worden gecreëerd wat mogelijk bij kan dragen in het aantonen van GDPR-compliance. Topicus wil daarom laten onderzoeken of Enterprise Architecture daadwerkelijk bij kan dragen in het aantonen van GDPR-compliance.

In dit onderzoek wordt de toepasbaarheid van Enterprise Architecture voor het aantonen van GDPR-compliance onderzocht. Er is een architectuurtekening opgesteld van een aantal componenten van de hypotheekoplossing FORCE. Dit is de applicatie die Topicus ontwikkelt voor het verwerken van hypotheekaanvragen. Aan de hand van dit model wordt er getracht tekortkomingen in GDPR-compliance te identificeren en daarmee te toetsen of Enterprise Architecture geschikt is om GDPR-compliance aan te tonen.

In deze scriptie is het onderzoek uit de vorige alinea beschreven. Allereerst wordt het vooronderzoek beschreven, bestaande uit de probleemanalyse, contextanalyse, behoefteanalyse en het literatuuronderzoek. Ook bevat het vooronderzoek twee hoofdstukken die ingaan op de inhoud van de GDPR en welke maatregelen Topicus reeds heeft getroffen om GDPR-compliant te zijn. Vervolgens komen de architectuurplaten aan bod met de bijbehorende analyse. Er wordt afgesloten met een conclusie die bestaat uit de geïdentificeerde tekortkomingen, maatregelen om deze tekortkomingen weg te nemen en een advies om Enterprise Architecture wel of niet toe te passen voor het aantonen van GDPR-compliance.

2 Begrippenlijst

FORCE: Front Office Reinvented Customer Empowerment, de applicatie die Topicus ontwikkeld voor het verwerken van hypotheekaanvragen.

FPS: Force Product Suite, de software suite waarin FORCE zich bevindt.

GDPR: General Data Protection Regulation, een Europese verordening die regels voor de verwerking van persoonsgegevens door particuliere bedrijven en overheidsinstanties in de hele Europese Unie standaardiseert.

AVG: Algemene verordening gegevensbescherming, de Nederlandse benaming voor de GDPR.

ArchiMate: modelleertaal voor het modelleren van Enterprise Architecture

NHG: Nationale Hypotheek Garantie

BKR: Bureau Krediet Registratie

VIS: Verificatie Informatie Systeem, het systeem waarmee BKR controleert of een identiteits- of reisdocument geldig is.

EVA: Externe Verwijzings Applicatie, het gezamenlijke fraudepreventiesysteem van de Nederlandse Vereniging van Banken (NVB) en de Vereniging van Financieringsondernemingen in Nederland (VFN). Het wordt door BKR gebruikt om te toetsen of een persoon betrokken is geweest bij fraude.

SFH: Het fraudepreventiesysteem van de Stichting Fraudebestrijding Hypotheken. In SFH staan personen en bedrijven geregistreerd die betrokken zijn geweest bij hypotheekfraude.

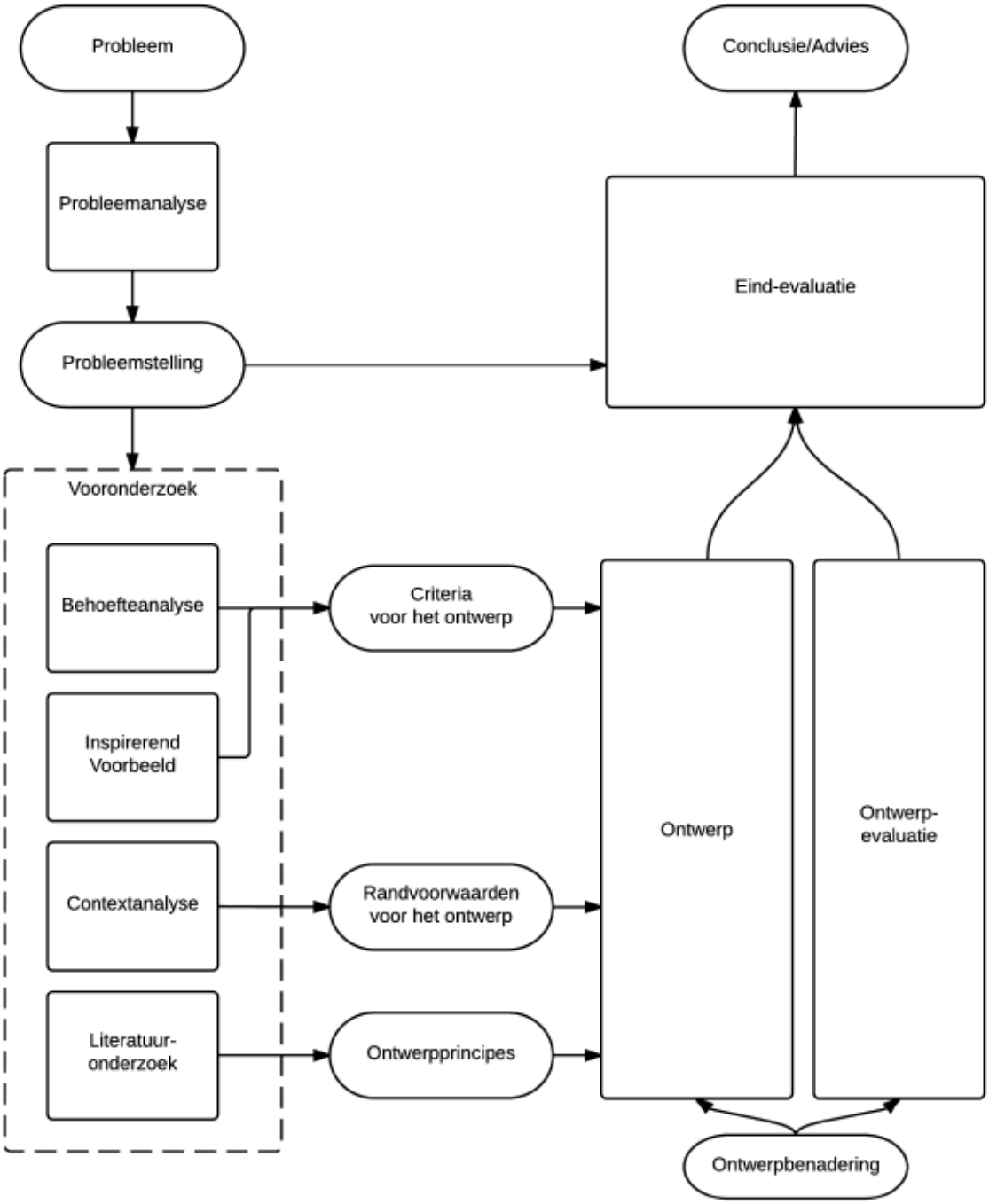
Confluence: De samenwerkingssoftware (ook wel groupware) waar Topicus interne gebruik van maakt. Dit is te vergelijken met een wiki.

3 Methodieken en onderzoeksopzet

In dit hoofdstuk worden de gebruikte methodieken beschreven.

3.1 Ontwerponderzoek

Ontwerponderzoek is een vorm van onderzoek waarbij wetenschappelijk verantwoord onderzoek resulteert in een interventie of een ontwerp voor een interventie waarmee een concreet probleem bij de opdrachtgever kan worden opgelost (Janssen, 2010). Figuur 1 is een schematische weergave van het gehele ontwerponderzoek.



Figuur 1: Schematische weergave ontwerponderzoek

3.2 Deskresearch

Voor het beantwoorden van onderzoeksvragen hoeft er niet altijd data verzameld te worden door middel van kwalitatief of kwantitatief onderzoek. Door gebruik te maken van bestaande informatie en gegevens, zogenaamde secundaire data, kunnen sommige vragen of problemen beantwoord worden (Krul, 2014). Dit wordt deskresearch genoemd.

3.3 Brainstormen

Brainstormen is een techniek om snel veel ideeën over een bepaald onderwerp of vraagstuk te genereren. Hierbij gelden er een aantal uitgangspunten, namelijk dat er geen kritiek op ideeën gegeven moet worden en dat er gericht moet worden op kwantiteit. Alle ideeën zijn welkom en het combineren van ideeën kan leiden tot weer nieuwe ideeën (De Vos, 2013). Aan het eind van de brainstormsessie waarin de ideeën worden gegenereerd, worden de ideeën geëvalueerd.

3.4 Perspectieven

De kijk op het probleem van de opdrachtgever is zeer waarschijnlijk niet de enige manier hoe er naar het probleem gekeken kan worden. Zo heeft iedere stakeholder eigen en misschien ook andere belangen waardoor zij vanuit een ander perspectief naar het probleem kijken. Een perspectief hoeft echter niet te overlappen met een actor, het gaat om de manier waarop het probleem wordt bekeken. Zo kan ook literatuur gezien worden als perspectief (Haveman, Hageraats, & van der Linden, 2016).

Om tot een goede probleemstelling en onderzoeksvragen te komen wordt er gebruik gemaakt van de perspectieven waardoor alle belangen van de stakeholders worden meegenomen in het onderzoek.

3.5 Interview

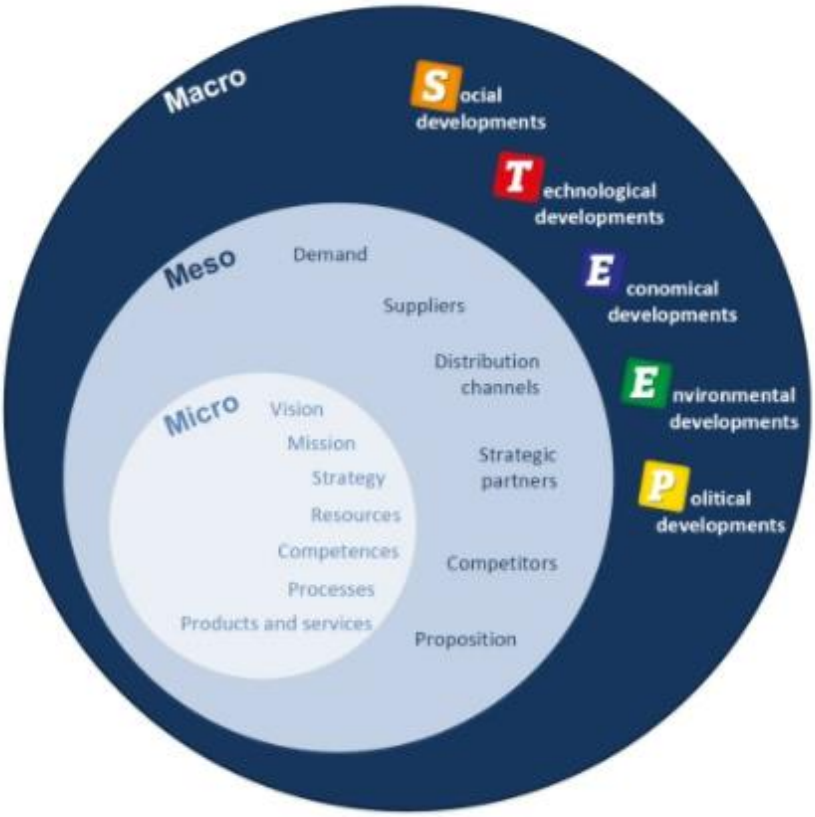
Er bestaan verschillende interviewvormen. De belangrijkste interviewvormen zijn het gestructureerde, het semigestructureerde en het ongestructureerde interview (Dingemanse, 2015). Bij het gestructureerde interview wordt er vastgehouden aan een vastgesteld vragenschema. Bij het semigestructureerde interview wordt er een algemeen vragenschema opgesteld, maar hier mag vanaf worden geweken. Zo kan er doorgevraagd worden wanneer de respondent interessante informatie geeft. Voor het ongestructureerde interview wordt er een lijst van onderwerpen opgesteld in plaats van vragen. Deze onderwerpen worden tijdens het interview besproken, maar hoe en in welke volgorde staat niet vast (Dingemanse, 2015).

3.6 Stakeholderanalyse

Een stakeholderanalyse is een tool voor het genereren van kennis over actoren binnen een project met als doel het in kaart brengen van hun intenties, onderlinge relaties, belangen en invloed zodat er afgewogen ontwerpkeuzes gemaakt kunnen worden (Varvasovszky & Brugha , 2000). Door een stakeholderanalyse uit te voeren worden de stakeholders en hun belangen in kaart gebracht en kunnen hierop requirements worden gebaseerd.

3.7 Aggregatiemodel en DESTEP

Een aggregatiemodel wordt gebruikt om de context van het project te bepalen. Hiervoor wordt er gebruik gemaakt van de Micro, Meso, en Macro-methode. Bij deze methode wordt er onderscheid gemaakt op drie verschillende niveaus (Foresight, 2018).



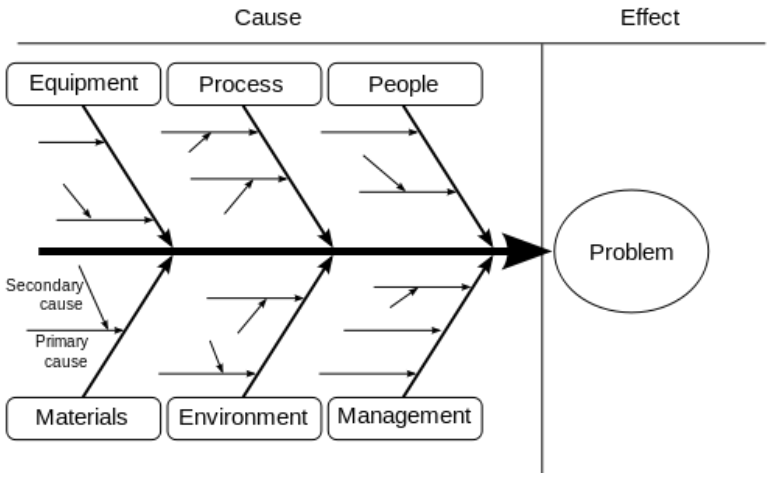
Figuur 2: Micro, Meso en Macro omgeving (Foresight, 2018)

Het laagste niveau is het Micro niveau. Op dit niveau wordt er binnen de organisatie naar context gekeken, zoals bijvoorbeeld de missie, visie, strategie, producten en diensten. Het middelste niveau is het Meso niveau. Op dit niveau wordt er naar de marktwerking gekeken, zoals bijvoorbeeld leveranciers, klanten, concurrenten en zakenpartners. Tot slot is er het Macro niveau. De DESTEP-methode wordt gebruikt om dit niveau te definiëren (Intemarketing , 2018). De methode bestaat uit:

- **Demografisch** – heeft betrekking op de bevolking
- **Economisch** – heeft betrekking op de economie
- **Sociaal-cultureel** – heeft betrekking op de cultuur en samenleving
- **Technologisch** – heeft betrekking op de technologische ontwikkelingen
- **Ecologisch** – heeft betrekking op de fysieke omgeving
- **Politiek-juridisch** – kenmerken van overheidsbeslissingen

3.8 Oorzaak-gevolgdiagram

Het oorzaak-gevolgdiagram, ook wel bekend als het Ishikawa-diagram of visgraatdiagram, is een tool om oorzaken van een probleem in kaart te brengen (Ishikawa, 1990). Door middel van de visgraadstructuur van het diagram ontstaat er een overzichtelijk beeld van de oorzaken van een probleem. De oorzaken kunnen worden ingedeeld in verschillende categorieën die worden gevisualiseerd als hoofdvertakkingen van de visgraad. De verdere vertakkingen geven de oorzaken aan. De onderstaande afbeelding is een voorbeeld van een oorzaak-gevolgdiagram.



Figuur 3: Voorbeeld van een Oorzaak-gevolgdiagram

4 Probleemanalyse

Om tot het gewenste onderzoeksresultaat te komen, is het van belang dat de oorzaak van het probleem duidelijk is. Om dit te bereiken is er een probleemanalyse uitgevoerd met als resultaat een hoofdvraag en daarbij behorende deelvragen. Deze hoofd- en deelvragen zullen de basis vormen voor de rest van het onderzoek.

4.1 Methodieken

Voor het uitvoeren van de probleemanalyse zijn er een aantal van de eerder genoemde onderzoeksmethodes toegepast, welke hieronder beschreven worden.

4.1.1 Deskresearch

Door Topicus is er een afstudeervoorstel uitgegeven met daarin de opdrachtomschrijving. Door dit document te bestuderen en analyseren is er een beeld ontstaan van de verwachtingen van het onderzoek.

4.1.2 Brainstormen

In samenwerking met de bedrijfsbegeleiders is er gebrainstormd om de perspectieven van de betrokken partijen in kaart te brengen. In de brainstormsessie zijn de volgende perspectieven naar voren gekomen:

Analisten (opdrachtgevers)
Binnen Topicus zijn de analisten verantwoordelijk voor het omzetten van de door de klant gewenste features naar werkzaamheden die verricht moeten worden om deze features te realiseren.

Programmateam
De klanten van Topicus verzamelen voor hun werkzaamheden persoonsgegevens van consumenten. Topicus vervult volgens de GDPR de rol van gegevensverwerker, omdat zij namens haar klanten persoonsgegevens verwerkt (Topicus, 2018). De klanten van Topicus blijven verantwoordelijk voor de verwerking van persoonsgegevens en vervullen daarmee de rol van verwerkingsverantwoordelijke. Vanwege deze verantwoordelijkheid hebben de klanten van Topicus de behoefte dat Topicus, als gegevensverwerker zijnde, aan kan tonen dat zij GDPR-compliant is.

Architecten
De architecten van Topicus zijn verantwoordelijk voor het opstellen en naleven van de architectuur. Zij zijn hierbij ook verantwoordelijk voor het inzichtelijk maken van de opbouw van FORCE.

Literatuur
De literatuur is geraadpleegd om te achterhalen of andere organisaties hetzelfde probleem ondervinden en of er onderzoeken zijn gedaan die de probleemstelling ondersteunen. Hiervoor is er gezocht naar de meest voorkomende en grootste obstakels die organisaties ervaren in het bereiken van GDPR-compliance.

4.1.3 Oorzaak-gevolgdiagram

Naar aanleiding van de brainstormsessie is er een initieel oorzaak-gevolgdiagram opgesteld. Het doel van dit diagram is het in kaart brengen van de oorzaken van het probleem bekeken vanuit de perspectieven. Het model heeft een oorzaak-gevolgstructuur. Het model is zo opgesteld dat de verschillende oorzaken zijn gegroepeerd onder de verschillende perspectieven.

4.1.4 Interviews

Naar aanleiding van de brainstormsessie en het oorzaak-gevolgdiagram zijn er een aantal interviews gehouden. Het doel van deze interviews was het verifiëren van de perspectieven en het oorzaak-gevolgdiagram. Naast dat er is gekeken of de perspectieven juist zijn, is er ook gekeken of deze volledig zijn. Er is door middel van een semigestructureerd interview doorgevraagd op antwoorden die de

geïnterviewden gaven om tot de kern van het probleem te komen en om na te gaan of er nog meer oorzaken spelen dan de oorzaken die in de brainstormsessies naar voren waren gekomen.

Allereerst is Stefan Hessels (Business Analist) geïnterviewd. Hij heeft de initiële probleemomschrijving en de afstudeeropdracht geschreven en kan daardoor worden gezien als de opdrachtgever. Tijdens dit interview is er dieper op het probleem ingegaan en zijn er namen naar voren gekomen van personen waarmee vervolginterviews konden worden gehouden.

Naar aanleiding van het interview met Stefan Hessels is Maarten Schopman geïnterviewd. Maarten Schopman is lid van het Programmateam en heeft zich in het verleden al bezig gehouden met de GDPR-compliance binnen Topicus. Het Programmateam bevindt zich boven de ontwikkelteams en geeft sturing aan deze teams. Hij is geïnterviewd om te achterhalen welke stappen er al gezet zijn om GDPR-compliant te zijn en welke stappen er nog gemaakt moeten worden.

Tot slot is Wietze Spijkerman geïnterviewd. Wietze Spijkerman is architect bij Topicus. Hij is geïnterviewd om te achterhalen hoe er vanuit een architectuur perspectief naar het probleem wordt gekeken.

4.2 Resultaten

Op basis van de informatie die naar voren is gekomen tijdens de interviews (die te vinden zijn in bijlage B tot en met D) zijn de perspectieven uitgewerkt. In de volgende paragraaf is de informatie uit de interviews samengevat en zijn de perspectieven uitgewerkt. In de paragrafen daarna is het oorzaak-gevolgdiagram opgesteld en zijn de businessrequirements gedefinieerd.

4.2.1 Perspectieven

Analisten (opdrachtgevers)
Het is voor de analisten van belang om inzicht te hebben in de processen en opbouw van FORCE. Zonder dit inzicht kunnen zij niet de gewenste features niet omzetten in werkzaamheden om deze features te realiseren. Hoewel het inzicht in de koppelingen tussen de verschillende componenten tot zekere mate aanwezig is, geldt dit niet voor de datastromen tussen de componenten. De analisten zouden daarom graag zien dat deze datastromen inzichtelijk worden.

Programmateam
Het programmateam heeft al veel maatregelen genomen om GDPR-compliant te zijn. Zo is er in overleg met de klanten een GDPR-beleid opgesteld en is er in kaart gebracht welk type persoonsgegevens in welk component van FORCE verwerkt worden. Ook zijn de API's van de componenten gedocumenteerd waardoor te achterhalen is welke gegevens er tussen de componenten uitgewisseld kunnen worden.

Daarnaast is er een Record Retention-functionaliteit toegevoegd om persoonsgegevens te kunnen verwijderen uit FORCE. Deze functionaliteit is echter gelimiteerd tot het verwijderen van persoonsgegevens uit de FORCE database. Overige persoonsgegevens op andere locaties, zoals logbestanden en andere databases, worden niet verwijderd.

Maarten Schopman heeft aangegeven dat het programmateam de wens heeft dat deze overige persoonsgegevens met de Record Retention-functionaliteit kunnen worden verwijderd. Op het moment is dit nog niet mogelijk, omdat het niet bekend is in welke logbestanden en databases deze gegevens staan.

Architecten
De functie en de verantwoordelijkheden van de architecten hebben zich, naarmate Topicus groeide, vormgegeven. Door deze natuurlijke groei is er nooit vastgegrepen aan een bepaald architectuurframework, maar zijn er in de afgelopen jaren naar behoefte onderdelen van verschillende architectuurframeworks gebruikt. Zo is er bijvoorbeeld een Architectuurbeleid opgesteld en zijn er Architectuurprincipes gedefinieerd. Ook zijn er richtlijnen opgesteld om de opbouw van de verschillende componenten van FORCE consistent te houden. Daarnaast zijn de onderlinge relaties van de componenten inzichtelijk voor de architecten. Het is hier echter zo dat deze relaties alleen inzichtelijk zijn voor de architecten en niet voor de overige medewerkers. Dit komt doordat het inzicht in de mensen (lees: architecten) zit, maar niet gedocumenteerd is.

Ten behoeve van de GDPR is er behoefte aan consistentie (Spijkerman, 2018). Door de opbouw van de onderlinge relaties consistent te houden, kan er inzichtelijkheid worden gecreëerd wat vervolgens bij kan dragen aan traceability. Traceability is een belangrijk middel om GDPR-compliance aan te kunnen tonen.

Concluderend is er vanuit de architecten behoefte aan (gedocumenteerd) inzicht van de onderlinge relaties tussen de componenten van FORCE. Dit ten behoeve van inzicht voor de overige medewerkers alsmede voor het bereiken van traceability.

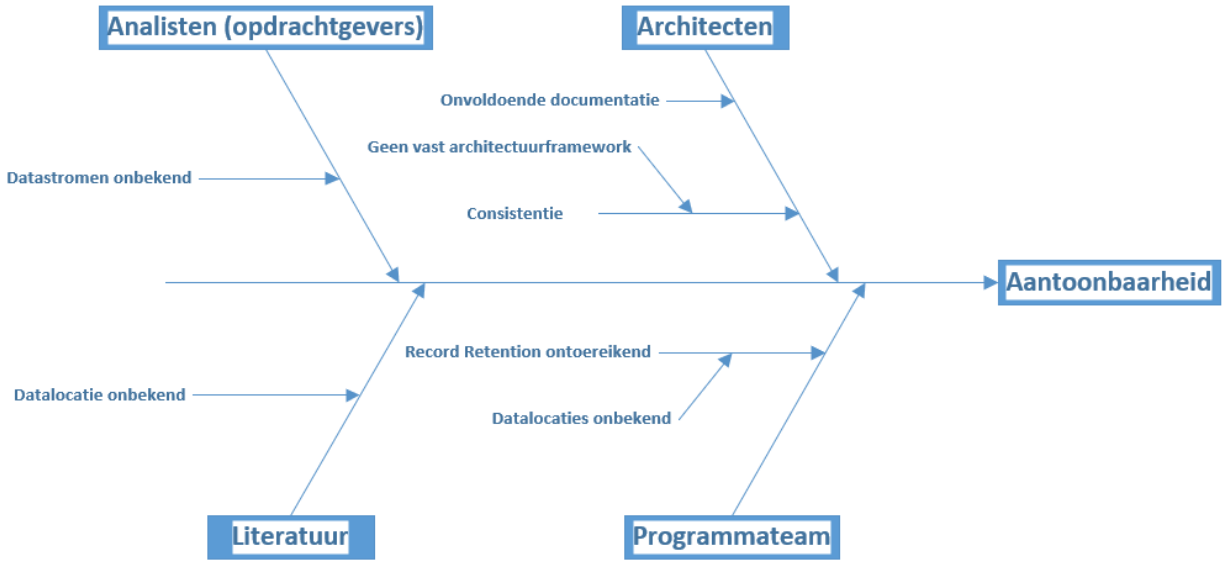
Literatuur
Het probleem dat Topicus ondervindt is een probleem dat bij meer bedrijven voorkomt. In Ipswitch's Europese online enquête uit 2014 die is gehouden onder 316 ICT-professionals, gaf 52% van de

respondenten aan dat zij niet klaar zijn voor de GDPR. Daarnaast gaf 35% aan dat zij niet weten of maatregelen die zij hebben genomen voldoende zijn en denkt maar 12% dat zij klaar zijn voor de GPDR (Ipswitch, 2014). Het aan kunnen tonen van GDPR-compliance is voor veel ICT-professionals en hun organisaties dus niet vanzelfsprekend.

Volgens (Boot, 2018) is de hoeveelheid data die in FORCE wordt verwerkt en opgeslagen van zodanige omvang dat er gesproken kan worden van Big Data. Kadenic's (2015) onderzoek bevestigt de theorie van (Ohlhorst, 2012) dat het lokaliseren van data het eerste probleem is omtrent security en governance in een Big Data omgeving. Doordat het niet duidelijk is waar data staat, wordt er niet voldaan aan de GDPR. Door middel van Enterprise Architecture kan inzichtelijk worden gemaakt waar data zich bevindt (Kadenic, 2015).

4.2.2 Oorzaak-gevolgdiagram

Uit de resultaten van de interviews is het oorzaak-gevolgdiagram tot stand gekomen. In het onderstaande diagram zijn de oorzaken van het probleem gegroepeerd onder de perspectieven. Hierdoor ontstaat er een duidelijk overzicht van de oorzaken van het probleem.



Figuur 4: Oorzaak-gevolgdiagram

De hoofdvertakkingen geven de vier perspectieven weer: De opdrachtgever, het programmateam, de architecten en de literatuur. De verdere vertakkingen per perspectief geven de oorzaken van het probleem.

4.3 Conclusie

Vanuit de verschillende perspectieven is er gekeken naar de oorzaak van het probleem. De kern ervan is dat Topicus er behoefte aan heeft om aan te kunnen tonen dat zij GDPR-compliant zijn. Er zijn meerdere oorzaken aan te wijzen die er voor zorgen dat zij dit nog niet kunnen. Vanuit het programmateam en de literatuur komt naar voren dat de onbekendheid van datalocaties een belangrijke oorzaak is voor het gebrek aan aantoonbaarheid van GDPR-compliance. Daarnaast geven de architecten aan dat er nooit vastgegrepen is aan een vast architectuurframework wat tot gevolg heeft dat er onvoldoende consistentie is in de onderlinge relaties van de componenten van FORCE. Samen met onvoldoende documentatie over deze relaties heeft dit tot gevolg dat er een gebrek is aan aantoonbaarheid van GDPR-compliance.

De probleemstelling kan worden opgedeeld in twee delen. Allereerst is er een gebrek in aantoonbaarheid van GDPR-compliance. Dit wordt veroorzaakt door het tweede deel van de probleemstelling, namelijk dat er geen inzicht is in de locatie van data.

Zoals aangegeven in de inleiding is de onderzoeksvraag of Enterprise Architecture bij kan dragen aan de aantoonbaarheid van GDPR-compliance. De gedachte hierachter is dat Enterprise Architecture inzicht creëert en daarmee aantoonbaarheid. Om te achterhalen of dit daadwerkelijk het geval is, zal er in dit onderzoek worden gefocust op een specifiek aantal componenten van FORCE. Dit leidt tot de volgende hoofdvraag:

"Welke tekortkomingen aan GDPR-compliance van de componenten FORCE.Mortages, Proposals, Morality, Agreements en NHGGateway binnen de hypotheekoplossing FORCE kunnen worden geïdentificeerd door middel van Enterprise Architecture en welke maatregelen kunnen hierop gebaseerd worden?"

4.3.1 Deelvragen

Naar aanleiding van de hoofdvraag zijn de volgende deelvragen naar voren gekomen:

1. Wat is de GDPR?
2. Welke eisen stelt de GDPR aan Topicus op data, applicatie- en infrastructuurniveau?
3. Wat is Enterprise Architecture en hoe dient dit toegepast te worden binnen Topicus?
4. Hoe zijn de componenten FORCE.Mortages, Proposals, Morality, Agreements en NHGGateway opgebouwd zoals gemodelleerd door middel van Enterprise Architecture?
5. Hoe zijn de businessprocessen die worden ondersteund door de componenten FORCE.Mortages, Proposals, Morality, Agreements en NHGGateway ingericht?
6. Waar worden deze componenten geraakt door de GDPR op data-, applicatie- en infrastructuurniveau?
7. Welke maatregelen heeft Topicus reeds genomen om aan de GDPR-eisen te voldoen?
8. Welke maatregelen op data-, applicatie- en infrastructuurniveau dienen er nog te worden genomen om aan de GDPR-eisen te voldoen?

4.3.2 Requirements

Uit de interviews met de vertegenwoordigers van de perspectieven kunnen eisen en wensen worden afgeleid. Deze eisen en wensen dienen duidelijk gedefinieerd te worden. Om dit te bereiken zijn de eisen en wensen vertaald naar initiële requirements. Omdat het onderzoek zich nog in de beginfase bevindt wordt er hier alleen ingegaan op de business requirements. In de behoefteanalyse zullen deze requirements verder worden gespecifieerd en uitgebreid. De initiële business requirements zijn:

- GDPR-compliance moet aangetoond kunnen worden.
- Datalocaties[1] moeten bekend worden.
- Er moet inzicht gecreëerd worden op het gebied van FORCE-componenten en hun onderlinge relaties.

[1] Het betreft hier datalocaties zoals databases, logbestanden, datastores, etc.

4.4 Leeswijzer voor de deelvragen

Uit de probleemanalyse zijn vrij veel deelvragen naar voren gekomen. Om de leesbaarheid en het overzicht te behouden, is in Tabel 2: Leeswijzer deelvragen weergegeven welke deelvraag in welk hoofdstuk wordt beantwoord. De hoofdvraag wordt in de conclusie beantwoord.

Nr	Deelvraag	Hoofdstuk
1	Wat is de GDPR?	6
2	Welke eisen stelt de GDPR aan Topicus op data, applicatie- en infrastructuurniveau?	6
3	Wat is Enterprise Architecture en hoe dient dit toegepast te worden binnen Topicus?	8
4	Hoe zijn de componenten FORCE.Mortages, Proposals, Morality, Agreements en NHGGateway opgebouwd zoals gemodelleerd door middel van Enterprise Architecture?	9
5	Hoe zijn de businessprocessen die worden ondersteund door de componenten FORCE.Mortages, Proposals, Morality, Agreements en NHGGateway ingericht?	9
6	Waar worden deze componenten geraakt door de GDPR op data-, applicatie- en infrastructuurniveau?	6 & 10
7	Welke maatregelen heeft Topicus reeds genomen om aan de GDPR-eisen te voldoen?	6
8	Welke maatregelen op data-, applicatie- en infrastructuurniveau dienen er nog te worden genomen om aan de GDPR-eisen te voldoen?	11

Tabel 2: Leeswijzer deelvragen

5 Contextanalyse

Het antwoord op de hoofdvraag en het advies dat aan het eind van het project wordt gegeven, moet geplaats kunnen worden binnen de context waarin het project zich bevindt. Uit deze context komen namelijk beperkingen en randvoorwaarden voort waar in het advies rekening mee gehouden moet worden. In dit hoofdstuk wordt deze context beschreven en worden de randvoorwaarden afgeleid waaraan het advies moet voldoen.

5.1 Methodieken

Er is gebruik gemaakt van meerdere methodieken om de context in kaart te brengen. De gekozen methodieken en de toepassing ervan worden in deze paragraaf besproken.

5.1.1 Brainstormen

Om de invulling van het Micro, Meso en Maso-aggregatiemodel te bepalen is er gebrainstormd samen met Wouter van der Waal (Analist, bedrijfsbegeleider). Wouter heeft als analist en bedrijfsbegeleider een goede kijk op de context waarin het project zich bevindt. Na de brainstormsessie zijn de resultaten geverifieerd bij de vertegenwoordigers van de aspecten uit de probleemanalyse.

5.1.2 Aggregatiemodel

Tijdens de brainstormsessie is de divisie Finance van Topicus naar voren gekomen als context op Microniveau. Onder deze context vallen de missie, visie en strategie van Finance evenals het product dat zij ontwikkelen, namelijk FORCE. De afnemers van FORCE komen naar voren als context op Mesoniveau. Het Macroniveau wordt ingevuld door de DESTEP-factor politiek-juridisch. Deze factor bevat de wet- en regelgeving die voor dit project relevant is, namelijk de GDPR. De GDPR is opgesteld en opgebouwd vanuit een zestal beginselen die de basis vormen voor de verordening. Deze zestal beginselen geven daardoor goed weer wat de achterliggende gedachte van de verordening is en welk doel het dient.

5.1.3 Deskresearch

Nadat de context van het aggregatiemodel bekend was, is er deskresearch gedaan naar deze context. Hierbij is er gekeken naar de documentatie over de GDPR die de Autoriteit Persoonsgegevens beschikbaar heeft gesteld en naar informatie over Topicus en FORCE. Het aggregatiemodel is vervolgens in paragraaf 5.2 uitgewerkt, zodat er randvoorwaarden uit afgeleid konden worden.

5.2 Resultaten

In deze paragraaf wordt het aggregatiemodel uitgewerkt. Deze uitwerking vormt de basis voor de randvoorwaarden die in de conclusie naar voren komen.

5.2.1 Micro

In deze paragraaf wordt de context beschreven op Micro niveau. De context op dit niveau bestaat uit de missie, visie en strategie van Topicus Finance en het product dat Finance levert.

5.2.1.1 Topicus Finance

Finance is de divisie binnen Topicus waar de afdeling Hypotheken onder valt. Naast Hypotheken zijn er ook de afdelingen Pensioen, Beleggen en sparen, Zakelijk financieren en tenslotte Claimafhandeling. Elke divisie heeft haar eigen missie, visie en strategie die losstaan van Topicus' algemene missie, visie en strategie.

Missie

"Een hypotheek afsluiten, een zakelijke financiering aanvragen, sparen, beleggen, pensioen opbouwen. Topicus wil een wereld creëren waarin de consument centraal staat door inzicht en overzicht te bieden en financiële situaties begrijpelijk te maken." (Topicus, sd)

Visie

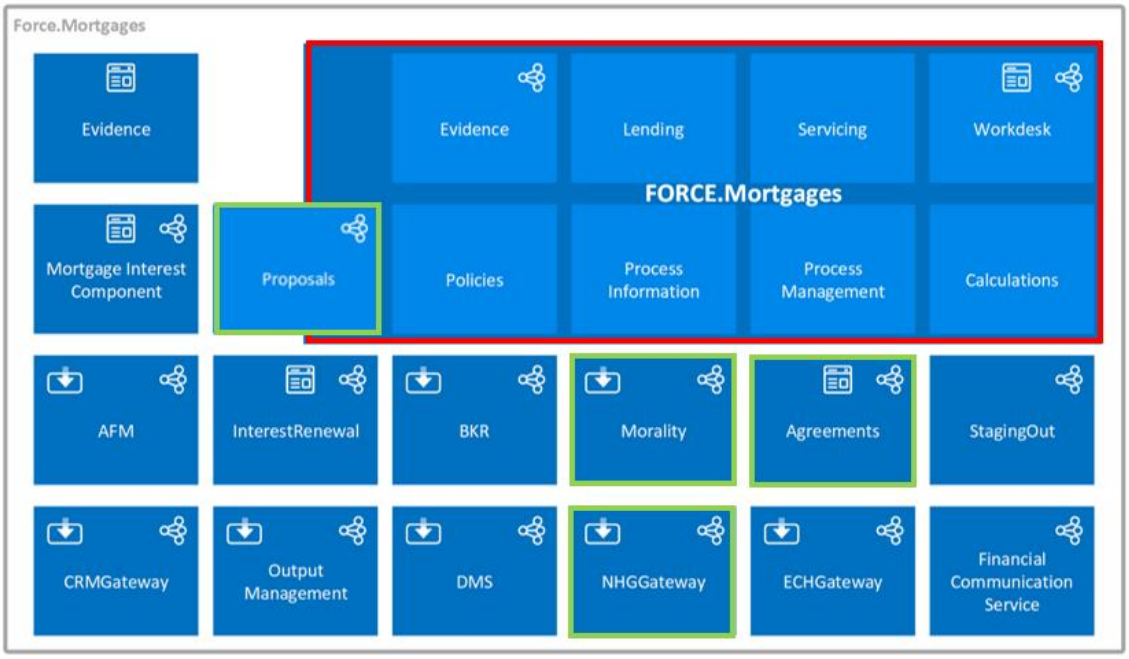
"Met behulp van slimme technologie verbinden wij mensen, systemen en data met elkaar waardoor jij verantwoorde en voordelige geldkeuzes kan maken, nu en later. We bouwen aan een 'connected banking' platform waarmee je grip en inzicht krijgt op de (toekomstige) financiële gevolgen van je beslissingen." (Topicus, sd)

Strategie

"Wij werken aan een financiële sector waarin financiën overzichtelijk en begrijpelijk worden. Een sector die consumenten in staat stelt om zelf verantwoorde en voordelige financiële keuzes te maken. Samen met banken, financieel dienstverleners en adviseurs ontwikkelen we slimme systemen die financiële gegevens efficiënt verwerken en inzichtelijk maken. Door die systemen te verbinden creëren we een eenduidig platform, waarmee je als consument al je financiële gegevens op één plek verzamelt en beheert. Daardoor kun je meer uit je geld halen, meer besteedbaar inkomen, nu en later. Zo vormen we samen een wereld die staat voor verbinding, transparantie en gemak. Een wereld waarin je grip hebt op je eigen financiële toekomst en kunt vertrouwen op de beste steun van professionals." (Topicus, sd)

5.2.1.2 FORCE

FORCE is de hypotheekoplossing van Topicus voor het verwerken van hypotheekaanvragen. Van FORCE worden alleen de componenten van behandeld die binnen de scope van het project vallen. De overige componenten van FORCE worden niet beschreven omdat een dergelijke beschrijving geen toegevoegde waarde zou hebben gezien de huidige context, scope en onderzoeksvraag. In Figuur 5: FORCE is het relevante onderdeel van de FPS afgebeeld. De FPS is de software suite waarin FORCE zich bevindt. De volledige FPS is te vinden in Bijlage G: FORCE Product Suite 2018. Het centrale component van FORCE is rood omlijnd en de voor dit onderzoek relevante losse componenten zijn groen omlijnd.



Figuur 5: FORCE

De toekomstvisie van FORCE is dat het product wordt opgebouwd volgens een service georiënteerde architectuur. Hierbij wordt FORCE opgedeeld in losse componenten waarbij elk component een eigen service levert, zoals bijvoorbeeld een koppeling met een CRM-systeem of het testen van iemands moraliteit. Naast dat nieuwe services en functionaliteiten volgens dit principe worden ontwikkeld, worden ook huidige services uit FORCE 'losgetrokken' en als losstaand component neergezet. Hierdoor kunnen FORCE en haar componenten dynamischer worden ingezet bij de klanten van Topicus.

Naast deze globale architectuur wordt er ook een architectuur gehanteerd voor de interne opbouw van de componenten. De interne opbouw is ingericht volgens de Microsoft Application Architecture Guide, 2nd Edition. De bijbehorende ontwerpprincipes zijn te vinden in Bijlage A: Architectuurprincipes FORCE.

Force.Mortgages
Force.Mortgages vormt de basis van FORCE. Rondom deze 'monoliet' zijn de overige componenten van FORCE opgebouwd. De monoliet is op te delen in drie bouwstenen, namelijk de workflow engine, de business rule engine en het product- en prijssysteem.

Een workflow engine zorgt er voor dat gebruikers een serie aan terugkomende taken moeten doorlopen die samen een businessproces of 'workflow' vormen. In FORCE is wordt de workflow engine toegepast om alle stappen in het hypotheekproces, van de eerste aanvraag voor een hypotheek tot en met het verstrekken er van, te doorlopen.

Dicht bij de workflow engine staat de business rule engine. De business rule engine levert condities waarmee de workflow engine rekening moet houden. Een simpel voorbeeld van een business rule zou kunnen zijn dat een consument met een inkomen X maximaal bedrag Y mag lenen. Het voordeel van een business rule engine is dat de condities aangepast kunnen worden via een user interface; er hoeft dus niet in de code gedoken te worden om de condities aan te passen.

Tot slot is er nog het product- en prijssysteem. In dit systeem worden de hypotheekproducten opgenomen en worden prijzen vastgesteld.

Proposals
Een kernaspect van de hypothecaire dienstverlening is de concrete wederzijdse afspraak die tussen de hypotheekverstrekker en de consument rond een woningfinanciering gemaakt wordt. De consument heeft een financieringswens, waarop de verstrekker middels een aanbod aangeeft bereid zijn geld te lenen tegen een rentetarief en eventuele extra kosten en voorwaarden. Binnen een bepaalde termijn is de verstrekker wettelijk verplicht zich aan dit aanbod te houden als de consument aangeeft in te willen gaan op het aanbod en zorgt de verstrekker ook voor naleving van de afspraken die hieruit voortkomen. Daarnaast heeft de consument de mogelijkheid om, ondanks eerdere toezegging, binnen een bepaalde termijn van het overeengekomen aanbod af te zien. Vanaf de eerste aanvraag voor een hypotheek tot aan het einde van een looptijd is het een terugkerend patroon binnen business processen om afspraken rond de financiering te maken en te herzien (Topicus, 2018).

Kern binnen dit patroon is het vertalen van het beleid van een verstrekker, samen met eventuele bestaande afspraken, naar een nieuw aanbod conform deze voorwaarden die toe te passen in het specifieke geval van die consument. Denk hierbij bijvoorbeeld aan:

- Een eerste hypotheek aanvraag, het bieden van een voorlopig- en bindend aanbod en deze uiteindelijk effectueren naar uit te keren en te innen gelden
- Idem voor het verhogen van de hypotheek (extra lenen)
- Een renteafspraak (bijvoorbeeld "10 jaar vast") die verloopt
- Vanuit de consument geïnitieerde wijzigingen die gevolgen kunnen hebben voor bestaande afspraken
    - Extra aflossing, die tot directe kosten (boete) en renteaanpassing kan leiden
    - Tussentijdse renteaanpassing, buiten het reguliere verloop
    - Woningwaarde wijziging die een renteaanpassing tot gevolg kan hebben

Deze informatie wordt verwerkt in het component Proposals en vanuit dit component worden de aanbiedingen naar de consument gedaan.

Agreements

Het component Agreements is verantwoordelijk voor het vastleggen van contractinformatie. Concreter zijn dit de contractafspraken die de consument met de geldverstrekker maakt bij aanvang van een hypothecaire lening. Ook wordt gedurende de looptijd van de hypothecaire lening bijgehouden wat de actuele renteafspraak is en wat de actuele stand is van de hoofdsommen van leningdelen. Dit is in het geval er een mutatie wordt doorgevoerd die aan contractadministratie wordt doorgegeven. Dit kan zijn een proces als een tussentijdse renteaanpassing of een extra aflossing (Topicus, 2017).

Agreements bestaat uit drie subcomponenten, namelijk het Services component, de WebApi en de Website. Het Services component biedt de mogelijkheid voor het opslaan en ophalen van contracten. De WebApi verzorgt de verbinding tussen de website en het Services component. De website verzorgt de User Interface.

Morality

De Wet ter voorkoming van witwassen en financieren van terrorisme (WWFT) en Sanctiewet (SW) verplicht financiële organisaties om gedegen onderzoek te doen naar klanten. Dit onderzoek moet financiële organisaties attent maken op bijvoorbeeld de prominentheid van een persoon of voorkomen dat er banden worden aangegaan met personen die misbruik willen maken van financiële diensten zoals witwassen, terrorismefinanciering en fraude. Het afhandelen van deze businessvraag vormt de scope van het Morality component (Topicus, 2018).

Morality gebruikt de InData koppeling van BKR voor het uitvoeren van toetsen. Om de InData koppeling aan te kunnen roepen moet de geldverstrekker over een door BKR verstrekt certificaat en deelnemernummer beschikken. Per geldverstrekker wordt er daarnaast nog een profiel meegegeven waarmee de InData koppeling vaststelt welke toetsen uitgevoerd moeten worden. In Force.Morality wordt per label het door te geven certificaat, deelnemernummer en profiel geconfigureerd. Nadat de toetsen door InData zijn uitgevoerd wordt er door InData een totaaloordeel verstrekt. Dit totaaloordeel wordt niet door het Force.Morality overgenomen maar door Force.Morality zelf bepaald (Topicus, 2017).

Morality kan op dit moment voor 1 of meerdere personen de volgende moraliteitstoetsingen uitvoeren:

- BKR InData: PEP (Politically Exposed Persons) Toets: Met de PEP Toets kan gecontroleerd worden of een aanvrager een ‘politiek prominente persoon’ is.
- BKR InData: LRS (Landelijk Register Schuldsaneringen) Toets: Met deze toets kan gecontroleerd worden of een aanvrager in de schuldsanering zit, heeft gezeten en hoe (al dan niet schone lei) en wanneer deze is beëindigd
- BKR InData: CIR (Centraal Insolventie Register) Toets: Hiermee kan gecontroleerd worden of een aanvrager failliet is verklaard (of binnenkort zal zijn), verklaard is geweest en/of hoe een faillissement is beëindigd.
- BKR InData: Status Toets: Met deze toets kan een intermediair globaal controleren of en hoe een aanvrager bij BKR geregistreerd staat.
- BKR InData: Sanctie Toets: Hiermee kan gecontroleerd worden of een consument vermeld staat als een ‘gesanctioneerd persoon’ op de EU Sanctielijst of de OFAC (SDN) Sanctielijst.

Naast de InData toetsen zijn er nog een drietal toetsen, namelijk de VIS/EVA/SFH toetsen. Deze toetsen zijn op dit moment nog losse services bij BKR. Op termijn zullen deze verplaatst worden naar InData. Deze toetsen zijn:

- BKR SFH toets: Hiermee kan gecontroleerd worden of de aanvrager mogelijk betrokken is geweest bij hypotheekfraude.
- BKR EVA toets: Hiermee kan gecontroleerd worden of de aanvrager mogelijk betrokken is geweest bij fraude.
- BKR VIS toets: Hiermee kan gecontroleerd worden of het identiteitsbewijs van de aanvrager is geregistreerd als vermist, gestolen of om een andere reden ongeldig is verklaard.

NHG Gateway

NHG staat voor Nationale Hypotheek Garantie en wordt verstrekt door de Stichting Waarborgfonds Eigen Woningen (WEW). Deze stichting werd in 1993 opgericht op initiatief van het Ministerie van VROM en de Vereniging Nederlandse Gemeenten (VNG), met als hoofddoel het particuliere woningbezit op een verantwoorde wijze te bevorderen (Topicus, 2018).

Voor de meeste mensen is de aankoop van een huis een grote investering. Aangezien vrijwel niemand een paar ton achter de hand heeft, betekent een koophuis bijna automatisch een hypotheek. Ofwel: een financiële verplichting waar een hypotheekgever (consument) tientallen jaren aan vastzit. Ontslag, arbeidsongeschiktheid, relatiebeëindiging of overlijden van een van de hypotheekgevers zijn zaken die iedereen kunnen overkomen. In veel gevallen gaan deze gepaard met een grote inkomensdaling, dat weer kan leiden tot betalingsachterstanden op de hypotheek en in het ergste geval tot gedwongen verkoop van een woning. Wanneer deze verkoop niet voldoende oplevert om de hypotheek af te lossen, is een restschuld het gevolg. Hier biedt NHG uitkomst. De Stichting Waarborgfonds Eigen Woningen zorgt er namelijk voor dat deze restschuld wordt afgelost, op voorwaarde dat de hypotheekgever heeft meegewerkt om die schuld zo laag mogelijk te houden door direct contact op te nemen met zijn geldgever, zodra er zich betalingsachterstanden voordoen. Het resterende bedrag wordt de geldgever dan kwijtgescholden (Topicus, 2018).

Vanuit FORCE worden er twee aanvragen aan NHG gesteld, namelijk de NHG Volledigheidstoets en de NHG Garantiemelding. Bij de NHG Volledigheidstoets wordt gecontroleerd of een (hypotheek)aanvraag onder NHG geregistreerd kan worden. Bij de NGH Garantiemelding wordt een hypotheek aangemeld voor de Nationale Hypotheek Garantie. De NHG Gateway zorgt voor de koppeling met de systemen van NGH zodat deze aanvragen gesteld kunnen worden.

5.2.2 Meso

In deze paragraaf wordt de context beschreven op Meso niveau.

5.2.2.1 Afnemers van FORCE

Banken en andere hypotheekverstrekkers kunnen hun hypotheekproces grotendeels automatisch laten verlopen door FORCE af te nemen. Voor het verwerken van een hypotheekaanvraag moeten de afnemers persoonsgegevens verzamelen en deze laten verwerken door FORCE. Volgens de GDPR blijven de afnemers daarom verwerkingsverantwoordelijke en zij zijn daarom eindverantwoordelijk voor het verwerken van deze gegevens.

5.2.3 Macro

In deze paragraaf wordt met behulp van DESTEP-methode de omgeving op Macro niveau in kaart gebracht. Van deze methode is de politiek-juridische factor relevant voor dit project. Deze factor wordt ingevuld door de GDPR.

5.2.3.1 Politiek-juridisch

De bescherming van persoonsgegevens is een grondrecht dat in het Handvest van de grondrechten van de Europese Unie is vastgelegd. De Algemene verordening gegevensbescherming ('GDPR', 'Verordening' of 'AVG') is een Europese wet die de bescherming van dit grondrecht regelt. De verordening vervangt vanaf 25 mei 2018 de Nederlandse Wet Bescherming Persoonsgegevens (Schermer, Hagenauw, & Falot, 2018).

De Verordening gaat uit van een zestal beginselen waar elke verwerking van persoonsgegevens aan moet voldoen (Schermer, Hagenauw, & Falot, 2018). De verordening is opgesteld vanuit deze beginselen waardoor deze beginselen eigenlijk de context van de vordering zijn en daarmee ook context voor dit project. In het kort zijn deze beginselen:

a) De verwerking van persoonsgegevens moet rechtmatig, behoorlijk en transparant zijn ("rechtmatigheid, behoorlijkheid en transparantie")

Het uitgangspunt is dat persoonsgegevens alleen mogen worden verwerkt voor gerechtvaardigde doeleinden. Dit betekent dat de verwerking noodzakelijk moet zijn om een specifiek doel te bereiken en dat degene waarvan de gegevens verwerkt worden hier toestemming voor heeft gegeven. Wanneer het gerechtvaardigd is om persoonsgegevens te werken, dan moet de verwerking ervan helder en verantwoord gebeuren.

b) De verwerking moet gebonden zijn aan specifieke verzameldoelen ("doelbinding")

Persoonsgegevens mogen alleen worden verzameld en verwerkt voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden (Schermer, Hagenauw, & Falot, 2018). Een nieuw doel waar de gegevens later voor worden gebruikt, moet verenigbaar zijn met het oorspronkelijke verzameldoel.

c) De gegevens moeten toereikend, ter zake dienend en beperkt tot het noodzakelijke zijn ("minimale gegevensverwerking")

Persoonsgegevens die verwerkt worden, moeten toereikend zijn voor het beoogde doel. Daarbij mogen er niet meer persoonsgegevens worden verwerkt dan noodzakelijk voor dit doel. Dit houdt in dat er, naast niet teveel, ook niet te weinig gegevens verwerkt moeten worden voor het doel. Wanneer er namelijk te weinig gegevens verwerkt worden, kan er ten onrechte een onvolledig beeld ontstaan van degene wiens gegevens verwerkt worden (ook wel: de betrokkene).

d) De gegevens moeten juist zijn ("juistheid")

De verwerkingsverantwoordelijke moet alle redelijke maatregelen nemen om ervoor te zorgen dat de gegevens correct en actueel zijn. Gegevens die dat niet (meer) zijn, dienen te worden gewist of gecorrigeerd.

e) De gegevens mogen niet langer worden bewaard dan nodig ("opslagbeperking")

Persoonsgegevens mogen niet langer bewaard worden dan noodzakelijk voor het doel van de verwerking. De gegevens dienen vernietigd of gewist te worden zodra zij niet langer noodzakelijk zijn.

f) De gegevens moeten goed beveiligd zijn en vertrouwelijk blijven ("integriteit en vertrouwelijkheid")

Persoonsgegevens moeten worden beschermd tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.

5.2.4 Aggregatieniveau

Nu de context op Micro, Meso en Macro bekend is, kan het aggregatieniveau van dit onderzoek bepaald worden. De meeste context voor het onderzoek bevind zicht op Micro niveau. Het onderzoek vindt dan ook op dit aggregatieniveau plaats. Zowel de functionaliteiten van FORCE en haar componenten als de toekomstvisie die Topicus van FORCE heeft zijn zeer belangrijk context van het onderzoek.

De Boer (2005) geeft aan dat het aanbevolen wordt om minimaal één aggregatieniveau boven het werkingsniveau van de interventie te kijken. Dit zou betekenen dat het Meso niveau mee wordt genomen. Echter is de context uit het Macro niveau veel belangrijker voor de context van dit onderzoek. De GDPR is een prominent onderdeel van dit onderzoek en dient daarom zeker meegenomen te worden in de relevante aggregatieniveaus van dit onderzoek.

5.3 Conclusie

Uit de aspecten en aggregatieniveaus komt context naar voren voor het project. Zo wil Topicus Finance een wereld creëren waarin de consument centraal staat door inzicht en overzicht te bieden en financiële situaties begrijpelijk te maken (Topicus, sd). Door middel van slimme technologie verbinden zij mensen, systemen en data met elkaar zodat er inzicht en grip wordt gecreëerd in de financiële gevolgen van keuzes die worden gemaakt.

Daarbij voorziet Topicus Finance een toekomst waarin de componenten van FORCE steeds verder van elkaar losgetrokken worden. De componenten worden gescheiden op hun functies en verantwoordelijkheden. Door met deze losstaande componenten te werken kunnen de componenten individueel bij klanten worden neergezet waardoor zij FORCE optimaal kunnen benutten.

Samenvattend wil Topicus naar een situatie waarin FORCE modulairer wordt, maar waarbij er wel binnen de architectuurprincipes van FORCE gebleven moeten. Dit resulteert in de volgende randvoorwaarden waar het antwoord op de hoofdvraag en het advies van dit project aan moeten voldoen:

- De modulariteit van FORCE mag niet afnemen.
- Er mag niet buiten de architectuurprincipes van FORCE worden getreden.

5.3.1 Toelichting randvoorwaarden

De modulariteit van FORCE mag niet afnemen.
Om FORCE optimaal in te kunnen zetten bij klanten is het van belang dat FORCE als losse componenten opgebouwd blijft. De maatregelen die aan het eind van het project worden geadviseerd mogen daarom niet de bijwerking hebben dat de modulariteit van FORCE afneemt.

Er mag niet buiten de architectuurprincipes van FORCE worden getreden.
Om de modulariteit van FORCE te waarborgen zijn architectuurprincipes opgesteld waaraan nieuwe en bestaande ontwerpen van FORCE moeten voldoen. De maatregelen in het advies moeten binnen deze architectuurprincipes passen. Een lijst van deze architectuurprincipes is in te vinden in Bijlage A: Architectuurprincipes FORCE.

6 Uitwerking General Data Protection Regulation (GDPR)

In dit hoofdstuk wordt de GDPR kort uitgewerkt, zodat er antwoord kan worden gegeven op drie deelvragen, namelijk wat de GDPR is, welke eisen de GDPR stelt aan Topicus en waar deze componenten geraakt worden door de GDPR op data-, applicatie- en infrastructuurniveau. Daarnaast wordt er antwoord gegeven op deelvraag 7: Welke maatregelen heeft Topicus reeds genomen om aan de GDPR-eisen te voldoen?

Dit hoofdstuk is een samenvatting van een uitgebreidere uitwerking van de GDPR die te vinden is in Bijlage E: Uitwerking GDPR. Zoals reeds is aangegeven in de contextanalyse is de GDPR opgebouwd vanuit een zestal beginselen. Wanneer deze beginselen verder worden uitgewerkt tot de wet ontstaan er vier categorieën waarover de GDPR uitspraken doet. De uitwerking van de GDPR zal per categorie worden beschreven.

Allereerst wordt er een overzicht gegeven van de GDPR. De hierboven genoemde categorieën komen terug in dit overzicht, waarna de inhoud van de vier categorieën aan bod komt. Vervolgens komen de reeds getroffen maatregelen aan bod. Naar aanleiding van deze maatregelen komt er nog enige scoping aan bod.

6.1 De GDPR in een notendop

De autoriteit persoonsgegevens heeft een overzicht opgesteld van de belangrijkste wijzigingen voor organisaties. Dit overzicht is weergegeven in Figuur 6: De AVG in een notendop.

Figuur 6: De AVG in een notendop (De Autoriteit Persoonsgegevens, 2018)

6.2 De grondslag

Het is allereerst van belang om te weten wat 'het verwerken van persoonsgegevens' inhoudt. Een verwerking is volgens de verordening elke bewerking of elk geheel van bewerkingen met betrekking tot persoonsgegevens. Deze verwerkingen zijn:

- Verzamelen;
- Vastleggen;
- Opslaan;
- Wijzigen;
- Opvragen;
- Raadplegen;
- Gebruiken;
- Verstrekken;
- Wissen en vernietigen.

Persoonsgegevens mogen niet zomaar worden verzameld. Er moet een welbepaald, uitdrukkelijk omschreven en gerechtvaardigd doel zijn waarom persoonsgegevens dienen te worden verwerkt. Gegevens verzamelen omdat deze "in de toekomst nog wel eens van pas kunnen komen" is dus niet toegestaan. De verwerking van persoonsgegevens is gerechtvaardigd wanneer het doel van de verwerking is gebaseerd op minimaal één van de zes rechtsgrondslagen die in de Verordening worden gegeven. De zes rechtsgrondslagen zijn:

a) De betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meerdere specifieke doeleinden;
b) De verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen;
c) De verwerking is noodzakelijk om te voldoen aan wettelijke verplichtingen die op de verwerkingsverantwoordelijke rust;
d) De verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke person te beschermen;
e) Verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen;
f) De verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is.

6.3 Zorgvuldigheid

Het veilig verwerken van persoonsgegevens begint bij de tekentafel door de beginselen Privacy by Design en Privacy by Default in acht te nemen. Privacy by Design houdt in dat de verwerkingsverantwoordelijke danwel de gegevensverwerker al tijdens de ontwikkeling van producten en diensten privacy en gegevensbescherming mee neemt als eisen. Daarnaast dient er aan dataminimalisatie te worden gedaan. Dit houdt in dat er zo min mogelijk persoonsgegevens verwerkt dienen te worden en dat alleen de gegevens die noodzakelijk zijn voor het doel van de verwerkingen gebruikt mogen worden. Privacy by Default houdt in dat er technische en organisatorische maatregelen getroffen moeten worden om er voor te zorgen dat er, als standaard, alléén persoonsgegevens verwerkt worden die noodzakelijk zijn voor het specifieke doel dat bereikt wil worden (Topicus, 2018).

Wanneer een voorgenomen verwerking van persoonsgegevens waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, dient er voorafgaand aan de verwerking een Data Protection Impact Assesment (DPIA) uitgevoerd te worden. Een goed uitgevoerde DPIA geeft inzicht in de risico's die de verwerking oplevert voor de betrokkenen, en in de maatregelen die de verantwoordelijke moet nemen om de risico's af te dekken (Autoriteit Persoonsgegevens, sd).

De GDPR kent een belangrijke rol toe aan de functionaris gegevensbescherming (FG). De FG houdt intern toezicht op en adviseert over de toepassing en naleving van de GDPR binnen een organisatie. De FG is tevens het aanspreekpunt voor de betrokkene.

6.4 Verplichtingen

Om de bescherming van persoonsgegevens te kunnen waarborgen, dienen er een aantal technische en organisatorische maatregelen getroffen te worden. Allereerst dient er een verwerkingsregister bijgehouden te worden. Het register van verwerkingsactiviteiten is een opsomming van de belangrijkste informatie over de verwerking van persoonsgegevens door een organisatie. Er dient een verwerkingsregister bijgehouden te worden wanneer een organisatie uit meer dan 250 personen bestaat of wanneer:

- De verwerking waarschijnlijk een risico voor betrokkenen met zich meebrengt;
- de verwerking niet-incidenteel is;
- er sprake is van de verwerking van bijzondere categorieën van persoonsgegevens of gegevens betreffende strafrechtelijke veroordelingen of strafbare feiten.

Naast het register dient er een gegevensbeschermingsbeleid te zijn. In de GDPR staat niet precies omschreven welke gegevens in het gegevensbeschermingsbeleid opgenomen moeten worden. Uit het beleid moet in ieder geval wel blijken hoe er wordt voldaan aan de GDPR als onderdeel van de verantwoordingsplicht.

Verder dienen er passende technische en organisatorische maatregelen getroffen te worden om de persoonsgegevens die worden verwerkt te beveiligen. De beveiliging dient passend te zijn. Er hoeven dus niet persé de zwaarst mogelijke beveiligingsmaatregelen getroffen te worden, maar maatregelen die in verhouding staan tot de gegevens en de bijbehorende risico's voor de betrokkenen. Hoe groter het risico voor de betrokkenen, des te zwaarder de beveiligingsmaatregelen die getroffen moeten worden

De GDPR schrijft niet voor welke exacte maatregelen er genomen dienen te worden. Deze invulling laat de GDPR over aan de verwerkingsverantwoordelijke en de gegevensverwerker. Wel geeft het een aantal voorbeelden zoals:

- Pseudonimisering en versleuteling van de persoonsgegevens;
- Het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;
- Het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;
- Een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.

6.5 Rechten van de betrokkenen

Mensen moeten controle kunnen uitvoeren op de verwerking van hun persoonsgegevens. De betrokkene heeft daarom een aantal rechten die hij of zij uit kan oefenen tegen de verwerkingsverantwoordelijke.

6.5.1 Recht op informatie

Allereerst is er het recht op informatie. De betrokkenen hebben het recht om te weten wat er met hun persoonsgegevens gebeurt en waarom. Ook moeten zij bewust worden gemaakt van de risico's van de gegevensverwerking, de regels die ervoor gelden, de waarborgen en de manier waarop zij hun rechten met betrekking tot de verwerking van gegevens kunnen uitoefenen.

6.5.2 Recht op inzage

Iedere betrokkene heeft het recht om de persoonsgegevens die van hem verzameld zijn in te zien. Een betrokkene mag daarom met redelijke tussenpozen aan een organisatie vragen welke persoonsgegevens van hem worden verwerkt. Organisaties zijn verplicht om gehoor te geven aan dergelijke verzoeken en de beschikbare informatie te verstrekken.

6.5.3 Recht op rectificatie

Vervolgens heeft de betrokkene recht op rectificatie. Wanneer er persoonsgegevens worden verwerkt, dienen deze gegevens accuraat te zijn en te blijven. Het kan voorkomen dat de gegevens niet (meer) kloppen. De betrokkene heeft dan het recht om deze gegevens te corrigeren.

6.5.4 Recht op beperking

Het recht op beperking van de verwerking van persoonsgegevens houdt in dat betrokkenen de mogelijkheid krijgen om de verwerking van hun persoonsgegevens tijdelijk 'stil te laten zetten'. De betrokkene heeft niet altijd recht op beperking van de verwerking, maar alleen in een bepaald aantal specifieke situaties.

6.5.5 Recht op verwijdering en recht om vergeten te worden

Onder bepaalde omstandigheden hebben betrokkenen het recht om hun gegevens door de verwerkingsverantwoordelijke te laten verwijderen, bijvoorbeeld wanneer de verwerking onrechtmatig is. Daarnaast heeft de betrokkene het recht om 'vergeten te worden'. Dit recht is met name in het leven geroepen zodat mensen op het internet niet voor altijd (ten onrechte) met hun verleden worden geconfronteerd.

Naast het recht op verwijdering heeft de betrokkene onder bepaalde omstandigheden ook het recht om 'vergeten te worden'. Dit recht ligt in het verlengde van het recht op verwijdering van gegevens. Het gaat dan om situaties waarbij de verwerkingsverantwoordelijke persoonsgegevens van de betrokkene openbaar heeft gemaakt (bijvoorbeeld door ze online te zetten) en de betrokkene aan de organisatie gevraagd heeft de gegevens te wissen. Naast het wissen van de gegevens uit de eigen systemen van de organisatie moeten redelijke technische en organisatorische maatregelen worden genomen om andere verwerkingsverantwoordelijken die de persoonsgegevens verwerken, ervan op de hoogte te stellen dat de betrokkene vergeten wil worden. Dit betekent dat iedere koppeling naar en kopie of reproductie van de gegevens gewist moet worden.

6.5.6 Recht op verzet

Een betrokkene kan onder omstandigheden bezwaar maken tegen de (verdere) verwerking van zijn gegevens en zijn recht op verzet inroepen. De verwerkingsverantwoordelijke moet dan de verwerking staken.

6.5.7 Recht op overdraagbaarheid van gegevens (dataportabiliteit)

Het recht op overdraagbaarheid van persoonsgegevens geeft de betrokkene het recht om een kopie te krijgen van de persoonsgegevens die hij aan een organisatie heeft verstrekt. De kopie moet in een gestructureerde, gangbare en machineleesbare vorm (CSV, JSON, XML et cetera) worden verstrekt. Het doel van het recht op gegevensoverdraagbaarheid is de zeggenschap van de betrokkene over zijn gegevens te vergroten. Het achterliggende idee is dat de betrokkene zijn gegevens mee kan nemen naar bijvoorbeeld een andere aanbieder en daardoor minder gebonden is aan de oorspronkelijke verwerkingsverantwoordelijke.

6.5.8 Het recht niet onderworpen te worden aan geautomatiseerde individuele besluitvorming waaronder profilering

Wanneer persoonsgegevens worden gebruikt om tot een bepaalde beslissing te komen en deze beslissing is uitsluitend gebaseerd op geautomatiseerde verwerking van persoonsgegevens en dus zonder (noemenswaardige) menselijke tussenkomst, dan is er sprake van geautomatiseerde individuele besluitvorming.

Profilering (*profiling*) is het indelen van personen in categorieën (profielen) op basis van hun persoonsgegevens. Op basis van deze profielen kunnen vervolgens (geautomatiseerde) individuele besluiten worden genomen, zoals bijvoorbeeld het verlenen van krediet door een financiële instelling. Profilering kan op de volgende drie manieren worden ingezet:

- Algemene profilering (nog zonder besluitvorming);
- Besluitvorming gebaseerd op profilering;
- Geautomatiseerde individuele besluitvorming gebaseerd op profilering.

Het verschil in toepassing 2 en 3 zit hem in de menselijke tussenkomst. Onder toepassing 2 is er nog sprake van noemenswaardige menselijke tussenkomst. Het profiel dient slechts ter ondersteuning van de besluitvorming, terwijl onder 3 het besluit geautomatiseerd wordt genomen en er geen sprake meer is van noemenswaardige menselijke tussenkomst.

Betrokkenen hebben het recht om niet onderworpen te worden aan een enkel op geautomatiseerde verwerking (waaronder profilering), gebaseerd besluit, wanneer dit rechtsgevolgen voor hen heeft of het hen anderszins in aanzienlijke mate treft. Hoewel deze bepaling in de GDPR als recht van de betrokkene is geformuleerd, gaat het in feite om een verbod voor de verwerkingsverantwoordelijke. Zo is een voorbeeld van profilering die mensen in aanzienlijke mate treft, het opstellen van een kredietwaardigheidsprofiel en enkel op basis dit profiel geautomatiseerde besluiten te geven om iemand geen lening te geven.

Echter zijn niet alle vormen van geautomatiseerde individuele besluitvorming verboden, ook al hebben zij rechtsgevolgen voor de betrokkenen of treffen zij hen in aanzienlijke mate. In de volgende situaties is het mogelijk om gebruik te maken van geautomatiseerde individuele besluitvorming, waaronder ook profilering:

- Wanneer dit noodzakelijk is voor de totstandkoming of de uitvoering van een overeenkomst tussen de betrokkene en een verwerkingsverantwoordelijke;
- Wanneer de betrokkene zijn uitdrukkelijke toestemming heeft gegeven;
- Wanneer dit is toegestaan bij een Unierechtelijke of lidstaatrechtelijke bepaling die op de verwerkingsverantwoordelijke van toepassing is en die ook voorziet in passende maatregelen ter bescherming van de rechten en vrijheden en gerechtvaardigde belangen van de betrokkene. (Voor profilering is dit niet geregeld in nationaal recht.)

6.6 Getroffen maatregelen

Topicus heeft een standpunt ingenomen voor alle onderwerpen van de GDPR zoals genoemd in Figuur 6: De AVG in een notendop uit paragraaf 6.1. In dit hoofdstuk wordt van deze standpunten een samenvatting gegeven. De volledige documentatie over de standpunten van Topicus is te vinden in Bijlage F: GDPR-standpunten Topicus.

6.6.1 Samenvatting van de maatregelen

Na analyse van de GDPR is Topicus tot de volgende standpunten en maatregelen gekomen om GDPR-compliant te worden:

- Topicus heeft op organisatorisch vlak een aantal zaken geregeld, namelijk:
  - Samen met elke verwerkingsverantwoordelijke danwel gegevensverwerker ervoor gezorgd dat er een Verwerkingsovereenkomst is tussen de betreffende verwerkingsverantwoordelijke danwel gegevensverwerker en Topicus als (sub)-gegevensverwerker.
  - Een Functionaris Gegevensbescherming (FG) aangesteld en gecommuniceerd wat de contactgegevens van de functionaris zijn naar de verwerkingsverantwoordelijken danwel gegevensverwerkers.
  - Een verwerkingsregister opgesteld.
  - Ondersteuning bieden aan de verwerkingsverantwoordelijken danwel gegevensverwerkers bij het opstellen van hun gegevensbeschermingsbeleid door inzage te geven in de gegevenscategorieën die in de systemen van Topicus worden vastgelegd en welke maatregelen Topicus reeds heeft genomen om deze gegevens te beschermen.
- Behalve de ontwikkeling van de Record Retention functionaliteit voor de centrale FORCE-database en de ingebruikname hiervan zijn er geen andere structurele functionele en/of technische aanpassingen aan FORCE gedaan.

Topicus geeft incidentele ondersteuning bij handelingen die nodig zijn op een specifiek dossier wanneer een betrokkene aanspraak maakt op een van zijn rechten, zoals bijvoorbeeld het recht op vergetelheid. In een dergelijk geval ondersteunt Topicus de verwerkingsverantwoordelijke danwel gegevensverwerker met het daadwerkelijk verwijderen van de gegevens, aangezien FORCE hiervoor niet over een standaard functionaliteit beschikt.

6.7 Scoping

Zoals uit de vorige paragrafen blijkt, is de GDPR erg breed. De GDPR stelt eisen op organisatorisch gebied, zoals het aanstellen van een functionaris gegevensbescherming, evenals eisen op technisch gebied zoals digitale beveiliging.

In de vorige paragraaf is naar voren gekomen dat Topicus op veel van deze punten al passende maatregelen heeft getroffen en is er voor deze punten geen verdere toetsing aan GDPR-compliance nodig is. De rechten van de betrokkenen zijn echter punten waarop Topicus nog niet helemaal tevreden is met de getroffen maatregelen, zoals de Record Retention functionaliteit. De opdrachtgevers hebben aangegeven dat de prioriteit hierbij op de verwerkingshandelingen verzamelen, vastleggen en opslaan van persoonsgegevens ligt. Er zal daarom gefocust worden op het identificeren van tekortkomingen die betrekking hebben op deze bewerkingshandelingen.

7 Behoefteanalyse

In dit hoofdstuk zullen de eisen en wensen van de stakeholders worden geïdentificeerd en gedefinieerd. Allereerst zullen de methodieken die gebruikt zijn worden behandeld om vervolgens de stakeholderanalyse uit te voeren. Tot slot worden de eisen en wensen van de stakeholders vertaald naar requirements.

7.1 Methodieken

Om tot de requirements te komen is, er gebruik gemaakt van een viertal methodieken. De resultaten komen voort uit een brainstormsessie, interviews met de stakeholders, het uitvoeren van de stakeholderanalyse en het prioriteren van de requirements door middel van de MoSCoW-methode.

7.1.1 Brainstormen

Gedurende het inventariseren van de stakeholders, het opstellen van interviewvragen en het vertalen van de eisen en wensen naar requirements is er meerdere malen samen met de bedrijfsbegeleiders gebrainstormd.

7.1.2 Stakeholderanalyse

Er is een stakeholderanalyse uitgevoerd om te bepalen welke actoren er belang hebben bij dit project. Deze analyse bestaat uit twee stappen. De eerste stap hierbij is het bepalen van de stakeholders. Door middel van een brainstormsessie is er een initiële lijst met stakeholders opgesteld die vervolgens zijn geïnterviewd. Varvasovszky en Brugha (2000) geven aan dat er gebruik gemaakt kan worden van een “sneeuwbal techniek” om tot alle stakeholders te komen. Bij deze techniek wordt er aan het eind van een interview met een stakeholder gevraagd welke andere stakeholders de respondent kan identificeren. Vervolgens worden deze stakeholders geïnterviewd en wordt er aan het eind van het interview de zelfde vraag gesteld. Dit proces wordt vervolgens herhaald totdat er geen nieuwe stakeholders meer naar voren komen.

Stakeholders zijn te verdelen in primaire en secundaire stakeholders (Preston, Post, & Sachs, 2002). Waar de primaire stakeholders een directe connectie met het project hebben, staan de secundaire stakeholders verder van het project af. Voorbeelden van secundaire stakeholders zijn overheidsinstanties, de media en belangengroepen zoals vakbonden. Er is gebruik gemaakt van een krachtenveld analyse om de primaire en secundaire stakeholders te bepalen. De interviews die gehouden zijn met de stakeholders zijn beperkt tot de primaire stakeholders. De belangen van de secundaire stakeholders zijn geïdentificeerd door gebruik te maken van bestaande literatuur.

Nadat de stakeholders zijn geïdentificeerd, geïnterviewd en gegroepeerd (primair en secundair), zijn de resultaten geanalyseerd. In deze analyse zijn zaken als interesse en belang bij het project meegenomen om te bepalen hoeveel invloed een stakeholder heeft op het project. Aan de hand van deze analyse zijn vervolgens de requirements geprioriteerd volgens de MoSCoW-methode.

7.1.3 Interview

Zoals aangegeven in de vorige paragraaf, is er gebruik gemaakt van semigestructureerde interviews om eisen en wensen van de primaire stakeholders in kaart te brengen. Tijdens de interviews met de vertegenwoordigers van de perspectieven uit de probleemanalyse, zijn ook meteen vragen gesteld voor de behoefteanalyse. Hierdoor hoefde er maar enkele interviews gehouden te worden wat voor efficiëntie heeft gezorgd.

Veel van de primaire stakeholders zijn groepen mensen. Er zijn vertegenwoordigers van deze stakeholders geïnterviewd om hun eisen en wensen te identificeren. Deze vertegenwoordigers zijn dezelfde personen

die voor probleemanalyse zijn geïnterviewd, namelijk Stefan Hessels, Maarten Schopman en Wietze Spijkerman.

7.1.4 MoSCoW

Met behulp van de MoSCoW-methode kunnen requirements worden geprioriteerd. Volgens van Vliet (2008) kunnen requirements één van de volgende prioriteringen meekrijgen:

- **M – Must haves:** Deze requirements moeten in het eindresultaat terugkomen. Zonder deze eisen is het product niet bruikbaar.
- **S – Should haves:** Deze requirements zijn zeer gewenst, maar zonder is het product wel bruikbaar.
- **C – Could Haves:** Deze requirements worden alleen meegenomen in het eindresultaat wanneer er voldoende tijd is.
- **W – Wont haves:** Deze eisen worden in het huidige project niet meegenomen maar kunnen in de toekomst bij een vervolgproject interessant zijn.

7.2 Translatie van de requirements

Requirements zijn te verdelen in Business, User en System requirements (Miller, 2008). De Business requirements beschrijven waarom het project wordt uitgevoerd en welke gewenste uitkomsten het project heeft. De User requirements beschrijven welke functionaliteiten het systeem moet bieden vanuit het oogpunt van de gebruiker. Tot slot geven de System Requirements aan welke functionaliteiten het systeem moeten bieden om aan de eisen en wensen van de users te voldoen. Tot slot kunnen deze type requirements nog worden onderverdeeld in functionele en niet-functionele requirements. Functionele requirements zeggen iets over de functies die het systeem moet bieden, terwijl niet-functionele requirements kwaliteitseisen zijn aan het systeem (Miller, 2008).

De bovenstaande definitie van Business, User en System requirements is goed toepasbaar wanneer er requirements voor een ontwerp opgesteld dienen te worden. Dit project heeft echter niet het doel om tot een ontwerp te komen, maar om antwoord te geven op de vraag of Enterprise Architecture bij kan dragen aan het aantonen van GDPR-compliance. Daarom moet er een translatie worden gemaakt naar een definitie van Business, User en System requirements die aansluiten bij dit project.

De Business requirements van dit project hebben daarom betrekking op het antwoord op deze vraag. De Business requirements beschrijven immers waarom een project wordt uitgevoerd en wat men wil bereiken.

User requirements bestaan uit functionaliteiten die een product dient te bieden. Een product kan bijvoorbeeld een softwareapplicatie of een informatiesysteem zijn, maar ook een tool of een stuk gereedschap. Om te bepalen wat het product is bij een project, is het van belang om na te gaan wie de users zijn. Binnen dit project kunnen de analisten en architecten als users worden geïdentificeerd waarbij de architectuurplaat de rol van product vervult. De users willen dat deze architectuurplaat bepaalde functionaliteiten biedt, zoals bijvoorbeeld het identificeren van businessprocessen waar data wordt verzameld.

Het product dient de gewenste functionaliteiten van de users aan te bieden. Om dit te kunnen doen, worden er ook requirements aan het product gesteld. De System requirements stellen dus eisen aan de architectuurplaat en haar opbouw. Voorbeelden van dit soort requirements zijn dat het detailniveau van de architectuurplaat overal consistent moet zijn en dat de architectuurplaat de componenten op business-, applicatie- en infrastructuurniveau moet beschrijven.

Ter verduidelijking is in Tabel 3: Requirements translatie de translatie van de requirements weergegeven.

Requirement	Standaard	Project
Business	Het te bereiken doel	Het te bereiken doel: antwoord op de onderzoeksvraag
User	Functionaliteiten	Functionaliteiten van de architectuurplaat
System	Systeemeisen	Eisen aan de (opbouw van de) architectuurplaat

Tabel 3: Requirements translatie

7.3 Macht-belangdiagram

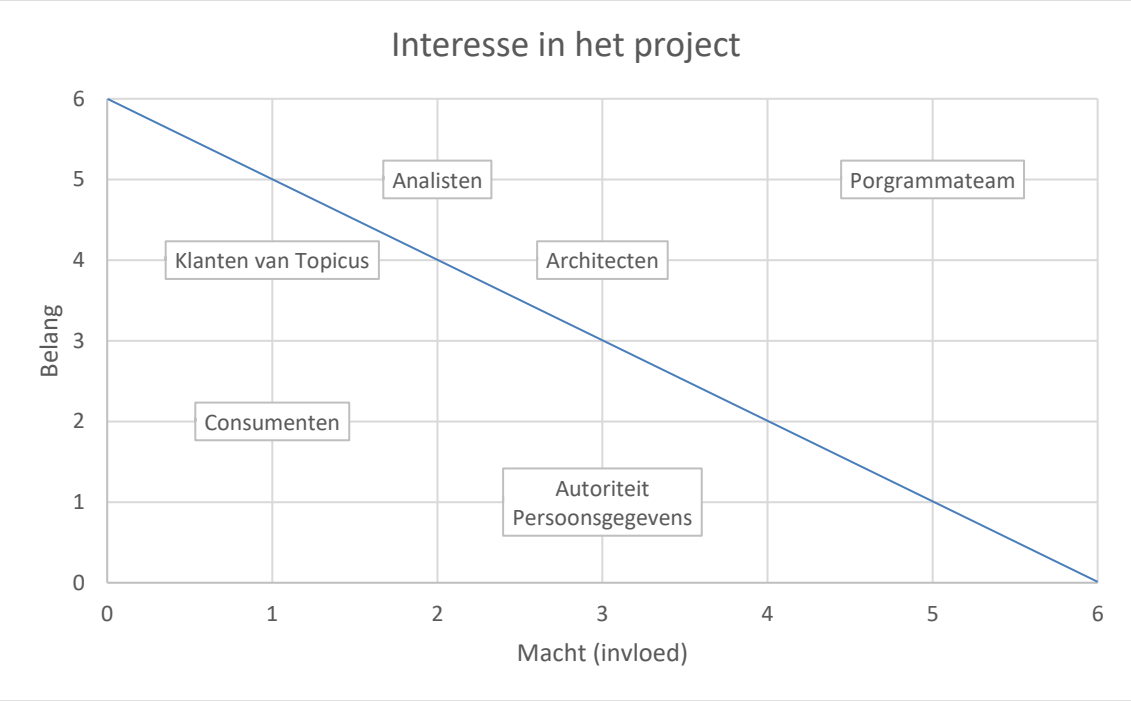
Tabellen of matrixen kunnen worden opgesteld om stakeholders' interesse in een project, hun invloed en hun houding ten opzichte van het project te kwantificeren (Varvasovszky & Brugha , 2000). Door middel van een macht-belangdiagram kan er inzicht worden gecreëerd in het belang van de diverse stakeholders.

In de onderstaande tabel hebben de stakeholders een cijfer gekregen van 1 tot en met 5 op het gebied van macht (invloed) en belang bij het project. Hierbij geeft 1 de laagste score en 5 de hoogste score.

	Macht (invloed)	Belang
Programmateam	5	5
Architecten	3	4
Analisten	2	5
Autoriteit Persoonsgegevens	3	1
Klanten van Topicus	1	4
Consumenten	1	2

Tabel 4: Macht en invloed stakeholders

Deze waardes zijn in Figuur 7: Macht-belangdiagram tegen elkaar uitgezet. Om te bepalen welke stakeholders primair en secundair zijn, is er een diagonaal getekend. Deze diagonaal geeft de scheiding aan waarbij de stakeholders boven de lijn primaire stakeholders zijn en stakeholders onder de lijn secundaire stakeholders.



Figuur 7: Macht-belangdiagram

7.4 Resultaten van de stakeholderinterviews

In deze paragraaf worden de resultaten van de stakeholderanalyse uitgewerkt. Allereerst worden de stakeholders uitgewerkt en gegroepeerd als primaire of secundaire stakeholder. Vervolgens worden de resultaten geanalyseerd ten behoeve van de MoSCoW-methode.

7.4.1 Primaire stakeholders

De primaire stakeholders zijn direct betrokken bij het project. Vertegenwoordigers van de stakeholders zijn geïnterviewd om hun standpunten en behoeftes te achterhalen.

7.4.1.1 Programmateam

Het programmateam is verantwoordelijk voor de aansturing van de ontwikkelteams binnen de afdeling hypotheken van Topicus Finance. Het programmateam wil aan de wens van de afnemers van FORCE voldoen, namelijk dat Topicus aan kan tonen dat zij (en FORCE) GDPR-compliant is.

Om GDPR-compliant te zijn hebben zij al een Record Retention Functionaliteit laten ontwikkelen. Deze functionaliteit is echter gelimiteerd tot het verwijderen van persoonsgegevens uit de FORCE database waardoor persoonsgegevens op nadere locaties zoals in logbestanden, niet worden verwijderd. De wens vanuit het programmateam is dan ook om te achterhalen waar zich persoonsgegevens bevinden en om aan te kunnen tonen dat alle data verwijderd is.

7.4.1.2 Architecten

De architecten zijn verantwoordelijk voor het bewaren van de architectuur van FORCE. Zij hebben daarom vanzelfsprekend een belang bij dit project en de resultaten ervan. De wens van de architecten is daarbij wel dat er vastgehouden kan worden aan de huidige architectuur- en designprincipes. Daarnaast hebben de architecten er behoefte aan dat FORCE inzichtelijker wordt gemaakt voor hun collega's; iets wat mogelijk behaald zou kunnen worden door Enterprise Architecture toe te passen. Een valkuil hierbij is echter dat het detailniveau van een architectuurtekening te hoog of juist te laag is. Hier dient daarom een goede middenweg in gevonden te worden.

7.4.1.3 Analisten (opdrachtgevers)

De analisten zijn verantwoordelijk voor het omzetten van gewenste features in werkzaamheden om deze features te realiseren. Zij moeten inzicht hebben in de opbouw van componenten, hun onderlinge communicatie en koppelingen en de data die daarbij wordt verwerkt. Voor hen is het van belang dat de werking van de component duidelijk wordt en dat datalocaties bekend worden.

7.4.2 Secundaire stakeholders

De secundaire stakeholders staan verder van het project en hebben geen directe relatie met het project.

7.4.2.1 Autoriteit Persoonsgegevens (GDPR)

De Autoriteit Persoonsgegevens houdt toezicht op de naleving van de GDPR. De autoriteit onderzoekt het gebruik van persoonsgegevens binnen bedrijven en overheidsorganisaties en legt boetes op bij overtredingen. Daarnaast adviseert de Autoriteit Persoonsgegevens de regering en het parlement over nieuwe wet- en regelgeving over persoonsgegevens. Verder levert de autoriteit informatie over privacy aan burgers (Rijksoverheid, sd).

7.4.2.2 Afnemers van FORCE

Banken en andere hypotheekverstrekkers nemen FORCE bij Topicus af zodat zij hun hypotheekproces grotendeels automatisch kunnen doorlopen. Om een hypotheekaanvraag te kunnen verwerken en verstrekken worden er persoonsgegevens verwerkt in FORCE. Deze gegevens worden echter door de afnemers van FORCE verzameld en niet door Topicus. Daarom vervullen de afnemers van FORCE volgens de GDPR de rol van verwerkingsverantwoordelijke.

Doordat de afnemers van FORCE de rol van verwerkingsverantwoordelijke vervullen hebben zij belang bij GDPR-compliance. De afnemers blijven immers verantwoordelijk voor een correcte verwerking van persoonsgegevens.

7.4.2.3 Consumenten

Consumenten die een hypotheek aanvraag indienen bij een afnemer van FORCE moeten hier persoonsgegevens voor vertrekken. Zij vervullen volgens de GDPR de rol van de betrokkene. Uiteindelijk gaat het om de persoonsgegevens van de consumenten die verwerkt worden in FORCE. Zij hebben vanzelfsprekend belang bij een nette en verantwoorde omgang met hun data die in lijn is met de GDPR.

7.5 Conclusie

Uit de interviews en de uitwerking van de GDPR zijn eisen en wensen naar voren gekomen. De conclusie van dit hoofdstuk bestaat uit het vertalen van deze eisen en wensen naar requirements.

7.5.1 Business requirements

Binnen de Business requirements zijn er twee verschillende groepen requirements te definiëren. Dit komt doordat er op de vraag of Enterprise Architecture bij kan dragen aan het aantonen van GDPR-compliance zowel ja als nee geantwoord kan worden. In het geval dat het antwoord op de vraag een ja is, geldt Tabel 5: Business requirements bij een ja. In het geval van een nee geldt Tabel 6: Business requirements bij een nee.

Afkorting	Requirement	Must have	Should have	Could have	Won't have now	Functioneel (F)/ Niet functioneel (N)
BR01	Tekortkomingen in GDPR-compliance moeten aangegeven worden.	X				N
BR02	Er moeten maatregelen worden geadviseerd om deze tekortkomingen weg te nemen.	X				N

Tabel 5: Business requirements bij een ja

Afkorting	Requirement	Must have	Should have	Could have	Won't have now	Functioneel (F)/ Niet functioneel (N)
BR03	Er moet aangegeven worden waarom Enterprise Architecture niet werkt voor het aantonen van GDPR-compliance.	X				N
BR04	Er moet advies worden gegeven hoe hoe GDPR-compliance wel aangetoond kan worden.	X				N

Tabel 6: Business requirements bij een nee

7.5.2 User requirements

Afkorting	Requirement	Must have	Should have	Could have	Won't have now	Functioneel (F)/ Niet functioneel (N)
UR01	Uit de architectuurplaat moet af te leiden zijn uit welke informatiesystemen data wordt verzameld.	X				F
UR02	Uit de architectuurplaat moet af te leiden zijn in welke businessprocessen data wordt verzameld.	X				F
UR03	Uit de architectuurplaat moet af te leiden zijn waar data opgeslagen wordt.	X				F
UR04	Uit de architectuurplaat moet af te leiden zijn welke data opgeslagen wordt.	X				F
UR05	Er mag maar van één modelleertaal en bijbehorende modelleertool gebruik gemaakt worden.	X				N

Tabel 7: User requirements

7.5.3 System requirements

Afkorting	Requirement	Must have	Should have	Could have	Won't have now	Functioneel (F) / Niet functioneel (N)
SR01	Voor elk component moet er een aparte architectuurplaat zijn.	X				N
SR02	Er moet een architectuurplaat zijn die alle losse architectuurplaten samenvoegt.	X				N
SR03	Het detailniveau voor alle architectuurplaaten moet consisten zijn.	X				N
SR04	De architectuurplaten moeten de componenten weergeven op businessniveau.	X				F
SR05	De architectuurplaten moeten de componenten weergeven op applicatieniveau.	X				F
SR06	De architectuurplaten moeten de componenten weergeven op infrastructuurniveau.	X				F

Tabel 8: System requirements

8 Literatuuronderzoek

Er bestaan meerdere Enterprise Architecture Frameworks die verschillen in hun aanpak en in de opbouw van hun framework. Dit literatuuronderzoek is gebruikt om verschillende frameworks met elkaar te vergelijken. Daarnaast is er onderzocht welke mate van detail er toegepast dient te worden tijdens het modelleren van een Enterprise Architecture. Hiermee wordt er antwoord gegeven op deelvraag 3: Wat is Enterprise Architecture en hoe dient dit toegepast te worden binnen Topicus?

Allereerst zullen de gebruikte methodieken worden behandeld en zal er een onderbouwde afbakening worden gemaakt van de Enterprise Architecture Frameworks die zijn vergeleken. Vervolgens worden de resultaten uit de literatuur behandeld. Er wordt afgesloten met een conclusie die bestaat uit ontwerpprincipes.

8.1 Methodieken

In deze paragraaf staan de methodieken beschreven die zijn toegepast voor het literatuuronderzoek. Er wordt een afbakening van de onderzochte Enterprise Architecture Frameworks gedaan en de zoekmethode wordt uitgewerkt.

8.1.1 Oriëntatie en afbakening

Er bestaan enkele tientallen Enterprise Architecture Frameworks met elk hun eigen aanpak, visie en soms ook een specifieke relatie tot een branche waarvoor het framework is ontwikkeld. Zo is bijvoorbeeld het Treasury Enterprise Architecture Framework (TEAF) ontwikkeld voor het US Department of the Treasury en is NATO Architecture Framework (NAF) het framework van de NAVO (NATO, 2018). Uit een initiële analyse zijn vier frameworks gekomen die zijn vergeleken.

Het eerste framework dat meegenomen is in de vergelijking is DYnamic Architecture (DYA). Dit framework is tijdens de opleiding voorafgaand aan dit onderzoek uitgebreid behandeld en wordt daarom meegenomen in de vergelijking. De overige drie frameworks zijn het Zachman Framework, FEAF en TOGAF. Deze frameworks zijn geselecteerd op hun populariteit. Volgens een jaarlijkse enquête van het Institute For Enterprise Architecture Developments (IFEAD) uit 2005 zijn dit de meest gebruikte Enterprise Architecture Frameworks. Respectievelijk hebben ze 25, 11 en 9 procent marktaandeel (Institute For Enterprise Architecture Developments, 2005).

Naast de architectuurframeworks die onderzocht zijn, is het detailniveau van Enterprise Architecturelagen een onderwerp waarover nagedacht dient te worden voor dit onderzoek. Het is noodzakelijk om te weten op welk detailniveau de architectuurplaten opgesteld dienen te worden om te kunnen bepalen of Enterprise Architecture bij kan dragen aan het aantonen van GDPR-compliance. Daarnaast is het de vraag of Enterprise Architecture wel geschikt is om op hoog detailniveau toegepast te worden. Er is daarom naar literatuur gezocht die antwoord geeft op deze vragen.

8.1.2 Bronnen

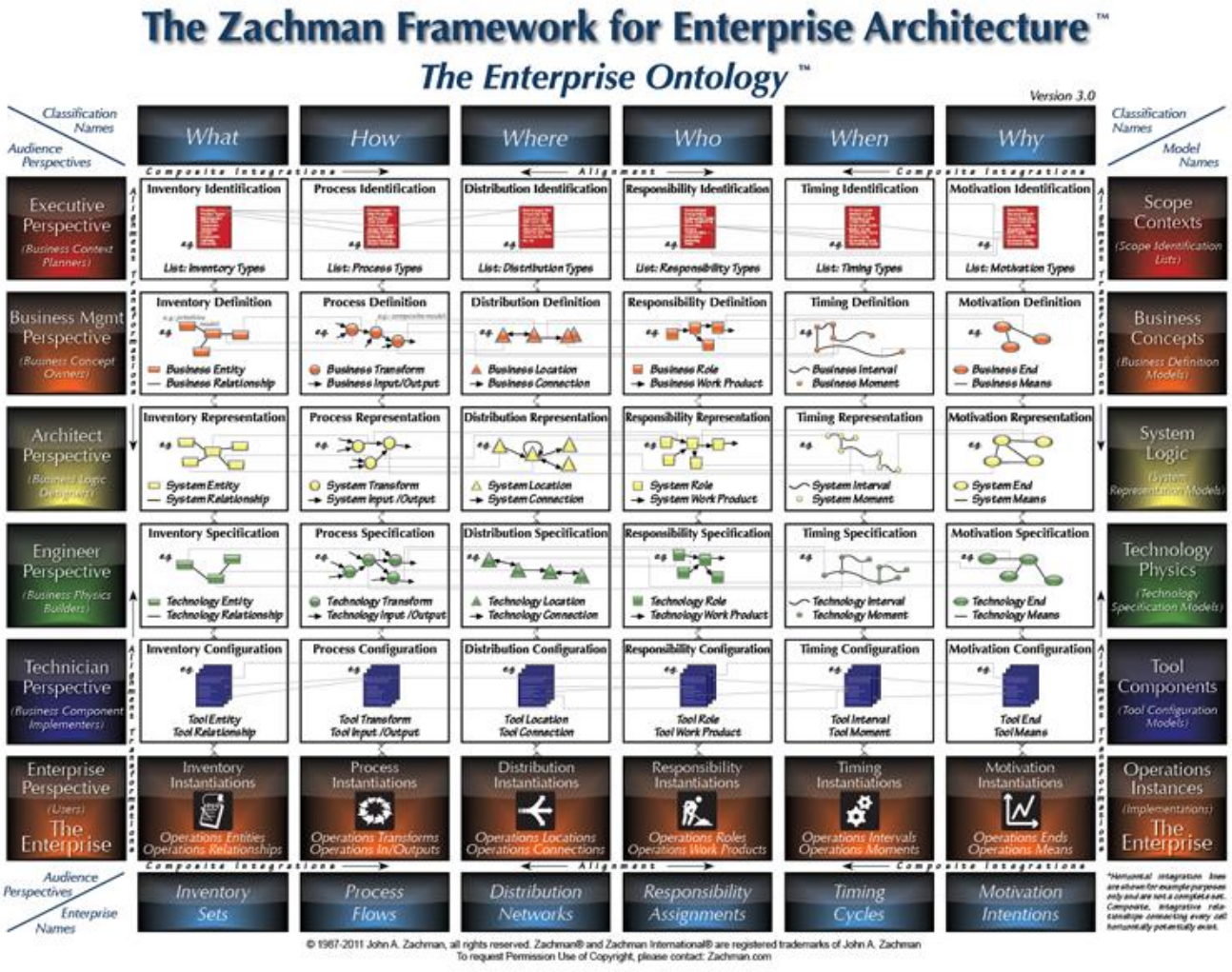
Om tot bronnen en informatie te komen, is er gebruik gemaakt van de sneewbalmethode. Deze methode houdt in dat de onderzoeker zich laat inspireren door de literatuurlijst van auteursrelevante artikelen. Uit de literatuurlijst van deze artikelen kunnen artikelen worden opgezocht en daaruit kunnen weer nieuwe referentielijsten uit voortvloeien. Het principe van de sneeuwbalmethode is dat dit zich steeds kan herhalen (Haveman, Hageraats, & van der Linden, 2016).

8.2 Resultaten

In deze paragraaf worden de resultaten van het literatuuronderzoek behandeld. Allereerst worden de verschillende architectuurframeworks met hun voor- en nadelen behandeld. Daarna komt het detailniveau van de architectuurlagen aan bod.

8.2.1 Zachman Framework

Het Zachman Framework is in 1987 geïntroduceerd door John Zachman. Zachman wordt door velen gezien als de pionier van Enterprise Architecture Frameworks (Goethals, 2005). Volgens Zachman (1999) is het zo dat “de toenemende scope van het ontwerpen van informatiesystemen en de mate van complexiteit daarvan, het gebruik van een logische constructie of architectuur wordt genoodzaakt”. Het Zachman Framework is gebaseerd op een aantal klassieke architectuurprincipes en een set aan perspectieven voor het beschrijven van complexe organisatiestructuren (Urbaczewsk & Mrdalj, 2006). De zes perspectieven van het framework zijn Planner, Owner, Designer, Builder, Subcontractor en User. De andere as is gebaseerd op de zes primitieve vraagwoorden: Why, How, What. Who, Where, When.

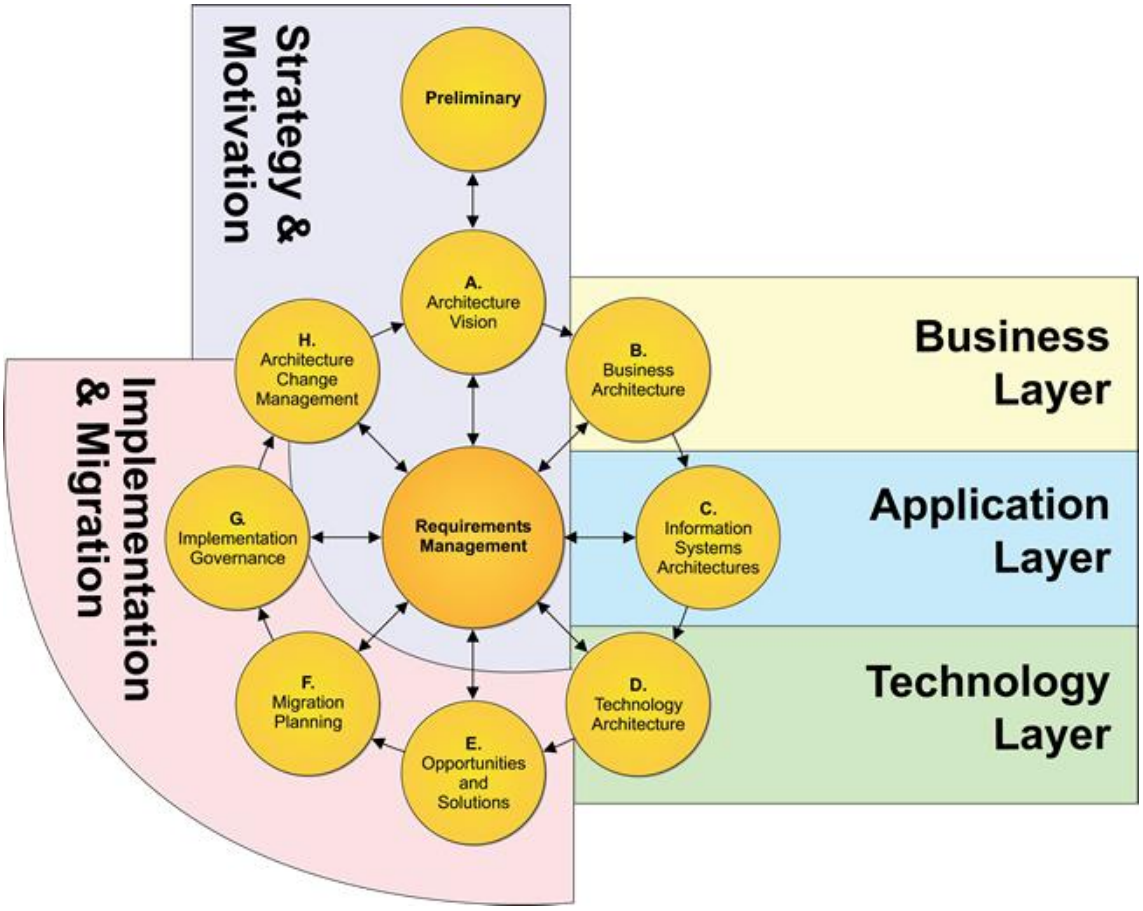


Figuur 8: Het Zachman Framework (Zachman J. A., About the Zachman Framework, 2008)

Het Zachman Framework is geen methodiek, maar een ontologie. Het geeft daarom geen richtlijn over de ontwikkeling en implementatie van architectuur, maar focust zich meer op het verzekeren van een compleet systeem onder architectuur. Dit is zowel het grootste voordeel als nadeel van het framework. Het geeft een compleet overzicht van architecturale aspecten die in acht moeten worden genomen, maar geeft geen beschrijving van het proces om tot die implementatie te komen (Tang, Han, & Chen, 2004).

8.2.2 TOGAF

The Open Group Architectural Framewrok (TOGAF) is voor het eerst ontwikkeld in 1995 en was gebaseerd op het Technical Architecture Framework for Information Management van het Amerikaanse Department of Defense. (The Open Group, 2005). TOGAF focust op kritieke bedrijfsapplicaties die gebruik maken van bouwstenen voor open systemen (Urbaczewsk & Mrdalj, 2006). “Een sleutelelement van TOGAF is de Architecture Development Method (ADM) welke een proces specifieert voor het ontwikkelen van Enterprise Architecture” (Tang, Han, & Chen, 2004). In plaats van het geven van architectuurprincipes, geeft TOGAF regels voor het ontwerpen van goede architectuurprincipes.

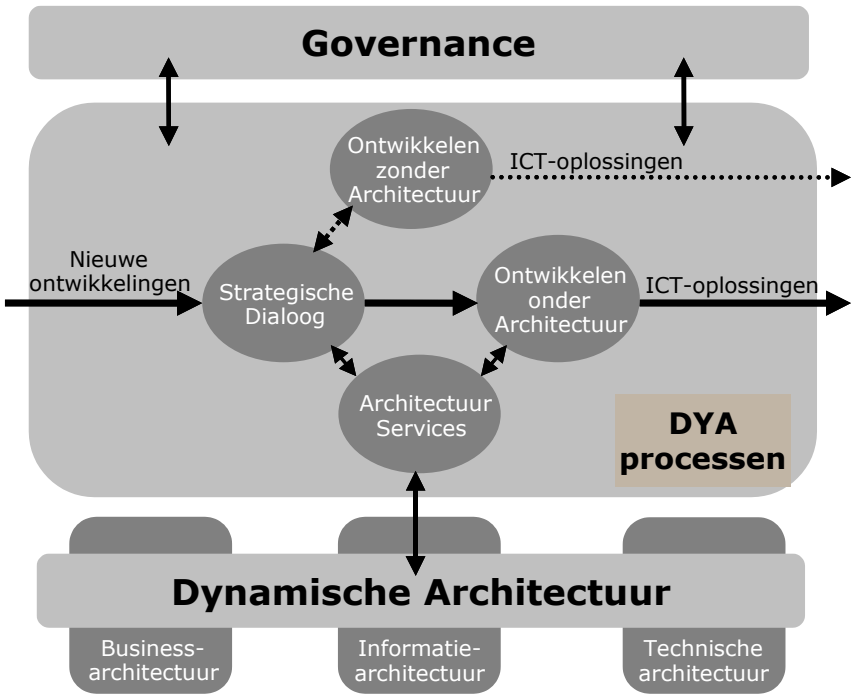


Figuur 9: Relatie tussen TOGAF ADM en ArchiMate (The Open Group, 2016)

De voordelen van TOGAF ADM zijn dat het een uitgebreide methodologie is die architectuur stuurt op zowel organisatieniveau, als op individueel systeemniveau en die de evolutie van architectuur ondersteund. De activiteiten van elke fase uit het ADM zijn goed gedefinieerd maar laten ruimte over voor flexibele implementatie zodat architecten zelf kunnen bepalen wat er gedefinieerd dient te worden voor een systeem (Tang, Han, & Chen, 2004). Daarnaast is een groot voordeel van TOGAF dat het zeer gemakkelijk samen met de modelleertaal ArchiMate kan worden gecombineerd (Lankhorst & van Drunen, 2007).

8.2.3 DYA

DYnamic Architecture is een Enterprise Architecture Framework ontwikkeld door consultingsbedrijf Sogeti en uitgebracht in 2007. Sogeti claimt er doormiddel van DYA dynamisch omgegaan kan worden met architectuur en dat daarmee mee rendement uit investeringen gehaald kan worden (de Boer D. , 2014). De visie van DYA is dat de informatiearchitectuur niet belemmerend is, maar juist versnellend en dus gangmaker in plaats van tegenwerker. Volgens het DYA denk- en werkmodel begint het ontwikkelen onder architectuur met het strategisch dialoog. Het strategische dialoog stuurt de ontwikkeling van systemen en kent meerdere scenario's, waaronder de mogelijkheid om niet onder architectuur te ontwikkelen.

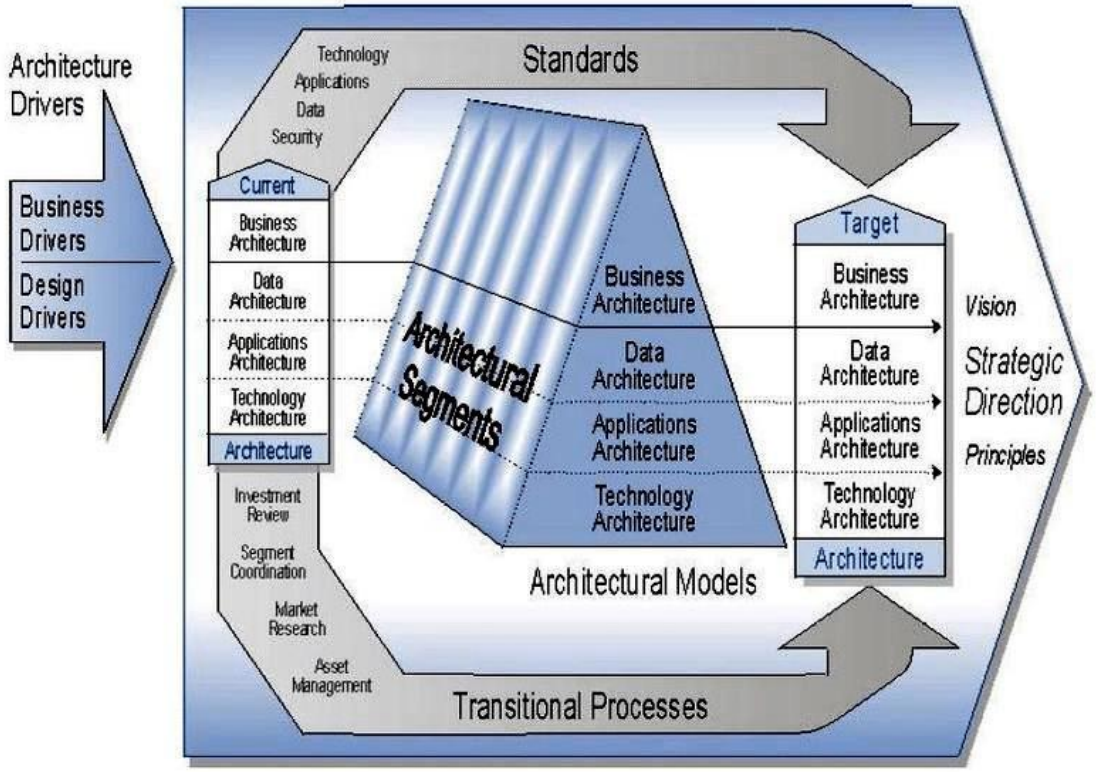


Figuur 10: DYA denk- en werkmodel

Het DYA-model geeft concrete handvatten voor het inrichten en professionaliseren van de architectuurprocessen. Daarnaast geeft het modellen en richtlijnen voor het ontwikkelen zowel onder architectuur, als zonder architectuur. Hierdoor biedt het model een goede slagkracht wanneer er op korte termijn iets ontwikkelt moet worden. Het nadeel van het framework is echter dat het framework zich met name focust op de technische infrastructuurlaag en minder op de overige architectuurlagen.

8.2.4 FEAF

Het Federal Enterprise Architecture Framework (FEAF) is ontwikkeld en uitgebracht door de US Federal Chief Information Officers (CIO) Council (Urbaczewsk & Mrdalj, 2006). Het doel van de CIO Council was om een standaard framework te hebben voor het verbeteren van ontwikkelen, moderniseren, gebruiken en delen van overheidsinformatiebronnen. Het framework is georganiseerd op vier niveaus, waarbij het hoogste niveau kijkt naar de strategische richting van architectuur. Niveau twee brengt meer detail door de buiness drivers en design drivers te analyseren. Het derde niveau schept weer meer detail door de doelarchitectuur van de business, data, applicatie en technologie laag te modelleren. Het laagste niveau maakt gebruik van het Zachman Framework en Spewak's Entrerpsie Architecture Planning (EAP) methodes om daadwerkelijk tot deze doelarchitecturen te komen. De EAP-methode houdt kort in dat er op 4 niveaus een planning wordt gemaakt om tot een Enterprise Architecture te komen.



Figuur 11: Het FEAF Framework

Het nadeel van het FEAF framework is dat het met name een framework is voor architecturale planning (Tang, Han, & Chen, 2004). Hierdoor geeft het geen concrete informatie over de uitvoering en implementatie van architectuur. Daarnaast ondersteunt het framework geen softwareconfiguratie modellering.

8.2.5 Detailniveau van Enterprise Architecturelagen

Een veelvoorkomend probleem bij Enterprise Architecture is dat het detailniveau te hoog of juist te laag is. Wanneer het detail niveau hoog en abstract is, schept het weinig inzicht en roept het mogelijk alleen maar meer vragen op dan dat het inzicht biedt. Wanneer het detailniveau te hoog is, bestaat de kans dat het overzicht kwijt wordt geraakt en daarmee het doel achter het modelleren. Het is daarom van belang om te weten welke mate van detail toegepast moet worden. Dit geldt niet alleen voor een gehele architectuurtekening, maar ook per architectuurlaag. Winter & Fischer (2006) geven een aantal richtlijnen over de inhoud en het detailniveau van de verschillende architectuurlagen:

- **Business en proces architectuur:** Businessprocessen moeten niet verder worden onderverdeeld dan sub-processen. Het gedetailleerd beschrijven van processen en procesactiviteiten valt buiten de scope van Enterprise Architecture en dient overgelaten te worden aan procesmodeleertools.
- **Datalaag architectuur:** Hoewel de connecties en afhankelijkheden tussen applicaties en hun componenten toebehoren tot Enterprise Architecture, moet hier niet tot teveel detail worden getreden. Zaken als interfacebeschrijvingen en remote procedure calls kunnen het beste worden beheerd door Enterprise Architecture Intergration (EAI) tools.
- **Software architectuur:** Gedetailleerde beschrijvingen van dataobjecten (e.g. attribute lists) zijn niet essentieel voor Enterprise Architecture doeleinden en dienen gemanaged te worden door datamodeleertools. Daarnaast valt de beschrijving van de interne werking van softwarecomponenten niet onder Enterprise Architecture.
- **Infrastructuur architectuur:** Gedetailleerde specificaties van IT-componenten zoals hardware specificaties zijn niet essentieel voor Enterprise Architecture.

8.3 Conclusie

Vanuit het literatuuronderzoek zijn er ontwerpprincipes naar voren gekomen. Deze architectuurprincipes richten zich op de verschillende architectuurframeworks en het detailniveau van Enterprise Architecture en de bijbehorende architectuurplaten.

Nr	Ontwerpprincipe
OP-01	Als er een architectuurframework gekozen moet worden om infrastructuur in te richten, dan moet DYA geselecteerd te worden, omdat het framework concrete handvatten voor het inrichten en professionaliseren van de architectuurprocessen geeft (de Boer D. , 2014).
OP-02	Als er een architectuurframework gekozen moet worden voor architecturele planning, dan moet het FEAF framework worden gekozen, omdat dit framework met name een framework is voor architecturele planning (Tang, Han, & Chen, 2004).
OP-03	Als er een model met ArchiMate gemodelleerd wordt, dan dient TOGAF als architectuurframework gekozen te worden omdat dit framework zeer makkelijk met ArchiMate gecombineerd kan worden (Lankhorst & van Drunen, 2007).
OP-04	Als er een architectuurframework gekozen moet worden om op verschillende niveaus te sturen en te modelleren, dan dient TOGAF gekozen te worden, omdat dit framework stuurt op zowel organisatie- als individueel systeemniveau (Tang, Han, & Chen, 2004).
OP-05	Als er een architectuurframework gekozen moet worden om een compleet overzicht van architecturele aandachtspunten te krijgen, dan moet het Zachman Framework worden gekozen omdat, framework een compleet overzicht geeft van architectuele aspecten die in acht moeten worden genomen (Tang, Han, & Chen, 2004)
OP-06	Als de businesslaag bruikbaar gemodelleerd moet worden, dienen businessprocessen niet verder worden onderverdeeld dan sub-processen, omdat dit buiten de scope van Enterprise Architecture valt en aan procesmodeleertools overgelaten dient te worden (Winter & Fischer, 2006).
0P-07	Als de datalaag bruikbaar gemodelleerd moet worden, dienen zaken als interfacebeschrijvingen en remote procedure calls buiten beschouwing worden gelaten in de architectuurmodelering, omdat deze een te hoog detailniveau vereisen (Winter & Fischer, 2006).
OP-08	Als de applicatielaag bruikbaar gemodelleerd moet worden, dienen dataobjecten niet gedetailleerd beschreven te worden omdat dit beter gedaan kan worden door datamodelleer-tools en talen zoals UML (Winter & Fischer, 2006).
OP-09	Als de applicatielaag bruikbaar gemodelleerd moet worden, dient de interne werking van applicatiecomponenten niet gemodelleerd te worden, omdat dit buiten de scope van Enterprise Architecture valt (Winter & Fischer, 2006).
OP-10	Als de infrastructuurlaag bruikbaar gemodelleerd moet worden, dienen gedetailleerde specificaties van IT-componenten zoals hardware specificaties buiten beschouwing gelaten te worden, omdat deze niet essentieel zijn voor Enterprise Architecture (Winter & Fischer, 2006).

Tabel 9: Ontwerpprincipes

9 Architectuurplaat

In dit hoofdstuk wordt er een modelering gepresenteerd van FORCE en de componenten NHG Gateway, Morality, Proposals en Agreements. In de eerste paragraaf wordt besproken hoe data is verzameld om deze componenten te kunnen modelleren. In de tweede paragraaf wordt er een architectuurframework geselecteerd zodat de modellen gemodelleerd kunnen worden. Daaropvolgend wordt er een model behandeld met een laag detailniveau om vervolgens het overzicht over de componenten weer te geven. Daarna worden de componenten apart behandeld op een hoger detailniveau. Tot slot worden deze sub-modellen samengevoegd tot één groot model. Daarmee wordt er antwoord gegeven op deelvragen 4 en 5:

- Hoe zijn de componenten FORCE.Mortages, Proposals, Morality, Agreements en NHGGateway opgebouwd zoals gemodelleerd door middel van Enterprise Archticture?
- Hoe zijn de businessprocessen die worden ondersteund door de componenten FORCE.Mortages, Proposals, Morality, Agreements en NHGGateway ingericht?

Veel van de architectuurtekeningen zijn te groot om duidelijk en leesbaar op een pagina van A4 formaat weer te geven. Daarom worden er aparte bestanden bijgevoegd die afbeeldingen bevatten van de architectuurtekeningen. In deze bestanden zijn alle tekeningen op volledige schaal te bekijken. Tevens wordt er een Archi-bestand bijgevoegd met daarin de architectuurmodellen. Archi is een applicatie om te modelleren met de modelleertaal Archimate.

9.1 Dataverzamelingsmethode

Voor veel componenten van FORCE is er documentatie beschikbaar op Confluence. Hier is zowel technische over de opbouw en werking van componenten te vinden als functionele informatie over componenten. Aan de hand van de informatie die op Confluence beschikbaar is zijn de modellen opgesteld. Echter is het zo dat niet elk component even uitgebreid gedocumenteerd is op Confluence. Indien dit het geval was, is er gesproken met de ‘componenteigenaren’ om te achterhalen hoe een component in elkaar zit. Dit zijn de ontwikkelteams die verantwoordelijk zijn voor het ontwikkelen en onderhouden van een bepaald component.

9.2 Keuze architectuurframework

De keuze van het architectuurframework kan gebaseerd worden op de ontwerpprincipes uit het literatuuronderzoek. Voor Topicus is het van belang dat zij een architectuurtekening krijgen die gemodelleerd is door middel van ArchiMate waarbij er inzicht wordt geboden op business, applicatie en infrastructuurniveau. Het framework dat zich het beste bij hierbij aansluit is TOGAF en TOGAF zal daarom ook worden gekozen als toe te passen architectuurframework. De keuze voor dit framework is gebaseerd op ontwerpprincipes OP-03 en OP-04:

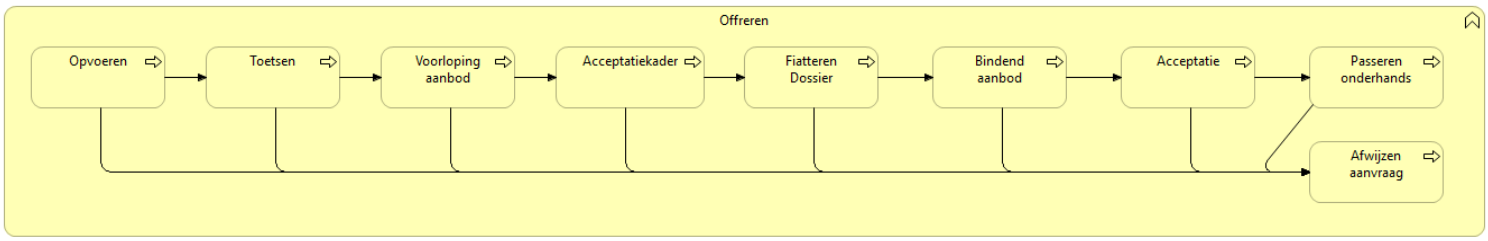
Nr	Ontwerpprincipe
OP-03	Als er een model met ArchiMate gemodelleerd wordt, dan dient TOGAF als architectuurframewrok gekozen te worden, omdat dit framework zeer makkelijk met ArchiMate gecombineerd kan worden (Lankhorst & van Drunen, 2007).
OP-04	Als er een architectuurframework gekozen moet worden om op verschillende niveaus te sturen en te modelleren, dan dient TOGAF gekozen te worden, omdat dit framework stuurt op zowel organisatie- als individueel systeemniveau (Tang, Han, & Chen, 2004).

Tabel 10: Ontwerpprincipes m.b.t. het gekozen architectuurframework

9.3 Hoog-over architectuur

De eerste modellen die worden behandeld, zijn verdeeld over de Business, Applicatie en Infrastructuur laag. Deze modellen zijn zeer globaal en bedoelt om een globaal beeld te geven van de processen en IT die relevant zijn voor de scope van de architectuurplaat.

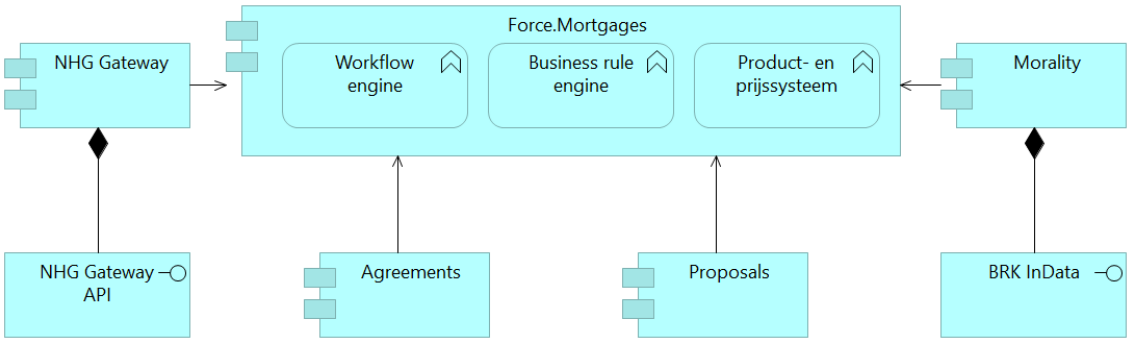
9.3.1 Business laag



Figuur 12: Business laag

De componenten die worden gemodelleerd ondersteunen hoofdzakelijk het offrerenproces. Het proces is op te delen in verschillende sub-processen waarbij er vanuit elk sub-proces over kan worden gegaan in het afwijzen proces.

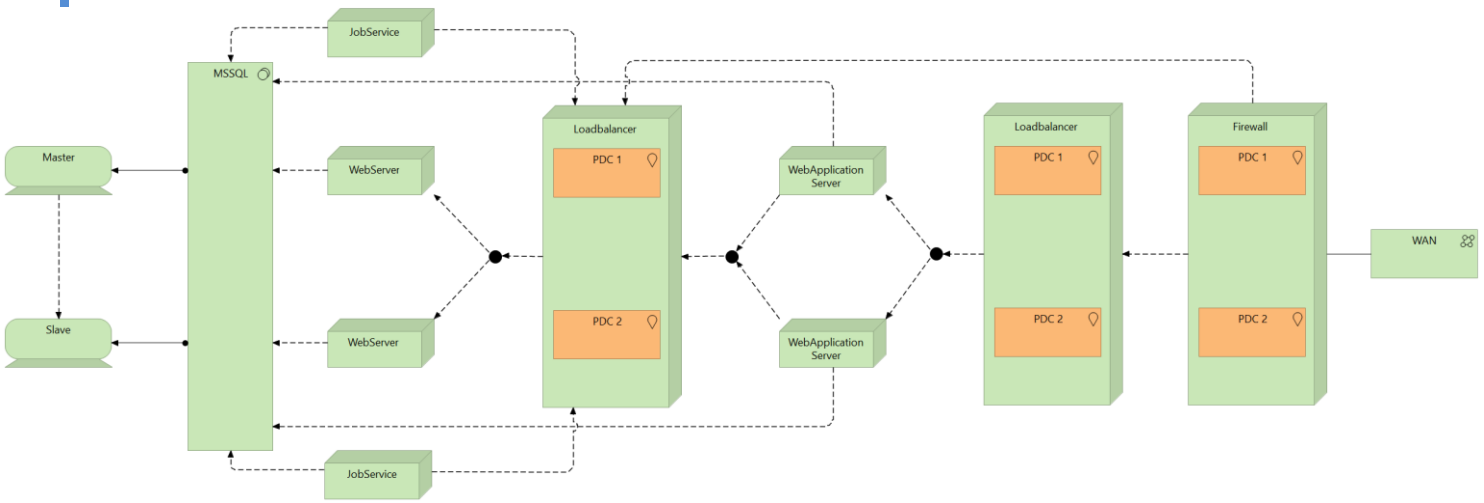
9.3.2 Applicatie laag



Figuur 13: Applicatie laag

De monoliet Force.Mortgages is het centrale componenten welke wordt ondersteunt door de overige componenten. De componenten NHG Gateway en Morality hebben een koppeling met externe componenten van derde partijen.

9.3.3 Infrastructuur laag



Figuur 14: Infrastructuur laag

De infrastructuur is verdeeld over twee datacenters, namelijk PDC 1 en PDC 2. Er wordt gebruik gemaakt van 4 type servers, namelijk applicatieservers, webservers, databaseservers en ten slotte JobService servers voor de afhandeling van de taken uit de workflow engine (zie Figuur 13: Applicatie laag).

9.4 Detailarchitectuur per component

Voor elk component is er een gedetailleerd model gemaakt. Hoewel er meestal volgens een bottom-down volgorde wordt gemodelleerd in ArchiMate, is er in dit speciale geval voor gekozen om vanuit de applicatie laag te modelleren. De reden hiervoor is dat de scope zich in plaats van op business niveau, focust op applicatieniveau. Vanuit de applicatie is gekeken welke businessprocessen er ondersteund worden en welke gemodelleerd dienen te worden. Deze werkvolgorde voorkomt het modelleren van businessprocessen die niet door de componenten binnen de scope worden geraakt.

Bij het modelleren van deze componenten zijn de meeste ontwerpprincipes met betrekking tot het detailniveau van de modellen in acht genomen. Dit zijn de ontwerpprincipes OP-06, OP-08, OP-09 en OP-10.

Nr	Ontwerpprincipe
OP-06	Als de businesslaag bruikbaar gemodelleerd moet worden, dienen businessprocessen niet verder worden onderverdeeld dan sub-processen omdat dit buiten de scope van Enterprise Architecture valt en aan procesmodeleertools overgelaten dient te worden (Winter & Fischer, 2006).
OP-08	Als de applicatielaag bruikbaar gemodelleerd moet worden, dienen dataobjecten niet gedetailleerd beschreven te worden omdat dit beter gedaan kan worden door datamodelleer-tools en talen zoals UML (Winter & Fischer, 2006).
OP-09	Als de applicatielaag bruikbaar gemodelleerd moet worden, dient de interne werking van applicatiecomponenten niet gemodelleerd te worden omdat dit buiten de scope van Enterprise Architecture valt (Winter & Fischer, 2006).
OP-10	Als de infrastructuurlaag bruikbaar gemodelleerd moet worden, dienen gedetailleerde specificaties van IT-componenten zoals hardware specificaties buiten beschouwing gelaten te worden omdat deze niet essentieel zijn voor Enterprise Architecture (Winter & Fischer, 2006).

Tabel 11: Toegepaste ontwerpprincipes

Hoewel ontwerpprincipe OP-07 ook over het detailniveau gaat, is deze niet volledig meegenomen. Het ontwerpprincipe zegt iets over het detailniveau op applicatieniveau, namelijk dat er niet in te veel detail moet worden getreden bij het modelleren van de applicatielaag. In dit onderzoek is het echter zo dat Topicus juist inzicht wil krijgen in haar softwarecomponenten en dat daarom een hoog detailniveau op applicatieniveau juist wenselijk is.

Nr	Ontwerpprincipe
0P-07	Als de datalaag bruikbaar gemodelleerd moet worden, dienen zaken als interfacebeschrijvingen en remote procedure calls buiten beschouwing worden gelaten in de architectuurmodelering omdat deze een te hoog detailniveau vereisen (Winter & Fischer, 2006).

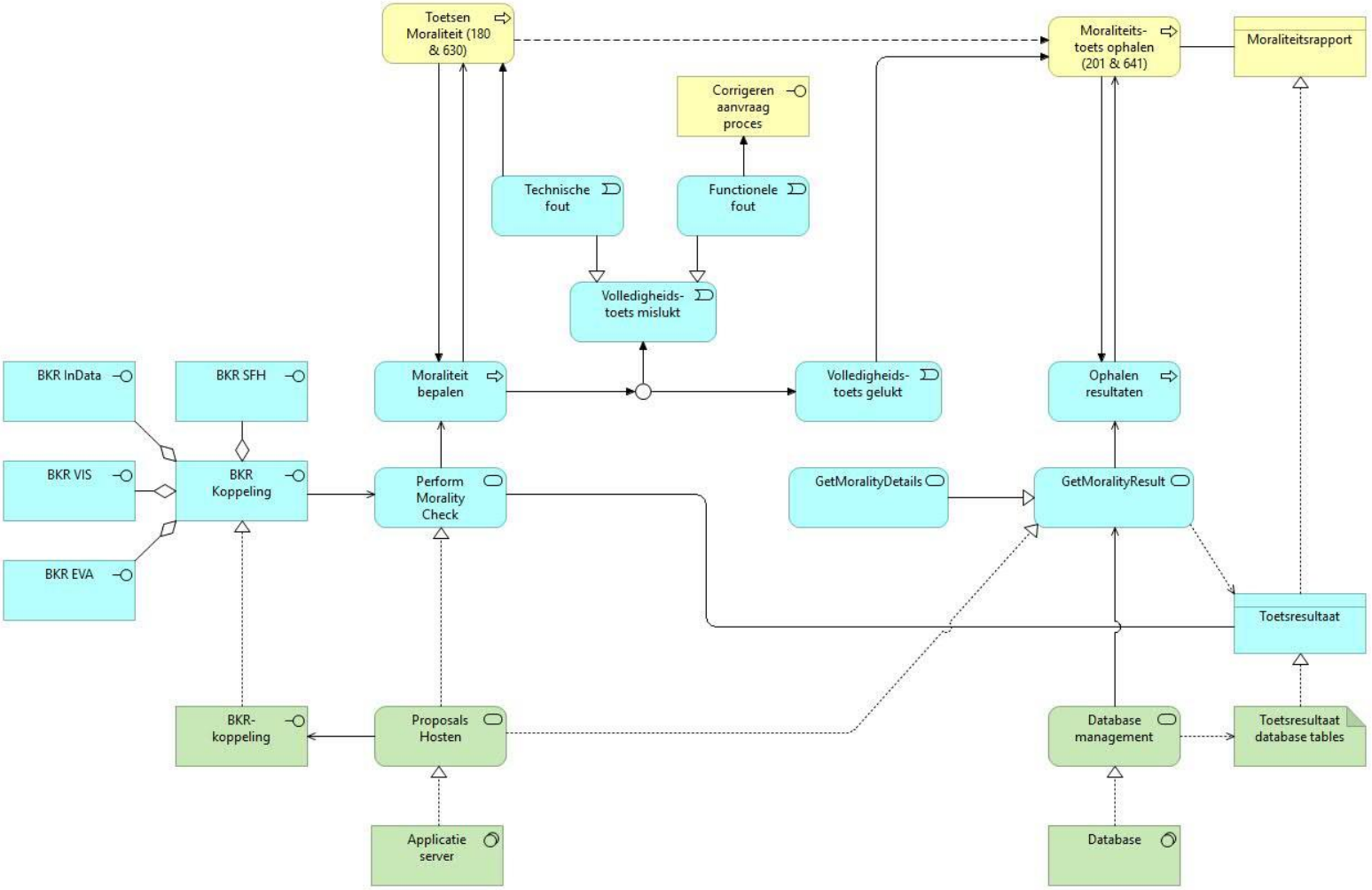
Tabel 12: Ontwerpprincipe OP-07

Ontwerpprincipe OP-07 is daarom aan de kaak gesteld. Twee van de componenten, Morality en NHG Gateway, zijn gemodelleerd vanuit procesmatig oogpunt. Er is gekeken hoe de communicatie tussen de interne componentonderdelen loopt en aan de hand daarvan is er een model opgesteld. Met deze twee modellen wordt er getracht om de ‘communicatieflow’ in het component weer te geven om daarmee inzicht te krijgen in datalocaties en mogelijk ook datastromen.

De twee andere componenten, Proposals en Agreements, zijn anders gemodelleerd. Deze componenten zijn opgebouwd volgens de applicatiearchitectuur Microsoft Application Architecture Guide, 2nd Edition. De modellen van deze twee componenten zijn vanuit het oogpunt van deze applicatiearchitectuur opgebouwd. Dit houdt in dat er niet is gekeken hoe de communicatieflow in het component is, maar uit welke sub-componenten het component bestaat en wat hun onderlinge relatie is.

Door de componenten op deze twee verschillende manieren te modelleren wordt er dubbel getoetst of Enterprise Architecture geschikt is voor het identificeren van tekortkomingen in GDPR-compliance en of ontwerpprincipe OP-07 correct is.

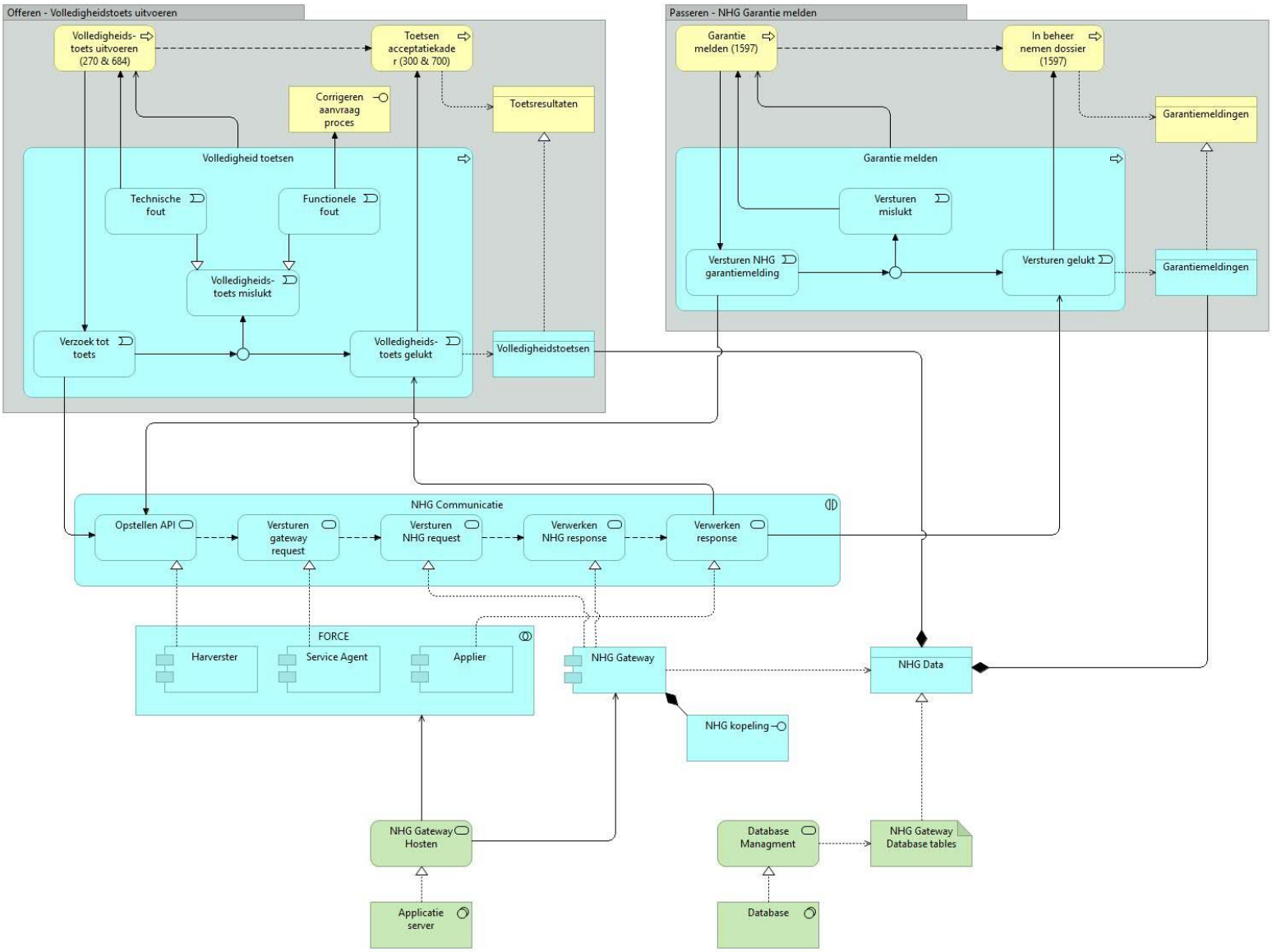
9.4.1 Morality



Figuur 15: Morality

Voor het businessproces *Toetsen Moraliteit* dient er een aanvraag richting BKR gestuurd te worden voor het uitvoeren van een aantal toetsen. Deze resultaten worden vervolgens teruggestuurd naar het Morality-component en opgeslagen in de bijbehorende database. Wanneer dit succesvol is gelukt zal de workflow engine de status doorzetten naar het businessproces *Moraliteitstoets ophalen.* Hierbij wordt het dataobject moraliteitsrapport opgehaald en klaargezet voor het volgende proces.

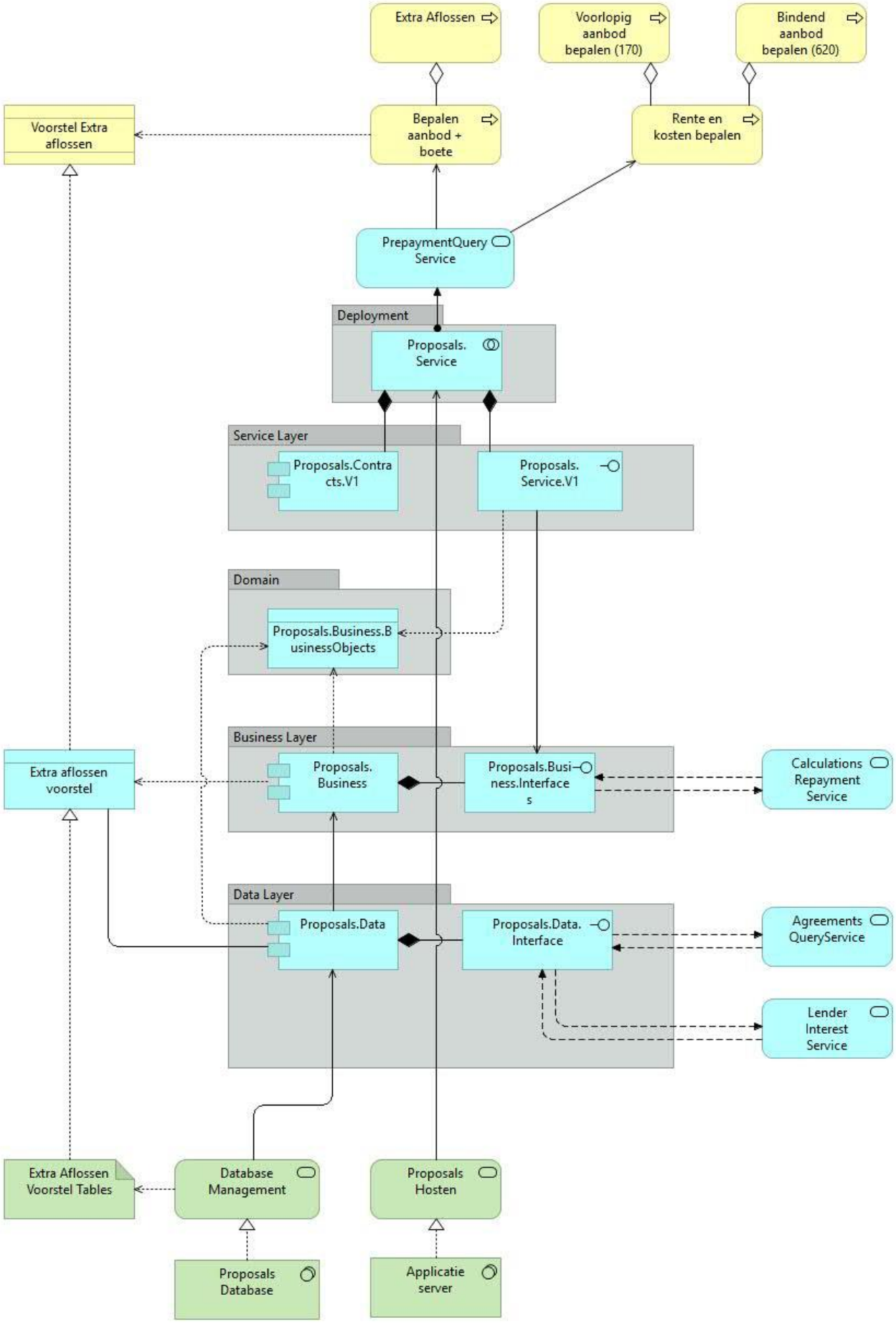
9.4.2 NHG Gateway



Figuur 16: NHG Gateway

De NHG Gateway voorziet de communicatie tussen FORCE en NHG. Het heeft hierbij twee hoofdfuncties waarvan de eerste het uit laten voeren van volledigheidstoetsen is om na te gaan of een hypotheekaanvraag in aanmerking komt voor NHG. De tweede hoofdfunctie is het melden aan NHG dat een hypotheek onder NHG is verstrekt. Zowel de testresultaten als de garantiemeldingen worden opgeslagen in de database van het component.

9.4.3 Proposals

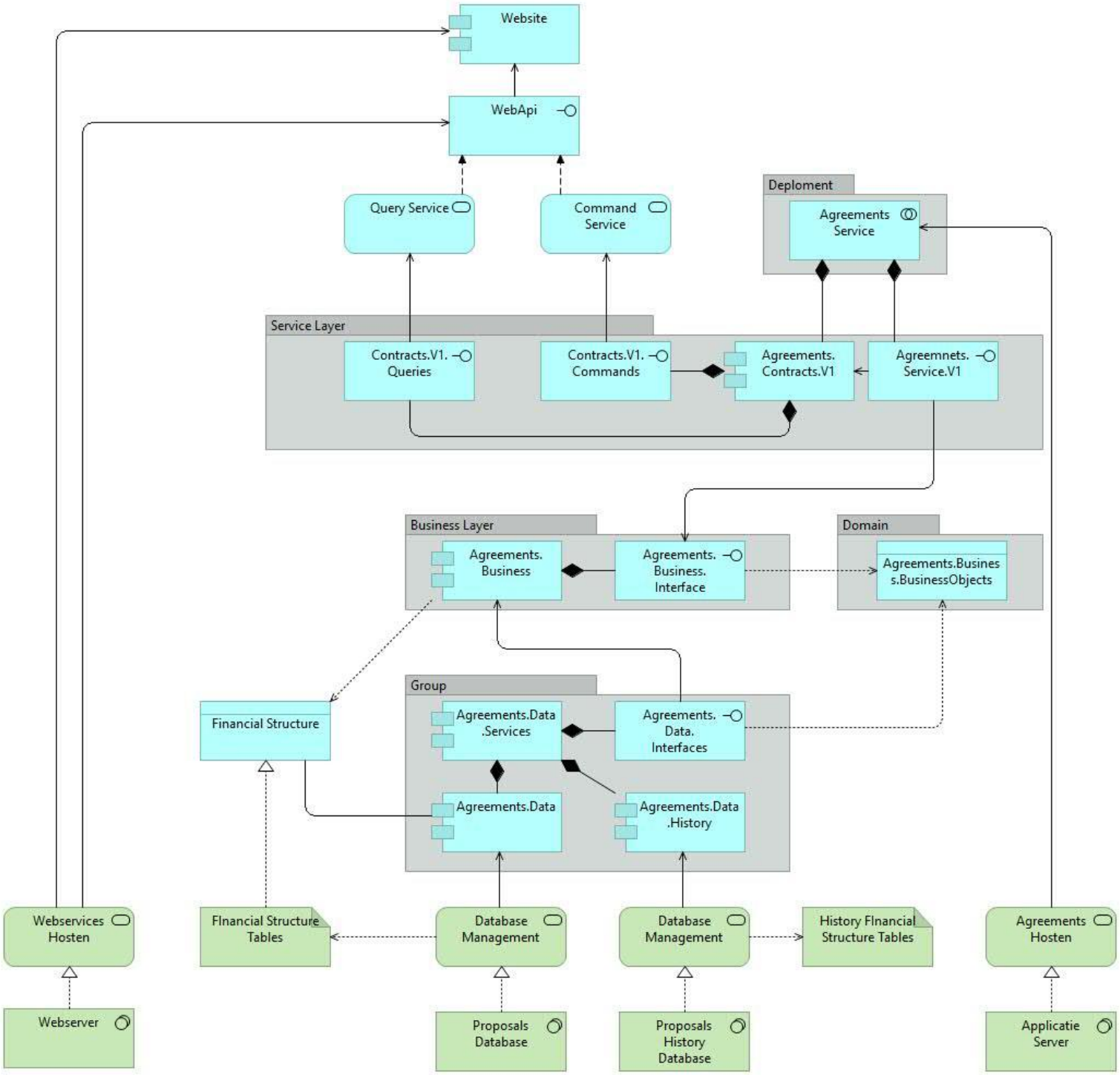


Figuur 17: Proposals

In de huidige situatie wordt het component Proposals gebruikt voor het bepalen van de rente en kosten die aan een hypotheek gebonden zijn. Deze rente en kosten worden berekend wanneer er een hypotheekvoorstel aan een consument wordt gedaan. Er zijn koppelingen tussen Proposals en andere componenten gerealiseerd om deze berekeningen uit te kunnen voeren. Er wordt hierbij geen data opgeslagen in het component.

Topicus is op het moment bezig met het toevoegen van de Extra aflossen-functionaliteit. Wanneer een consument extra wil aflossen, wordt er in het component een aanbod en boete bepaald die voorgelegd wordt aan de klant. Al deze voorstellen zullen worden bewaard in een database die gekoppeld is aan het component.

9.4.4 Agreements

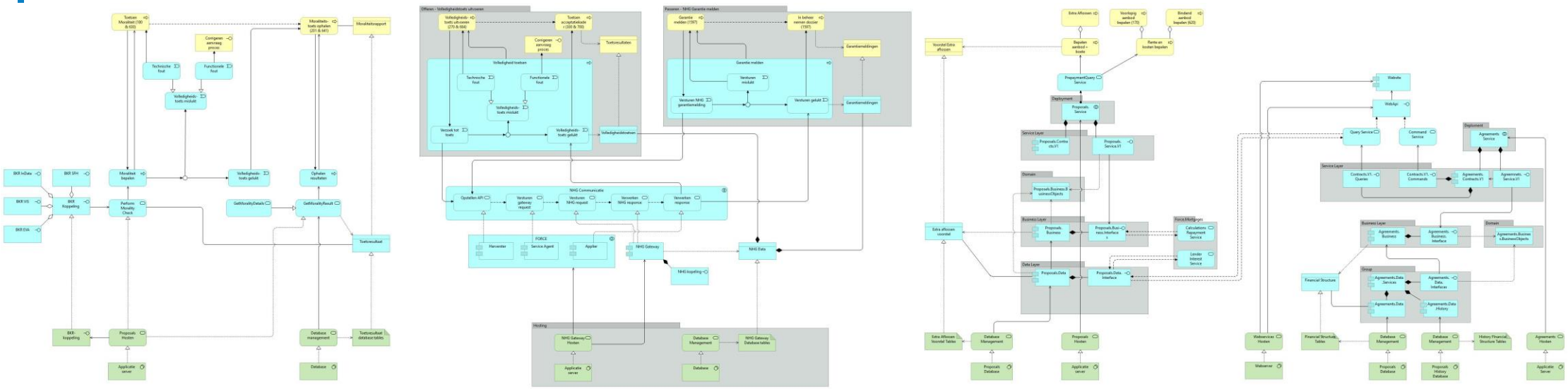


Figuur 18: Agreements

Het component Agreements is volledig gericht op het opslaan en ophalen van hypothecaire financieringsovereenkomsten. Het component heeft hiervoor een query service en een command service. De query service verzorgt de leesoperaties en de command service verzorgt de schrijfoperaties.

Naast het component is er een website die de UI van het component realiseert. De WebApi zorgt voor de koppeling tussen het component en de website.

9.5 Volledige Architectuurplaat



Figuur 19: Volledige Architectuurplaat

In het bovenstaande figuur is de volledige architectuurplaat weergegeven. Hierbij zijn de onderlinge relaties van de componenten en businessprocessen weergegeven. Om de afbeelding van een te groot formaat is, wordt er aangeraden om de afbeelding te bekijken in de losse bestanden die zijn bijgeleverd.

10 Analyse

In dit hoofdstuk worden de architectuurplaten naast de GDPR gelegd zodat er geanalyseerd kan worden of tekortkomingen in GDPR-compliance af te leiden van de architectuurplaten. Hierbij wordt er dus antwoord gegeven op deelvraag 8: welke maatregelen op data-, applicatie- en infrastructuurniveau dienen er nog te worden genomen om aan deze eisen te voldoen? Zoals reeds aangegeven in paragraaf 6.6 wordt er gekeken naar de verwerkingshandelingen verzamelen, vastleggen en opslaan van persoonsgegevens. Samen met de User requirements vormen zij de zaken die afgeleid moeten kunnen worden uit de architectuurplaten.

Voor deze analyse zal allereerst worden behandeld wat er wél uit de architectuurplaten afgeleid kan worden. Vervolgens worden de zaken die niet uit de architectuurplaten afgeleid kunnen worden behandeld en wordt er besproken hoe het komt dat deze zaken niet afgeleid kunnen worden uit de architectuurplaten. Tot slot komen de tekortkomingen in GDPR-compliance aan bod.

10.1 Wat kan er afgeleid worden?

De zaken die Topicus wenst af te leiden uit de architectuurplaat worden weergegeven door de User Requirements. Ter herhaling zijn de User requirements weergegeven in Tabel 13: User requirement.

Afkorting	Requirement
UR01	Uit de architectuurplaat moet af te leiden zijn uit welke informatiesystemen data wordt verzameld.
UR02	Uit de architectuurplaat moet af te leiden zijn in welke businessprocessen er data wordt verzameld.
UR03	Uit de architectuurplaat moet af te leiden zijn waar data opgeslagen wordt.
UR04	Uit de architectuurplaat moet af te leiden zijn welke data opgeslagen wordt.
UR05	Er mag maar van één modelleertaal en bijbehorende modelleertool gebruik gemaakt worden.

Tabel 13: User requirements

Het antwoord op de User requirement UR01 is ja: uit de architectuurplaten kan worden afgeleid worden waar data vandaan komt. Koppelingen met andere informatiesystemen zijn goed te modelleren in ArchiMate. Er kan duidelijk worden aangegeven dat er data uit een ander informatiesysteem overkomt wat vervolgens in FORCE of een van haar componenten wordt opgeslagen.

User Requirement UR02 kan ook positief beantwoord worden. Uit te architectuurplaten is af te leiden welke componenten van FORCE welke businessprocessen ondersteunen. Vanuit deze componenten is vervolgens af te leiden waar en uit welke informatiesystemen er data wordt verzameld.

In tegenstelling tot de antwoorden op UR01 en UR02 ligt het antwoord op UR03 iets genuanceerder. Dit komt doordat het antwoord op deze User requirement gedeeltelijk ja is: Ja er is af te leiden waar data wordt opgeslagen, maar het is niet met zekerheid te zeggen of dit alle locaties zijn waar data wordt opgeslagen. In paragraaf 10.2 zal dit verder worden toegelicht.

Hetzelfde geldt voor het antwoord op UR04. Ja, uit de architectuurplaat is af te leiden welke data er opgeslagen wordt, maar dit is maar gedeeltelijk mogelijk. Ook hierover meer in paragraaf 10.2.

Het antwoord op User Requirement UR05 heeft een relatie met de antwoorden op UR03 en UR04. De antwoorden op UR03 en UR04 blijven ‘ja, gedeeltelijk’ wanneer UR05 in stand blijft en er dus maar van één modelleertaal en tool gebruikt mag worden. Echter, het antwoord op deze twee User requirements zou anders kunnen zijn wanneer er van UR05 afgeweken zou mogen worden waarover meer in paragraaf 10.3.

10.2 Wat kan er niet afgeleid worden?

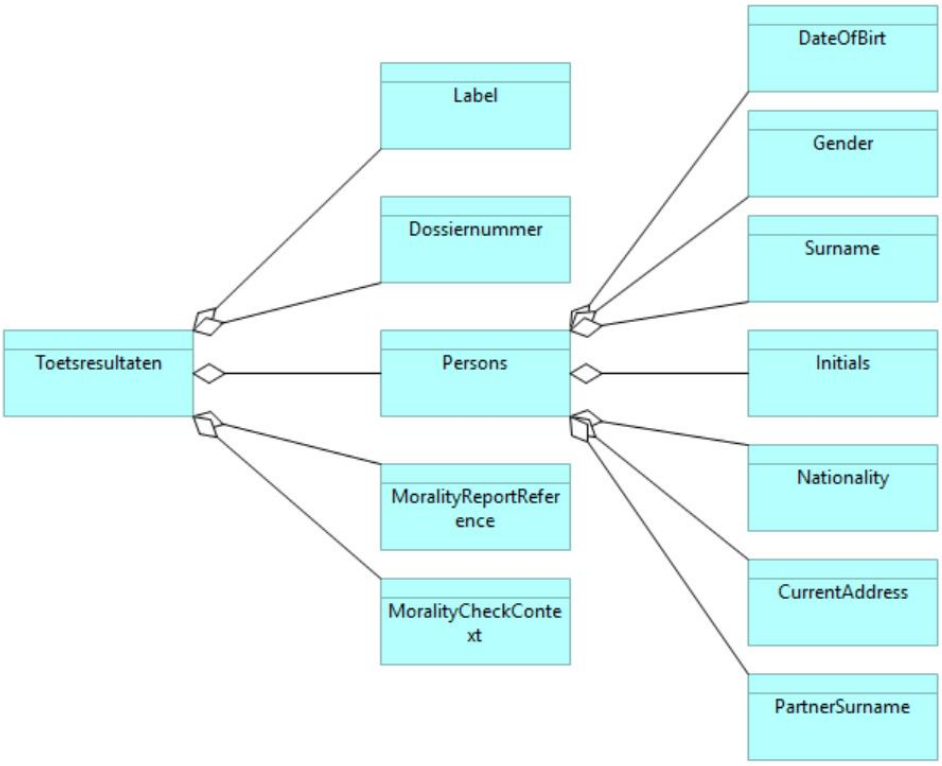
In paragraaf 10.1 is aangegeven dat de antwoorden op User requirements UR03 en UR04 ‘ja, gedeeltelijk’ zijn. In deze paragraaf wordt uitgelegd waarom het antwoord ‘gedeeltelijk’ bevat.

Allereerst wordt er gekeken naar UR03. Zoals aangegeven in paragraaf 10.1 is er af te leiden waar data staat, maar is het niet te garanderen dat dit alle locaties zijn waar data wordt opgeslagen. Zo zijn databases wel af te leiden uit de architectuurplaten, maar de opslaglocaties van bijvoorbeeld logbestanden niet. Zoals aangegeven in paragraaf 4.2.1 van de probleemanalyse is juist het identificeren van datalocaties buiten de FORCE-database van belang voor Topicus. De architectuurplaten bieden hierin dus niet voldoende oplossing voor het probleem.

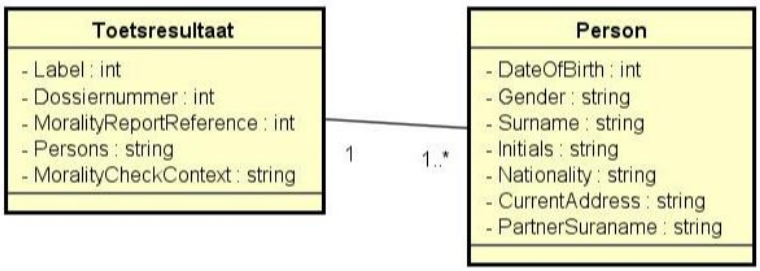
Voor UR04 geldt dat er uit de architectuurplaat globaal afgeleid kan worden welke data er opgeslagen wordt, maar niet tot in detail. Een voorbeeld hiervan is de architectuurplaat van Morality. Uit die plaat is op te maken dat er toetsresultaten wordt opgeslagen in de database. Echter is er niet af te leiden welke gegevens er precies worden opgeslagen zoals NAW-gegevens, leeftijd, hypotheeksoort, onderpand, renteperiode etc.

10.3 Oorzaken

De oorzaken voor de in paragraaf 10.2 genoemde problemen hebben te maken met Enterprise Architecture en User requirement UR05. Sommige dingen zijn simpelweg niet of niet goed met Enterprise Architecture en dus ArchiMate te modelleren. Een voorbeeld hiervan is data. Theoretisch gezien kan alle relevante data van bijvoorbeeld toetsresultaten weergegeven worden in een architectuurplaat. Hier zitten echter veel nadelen aan. Zo kan bijvoorbeeld niet aangeven worden of een datagegeven verplicht of optioneel is en hoeveel instanties ervan kunnen zijn. Ook moet er voor elk gegeven een apart “blokje” in de architectuurplaat worden weergegeven zoals in In Figuur 20: Voorbeeld datamodelring in ArchiMate te zien is. In dit figuur is een deel van het datamodel van Toetsresultaten gemodelleerd in ArchiMate afgebeeld. In Figuur 21: Voorbeeld datamodellering in UML is hetzelfde datamodel gemodelleerd in een UML Classdiagram.



Figuur 20: Voorbeeld datamodelring in ArchiMate



Figuur 21: Voorbeeld datamodellering in UML

Zoals uit de figuren op te maken is en ontwerpprincipe OP-08 ook aangeeft, zijn tools zoals UML Classdiagrammen veel beter en efficiënter in het modelleren van datamodellen dan Enterprise Archtiecture.

Dit probleem geldt tevens voor het modelleren van een gedetailleerde interne opbouw van applicaties. Data die bijvoorbeeld door een service call wordt aangeroepen of verstuurd is zeer lastig, dan wel niet te modelleren in Enterprise Architecture. Dit komt doordat ArchiMate niet ontwikkeld is om interne applicatiewerking te modelleren maar om relaties tussen business, applicatie en systeem te modelleren. Modelleertools zoals UML Sequence diagrammen zijn hier veel beter en efficiënter in.

10.4 Tekortkomingen

Het gevolg van de in paragraaf 10.3 genoemde oorzaken is dat het lastig is om tekortkomingen in GDPR-compliance te ontdekken. Hoewel de architectuurplaten het wel inzichtelijker maken welke databases er zijn, geldt dit niet voor andere dataopslaglocaties. Tevens is het niet inzichtelijk welke data er precies opgeslagen wordt. Een tekortkoming in GDPR-compliance die daarom geïdentificeerd kan worden is dat de Record Retention functionaliteit niet alle databases raakt. Door middel van de architectuurplaten is het wel inzichtelijk welke databases aan welke componenten hangen en welke dus geraakt moeten worden door de Record Retention functionaliteit.

Daarnaast kan er gesteld worden dat de onwetendheid over welke data er opgeslagen wordt, een tekortkoming in GDPR-compliance op zichzelf is. Immers, hoe kan er aan dataminimalisatie worden gedaan wanneer het onbekend is welke data er wordt opgeslagen? Zoals uit de vorige paragrafen van dit hoofdstuk blijkt is Enterprise Architectuur alleenstaand niet in staat om dit inzicht te bieden, maar zijn er wel aanwijzingen dat dit kan in combinatie met UML-diagrammen. Deze samenwerking van methodieken en modellen zou daarom verder onderzocht moeten worden.

11 Conclusie

In de vorige vijf hoofdstukken is er antwoord gegeven op de deelvragen. Vanuit deze antwoorden kan er antwoord worden gegeven op de hoofdvraag. Echter voor dat er antwoord wordt gegeven op de hoofdvraag zullen de antwoorden op de deelvragen ter herhaling kort worden samengevat.

11.1 Antwoord op de deelvragen

In deze paragraaf worden de antwoorden op de deelvragen kort samengevat. Voor verdere uitwerking van de antwoorden wordt er verwezen daar de bijbehorende hoofdstukken.

1. **Wat is de GDPR? – H6**
   De GDPR is een Europese verordening wat je allemaal mag doen met persoonsgegevens en hoe je deze gegevens moet beschermen (Ministerie van Justitie en Veiligheid).

2. **Welke eisen stelt de GDPR aan Topicus op data, applicatie- en infrastructuurniveau? – H6**
   Er moet een grondslag zijn voor het verzamelen van persoonsgegevens, er moet ontwikkeld worden door middel van Privacy by Design, er moet een gegevensbeschermingsbeleid zijn en mensen moeten controle kunnen uitoefenen op de omgang met hun persoonsgegevens.

3. **Wat is Enterprise Architecture en hoe dient dit toegepast te worden binnen Topicus? – H8 & H9**
   Enterprise Architecture is goed gedefinieerde uitoefening van ondernemingsanalyse, -ontwerp, -planning en -implementatie waarbij er altijd gebruik wordt gemaakt van dezelfde architecturele aanpak op business, informatie, proces en technologieniveau (Feaderation of EA Professional Organizations, 2013). Binnen Topicus dient dit toegepast te worden door middel van het TOGAF framework.

4. **Hoe zijn de componenten FORCE.Mortages, Proposals, Morality, Agreements en NHGGateway opgebouwd zoals gemodelleerd door middel van Enterprise Architecture? – H9**
   De componenten zijn opgebouwd volgens de Microsoft Application Architecture Guide. 2nd Edition. Gemodelleerd door middel van Enterprise Architecture resulteert dit in de architectuurplaten.

5. **Hoe zijn de businessprocessen die worden ondersteund door de componenten FORCE.Mortages, Proposals, Morality, Agreements en NHGGateway ingericht? – H9**
   De businessprocessen die ondersteund worden door de relevante componenten zijn gemodelleerd in de architectuurplaten.

6. **Waar worden deze componenten geraakt door de GDPR op data-, applicatie- en infrastructuurniveau? – H6 & h10**
   De componenten worden door de GDPR op data- en applicatieniveau geraakt wanneer er in een ondersteund businessproces persoonsgegevens worden verzameld en wanneer er uit een ander informatiesysteem persoonsgegevens worden verzameld. De componenten worden op infrastructuurniveau geraakt wanneer er data wordt opgeslagen in een database.

7. **Welke maatregelen heeft Topicus reeds genomen om aan de GDPR-eisen te voldoen? – H6**
   De belangrijkste maatregel is dat Topicus de Record Retention functionaliteit heeft ontwikkeld voor de centrale FORCE-database.

8. **Welke maatregelen op data-, applicatie- en infrastructuurniveau dienen er nog te worden genomen om aan de GDPR-eisen te voldoen? – H10**
   Topicus dient de Record Retention functionaliteit uit te breiden naar alle databases. Daarnaast dient er onderzocht te worden of er meer tekortkomingen in GDPR-compliance kunnen worden geïdentificeerd door Enterprise Architecture te combineren met UML. Hier kunnen mogelijk verdere maatregelen op worden gebaseerd.

11.2 Antwoord op de hoofdvraag

Nu er antwoord is gegeven op alle deelvragen kan er antwoord worden gegeven op de hoofdvraag, namelijk *"Welke tekortkomingen aan GDPR-compliance van de componenten FORCE.Mortages, Proposals, Morality, Agreements en NHGGateway binnen de hypotheekoplossing FORCE kunnen worden geïdentificeerd door middel van Enterprise Architecture en welke maatregelen kunnen hierop gebaseerd worden?"*

Zoals in hoofdstuk 10 is aangegeven is er maar een tekortkoming in GDPR-compliance te identificeren aan de hand van de architectuurplaten. Dit betreft de Record Retention functionaliteit die op het moment nog alleen maar data uit de FORCE-database verwijdert en niets uit de databases van de losse componenten. De enige maatregel die hierop gebaseerd kan worden is dan ook dat de Record Retention functionaliteit uitgebreid moet worden zodat deze ook data uit de andere databases verwijderd.

11.3 Discussie

Naar aanleiding van de beperkte hoeveelheid af te leiden tekortkomingen kan de vraag worden gesteld of Enterprise Architecture wel geschikt is om tekortkomingen in GDPR-compliance te identificeren en of Topicus Enterprise Architecture hiervoor moet toepassen. Het advies en antwoord op deze vraag is "nee, maar…". De onderbouwing en verdere toelichting voor dit antwoord is in de komende alinea's uitgewerkt.

In hoofdstuk 10 is naar voren gekomen dat er zaken zijn die niet uit de architectuurplaat afgeleid kunnen worden. De belangrijkste zaken zijn hier de opslaglocaties van data zoals logbestanden en databases, en de gedetailleerde informatie over het type data dat wordt opgeslagen, zoals NAW-gegevens, schulden, medische informatie, etc. Het zijn juist deze zaken waar Topicus inzicht in wil krijgen. Het is daarom dat Enterprise Architecture niet de volledige oplossing is voor de problemen die Topicus ondervindt.

Toch is het niet zo dat Enterprise Architecture en de architectuurmodellen volledig nutteloos zijn voor Topicus. Wanneer er naar de oorzaak-gevolgdiagram uit de probleemanalyse wordt gekeken, worden er toch een aantal oorzaken (deels) weggenomen door Enterprise Architecture en de architectuurmodellen. Zo ontstaat er documentatie over de architectuur, komt er een vast architectuurframework en worden datalocaties (deels) bekend. Ook ontstaat er een duidelijk overzicht van onderlinge koppelingen van systemen en componenten.

De Enterprise Architecture-modellen brengen het overzicht dat nodig is, maar niet het detailniveau dat ook nodig is. Uit de analyse van hoofdstuk 10 blijkt dat er UML-diagrammen dit detail mogelijk wel kunnen brengen. Een combinatie van Enterprise Architecture voor het overzicht en UML-diagrammen voor het detail is daarom mogelijk de oplossing die Topicus zoekt. Zo zouden bijvoorbeeld UML Classdiagrammen kunnen helpen bij het bepalen van data die door de Record Retention functionaliteit verwijderd moet kunnen worden. Het antwoord op de vraag of Topicus Enterprise Architecture toe dient te passen luidt daarom: Nee, opzichzelfstaand biedt Enterprise Architecture niet voldoende inzicht, maar mogelijk wel in combinatie met UML. Het advies luidt dan ook om deze combinatie verder te onderzoeken.

11.4 Beperkingen en suggesties voor verder onderzoek

Dit onderzoek kent enkele beperkingen. In deze paragraaf worden deze beperkingen behandeld en worden er suggesties voor verder onderzoek gedaan.

Een van de beperkingen van dit onderzoek is dat er alleen is gekeken naar de architectuurplaten die door middel van ArchiMate zijn gemodelleerd. De architectuurplaten zijn echter maar een deel van wat Enterprise Architecture en de bijbehorende frameworks inhouden. Afhankelijk van het gekozen Enterprise Architecture framework zijn er meerdere modellen, structuren en documenten die uitgewerkt en toegepast kunnen worden om Enterprise Architecture toe te passen in de organisatie. Mogelijk biedt deze uitgebreidere toepassing van Enterprise Architecture een beter inzicht in de GDPR-compliance van Topicus.

Een andere beperking is dat er in dit onderzoek (en met name in het literatuuronderzoek) alleen is gekeken naar Enterprise Architecture als oplossing voor Topicus' probleem. Zoals in de architectuurprincipes is aangeven, is Enteprise Architecture niet geschikt is voor een zeer hoog detailniveau. Aan de hand hiervan had er misschien al naar andere applicatie- en datamodelleertechnieken gekeken moeten worden. Hoewel het doel van het onderzoek was om expliciet de toepasbaarheid van Enterprise Architecture te onderzoeken, heeft dit mogelijk geleid tot een tunnelvisie.

Zoals in paragraaf 11.3 is aangegeven is het mogelijk dat Enterprise Architecture en de architectuurplaten wel toepasbaar zijn voor het identificeren van tekortkomingen in GDPR-compliance wanneer het gecombineerd wordt met andere tools en modelleertalen. Deze tools en modelleertalen kunnen Enterprise Architecture aanvullen en daarmee de gebreken ervan (zoals genoemd paragraaf 10.2) wegnemen. Voorbeelden van dit soort tools zijn UML klasse- en sequence-diagrammen. Waar bijvoorbeeld een architectuurplaat het overzicht kan bieden van dataobjecten in een applicatie, kan het klasse diagram een gedetailleerde weergaven van de daadwerkelijke data weergeven. Deze oplossing zou echter in strijd zijn User requirement UR05, namelijk dat er maar gebruik gemaakt mag worden van één modelleertaal en bijbehorende modeleertool. Topicus zou van deze User requirement af kunnen wijken en onderzoeken of deze oplossing werkt.

Tot slot is het de vraag of de uitkomst van het onderzoek ook geldt voor andere bedrijven dan Topicus. Topicus is een organisatie die als core business het ontwikkelen van software heeft. Het probleem dat Topicus ondervindt ligt dan ook in de software en de code. Gegeven dat juist het modelleren van data en software niet goed uitvoerbaar is met ArchiMate, verklaart dat het niet goed werkt voor Topicus. Daarnaast is de architectuur van Topicus relatief beperkt en kent Topicus al haar softwarecomponenten goed, omdat het haar core business is. Echter hoeft dit niet zo te zijn wanneer een organisatie een andere core business dan softwareontwikkeling heeft; applicaties worden ter ondersteuning van die core business gebruikt. Zou de architectuur van een dergelijke organisatie zeer groot zijn, dan bestaat de kans dat men door Enterprise Architecture bijvoorbeeld achter het bestaan van een database komt waarvan men in eerste instantie het bestaan niet eens wist. Daarom zou er verder onderzoek gedaan moeten worden naar toepasbaarheid van Enterprise Architecture voor het bepalen van GDPR-compliance binnen organisaties die een andere core business hebben dan IT.

12 Reflectie

Het afgelopen half jaar bestond voor mij uit een aantal intensieve maanden. Na een stroeve start met het Plan van Aanpak kon ik eindelijk beginnen met mijn vooronderzoek. De probleemanalyse verliep gelukkig vrij snel en vlot. De mensen die ik heb gesproken voor de probleemanalyse hebben veel bruikbare informatie kunnen leveren waardoor het probleem en de achterliggende oorzaken vrij snel duidelijk werden. Dit bevorderde zeker de snelheid waarmee ik door de probleemanalyse heen ging. Ook was ik goed gemotiveerd om het daadwerkelijke probleem boven tafel te krijgen. Ook denk ik zeker dat ik met de juiste mensen heb gesproken om het probleem in kaart te brengen. Daardoor ben ik er vrij zeker van dat het probleem dat in de probleemanalyse wordt beschreven ook daadwerkelijk het probleem is.

De contextanalyse en behoefteanalyse waren echter een ander verhaal. Helaas vond ik het lastig om bij deze twee analyses de vaart erin te houden. Dit resulteerde in een erg langdurig vooronderzoek. Ik merkte dat ik totaal niet opschoot en ook vaak moeite had om me te concentreren op het verwoorden van de analyses die ik had gedaan. Het uitdenken en verzamelen van data ging prima, alleen het op papier zetten bleek een lastige klus. Omdat ik van mijzelf wist dat ik er wel vaker lang over doe om iets op papier te krijgen, had ik hier juist voor mezelf een doel gesteld om dit niet weer te laten gebeuren. Ik was daarom ook fanatiek begonnen met het PvA en de probleemanalyse, maar het ging hierna helaas mis. Ik denk dat hier twee oorzaken voor zijn. Allereerst vind ik iets uitschrijven gewoon niet leuk waardoor ik er lastig doorheen kom. Ten tweede denk ik dat de lange doorlooptijd ook kwam door de hoeveelheid feedback die ik kreeg. Hoewel de feedback goed, terecht en uitgebreid was, zorgde dit er bij mij wel voor dat ik enigszins gedemotiveerd raakte om de feedback te verwerken. Voor mijn doen had ik al heel wat geschreven en daar erg mijn best voor gedaan. Dat ik daarna te horen krijg dat ik dingen moet aanpassen, omgooien of toevoegen werkt voor mij, hoewel de feedback wel terecht is, helaas demotiverend. Ik moet dan namelijk weer bezig gaan met schrijven. Dit is zeker een iets waar ik mijzelf in de toekomst in moet verbeteren. Het kost namelijk onnodig veel tijd die anders effectief gebruikt zou kunnen worden.

Toch denk ik wel dat het resultaat van de context- en behoefteanalyse wel van goede kwaliteit is. Voor zaken als de requirements heb ik heel vaak met de stakeholders gepraat en gebrainstormd om er zeker van te zijn dat de requirements juist waren. Daarnaast is er door de docenten uitgebreid feedback gegeven die is verwerkt.

Het literatuuronderzoek vind ik lastig om te beoordelen. Hoewel ik denk dat ik goede informatie heb gevonden en ook heb gevonden waar ik naar op zoek was, heeft er misschien toch enige tunnelvisie plaatsgevonden. In het literatuuronderzoek is informatie gevonden die aangaf dat Enterprise Architecture niet heel geschikt is om gedetailleerd data en applicaties te modelleren. Hier is verder niet op doorgezocht. Zo is er niet veel verder onderzocht hoe dit wel zou moeten. Er zijn wel enige vermoedens ontstaan hoe dit zou moeten, zoals UML, maar er is niet verder naar gekeken. Naast dat dit misschien ook wel buiten de scope viel, was er door de langdurige behoefte- en contextanalyse ook geen tijd meer voor.

Na het literatuuronderzoek ben ik begonnen met het modelleren van de componenten. Dit was zeker een lastige opgave. De componenten zijn vrij uitgebreid en soms ook best complex. Het hielp niet altijd mee dat lang niet elk component goed gedocumenteerd is. Wel is het zo dat ik van mening ben dat dit bij heeft gedragen aan architectuurplaten waarvan ik de correctheid zeer hoog acht. Doordat niet alles altijd even goed gedocumenteerd was, ben ik zeer kritisch naar de informatie gaan kijken. Op het moment dat zaken naar mijn mening net niet helemaal klopten of net iets te vaag waren, ben ik er verder ingedoken. Ik heb mensen aangesproken om achter de juiste informatie te komen en ik heb de architectuurplaten ook bij hen geverifieerd.

Ook denk ik dat ik systematisch gezien goed te werk ben gegaan met het modelleren van de architectuurplaten. Door eerst een globale opbouw van een component in beeld te krijgen, was ik in staat om verder detail aan te brengen. Helaas was het hier ook zo dat ik met sommige architectuurplaten langer bezig was dan met andere. Dit kwam deels doordat er niet altijd evenveel gedocumenteerd was, maar

ook doordat ik dan moest wachten op een afspraak met een medewerker van Topicus om deze informatie boven tafel te krijgen. Hier was ik denk ik soms toch iets te passief in. Ik merkte dat ik vaak het sturen van mailtjes om een afspraak te maken uitstelde. Waarom weet ik niet goed, maar toch stond ik niet te springen om dit te doen. Misschien uit angst dat een medewerker er niet zo veel zin in had of er geen tijd voor zou hebben. Uiteindelijk was dit natuurlijk allesbehalve waar. De medewerkers van Topicus waren juist zeer behulpzaam en enthousiast wanneer ik hen om hulp vroeg. Ik moet in de toekomst gewoon vaker om hulp vragen en niet bang zijn voor een negatieve reactie.

Wanneer het aankomt op de conclusie ben ik wel tevreden, maar er zijn ook zaken die beter hadden gekund. Zo denk ben ik van mening dat ik goed heb kunnen beantwoorden wat de opdrachtgevers wilde weten. Na een presentatie die ik bij Topicus heb gegeven heb ik hier met hen ook even over nagepraat. Zij gaven toen ook aan dat ze inderdaad gewoon antwoord wilden op de vraag of ze Enterprise Architecture toe moeten passen, en waarom wel of niet. Het antwoord dat het mogelijk alleen werkt met UML is voor hen duidelijk en te begrijpen. De ideeën zijn er zelfs om, wanneer er een nieuw component gebouwd moet worden, dit met Enterprise Architecture in combinatie met UML te doen naar aanleiding van mijn onderzoek. Dit geeft zeker een goed gevoel aangezien mijn onderzoek dus niet voor niets is geweest en de opdrachtgevers het ook zeker kunnen waarderen. Wat beter had gekund aan mijn conclusie, was dat ik graag had onderzocht of Enterprise Architecture in combinatie met UML daadwerkelijk de oplossing was geweest. Voor nu blijft dat helaas alleen bij een vermoeden.

De laatste twee maanden van het onderzoek waren voor mij best wel zwaar. Doordat ik achterliep op de planning heb ik tijd in moeten halen. Een aantal keer heb ik een heel weekend gespendeerd aan het op papier uitwerken van mijn onderzoek. Ik merkte dat, naarmate de deadline dichterbij kwam, ik veel sneller en geconcentreerder kon werken dan eerst. Ik wilde dan ook koste wat het kost de eerste deadline halen zodat ik niet hoefde te verlengen. Dit zorgde er echter wel voor dat ik bijvoorbeeld de hele kerstvakantie met de scriptie bezig ben geweest. Hoewel ik de deadline dus netjes gehaald heb, ben ik niet tevreden met de manier waarop. Het heeft me veel vrije tijd gekost, terwijl ik het ook gewoon tijdens ‘werktijd’ had kunnen doen als ik aan het begin meer had gedaan. Ik denk dat ik in de toekomst meer harde deadlines voor mijzelf moet zetten. De enige harde deadlines waar ik mezelf nu aan hield, waren de momenten waarop ik iets op moest leveren voor feedback. Dit zorgde ervoor dat ik eens in de maand een harde deadline had, terwijl het beter zou zijn om dit bijvoorbeeld eens per twee weken te hebben.

Uiteindelijk ben ik tevreden met het resultaat. Op een paar punten na denk ik dat ik een goed en bruikbaar onderzoek heb opgeleverd. Het grootste verbeterpunt voor mij is het stellen van harde tussentijdse deadlines. Door mij hier beter aan te houden moet ik op schema kunnen blijven met het onderzoek en zou alles netjes op tijd af moeten zijn.

13 Bibliografie

Autoriteit Persoonsgegevens. (sd). *Data protection impact assesment (DPIA) | Autoriteit Persoonsgegevens*. Opgeroepen op november 19, 2018, van autoriteitpersoonsgegevens.nl: https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia

Boot, L. (2018, september 11). (R. Stam, Interviewer)

De Autoriteit Persoonsgegevens. (2018). *De AVG in een notendop.* Opgehaald van https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/avg_in_een_notendop.pdf

de Boer, D. (2014). Architectuurmethoden & Frameworks. *Inleiding Architectuur 2*. Saxion.

de Boer, S. (2005). *Meso level analysis*.

De Vos, K. (2013). *Brainstormen.* Pearson Benelux B.V.

Dingemanse, K. (2015, september 8). *Soorten interviews*. Opgehaald van www.scribbr.nl: https://www.scribbr.nl/onderzoeksmethoden/soorten-interviews/

Feaderation of EA Professional Organizations. (2013). Common Perspectives on Enterprise Architecture. *Architecture and Governance Magazine*(9-4).

Foresight. (2018, April 12). *Macro, Meso and Micro environment*. Opgehaald van foresightcards: https://foresightcards.com/background-information/macro-meso-and-micro-environment/

Goethals, F. G. (2005, mei). An Overview of Enterprise Architecture Framework Deliverables. *SSRN Electronic Journal*. doi:10.2139/ssrn.870207

Haveman, K., Hageraats, E., & van der Linden, S. (2016, September). Ontwerponderzoek. *Reader Ontwerponderzoek v2*. Enschede.

Institute For Enterprise Architecture Developments. (2005). *Trents in Enterprise Architecture 2005: How are Organizations Progressing?* Web-based enquête, Institute For Enterprise Architecture Developments. Opgehaald van http://ce.sharif.edu/courses/87-88/1/ce448/resources/root/eap-trend2005.pdf

Intemarketing . (2018, Juni 9). *DESTEP analyse*. Opgehaald van intemarketing: http://www.intemarketing.nl/marketing/analyses/destep

Ipswitch. (2014, novermber 12). *European IT Teams Woeful Lack of Preparation for General Data Protection Regulation (GDPR) May Mean Painful Compliance Audits Ahead* . Opgehaald van www.ipswitch.com: https://www.ipswitch.com/about/news-and-events/ipswitch-news/european-it-teams-woeful-lack-of-preparation-for-general-data-protection-regulation-may-mean-painful-compliance-audits-ahead

Ishikawa, K. (1990). *Introduction to Quality Control.* (J. H. Loftus, Vert.) 3a Corporation.

Janssen, T. (2010). De onderzoekende docent. In T. Janssen, *Academisch werk in uitvoering: opleiden, onderzoek en onderwijs in de Academische Opleidingsschool Amsterdam* (pp. 35-58). Amsterdam: Vossiuspers. Opgehaald van https://dare.uva.nl/search?identifier=98de39dc-448b-4ba4-bfa0-b76cad2b4c85

Kadenic, V. (2015). *Compliance of Data Lake Enterprise Architecture Model with the General Data Protection Regulation (GDPR).* Bacheor Thesis, Luleå University of Technology, Department of

Computer science, Electrical and Space engineering. Opgehaald van http://www.diva-portal.org/smash/get/diva2:1022086/FULLTEXT02.pdf

Krul, A. (2014, april 24). *Hoe doe je deskresearch?* Opgehaald van www.scribbr.nl: https://www.scribbr.nl/scriptie-structuur/hoe-doe-je-deskresearch/

Lankhorst, M., & van Drunen, H. (2007). *Enterprise Architecture Development and Modelling: Combining TOGAF and ArchiMate.* Artikel, Via Nova Architectura. Opgehaald van http://api.ning.com/files/1vDSdWV6JAgpNXvLL9hU3l21jWMxztv9AzOoqrfwJLi-U79-UyYIIu1ll34yynga44xabZUmLaOdAiTUJx1I1K8btmziOt3N/Lankhorst.pdf

Miller, R. (2008). *What are requirement types?* Opgehaald van searchsoftwarequality.techtarget: https://searchsoftwarequality.techtarget.com/answer/What-are-requirements-types

Ministerie van Justitie en Veiligheid. (sd). *avg_brochure_wat_betekend_het_voor_jou_als_ondernemer.pdf.* Opgeroepen op oktober 6, 2018, van Autoriteit Persoonsgegevens: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/avg_brochure_wat_betekent_het_voor_jou_als_ondernemer.pdf

NATO. (2018, augustus 01). *NATO-NATO architecture Framework, Version 4*. Opgehaald van https://www.nato.int/cps/en/natohq/topics_157575.htm

Ohlhorst, F. J. (2012). *Big Data Analytics: Turning Big Data into Big Money.* Wiley & Sons.

Preston, L., Post, J., & Sachs, S. (2002). Managing the extended enterprise: The new stakeholder . *California Management Review 45 (1)*, 6-28.

Rijksoverheid. (sd). *Autoriteit Persoonsgegevens | Contact | Rijksoverheid.nl*. Opgeroepen op november 19, 2018, van rijksoverheid.nl: https://www.rijksoverheid.nl/contact/contactgids/autoriteit-persoonsgegevens

Schermer, B. W., Hagenauw, D., & Falot, N. (2018). *Handleiding Algemene verordening gegevensbescherming.* Ministerie van Justitie en Veiligheid.

Spijkerman, W. (2018, september 26). (R. Stam, Interviewer)

Tang, A., Han, J., & Chen, P. (2004). A Comparative Analysis of Achitecture Frameworks. Busan, Korea. doi:10.1109/APSEC.2004.2

The Open Group. (2005). *The Open Group Architectural Framwork (TOGAF) Version 7 - an open, industry consensus framework and method for IT Architecture*. Opgehaald van http://pubs.opengroup.org/architecture/togaf7-doc/arch/

The Open Group. (2016). *What is New in Archimatte 3.0.1? | The Open Group*. Opgehaald van http://www3.opengroup.org/subjectareas/enterprise/archimate/3.0-whats-new

Topicus. (2017, november 10). Agreements. Opgeroepen op oktober 23, 2018, van https://confluence.topicus.nl/display/FPD/Agreements

Topicus. (2017, december 11). Force.Morality component. Opgeroepen op oktober 10, 2018, van https://confluence.topicus.nl/display/FPD/Force.Morality+component

Topicus. (2018, februari 9). GDPR. Opgeroepen op september 19, 2018, van https://confluence.topicus.nl/display/FPS/GDPR

Topicus. (2018, februari 9). GDPR - Definitief voorstel. Opgeroepen op november 19, 2018, van https://confluence.topicus.nl/display/FPS/GDPR+-+Definitief+voorstel+09-02-2018

Topicus. (2018, februari 15). Moraliteitsbepaling. Opgeroepen op oktober 22, 2018, van https://confluence.topicus.nl/display/FPD/Moraliteitbepaling

Topicus. (2018, oktober 5). Mortgages Proposals. Opgeroepen op oktober 23, 2018, van https://confluence.topicus.nl/display/FPS/Mortgages+Proposals

Topicus. (2018, mei 28). NHG. Opgeroepen op oktober 23, 2018, van https://confluence.topicus.nl/display/FPD/NHG

Topicus. (sd). *IT met impact in finance door meer grip op je financien*. Opgeroepen op oktober 23, 2018, van topicus.nl: https://topicus.nl/campagnes/impact-finance/?_ga=2.197042028.1178228046.1540297777-1536640918.1535961860

Topicus. (sd). *Topicus & Finance: Grip op je financiële toekomst met connected banking*. Opgeroepen op oktober 23, 2018, van topicus.nl/finance: https://topicus.nl/finance/?_ga=2.152948857.1178228046.1540297777-1536640918.1535961860

Urbaczewsk, L., & Mrdalj, S. (2006, januari). A comparison of enterprise architecture frameworks. Opgehaald van https://www.researchgate.net/publication/253110513_A_comparison_of_enterprise_architecture_frameworks

van Vliet, H. (2008). *Software Engineering: Principles and Practices* (3e ed.). Chichester (UK): Wiley.

Varvasovszky, Z., & Brugha , R. (2000, september 1). A stakeholder analysis. *Health Policy and Planning*, 338-345. doi:https://doi.org/10.1093/heapol/15.3.338

Winter, R., & Fischer, R. (2006). Essential Layers, Artifacts, and Dependencies of Enterprise Architecture. *10th IEEE International Enterprise Distributed Object Computing Conference Workshops (EDOCW'06).* Hong Kong, China: IEEE. doi:10.1109/EDOCW.2006.2

Zachman, J. (1999). A Framework for Information System Architecture. *IBM Systems Journal 38*, 454-470. doi:10.1147/sj.382.0454

Zachman, J. A. (2008, januari). *About the Zachman Framework*. Opgehaald van https://www.zachman.com/about-the-zachman-framework

14 Figurenlijst

Figuur 1: Schematische weergave ontwerponderzoek 8
Figuur 2: Micro, Meso en Macro omgeving (Foresight, 2018) 10
Figuur 3: Voorbeeld van een Oorzaak-gevolgdiagram 11
Figuur 4: Oorzaak-gevolgdiagram 15
Figuur 5: FORCE 20
Figuur 6: De AVG in een notendop (De Autoriteit Persoonsgegevens, 2018) 28
Figuur 6: Macht-belangdiagram 37
Figuur 8: Het Zachman Framework (Zachman J. A., About the Zachman Framework, 2008) 44
Figuur 9: Relatie tussen TOGAF ADM en ArchiMate (The Open Group, 2016) 45
Figuur 10: DYA denk- en werkmodel 46
Figuur 11: Het FEAF Framework 47
Figuur 12: Business laag 51
Figuur 13: Applicatie laag 51
Figuur 14: Infrastructuur laag 51
Figuur 15: Morality 53
Figuur 16: NHG Gateway 54
Figuur 17: Proposals 55
Figuur 18: Agreements 57
Figuur 19: Volledige Architectuurplaat 58
Figuur 20: Voorbeeld datamodelring in ArchiMate 60
Figuur 21: Voorbeeld datamodellering in UML 61
Figuur 22: Force Product Suite 2018 91

15 Tabellenlijst

Tabel 1 Versiehistorie 2
Tabel 2: Leeswijzer deelvragen 17
Tabel 3: Requirements translatie 36
Tabel 4: Macht en invloed stakeholders 37
Tabel 5: Business requirements bij een ja 40
Tabel 6: Business requirements bij een nee 40
Tabel 7: User requirements 41
Tabel 8: System requirements 42
Tabel 9: Ontwerpprincipes 49
Tabel 10: Ontwerpprincipes m.b.t. het gekozen architectuurframework 50
Tabel 11: Toegepaste ontwerpprincipes 52
Tabel 12: Ontwerpprincipe OP-07 52
Tabel 13: User requirements 59

16 Bijlage

16.1 Bijlage A: Architectuurprincipes FORCE

Key Design Principles

When getting started with your design, keep in mind the key principles that will help you to create an architecture that adheres to proven principles, minimizes costs and maintenance requirements, and promotes usability and extendibility. The key principles are:

- **Separation of concerns**. Divide your application into distinct features with as little overlap in functionality as possible. The important factor is minimization of interaction points to achieve high cohesion and low coupling. However, separating functionality at the wrong boundaries can result in high coupling and complexity between features even though the contained functionality within a feature does not significantly overlap.
- **Single Responsibility principle**. Each component or module should be responsible for only a specific feature or functionality, or aggregation of cohesive functionality.
- **Principle of Least Knowledge** (also known as the Law of Demeter or LoD). A component or object should not know about internal details of other components or objects.
- **Don’t repeat yourself (DRY)**. You should only need to specify intent in one place. For example, in terms of application design, specific functionality should be implemented in only one component; the functionality should not be duplicated in any other component.
- **Minimize upfront design.** Only design what is necessary. In some cases, you may require upfront comprehensive design and testing if the cost of development or a failure in the design is very high. In other cases, especially for agile development, you can avoid big design upfront (BDUF). If your application requirements are unclear, or if there is a possibility of the design evolving over time, avoid making a large design effort prematurely. This principle is sometimes known as YAGNI ("You ain’t gonna need it").

16.2 Bijlage B: Interviewvragen Stefan Hessels

- Waarom is GDPR-compliance een probleem?
- Waarom willen jullie kijken naar Enterprise Architecture en niet naar een ander concept of andere methodiek?
- In hoeverre hebben jullie inzicht in de datastromen?
- Wat wordt er verwacht van het project?
- Aan welke eisen moet het advies voldoen?

16.3 Bijlage C: Interviewvragen Wietze Spijkerman

Achtergrondinformatie voor Wietze

Allereerst even een stukje achtergrondinformatie zodat de context van mijn vragen duidelijker is.

Van Stefan Hessels heb ik begrepen dat er op het moment geen overzicht is van de onderlinge relaties van de verschillende componenten van de FPS. Denk hierbij aan datastromen, koppelingen etc. Dit resulteert erin dat, wanneer er een GDPR-audit plaats zou vinden, er geen bewijslast aangeleverd kan worden wat GDPR-compliance betreft. Het kan namelijk niet worden aangetoond dat persoonsgegeven X zich enkel in Component Y bevindt en niet in componenten waar dat persoonsgegeven niet persé nodig is.

Het idee van mijn afstudeeropdracht is dat Enterprise Architecture kan bijdragen aan het creëren van inzicht en overzicht van de FPS. Aan de hand van dit overzicht kunnen mogelijk tekortkomingen in GDPR-compliance worden geïdentificeerd en kunnen er maatregelen worden opgesteld.

Algemene vragen

- Wat houdt jouw functie precies in en waar ben je verantwoordelijk voor?
- Hoe wordt architectuur nu binnen Topicus (Finance) toegepast?
    - Welk(e) Framework(s)?
    - Welke onderdelen/componenten van die frameworks worden gebruikt?
    - Op welk detailniveau wordt er gewerkt?
    - Hoe komt dit in de dagelijkse werkzaamheden terug?
    - Etc.

Inzicht

- In hoeverre heb jij als architect inzicht in- en overzicht van de onderlinge relaties van de componenten in de FPS?
- Zou Enterprise Architecture voor jouw werkzaamheden van toegevoegde waarde kunnen zijn? En zo ja, hoe?
- Zou Enterprise Architecture volgens jou bij kunnen dragen aan uniformiteit (in de opbouw van componenten bijvoorbeeld) doordat er meer inzicht en overzicht wordt gecreëerd?

Eisen en randvoorwaarden

- Wanneer er een nieuw component wordt ontwikkeld, aan welke eisen en randvoorwaarden moet dit component dan voldoen?
- Hoe worden deze eisen en randvoorwaarden bepaald? Wordt hier bijvoorbeeld een component vanuit een framework gebruik zoals bijvoorbeeld architectuurprincipes?
- Als er standaard eisen en randvoorwaarden zijn, is hier dan een overzicht van?

16.4 Bijlage D: Vragen Maarten Schopman

Record Retention functionaliteit

- Hoe is het aangepakt? Hoe zijn jullie te werk gegaan? Welke stappen?
- Wat is de huidige status?
- Zijn er nog gaten?
- Wat voor eisen stellen klanten? Zijn er klanten misgelopen etc?
- Op welk detailniveau hebben jullie gekeken?
- Hebben jullie gekeken naar dataminimalisatie?
- Wordt het beleid periodiek herzien?
- Hoe erg hamert de klant op GDPR-compliance?
- Had het een hoge prioriteit voor het management?
- Stefan en Lennart geven aan dat er totaal geen inzicht is, kan je je daar in vinden?
- Kunnen jullie aantonen dat jullie compliant zijn?

Algemeen

- Gegevensbeschermingsbeleid: wordt op verzoek opgeleverd per specifieke afnemer. Is er een voorbeeld?
- Digitale beveiliging: hoe en wat? Inzichtelijk?
- Recht op inzage: wordt gebruik gemaakt van de UI, maar hoe wordt er nagegaan of data niet in een systeem staat waar het niet hoort?
- Record retention voor standaard componenten. Nevensystemen dus niet. Hoe kan er dan worden verzekerd dat daar data niet te lang staat?

16.5 Bijlage E: Uitwerking GDPR

Zoals reeds is aangegeven in de contextanalyse is de GDPR opgebouwd vanuit een zestal beginselen. Wanneer deze beginselen verder worden uitgewerkt tot de wet ontstaan er vier categorieën waarover de GDPR iets zegt. De uitwerking van de GDPR zal per categorie worden beschreven.

16.5.1 De grondslag

Persoonsgegevens mogen niet zomaar worden verzameld. Er moet een welbepaald, uitdrukkelijk omschreven en gerechtvaardigd doel zijn waarom persoonsgegevens dienen te worden verwerkt. Gegevens verzamelen omdat deze “in de toekomst nog wel eens van pas kunnen komen” is dus niet toegestaan. De verwerking van persoonsgegevens is gerechtvaardigd wanneer het doel van de verwerking is gebaseerd op minimaal één van de zes rechtsgrondslagen die in de Verordening worden gegeven. De zes rechtsgrondslagen zijn:

g) De betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meerdere specifieke doeleinden;
h) De verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen;
i) De verwerking is noodzakelijk om te voldoen aan wettelijke verplichtingen die op de verwerkingsverantwoordelijke rust;
j) De verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke person te beschermen;
k) Verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen;
l) De verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is.

De grondslagen b tot en met f zijn ‘noodzakelijkheidsgrondslagen’: alleen wanneer de verwerking noodzakelijk zijn voor de in deze grondslagen genoemde doelen, is de verwerking gerechtvaardigd. In de vraag of de verwerking noodzakelijk is ligt besloten of de verwerking van de persoonsgegevens proportioneel is en of het beoogde doel niet op een andere manier bereikt kan worden. Wanneer er hard gemaakt kan worden dat de verwerking van persoonsgegevens genoodzaakt is voor één van de onder b tot en met f genoemde doelen, hoeft er geen toestemming van de betrokkenen te worden gegeven.

16.5.2 Zorgvuldigheid

Het veilig verwerken van persoonsgegevens begint bij de tekentafel door de beginselen Privacy by Design en Privacy by Default in acht te nemen. Privacy by Design houdt in dat de verwerkingsverantwoordelijke danwel de gegevensverwerker al tijdens de ontwikkeling van producten en diensten privacy en gegevensbescherming mee neemt als eisen. Daarnaast dient er aan dataminimalisatie te worden gedaan. Dit houdt in dat er zo min mogelijk persoonsgegevens verwerkt dienen te worden en dat alleen de gegevens die noodzakelijk zijn voor het doel van de verwerkingen gebruikt mogen worden. Privacy by Default houdt in dat er technische en organisatorische maatregelen getroffen moeten worden om er voor te zorgen dat er, als standaard, alléén persoonsgegevens verwerkt worden die noodzakelijk zijn voor het specifieke doel dat bereikt wil worden (Topicus, 2018).

Wanneer er een voorgenomen verwerking van persoonsgegevens waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, dient er voorafgaand aan de verwerking een Data Protection Impact Assesment (DPIA) uitgevoerd te worden. Een goed uitgevoerde DPIA geeft inzicht in de

risico's die de verwerking oplevert voor de betrokkenen, en in de maatregelen die de verantwoordelijke moet nemen om de risico's af te dekken (Autoriteit Persoonsgegevens, sd).

De GDPR kent een belangrijke rol toe aan de functionaris gegevensbescherming (FG). De FG houdt intern toezicht op en adviseert over de toepassing en naleving van de GDPR binnen een organisatie. De FG is tevens het aanspreekpunt voor de betrokkene. Het aanstellen van een FG is niet altijd verplicht, maar is dit wel wanneer:

1. De organisatie een overheidsinstantie of overheidsorgaan is;
2. De organisatie hoofdzakelijk belast is met verwerkingen die vanwege hun aard, hun omvang en/of hun doeleinde regelmatige en stelselmatige observatie op grote schaal van betrokkenen vereisen;
3. De organisatie hoofdzakelijk belast is met verwerkingen die de grootschalige verwerking van bijzondere categorieën van persoonsgegevens en van persoonsgegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten behelzen.

16.5.3 Verplichtingen

Om de bescherming van persoonsgegevens te kunnen waarborgen dienen er een aantal technische en organisatorische maatregelen getroffen te worden. Allereerst dient er een verwerkingsregister bijgehouden te worden wanneer een organisatie uit meer dan 250 personen bestaat of wanneer:

- De verwerking waarschijnlijk een risico voor betrokkenen met zich meebrengt;
- De verwerking niet-incidenteel is;
- Er sprake is van de verwerking van bijzondere categorieën van persoonsgegevens of gegevens betreffende strafrechtelijke veroordelingen of strafbare feiten.

Het register van verwerkingsactiviteiten is een opsomming van de belangrijkste informatie over de verwerking van persoonsgegevens door een organisatie. In het register moeten de volgende onderdelen worden opgenomen:

- De naam van de organisatie en haar contactgegevens, of indien van toepassing die van haar vertegenwoordiger;
- Waar van toepassing de naam en contactgegevens van partijen waarmee de organisatie gezamenlijk verwerkingsverantwoordelijke bent;
- De contactgegevens van de functionaris voor gegevensbescherming als die is aangesteld;
- De verwerkingsdoeleinden;
- Een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens;
- De categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt, onder meer ontvangers in derde landen of internationale organisaties;
- Indien van toepassing, doorgiften van persoonsgegevens aan een derde land of een internationale organisatie. Daarbij dienen ook de documenten inzake de passende waarborgen te vermelden;
- Indien mogelijk, de beoogde termijnen waarbinnen de verschillende categorieën van gegevens moeten worden gewist;
- Indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen.

Naast het register dient er een gegevensbeschermingsbeleid te zijn. In de GDPR staat niet precies omschreven welke gegevens in het gegevensbeschermingsbeleid opgenomen moeten worden. Uit het beleid moet in ieder geval wel blijken hoe er wordt voldaan aan de GDPR als onderdeel van de

verantwoordingsplicht. Om aan te tonen dat er wordt voldaan aan de GDPR kan de volgende informatie opgenomen worden in het gegevensbeschermingsbeleid:

- Een omschrijving van de categorieën persoonsgegevens die worden verwerkt;
- Een beschrijving van de doeleinden waarvoor persoonsgegevens worden verwerkt en wat de juridische grondslag daarvan is;
- Hoe er wordt voldaan aan de beginselen van verwerking van persoonsgegevens zoals de verplichting om niet meer gegevens te verwerken dan noodzakelijk;
- Welke rechten betrokkenen hebben en hoe zij die rechten kunnen uitoefenen. Zoals het recht om een klacht in te dienen bij de Autoriteit Persoonsgegevens (AP). Maar ook het recht op inzage, wijzigen, wissen en het ontvangen van alle geregistreerde gegevens;
- Welke organisatorische en technische maatregelen er genomen zijn om de persoonsgegevens te beveiligen;
- Hoe lang de persoonsgegevens bewaart worden.

Verder dienen er passende technische en organisatorische maatregelen getroffen te worden om de persoonsgegevens die worden verwerkt te beveiligen. De beveiliging dient passend te zijn. Er hoeven dus niet persé de zwaarst mogelijke beveiligingsmaatregelen getroffen te worden, maar maatregelen die in verhouding staan tot de gegevens en de bijbehorende risico's voor de betrokkenen. Hoe groter het risico voor de betrokkenen, des te zwaarder de beveiligingsmaatregelen die getroffen moeten worden. Bij het vaststellen van passende beveiligingsmaatregelen dient rekening gehouden te worden met:

- De stand van de techniek;
- De uitvoeringskosten;
- De aard van de verwerking;
- De omvang van de verwerking;
- De context van de verwerking;
- De verwerkingsdoeleinden;
- De ernst van de vastgestelde risico's; en
- De waarschijnlijkheid dat de vastgestelde risico's zich zullen verwezenlijken.

De GDPR schrijft niet voor welke exacte maatregelen er genomen dienen te worden. Deze invulling laat de GDPR over aan de verwerkingsverantwoordelijke en de gegevensverwerker. Wel geeft het een aantal voorbeelden zoals:

- Pseudonimisering en versleuteling van de persoonsgegevens;
- Het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;
- Het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;
- Een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.

16.5.4 Rechten van de betrokkenen

Mensen moeten controle kunnen uitvoeren op de verwerking van hun persoonsgegevens. De betrokkene heeft daarom een aantal rechten die hij of zij uit kan oefenen tegen de verwerkingsverantwoordelijke.

16.5.4.1 Recht op informatie

Allereerst is er het recht op informatie. De betrokkenen hebben het recht om te weten wat er met hun persoonsgegevens gebeurt en waarom. Ook moeten zij bewust worden gemaakt van de risico's van de gegevensverwerking, de regels die ervoor gelden, de waarborgen en de manier waarop zij hun rechten met betrekking tot de verwerking van gegevens kunnen uitoefenen. Wanneer een organisatie direct gegevens bij de betrokkenen verzameld, dient de betrokkene te worden geïnformeerd over:

- De identiteit en contactgegevens van de verwerkingsverantwoordelijke c.q. diens vertegenwoordiger;
- De contactgegevens van de functionaris voor gegevensbescherming (indien aanwezig);
- De doeleinden waarvoor de persoonsgegevens zijn bestemd, inclusief de rechtsgrond voor de verwerking;
- De ontvangers of categorieën van ontvangers van de persoonsgegevens;
- Het voornemen de persoonsgegevens door te geven aan een derde land of een internationale organisatie, de aanwezigheid van besluiten zoals Privacy Shield of een indicatie van welke waarborgen er zijn en hoe een kopie kan worden verkregen danwel waar de gegevens kunnen worden geraadpleegd;
- De periode gedurende welke de persoonsgegevens worden opgeslagen, danwel de criteria waarop de termijn wordt bepaald;
- Dat de betrokkene het recht heeft om de verwerkingsverantwoordelijke te vragen om inzage, rectificatie of wissing van de persoonsgegevens of beperking van de verwerking te verzoeken
- Dat de betrokkene het recht heeft om tegen de verwerking bezwaar te maken en de verwerking te beperken;
- Dat de betrokkene het recht heeft op overdraagbaarheid van de persoonsgegevens;
- Dat de betrokkene, indien de verwerking gebaseerd is op toestemming, het recht heeft om de toestemming te allen tijde in te trekken;
- Dat de betrokkene het recht heeft om een klacht in te dienen bij een toezichthoudende autoriteit;
- Of de verstrekking van de persoonsgegevens een wettelijke of contractuele verplichting is, danwel een noodzakelijke voorwaarde om een overeenkomst te sluiten;
- Of de betrokkene verplicht is om de persoonsgegevens te verstrekken en wat de mogelijke gevolgen zijn wanneer deze gegevens niet worden verstrekt;
- Of er sprake is van geautomatiseerde besluitvorming, met inbegrip van profilering en nuttige informatie over de onderliggende logica en het belang en de verwachte gevolgen van die verwerking voor de betrokkene;

16.5.4.2 Recht op inzage

Iedere betrokkene heeft het recht om de persoonsgegevens die van hem verzameld zijn in te zien. Een betrokkene mag daarom met redelijke tussenpozen aan een organisatie vragen welke persoonsgegevens van hem worden verwerkt. Organisaties zijn verplicht om gehoor te geven aan dergelijke verzoeken en de beschikbare informatie te verstrekken. Wanneer een betrokkene een vraag op inzage indient moet het overzicht dat er wordt aangeboden tenminste de volgende informatie bevatten:

- De doelen waarvoor de gegevens worden verwerkt;
- De categorieën persoonsgegevens die van de betrokkene worden verwerkt;
- De ontvangers of categorieën van ontvangers aan wie de persoonsgegevens zijn of worden doorgegeven, met name ontvangers in derde landen of internationale organisaties;

- Indien mogelijk hoe lang de gegevens worden bewaard, of indien dat niet mogelijk is, de criteria om de bewaartermijn te bepalen;
- Het op recht op wijziging, verwijdering, beperking of bezwaar;
- Het recht om een klacht in te dienen bij de toezichthouder;
- Wanneer de persoonsgegevens niet bij de betrokkene worden verzameld, alle beschikbare informatie over de bron van die gegevens; en
- Het bestaan van geautomatiseerde besluitvorming waaronder profilering, en indien dit het geval is, nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene.

Tevens moet er een kopie van de gegevens van de betrokkene aan de betrokkene worden verstrekt wanneer deze daar om vraagt.

16.5.4.3 Recht op rectificatie

Vervolgens heeft de betrokkene recht op rectificatie. Wanneer er persoonsgegevens worden verwerkt, dienen deze gegevens accuraat te zijn en te blijven. Het kan voorkomen dat de gegevens niet (meer) kloppen. De betrokkene heeft dan het recht om deze gegevens te corrigeren.

16.5.4.4 Recht op beperking

Het recht op beperking van de verwerking van persoonsgegevens houdt in dat betrokkenen de mogelijkheid krijgen om de verwerking van hun persoonsgegevens tijdelijk ‘stil te laten zetten’. De gegevens mogen dan alleen nog worden verwerkt in de volgende gevallen:

- Met de toestemming van de betrokkene;
- Voor de instelling, uitoefening of onderbouwing van een rechtsvordering;
- Ter bescherming van de rechten van anderen of om gewichtige redenen van algemeen belang voor de Europese Unie of voor een lidstaat.

De betrokkene heeft niet altijd recht op beperking van de verwerking. Een betrokkene kan zijn recht op beperking in werking roepen in de volgende situaties:

- De juistheid van de persoonsgegevens wordt betwist door de betrokkene, gedurende een periode die de verwerkingsverantwoordelijke in staat stelt om de juistheid van de persoonsgegevens te controleren;
- De verwerking is onrechtmatig en de betrokkene verzet zich tegen het wissen van de persoonsgegevens en verzoekt in de plaats daarvan om beperking van het gebruik ervan;
- De verwerkingsverantwoordelijke heeft de persoonsgegevens niet meer nodig voor de verwerkingsdoeleinden, maar de betrokkene heeft deze nodig voor de instelling, uitoefening of onderbouwing van een rechtsvordering;
- De betrokkene heeft bezwaar gemaakt tegen de verwerking, in afwachting van het antwoord op de vraag of de gerechtvaardigde gronden van de verwerkingsverantwoordelijke zwaarder wegen dan die van de betrokkene.

16.5.4.5 Recht op verwijdering en recht om vergeten te worden

Onder bepaalde omstandigheden hebben betrokkenen het recht om hun gegevens door de verwerkingsverantwoordelijke te laten verwijderen, bijvoorbeeld wanneer de verwerking onrechtmatig is. Daarnaast heeft de betrokkene het recht om ‘vergeten te worden’. Dit recht is met name in het leven geroepen zodat mensen op het internet niet voor altijd (ten onrechte) met hun verleden worden geconfronteerd.

De betrokkene kan aanspraak maken op het recht op verwijdering in de volgende gevallen:

- De persoonsgegevens zijn niet langer nodig voor de doeleinden waarvoor zij zijn verzameld of anderszins verwerkt;
- De betrokkene trekt zijn toestemming voor het verwerken in en dit is de enige grondslag waarop de verwerking berust of kan berusten;
- De betrokkene heeft gegrond bezwaar gemaakt tegen de verwerking;
- De persoonsgegevens zijn onrechtmatig verwerkt;
- De persoonsgegevens moeten worden gewist om te voldoen aan een wettelijke verplichting die op de organisatie rust;
- De persoonsgegevens zijn verzameld in verband met een rechtstreeks aanbod van internetdiensten aan een kind.

Naast het recht op verwijdering heeft de betrokkene onder bepaalde omstandigheden ook het recht om 'vergeten te worden'. Dit recht ligt in het verlengde van het recht op verwijdering van gegevens. Het gaat dan om situaties waarbij de verwerkingsverantwoordelijke persoonsgegevens van de betrokkene openbaar heeft gemaakt (bijvoorbeeld door ze online te zetten) en de betrokkene aan de organisatie gevraagd heeft de gegevens te wissen. Naast het wissen van de gegevens uit de eigen systemen van de organisatie moeten redelijke technische en organisatorische maatregelen worden genomen om andere verwerkingsverantwoordelijken die de persoonsgegevens verwerken, ervan op de hoogte te stellen dat de betrokkene vergeten wil worden. Dit betekent dat iedere koppeling naar en kopie of reproductie van de gegevens gewist moet worden.

16.5.4.6 Recht op verzet

Een betrokkene kan onder omstandigheden bezwaar maken tegen de (verdere) verwerking van zijn gegevens en zijn recht op verzet inroepen. De verwerkingsverantwoordelijke moet dan de verwerking staken. De betrokkene kan zijn recht op verzet in een drietal situaties inroepen:

- De betrokkene kan vanwege persoonlijke omstandigheden bezwaar maken tegen verwerkingen die gebaseerd zijn op de grondslagen:
  - Noodzakelijk voor de uitoefening van een taak van algemeen belang of openbaar gezag; of
  - Het gerechtvaardigd belang van de verwerkingsverantwoordelijke.
- De verwerking van persoonsgegevens met het oog op marketing.
- De verwerking van persoonsgegevens voor wetenschappelijk of historisch onderzoek of voor statistische doeleinden.

16.5.4.7 Recht op overdraagbaarheid van gegevens (dataportabiliteit)

Het recht op overdraagbaarheid van persoonsgegevens geeft de betrokkene het recht om een kopie te krijgen van de persoonsgegevens die hij aan een organisatie heeft verstrekt. De kopie moet in een gestructureerde, gangbare en machineleesbare vorm (CSV, JSON, XML et cetera) worden verstrekt. Het doel van het recht op gegevensoverdraagbaarheid is de zeggenschap van de betrokkene over zijn gegevens te vergroten. Het achterliggende idee is dat de betrokkene zijn gegevens mee kan nemen naar bijvoorbeeld een andere aanbieder en daardoor minder gebonden is aan de oorspronkelijke verwerkingsverantwoordelijke.

16.5.4.8 Het recht niet onderworpen te worden aan geautomatiseerde individuele besluitvorming waaronder profilering

Wanneer persoonsgegevens worden gebruikt om tot een bepaalde beslissing te komen en deze beslissing is uitsluitend gebaseerd op geautomatiseerde verwerking van persoonsgegevens en dus zonder (noemenswaardige) menselijke tussenkomst, dan is er spraak van geautomatiseerde individuele besluitvorming.

Profilering (*profiling*) is het indelen van personen in categorieën (profielen) op basis van hun persoonsgegevens. Op basis van deze profielen kunnen vervolgens (geautomatiseerde) individuele besluiten worden genomen, zoals bijvoorbeeld het verlenen van krediet door een financiële instelling. Profilering kan op de volgende drie manieren worden ingezet:

1. Algemene profilering (nog zonder besluitvorming);
2. Besluitvorming gebaseerd op profilering;
3. Geautomatiseerde individuele besluitvorming gebaseerd op profilering.

Het verschil in toepassing 2 en 3 zit hem in de menselijke tussenkomst. Onder toepassing 2 is er nog sprake van noemenswaardige menselijke tussenkomst. Het profiel dient slechts ter ondersteuning van de besluitvorming, terwijl onder 3 het besluit geautomatiseerd wordt genomen en er geen sprake meer is van noemenswaardige menselijke tussenkomst.

Betrokkenen hebben het recht om niet onderworpen te worden aan een enkel op geautomatiseerde verwerking (waaronder profilering), gebaseerd besluit, wanneer dit rechtsgevolgen voor hen heeft of het hen anderszins in aanzienlijke mate treft. Hoewel deze bepaling in de GDPR als recht van de betrokkene is geformuleerd, gaat het in feite om een verbod voor de verwerkingsverantwoordelijke. Zo is een voorbeeld van profilering die mensen in aanzienlijke mate treft, het opstellen van een kredietwaardigheidsprofiel en enkel op basis dit profiel geautomatiseerde besluiten te geven om iemand geen lening te geven.

Echter zijn niet alle vormen van geautomatiseerde individuele besluitvorming verboden, ook al hebben zij rechtsgevolgen voor de betrokkenen of treffen zij hen in aanzienlijke mate. In de volgende situaties is het mogelijk om gebruik te maken van geautomatiseerde individuele besluitvorming, waaronder ook profilering:

- Wanneer dit noodzakelijk is voor de totstandkoming of de uitvoering van een overeenkomst tussen de betrokkene en een verwerkingsverantwoordelijke;
- Wanneer de betrokkene zijn uitdrukkelijke toestemming heeft gegeven;
- Wanneer dit is toegestaan bij een Unierechtelijke of lidstaatrechtelijke bepaling die op de verwerkingsverantwoordelijke van toepassing is en die ook voorziet in passende maatregelen ter bescherming van de rechten en vrijheden en gerechtvaardigde belangen van de betrokkene. (Voor profilering is dit niet geregeld in nationaal recht.)

16.6 Bijlage F: GDPR-standpunten Topicus

16.6.1 Grondslag

De GDPR maakt onderscheid tussen verwerkingsverantwoordelijken en gegevensverwerkers. Verwerkingsverantwoordelijken zijn de organisaties die persoonsgegevens verzamelen en gebruiken bij het uitvoeren van hun organisatorische werkzaamheden. Ze zijn er zelf direct eindverantwoordelijk voor dat de organisatie de GDPR naleeft en worden actief direct gemonitord door de toezichthouder. Gegevensverwerkers zijn organisaties die in opdracht van verwerkingsverantwoordelijken de opslag, verwerking en het gebruik van persoonsgegevens faciliteren middels softwaresystemen, databases, et cetera. Topicus vervult bij de verschillende implementaties van FORCE altijd de rol van gegevensverwerker of van sub-gegevensverwerker.

Standpunt Topicus

De verwerkingsverantwoordelijke dient zelf zorg te dragen dat er voldoende grondslag/ doelbinding is voor het vergaren, opslaan en verwerken van gegevens. Wel dient Topicus ervoor te zorgen dat zij als (sub-)gegevensverwerker voldoet aan de eisen met betrekking tot het toepassen van passende technische en organisatorische maatregelen ten behoeve van de bescherming van gegevens en daarmee de rechten van de betrokkenen. Ook dient Topicus ervoor te zorgen dat met elk van bovengenoemde partijen een zogenoemde "Verwerkersovereenkomst" is afgesloten. Deze "Verwerkersovereenkomst" dient te voldoen aan de hierin genoemde zaken: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/algemene-informatie-avg#waar-moet-de-verwerkersovereenkomst-onder-de-avg-aan-voldoen-5996.
In deze verwerkersovereenkomst dient te zijn opgenomen met welke ketenpartijen (denk o.a. aan NHG, BKR, ECH) de verwerkingsverantwoordelijke een overeenkomst heeft, en dat Topicus als (sub-)gegevensverwerker toestemming heeft om gegevens te verwerken die met deze partijen wordt uitgewisseld.
Alle grondslagen, behalve de toestemming van de gebruiker (betrokkene), zijn organisatorisch van aard en vergen op zichzelf geen verdere automatisering. Bij de toestemming van de gebruiker is dat mogelijk wel het geval, deze behandelen we daarom expliciet.

16.6.1.1 Toestemming van de gebruiker

In de GDPR staat vermeld dat de betrokkene toestemming moet hebben gegeven voor het registreren en verwerken van zijn/haar persoonsgegevens.

Standpunt Topicus

Het uitgangspunt van Topicus is dat de betrokkene in het gesprek met de adviseur eveneens toestemming geeft aan de geldverstrekker voor het verwerken van zijn persoonsgegevens voor de dienst van het beoordelen en eventueel verstrekken van een hypotheek. Deze toestemming zal vervolgens worden overgedragen aan de partij die deze beoordeling en verstrekking uitvoert. Voor de geldverstrekker die werkt met externe adviseurs gaat Topicus ervan uit dat de adviseur de toestemming heeft en het bewijs hiervan gedurende het aanvraag proces aanlevert. Op dit moment kan dit niet anders dan door middel van een dossierstuk worden aangeleverd. De inrichting van dit dossierstuk vergt configuratie die per klant moet worden uitgevoerd.
Topicus haakt graag aan bij initiatieven die het overdragen van toestemmingen of centrale registratie van toestemmingen binnen de gehele keten faciliteren.

16.6.2 Zorgvuldigheid

16.6.2.1 Functionaris gegevensbescherming

Vanaf het moment dat de GDPR in gaat kunnen organisaties in de rol van verwerkingsverantwoordelijke danwel gegevensverwerker verplicht zijn een functionaris voor de gegevensbescherming (FG) aan te stellen. Dit is iemand die binnen de organisatie toezicht houdt op de toepassing en naleving van de GDPR.

Standpunt Topicus

Topicus gaat een FG aanstellen. Topicus stelt de contactgegevens van de functionaris beschikbaar, deze worden uiterlijk 25 mei 2018 gedeeld.

16.6.2.2 Privacy by design en privacy by default

Privacy by design houdt in dat u als organisatie in de rol van verwerkingsverantwoordelijke danwel gegevensverwerker al tijdens de ontwikkeling van producten en diensten (zoals informatiesystemen) ten eerste aandacht besteedt aan privacyverhogende maatregelen, ook wel privacy enhancing technologies (PET) genoemd. Ten tweede houdt u rekening met dataminimalisatie: u verwerkt zo min mogelijk persoonsgegevens, dat wil zeggen alleen de gegevens die noodzakelijk zijn voor het doel van de verwerking. Op deze manier kunt u een zorgvuldige en verantwoorde omgang met persoonsgegevens technisch afdwingen.

Privacy by default houdt in dat u technische en organisatorische maatregelen moet nemen om ervoor te zorgen dat u, als standaard, alléén persoonsgegevens verwerkt die noodzakelijk zijn voor het specifieke doel dat u wilt bereiken.

Standpunt Topicus

FORCE verwerkt als oplossing van Topicus voor de hypothecaire markt in basis alleen persoonsgegevens die relevant zijn binnen het hypothecaire domein. Afhankelijk van het specifieke beleid van de verwerkingsverantwoordelijke danwel gegevensverwerker is het echter mogelijk dat bepaalde persoonsgegevens niet gebruikt worden voor alle of een bepaalde categorie aanvragen. FORCE als standaard product moet de volledige reikwijdte van beleid en soorten aanvragen kunnen ondersteunen. Het uitgangspunt van Topicus is dat de afnemer van het systeem alleen *die* gegevens opvraagt en invoert die relevant zijn op basis van zijn beleid en op basis van de specifieke aanvraag. Topicus gaat er derhalve van uit dat er alleen gegevens in FORCE terecht komen die relevant zijn voor de verwerking van hypothecaire aanvragen en het beheer van hypothecaire financieringen.
Afnemers van FORCE mogen van Topicus verwachten dat Topicus technische en organisatorische maatregelen neemt om zorg te dragen voor bescherming van privacygevoelige gegevens. Hoe Topicus dit heeft geregeld, staat beschreven onder "(Digitale) beveiliging".

16.6.2.3 Data protection impact assessment (DPIA)

Als verwerkingsverantwoordelijke moet een data protection impact assessment (DPIA) worden uitgevoerd wanneer de gegevensverwerking waarschijnlijk een hoog privacyrisico oplevert. De Autoriteit Persoonsgegevens geeft een aantal criteria om te toetsen of een verwerkingsverantwoordelijke een DPIA moet uitvoeren, zie hiervoor https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/data-protection-impact-assessment-dpia.

Standpunt Topicus

In de rol van gegevensverwerker hoeft Topicus niet *zelf* een DPIA uit te voeren voor haar klanten. Naar verwachting van Topicus zal elke verwerkingsverantwoordelijke waarvoor Topicus als gegevensverwerker optreedt (danwel gegevensverwerker waarvoor Topicus als sub-gegevensverwerker optreedt) een DPIA op de FORCE implementatie uit moeten voeren bij ingebruikname van nieuwe functionaliteit die betrekking heeft op privacygevoelige gegevens. Het spreekt voor zich dat Topicus hierbij ondersteuning zal bieden, informatie omtrent vastgelegde gegevens zal leveren en zal aangeven welke maatregelen Topicus zelf reeds heeft genomen om de privacygevoelige gegevens op organisatorisch en technisch niveau te beschermen. Zie hiervoor ook het standpunt van Topicus bij de punten "Verwerkingsregister", "Gegevensbeschermingsbeleid" en "(Digitale) beveiliging".

16.6.3 Verplichtingen

16.6.3.1 Verwerkingsregister

Op basis van zowel de organisatie-omvang van Topicus als op basis van de gegevens die Topicus (en haar klanten) verwerkt dient Topicus volgens de GDPR een verwerkingsregister bij te houden. (Zie ook https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/verantwoordingsplicht#ben-ik-verplicht-om-een-register-van-verwerkingsactiviteiten-op-te-stellen-6101, kopje "Is uw organisatie een 'verwerker'?")

Standpunt Topicus

Topicus dient in de rol van (sub-)gegevensverwerker te beschikken over een verwerkingsregister waarin de volgende gegevens zijn vastgelegd:

- Naam en contactgegevens van de verwerkingsverantwoordelijke
- Naam en contactgegevens van de Functionaris voor gegevensbescherming (FG) indien deze door Topicus is aangesteld
- Een beschrijving van de categorieën van verwerkingen die Topicus in opdracht van iedere verantwoordelijke uitvoert
- Naam en contactgegevens van eventuele andere internationale organisaties met wie Topicus persoonsgegevens deelt
- Naam en contactgegevens van eventuele landen of internationale organisaties buiten de EU met wie Topicus persoonsgegevens deelt
- Een algemene beschrijving van de technische en organisatorische maatregelen die Topicus heeft genomen om persoonsgegevens die zij verwerkt te beveiligen

Topicus stelt (het relevante deel van) het verwerkingsregister beschikbaar aan de verwerkingsverantwoordelijken en gegevensverwerkers waarvoor Topicus als (sub-)gegevensverwerker optreedt. Het verwerkingsregister en bijbehorende proces om deze bij te werken wordt uitgewerkt als onderdeel van dit GDPR initiative voor 25 mei 2018.

16.6.3.2 Gegevensbeschermingsbeleid

In de GDPR staat niet precies omschreven welke gegevens er in het gegevensbeschermingsbeleid (ook wel privacybeleid genoemd) moet opnemen. Uit het beleid moet in ieder geval wèl blijken hoe wordt voldaan aan de GDPR. Dat is onderdeel van de verantwoordingsplicht. U kunt laten zien hoe u voldoet aan de GDPR door onder andere deze informatie op te nemen (zie ook https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/verantwoordingsplicht#wat-moet-er-volgens-de-avg-in-een-gegevensbeschermingsbeleid-staan-6161):

Standpunt Topicus

In aanvulling op het verwerkingsregister zal Topicus ook een overzicht opstellen met per FORCE implementatie (oftewel: per verwerkingsverantwoordelijke waarvoor Topicus in opdracht als gegevensverwerker optreedt) de volgende gegevens:

- een omschrijving van de categorieën persoonsgegevens die worden verwerkt
- welke organisatorische en technische maatregelen er door Topicus zijn genomen om de persoonsgegevens te beveiligen

Topicus levert deze gegevens op verzoek per specifieke FORCE afnemer aan, waarmee de afnemer als verwerkingsverantwoordelijke danwel gegevensverwerker haar eigen gegevensbeschermingsbeleid kan aanvullen. Het is aan de verwerkingsverantwoordelijke danwel gegevensverwerker zelf om haar gegevensbeschermingsbeleid te formuleren en in aanvulling op de bovenstaande twee punten ook de volgende zaken vast te leggen:

- een beschrijving van de doeleinden waarvoor de persoonsgegevens worden verwerkt en wat de juridische grondslag daarvan is
- hoe de verwerkingsverantwoordelijke danwel gegevensverwerker voldoet aan de beginselen van verwerking van persoonsgegevens, zoals de verplichting om niet meer gegevens te verwerken dan noodzakelijk
- welke rechten betrokkenen hebben en hoe zij die rechten kunnen uitoefenen, zoals het recht om een klacht in te dienen bij de Autoriteit Persoonsgegevens (AP), maar ook het recht op inzage, wijzigen, wissen en het ontvangen van alle geregistreerde gegevens
- hoe lang de verwerkingsverantwoordelijke danwel de gegevensverwerker de persoonsgegevens bewaart

16.6.3.3 (Digitale) beveiliging

Welke organisatorische en technische maatregelen u genomen heeft om de persoonsgegevens te beveiligen?

Standpunt Topicus

Vanuit de bestaande contracten zijn reeds afspraken gemaakt t.a.v. de (digitale) beveiliging, bijvoorbeeld op basis van ISO of ISAE certificeringen. De GDPR wetgeving stelt dat deze afspraken in place moeten zijn. Dit is het geval; Topicus ziet op dit moment daarom geen aanleiding om deze afspraken inhoudelijk verder te behandelen.

16.6.4 Rechten van de betrokkenen

16.6.4.1 Recht op informatie

Op het moment dat de verwerkingsverantwoordelijke persoonsgegevens verkrijgt, dient hij de betrokkene te informeren omtrent:

- de identiteit en contactgegevens van de verwerkingsverantwoordelijke c.q. diens vertegenwoordiger
- de contactgegevens van de functionaris voor gegevensbescherming (indien aanwezig)
- de doeleinden waarvoor de persoonsgegevens zijn bestemd, inclusief de rechtsgrond voor de verwerking
- de ontvangers of categorieën van ontvangers van de persoonsgegevens
- het voornemen de persoonsgegevens door te geven aan een derde land of een internationale organisatie, de aanwezigheid van besluiten zoals Privacy Shield of een indicatie van welke waarborgen er zijn en hoe een kopie kan worden verkregen danwel waar de gegevens kunnen worden geraadpleegd
- de periode gedurende welke de persoonsgegevens worden opgeslagen, danwel de criteria waarop de termijn wordt bepaald
- dat de betrokkene het recht heeft om de verwerkingsverantwoordelijke te vragen om inzage, rectificatie of wissing van de persoonsgegevens of beperking van de verwerking te verzoeken
- dat de betrokkene het recht heeft om tegen de verwerking bezwaar te maken en de verwerking te beperken
- dat de betrokkene het recht heeft op overdraagbaarheid van de persoonsgegevens
- dat de betrokkene, indien de verwerking gebaseerd is op toestemming, het recht heeft om de toestemming te allen tijde in te trekken
- dat de betrokkene het recht heeft om een klacht in te dienen bij een toezichthoudende autoriteit
- of de verstrekking van de persoonsgegevens een wettelijke of contractuele verplichting is, danwel een noodzakelijke voorwaarde om een overeenkomst te sluiten
- of de betrokkene verplicht is om de persoonsgegevens te verstrekken en wat de mogelijke gevolgen zijn wanneer deze gegevens niet worden verstrekt
- of er sprake is van geautomatiseerde besluitvorming, met inbegrip van profilering en nuttige informatie over de onderliggende logica en het belang en de verwachte gevolgen van die verwerking voor de betrokkene

Bij verdere verwerking voor een ander doel is het vereist dat de verwerkingsverantwoordelijke de betrokkenen voor de verdere verwerking informatie over dat andere doel en alle relevante verdere informatie (zoals hierboven vermeld) verstrekt. Deze informatie behoeft niet te worden verstrekt als de betrokkene al over de informatie beschikt.

Standpunt Topicus

Het informeren van de betrokkene vindt plaats buiten FORCE (bijvoorbeeld via een algemeen informatieblad dat initieel bij ontvangst van de aanvraag aan de betrokkene wordt verstrekt). Voor invulling van dit recht zijn derhalve geen aanpassingen in FORCE benodigd.

16.6.4.2 Recht op inzage

Betrokkenen hebben recht op inzage in hun persoonsgegevens. Dat houdt in dat zij een organisatie mogen vragen of deze persoonsgegevens van hen heeft vastgelegd en zo ja, welke. Zij hoeven geen reden te geven voor een inzageverzoek. De organisatie moet vervolgens aangeven:

- of de organisatie zijn persoonsgegevens gebruikt, en zo ja:
- om welke gegevens het gaat;
- wat het doel is van het gebruik;
- aan wie de organisatie de gegevens eventueel heeft verstrekt;
- wat de herkomst is van de gegevens, als deze bekend is.

Standpunt Topicus

Vanuit de afnemers van FORCE (zoals besproken in de customer board) is aangegeven dat het aantal inzage verzoeken dermate beperkt gaat zijn dat automatisering hiervan niet opportuun is. Topicus gaat ervan uit dat met behulp van de UI van FORCE de benodigde gegevens worden verzameld.
Op basis van verschillende antwoorden blijkt dat enige automatisering toch wenselijk is. Hiervoor ziet Topicus ook verschillende mogelijkheden. De diversiteit van de antwoorden maakt echter dat er niet direct één uniforme oplossing de voorkeur heeft danwel voorhanden is. Als gevolg hiervan en in verband met de korte tijdslijnen houden we voor 25 mei vast aan het eerdere standpunt.

16.6.4.3 Recht om te wijzigen

Mensen hebben het recht om correctie van hun persoonsgegevens te vragen. Dat houdt in dat zij een organisatie mogen vragen hun persoonsgegevens te verbeteren, aan te vullen, te verwijderen of af te schermen.

Standpunt Topicus

Op het moment dat de betrokkene aangeeft dat bepaalde persoonsgegevens incorrect of onvolledig zijn, dan kan een medewerker van de verwerkingsverantwoordelijke danwel gegevensverwerker deze gegevens direct in FORCE corrigeren of aanvullen via de reguliere user interface van FORCE. In een aantal gevallen kan de betrokkene dit ook zelf doorvoeren indien FORCE via een webportaal is ontsloten aan betrokkenen. Er zijn geen aanvullende maatregelen in FORCE nodig om te kunnen voldoen aan dit recht van de betrokkene.
Topicus gaat er hierbij van uit dat correcties alleen worden doorgevoerd in actieve / lopende dossiers en dat bijvoorbeeld een afgeronde aanvraag niet meer wordt aangepast.

16.6.4.4 Recht op beperking van de verwerking

De betrokkene heeft het recht op beperking van de verwerking, indien:

- de juistheid van de persoonsgegevens wordt betwist, gedurende de periode die de verwerkingsverantwoordelijke nodig heeft om de juistheid te controleren;
- de verwerking onrechtmatig is en de betrokkene zich verzet tegen het wissen en in plaats daarvan de beperking van het gebruik ervan verzoekt;
- de verwerkingsverantwoordelijke de persoonsgegevens niet meer nodig heeft voor de verwerkingsdoeleinden, maar de betrokkene ze nodig heeft voor de instelling, uitoefening of onderbouwing van een rechtsvordering;
- de betrokkene bezwaar heeft gemaakt tegen de verwerking en in afwachting is van de vraag of het bezwaar gehonoreerd kan worden.

Indien de beperking wordt opgegeven, dan dient de verwerkingsverantwoordelijke de betrokkene daarvan op de hoogte te stellen. De verantwoordelijke dient alle ontvangers op de hoogte te stellen van de wissing, rectificatie of beperking van de verwerking van de persoonsgegevens, tenzij dit onmogelijk is of onevenredig veel inspanning vergt. De verwerkingsverantwoordelijke verstrekt aan betrokkene op diens verzoek informatie over deze ontvangers.

Standpunt Topicus

Uitgangspunt is dat FORCE de mogelijkheid zal bieden om op een per-case basis de verwerking van gegevens te beperken. De mate van beperking is afhankelijk van de status van het dossier en de door de betrokkene opgegeven reden voor de beperking. Als gevolg hiervan is er geen uniforme oplossing mogelijk en zal voor ieder verzoek separaat bepaald moeten worden hoe dit te realiseren in FORCE en relevante randsystemen. Hierbij is mogelijk ondersteuning nodig van Topicus. Dit is echter eveneens afhankelijk van de specifieke situatie. De ondersteuning wordt indien nodig geleverd voor alle relevante door Topicus geleverde producten.

16.6.4.5 Recht om vergeten te worden

Het recht op vergetelheid houdt in dat organisaties in een aantal gevallen persoonsgegevens moeten wissen als een betrokkene hierom vraagt. Het recht op vergetelheid geldt niet altijd. Alleen in specifieke situaties (https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/rechten-van-betrokkenen#wat-houdt-het-recht-op-vergetelheid-uit-de-avg-in-5976) is het recht op vergetelheid van toepassing:

- de gegevens zijn niet meer nodig
- de betrokkene trekt zijn/haar toestemming tot verwerking in
- de betrokkene maakt bezwaar tegen verdere opslag en verwerking van de gegevens
- de verwerking is onrechtmatig wegens het ontbreken van een grondslag
- de wettelijke bewaartermijnen zijn verstreken
- de betrokkene is jonger dan 16 jaar en de persoonsgegevens zijn verzameld via een app of website

Standpunt Topicus

Topicus is van mening dat een betrokkene slechts in zeer uitzonderlijke gevallen daadwerkelijk aanspraak zal kunnen maken op het recht op vergetelheid. De verwerkingsverantwoordelijke heeft voldoende grondslag om de gegevens vast te leggen en te verwerken en gegevens komen derhalve altijd met een valide reden in FORCE terecht. Zolang een aanvraag nog in behandeling is en zolang een hypotheek nog loopt zijn de gegevens nodig om de door de betrokkene gevraagde financiële dienst te kunnen leveren. In de periode na het beëindigen van een aanvraag of hypotheek dienen de gegevens rechtswege nog gedurende de wettelijk bepaalde bewaartermijnen door de verwerkingsverantwoordelijke te worden bewaard.

In die gevallen dat een betrokkene bezwaar maakt tegen verdere opslag en verwerking van de gegevens en de verwerkingsverantwoordelijke kent dit bezwaar toe, dan zal Topicus ondersteunen bij het verwijderen van de persoonsgegevens. Naar verwachting gaat het hier in de praktijk echter om dermate weinig gevallen dat het niet zinvol is om geautomatiseerde verwijder-functionaliteit in FORCE te realiseren. Dit soort situaties zullen derhalve op een case-by-case basis worden afgehandeld.

Indien betrokkenen geen bezwaar maken, dan zullen de persoonsgegevens na het verstrijken van de wettelijke bewaartermijnen alsnog verwijderd moeten worden. In beginsel beschikt FORCE hiervoor over functionaliteit in het kader van Record Retention. Met deze functionaliteit worden gegevens van afgeronde aanvagen en beëindigde hypotheken automatisch uit FORCE verwijderd. Deze functionaliteit is echter nog niet volledig (de FORCE Record Retention functionaliteit dekt nog niet alle componenten waarin persoonsgegevens worden opgeslagen af) en is bovendien nog niet geactiveerd bij alle afnemers van FORCE. In het kader van GDPR dient de Record Retention functionaliteit derhalve door Topicus te worden uitgebreid zodat deze voldoende "dekking" biedt en dient de Record Retention functionaliteit te worden geactiveerd bij afnemers die deze functionaliteit momenteel nog niet in gebruik hebben.

De scope van de Record Retention functionaliteit beslaat alle standaad componenten van de FORCE Product Suite waarin persoonsgegevens worden vastgelegd. Nevensystemen die onder het beheer van Topicus vallen moeten case-by-case beoordeeld worden, aangezien deze buiten de standaard record retention functionaliteit vallen (te denken aan: CRM, DMS, logbestanden en zulks).

Persoonsgegevens moeten ook uit backups worden verwijderd. Hierbij moet onderscheid worden gemaakt tussen de situaties waarbij de verwerkingsverantwoordelijke zelf verantwoordelijk is voor het maken en beheren van backups en de situaties waarbij deze verantwoordelijkheid bij Topicus is belegd. In beide gevallen geldt echter dat backups nooit langer worden bewaard dan de wettelijke bewaartermijnen en derhalve tijdig verwijderd worden. Indien een backup wordt teruggeplaatst, dient de verantwoordelijke (in samenwerking met Topicus) als onderdeel van de herstelprocedure opnieuw de verwijdering van de betreffende persoonsgegevens uit te voeren.

Een verwerkingsverantwoordelijke danwel gegevensverwerker hoeft niet aan te kunnen tonen dat de gegevens van de betrokkene ook daadwerkelijk zijn verwijderd. Derhalve hoeft ook hiervoor in FORCE geen functionaliteit gerealiseerd te worden.

Topicus zorgt ervoor dat voor 25 mei 2018 de Record Retention functionaliteit is uitgebreid zodat deze alle componenten in de FORCE Product Suite beslaat waarin persoonsgegevens zijn vastgelegd. Topicus treedt in overleg met afnemers van FORCE die de Record Retention functionaliteit momenteel nog niet gebruiken, om gezamenlijk te bepalen wanneer en op welke wijze deze functionaliteit alsnog in gebruik wordt genomen.

16.6.4.6 Recht op dataportabiliteit

Bij het recht op dataportabiliteit moeten organisaties de gegevens verstrekken in een vorm die het voor betrokkenen makkelijk maakt om hun gegevens te hergebruiken en door te geven aan een andere organisatie. Organisaties zijn daarom wettelijk verplicht om de gegevens in een gestructureerd, veelgebruikt en machineleesbaar formaat te verstrekken.

Standpunt Topicus

Het recht op dataportabiliteit beoogt betrokkenen in staat te stellen om gegevens die zij aan de ene verwerkingsverantwoordelijke heeft verstrekt weer op te vragen en vervolgens aan te kunnen leveren aan een andere verwerkingsverantwoordelijke. In de praktijk hebben we het binnen het hypotheekdomein dan bijvoorbeeld om een consument die zijn persoonsgegevens en actuele financieringsgegevens opvraagt bij een hypotheekverstrekker, zodat hij deze door kan sturen naar een adviseur in het kader van een adviesgesprek voor een verhoging van zijn hypotheek (soortgelijke scenario's betreffen een consument die zijn hypotheek wil omzetten, tussentijds wil aflossen, zijn rente wil aanpassen, oversluiten, et cetera).
Het exporteren van persoonsgegevens (in de breedste zin van het woord, dus ook productgegevens van de actuele financiering van de betrokkene) heeft pas zin als er een marktbrede gegevensstandaard is om deze gegevens tussen verwerkingsverantwoordelijken en gegevensverwerkers uit te wisselen en als de ontvangende partij de geëxporteerde gegevens ook daadwerkelijk in kan lezen. Een dergelijke marktbrede standaard in een gestructureerd, veelgebruikt en machineleesbaar formaat is er momenteel niet. Topicus adviseert aan de verwerkingsverantwoordelijken en gegevensverwerkers die gebruik maken van FORCE implementaties om samen met marktpartijen die gespecialiseerd zijn in het definiëren van standaarden voor gegevensuitwisseling in het hypotheekdomein (bijvoorbeeld HDN) om een dergelijke standaard op te stellen. Topicus voorziet dat er initiatieven komen voor de ontwikkeling van een dergelijke standaard (bijvoorbeeld geïnitieerd vanuit HDN), maar acht het niet realistisch dat deze voor 25 mei 2018 beschikbaar zijn. Topicus haakt vanzelfsprekend graag aan bij toekomstige initiatieven die een dergelijke standaard voor informatie-uitwisseling faciliteren. Dit uiteraard wel in samenwerking met een launching customer voor directe toepasbaarheid van dit scenario.
Alternatieve invullingen van dit recht (bijvoorbeeld het exporteren van gegevens in een niet-muteerbaar, niet-machineleesbaar formaat als PDF) vallen wat Topicus betreft niet onder de default productwerking. Indien een dergelijke oplossing toch gewenst is door een verwerkingsverantwoordelijke danwel gegevensverwerker, dan zullen er afzonderlijke afspraken gemaakt dienen te worden voor de eventuele realisatie hiervan als maatwerk.

16.6.4.7 Recht op bezwaar tegen geautomatiseerde individuele besluitvorming, waaronder profilering

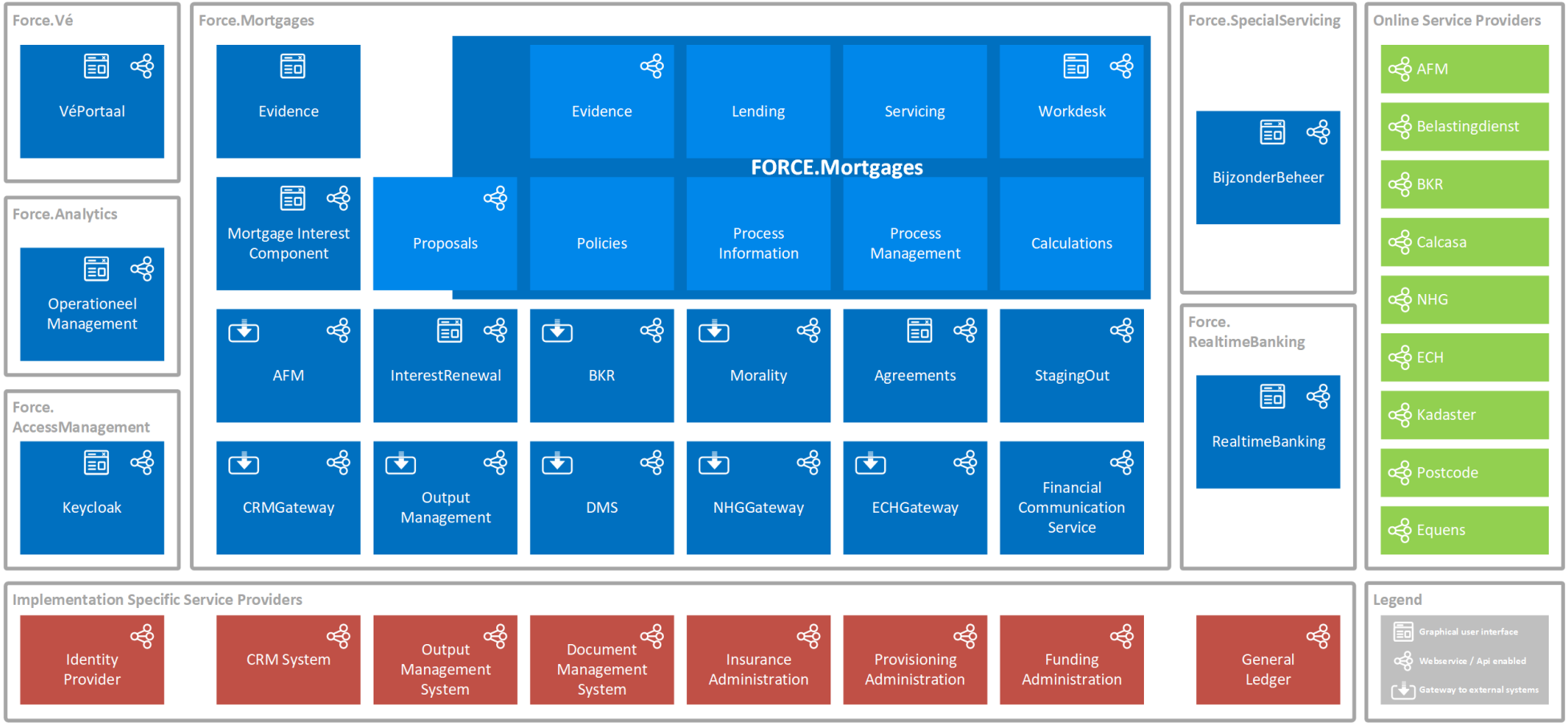
De betrokkene heeft het recht niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking, waaronder profilering, gebaseerd besluit waaraan voor hem rechtsgevolgen zijn verbonden of dat hem anderszins in aanmerkelijke mate treft (zie ook http://www.privacy-regulation.eu/nl/artikel-22-geautomatiseerde-individuele-besluitvorming-waaronder-profilering-EU-AVG.htm).

Standpunt Topicus

Geautomatiseerde besluitvorming is nodig om (o.a. in het kader van de wettelijke zorgplicht) in gelijke gevallen tot eenzelfde, eenduidig oordeel te komen van de maximaal verantwoorde leencapaciteit in relatie tot het inkomen en tot het te financieren object. Geautomatiseerde verwerking is bovendien een intrinsiek onderdeel van de dienstverlening om snel een hypotheekaanvraag te kunnen beoordelen en eventueel ook snel de hypotheek te kunnen verstrekken. In het licht van de GDPR is het echter wel noodzakelijk dat de betrokkene wordt gewezen op het feit dat de gegevens van de betrokkene geautomatiseerd worden verwerkt en dat de betrokkene hier toestemming voor geeft; Topicus gaat ervan uit dat dit onderdeel is van de toestemming die de betrokkene in algemene zin al moet geven voor het feit dat zijn of haar persoonsgegevens door de adviseur en verstrekker worden verwerkt (zie "Toestemming van de gebruiker"). De betrokkene kiest bewust voor de dienstverlening en heeft, indien de betrokkene bezwaar heeft tegen geautomatiseerde verwerking en besluitvorming, ook de mogelijkheid om géén gebruik te maken van de dienstverlening.
Tevens heeft de betrokkene over het algemeen de mogelijkheid om, indien de hypotheekaanvraag via geautomatiseerde weg wordt afgewezen, de mogelijkheid om hiertegen bezwaar te maken en aan te geven waarom de betrokkene het niet eens is met de uitkomst. Vervolgens is het mogelijk om via menselijke tussenkomst de aanvraag te herbeoordelen en op basis hiervan tot een definitief besluit te komen (om de betrokkene in het gelijk te stellen en de hypotheek alsnog te verstrekken, danwel om de aanvraag definitief af te wijzen).
Specifiek op het gebied van profilering stelt Topicus dat FORCE zelf niet over profileringsfunctionaliteit beschikt. Het bezwaar tegen profilering ziet Topicus in basis als relevant gegeven om in FORCE dan wel een gekoppeld CRM vast te leggen. Indien een verwerkingsverantwoordelijke danwel gegevensverwerker die gebruik maakt van FORCE aan profilering doet, dan dient de exacte vastlegging van het bezwaar per situatie bekeken te worden, aangezien niet elke verwerkingsverantwoordelijke danwel gegevensverwerker op dezelfde manier omgaat met de persoonsgegevens van betrokkenen: sommige organisaties leggen de directe persoonsgegevens vast in een CRM, anderen gebruiken FORCE als leidend systeem voor deze persoonsgegevens. De exacte werkwijze is bepalend voor de plek en wijze waarop het bezwaar dient te worden vastgelegd.

16.8 Bijlage G: FORCE Product Suite 2018

In de onderstaande afbeelding is de FORCE Product Suite (FPS) weergegeven. Hierbij zijn alle blauwe blokken componenten die door Topicus zijn ontwikkeld. Alle blauwe componenten binnen het kader Force.Mortgages zijn puur gericht op hypotheken. De overige blauwe blokken zijn niet puur op hypotheken gericht, maar hebben hier wel mee te maken als nevenfunctie. De rode blokken stellen systemen van klanten voor waar FORCE mee kan koppelen, zoals bijvoorbeeld een CRM-systeem. De groene blokken stellen systemen van instanties voor waar informatie wordt opgevraagd die nodig is om een hypotheekaanvraag te kunnen behandelen. Denk hierbij aan gegevens van de belastingdienst en BKR-registraties.



Figuur 22: Force Product Suite 2018