|  |  |
| --- | --- |
| **AVG -proof?** |  (logo) |
| Praktijkgericht juridisch onderzoek naar de gevolgen van de Algemene Verordening Gegevensbescherming voor financiële dienstverlener A |  |

A.A.F.A. (Anique) Smits

Tilburg, januari 2018

**AVG-proof?**

Praktijkgericht juridisch onderzoek naar de gevolgen van de Algemene Verordening Gegevensbescherming voor financiële dienstverlener A

**Auteur** A.A.F.A. (Anique) Smits

**Studentnummer** 2081419

**Afstudeerperiode** september 2017 – januari 2018

**Afstudeerorganisatie** A

**Afstudeermentor** X

**Onderwijsinstelling** Juridische Hogeschool Avans-Fontys

**Opleiding** HBO-rechten

**Locatie** Tilburg

**Eerste afstudeerdocent** Mevrouw Mr. M.M.J. van den Haspel

**Tweede afstudeerdocent** De heer Mr. F.A.C. Klaassen

Tilburg, januari 2018

**Voorwoord**

Ter afsluiting van mijn studie HBO-rechten aan de Juridische Hogeschool Avans-Fontys in Tilburg, heb ik een praktijkgericht juridisch onderzoek uitgevoerd voor A in Tilburg. Het resultaat van dit onderzoek is het onderzoeksrapport met aanbevelingen dat nu voor u ligt. In overleg met A is ervoor gekozen een onderzoek uit te voeren naar nieuwe privacywetgeving die op 25 mei 2018 van toepassing zal worden. Omdat A bij het verlenen van financiële diensten vele persoonsgegevens van klanten verwerkt, is de keuze gemaakt om de bedrijfsvoering van A onder de loep te nemen en te evalueren. Met dit onderzoek heb ik getracht om aan A handvatten te bieden zodat zij de verwerking van persoonsgegevens binnen haar organisatie in overeenstemming kan brengen met de toekomstige wetgeving.

Tijdens mijn stage heb ik veel geleerd over financiële dienstverlening. Deze branche was mij eerder niet bekend. Naast dat ik mij verdiept heb in het verlenen van financiële diensten, heb ik mij verdiept in informatie- en communicatietechnologie. Ik heb mijn stage hierdoor als erg divers en uitdagend ervaren. Graag wil ik een dankwoord uitspreken naar de personen die mij geholpen hebben deze scriptie tot stand te brengen. Allereerst wil ik graag mijn stagementor, de heer X, bedanken voor de prettige begeleiding en de feedback op mijn onderzoek. Daarnaast wil ik de heer X en de heer X bedanken voor het verlenen van medewerking aan de observaties die ik heb verricht en het beantwoorden van mijn vragen. Verder wil ik de heer Kevin van Dijck, IT specialist bij IT Support groep, bedanken voor de inzichten die hij mij gegeven heeft wat betreft IT oplossingen. Tot slot wil ik mijn stagedocent, Maria van den Haspel, bedanken voor haar ondersteuning en de terugkoppelingen tijdens mijn stage.

Anique Smits

Tilburg, januari 2018

Inhoudsopgave

**Samenvatting**

**Lijst van afkortingen**

**Begrippenlijst**

[Hoofdstuk 1. Inleiding 8](#_Toc506295432)

[1.1 De organisatie 8](#_Toc506295433)

[1.2 Probleembeschrijving 8](#_Toc506295434)

[1.3 Centrale vraag 9](#_Toc506295435)

[1.4 Doelstelling 9](#_Toc506295436)

[1.5 Deelvragen 9](#_Toc506295437)

[1.6 Onderzoeksstrategieën, bronnen, methoden en methodische verantwoording 10](#_Toc506295438)

[1.7 Leeswijzer 12](#_Toc506295439)

[Hoofdstuk 2. Huidige vormgeving privacybescherming 13](#_Toc506295440)

[2.1 Huidige beleid 13](#_Toc506295441)

[2.2 Communicatie met de klant 13](#_Toc506295442)

[2.3 Uitgangspunt 13](#_Toc506295443)

[2.4 Informering en instruering personeel 14](#_Toc506295444)

[2.5 Visie 14](#_Toc506295445)

[2.6 Samenvatting 14](#_Toc506295446)

[Hoofdstuk 3. Huidige werkwijze 15](#_Toc506295447)

[3.1 Fysieke dossiers 15](#_Toc506295448)

[*3.1.1 Verwerkte gegevens en kwalificatie* 15](#_Toc506295449)

[*3.1.2 Opslag en inzage* 17](#_Toc506295450)

[*3.1.3 Archief* 17](#_Toc506295451)

[3.2 C 17](#_Toc506295452)

[*3.2.1 Verwerkte gegevens en kwalificatie* 18](#_Toc506295453)

[*3.2.2 Opslag en inzage* 19](#_Toc506295454)

[*3.2.3 Bewerkersovereenkomst* 19](#_Toc506295455)

[3.3 Adviesbox 21](#_Toc506295456)

[*3.3.1 Verwerkte gegevens en kwalificatie* 21](#_Toc506295457)

[*3.3.2 Opslag en inzage* 21](#_Toc506295458)

[3.4 Juistheid gegevens en gegevenswissing 22](#_Toc506295459)

[3.5 Controle werkwijze 22](#_Toc506295460)

[3.6 Beveiliging 22](#_Toc506295461)

[3.7 Verwerker of verwerkingsverantwoordelijke 23](#_Toc506295462)

[*3.4.1 Fysieke dossiers* 23](#_Toc506295463)

[*3.4.2 C en Adviesbox* 24](#_Toc506295464)

[3.8 Samenvatting 24](#_Toc506295465)

[Hoofdstuk 4. De Algemene verordening gegevensbescherming 25](#_Toc506295466)

[4.1 Bekendmaking en inwerkingtreding 25](#_Toc506295467)

[4.2 Geschiedenis 25](#_Toc506295468)

[4.3 Toepassingsgebied 25](#_Toc506295469)

[4.4 Doelstelling 26](#_Toc506295470)

[4.5 Verwerkingsregels 26](#_Toc506295471)

[4.6 Verplichtingen verwerkingsverantwoordelijke 29](#_Toc506295472)

[4.7 Controlerende autoriteit 33](#_Toc506295473)

[4.8 Samenvatting 34](#_Toc506295474)

[Hoofdstuk 5. Toetsing aan AVG 35](#_Toc506295475)

[5.1 Beginselen en verplichtingen 35](#_Toc506295476)

[5.2 Verwerkte persoonsgegevens en grondslag 37](#_Toc506295477)

[5.3 Bewerkersovereenkomst B 39](#_Toc506295478)

[5.4 Samenvatting 40](#_Toc506295479)

[Hoofdstuk 6. Privacybeleid 41](#_Toc506295480)

[6.1 Inhoud 41](#_Toc506295481)

[6.2 Vormgeving 41](#_Toc506295482)

[6.3 Samenvatting 44](#_Toc506295483)

[Hoofdstuk 7. Conclusies en aanbevelingen 45](#_Toc506295484)

[7.1 Beginsel van doelbinding 45](#_Toc506295485)

[7.2 Juistheid en gegevenswissing 45](#_Toc506295486)

[7.3 Passende technische en organisatorische maatregelen 45](#_Toc506295487)

[*7.3.1 Technische maatregelen* 45](#_Toc506295488)

[*Laptops* 45](#_Toc506295489)

[*C en Adviesbox* 46](#_Toc506295490)

[*Back-up* 46](#_Toc506295491)

[*Klantpagina en klantennetwerk* 46](#_Toc506295492)

[*E-mail* 46](#_Toc506295493)

[*Personeel* 46](#_Toc506295494)

[*7.3.2 Organisatorische maatregelen* 46](#_Toc506295495)

[7.4 Overeenkomstenplicht 47](#_Toc506295496)

[7.5 Registratieplicht 47](#_Toc506295497)

[7.6 Informatieplicht 47](#_Toc506295498)

[7.7 Gegevensbeschermingseffectbeoordeling 47](#_Toc506295499)

[7.8 Functionaris voor gegevensbescherming 47](#_Toc506295500)

[7.9 Beleid 47](#_Toc506295501)

[Bronnenlijst 47](#_Toc506295502)

**Bijlagen**

Bijlage 1 Strategieën, bronnen, methoden en methodische verantwoording

Bijlage 2 Gespreksleidraad 1

Bijlage 3 Gespreksleidraad 2

Bijlage 4 Transcript interview X

Bijlage 5 Transcript interview X

Bijlage 6 Transcript interview X

Bijlage 7 Transcript interview X

Bijlage 8 Routing

Bijlage 9 Algemene voorwaarden A

Bijlage 10 Handboek en checklist Wft SVC Compliance B.V.

Bijlage 11 Vergunningen AFM

Bijlage 12 Waarnemingsschema

Bijlage 13 Observatieverslag

Bijlage 14 Inventarisatieformulier

Bijlage 15 Bewerkersovereenkomst B inzake C

Bijlage 16 Mail X

Bijlage 17 Rechten betrokkenen

Bijlage 18 Gespreksverslag X

Bijlage 19 Transcript interview Kevin van Dijck

**Samenvatting**

A is een financiële dienstverlener die advies geeft met betrekking tot hypotheken, verzekeringen, sparen, beleggen en leningen. In dit onderzoek staat het verlenen van hypotheekadvies centraal. Voor het verlenen van hypotheekadvies verwerkt A vele persoonsgegevens van klanten. Op 25 mei 2018 wordt nieuwe wetgeving betreffende de verwerking van persoonsgegevens van kracht. Deze nieuwe wetgeving vormde de aanleiding om de huidige omgang van A met persoonsgegevens te onderzoeken. Gedurende dit onderzoek heeft de vraag centraal gestaan: ‘Welke aanbevelingen voor een privacybeleid en de werkwijze met betrekking tot de verwerking van persoonsgegevens van klanten in fysieke dossiers en de systemen C en Adviesbox in het kader van hypotheekadvisering kunnen worden gegeven aan A, afgeleid uit een toetsing van de huidige werkwijze aan de AVG?’

Ter beantwoording van deze vraag is bekeken wat het huidige beleid en de huidige werkwijze is van A. Dit is in kaart gebracht aan de hand van interviews, observaties en documentanalyse. Hieruit is gebleken dat A geen privacybeleid heeft opgesteld en dat A gevoelige gegevens, persoonsgegevens en bijzondere persoonsgegevens verwerkt en hierbij is aan te merken als verwerkingsverantwoordelijke. Vervolgens is de AVG geanalyseerd en is de huidige werkwijze van A aan de AVG getoetst. Hieruit is gebleken dat A niet aan alle verplichtingen en beginselen van de AVG voldoet. A moet klanten beter informeren over de verwerking van persoonsgegevens en de rechten die zij hebben. Daarnaast bleek uit de toetsing dat A niet voldoet aan het rechtmatigheidsbeginsel, dat zij de juistheid van gegevens niet controleert en dat zij geen passende technische en organisatorische maatregelen heeft genomen. Daarnaast houdt zij geen register bij van verwerkingsactiviteiten, heeft A geen gegevensbeschermingseffectbeoordeling uitgevoerd en geen functionaris voor gegevensbescherming aangesteld. In dit onderzoek is ook in kaart gebracht op welke wijze A een privacybeleid vorm kan geven gelet op de AVG en literatuuronderzoek. Hieruit is gebleken dat klanten door middel van een beleid in vraag en antwoordvorm op duidelijke en begrijpelijke wijze op de hoogte worden gesteld van onder andere doeleinden van en grondslag voor de verwerking van hun persoonsgegevens evenals de rechten die zij hebben bij deze verwerking.

Het wordt A aanbevolen om doeleinden op te stellen die welbepaald, uitdrukkelijk en gerechtvaardigd zijn. Op dit moment voldoet A niet aan het beginsel van doelbinding omdat zij geen doeleinden voor de verwerking heeft vastgesteld. Naast dit beginsel dient A de juistheid van de gegevens die zij verwerkt beter te controleren en moet zij verwerkte persoonsgegevens verwijderen na het verstrijken van de bewaartermijn. Dit kan A doen door de klanten jaarlijks te vragen naar wijzigingen in hun persoonlijke situatie. Verder wordt het A aanbevolen om fysieke dossiers op te bergen in kasten, deze kasten af te sluiten en om een alarmsysteem te installeren op het kantoor. De beveiliging van de laptops en programma’s die A gebruikt behoeft ook een verbeterslag. Hierdoor kan A aantonen dat zij passende technische en organisatorische maatregelen heeft genomen ter bescherming van de persoonsgegevens. Andere aanbevelingen die aan A worden gedaan, zijn het opstellen van overeenkomsten met alle verwerkers, het bijhouden van een register van de verwerkingsactiviteiten en het bieden van transparantie aan haar klanten inzake de verwerking en de rechten die zij bij deze verwerking hebben. Deze transparantie kan worden geboden door middel van een privacybeleid. Tot slot wordt aanbevolen om een gegevensbeschermingseffectbeoordeling uit te voeren en een functionaris voor gegevensbescherming aan te stellen. Indien A de voornoemde aanbevelingen niet opvolgt, loopt zij het risico hoge boetes opgelegd te krijgen.

**Lijst van afkortingen**

ADN Assurantie Data Netwerk

AFM Autoriteit financiële markten

Art. Artikel

AVG Algemene Verordening Gegevensbescherming

AWR Algemene wet inzake rijksbelastingen

Bgfo Besluit gedragstoezicht financiële ondernemingen

BMfo Besluit markttoegang financiële ondernemingen Wft

BSN Burgerservicenummer

CBP College Bescherming Persoonsgegevens

CDDN Communicatie Data Diensten Nederland

EU Europese Unie

FDN Financieel Data Netwerk

HDN Hypotheek Data Netwerk

ICT Informatie- en communicatietechnologie

IT Informatietechnologie

Jo. Juncto

Kifid Klachteninstituut voor de Financiële Dienstverlening

KvK Kamer van Koophandel

SEPA Single Euro Payments

USP Unique Selling Point

UTP Unshielded Twisted Pair

VOG Verklaring omtrent gedrag

Wbp Wet bescherming persoonsgegevens

Wft Wet financieel toezicht

WiFi Wireless Fidelity

Wwft Wet ter voorkoming van witwassen en financiering terrorisme

zzp’er Zelfstandige zonder personeel

**Begrippenlijst**

**Autoriteit Persoonsgegevens**

Onafhankelijke toezichthoudende autoriteit die controleert of de AVG wordt nageleefd. In Nederland is de Autoriteit Persoonsgegevens de toezichthoudende autoriteit.[[1]](#footnote-1)

**Bestand**

Een gestructureerd geheel van persoonsgegevens dat volgens bepaalde criteria toegankelijk is en gaat over meerdere personen.[[2]](#footnote-2) Hierbij is er samenhang in de structuur van de dossiers.

**Betrokkene**

Een betrokkene is de natuurlijke persoon op wie een persoonsgegeven betrekking heeft.[[3]](#footnote-3)

**Bijzonder persoonsgegeven**

Persoonsgegevens worden als bijzonder aangemerkt als zij informatie verschaffen waaruit ras, etniciteit, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, lidmaatschap van een vakbond, genetische gegevens, biometrische gegevens, gezondheidsgegevens of gegevens over seksueel gedrag dan wel seksuele gerichtheid blijken.[[4]](#footnote-4)

**Persoonsgegeven**

Een persoonsgegeven geeft informatie over een geïdentificeerde of identificeerbare natuurlijke persoon.[[5]](#footnote-5) Het gaat hierbij dus om alle gegevens die iets vertellen over de klant waardoor de klant kan worden geïdentificeerd.

**Verwerker**

Partij die een aparte rechtspersoon is, die losstaat van de verwerkingsverantwoordelijke en persoonsgegevens verwerkt ten behoeve van een verwerkingsverantwoordelijke.[[6]](#footnote-6)

**Verwerking**

Elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens. Hieronder wordt in elk geval verstaan het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.[[7]](#footnote-7)

**Verwerkingsverantwoordelijke**

Partij die voor de verwerking verantwoordelijk is en ook verantwoordelijk kan worden gehouden voor de naleving van de verplichtingen uit de AVG en alleen of samen met andere het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.[[8]](#footnote-8)

# Hoofdstuk 1. Inleiding

*In dit hoofdstuk is de organisatie waarvoor dit onderzoek wordt uitgevoerd en het probleem dat ten grondslag ligt aan dit onderzoek beschreven gevolgd door de centrale vraag. Vervolgens zijn de doelstelling en de deelvragen van dit onderzoek vermeld. Daarna is weergegeven welke onderzoeksstrategie, bronnen en methoden zijn gebruikt tijdens dit onderzoek en de verantwoording hiervan. Tot slot is een leeswijzer van dit onderzoek opgenomen.*

## 1.1 De organisatie

A is een jonge onderneming gevestigd in Tilburg die zich bezighoudt met het verlenen van financieel advies met betrekking tot hypotheken, verzekeringen, sparen, beleggen en leningen. Binnen de organisatie wordt veel belang gehecht aan kwalitatief goed advies en persoonlijk contact met de klant. Doordat de adviseurs de tijd nemen om de persoon achter de vraag te leren kennen, kunnen zij een advies geven dat zo goed mogelijk aansluit op de persoonlijke situatie van hun klanten.

## 1.2 Probleembeschrijving

Voor het geven van adequaat advies aan haar klanten, heeft A veel persoonlijke informatie van haar klanten nodig. Zonder deze informatie is het namelijk niet mogelijk te bepalen hoe hoog een te verkrijgen hypotheek is, welke vorm hypotheek het beste past bij de klant en welke verzekeringen de klant dient af te sluiten. Daarnaast geeft zij ook advies met betrekking tot sparen, beleggen en leningen. De gegevens die A nodig heeft voor deze advisering worden opgeslagen in verschillende digitale omgevingen. Het hoofdsysteem waarin persoonsgegevens worden opgeslagen is het CRM-systeem van B genaamd C. In dit systeem verwerkt A informatie met betrekking tot pensioenen, belastingen, inkomen, legitimatiebewijzen, schadeverzekeringen en levensverzekeringen. Ter ondersteuning van dit systeem maakt A gebruik van de volgende programma’s: Hypotheekbond, Adviesbox, Nedasco, Hypotheek Data Netwerk (HDN), Assurantie Data Netwerk (ADN), Financieel Data Netwerk (FDN) en Communicatie Data Diensten Nederland (CDDN). In deze digitale omgevingen worden persoonlijke gegevens van klanten verwerkt of worden klantgegevens opgehaald. Het belangrijkste ondersteunende programma is Adviesbox. Naast dat er in de digitale omgevingen persoonsgegevens worden verwerkt, vindt verwerking van persoonsgegevens ook fysiek plaats binnen het kantoor. Er worden namelijk papieren dossiers aangemaakt waarin alle persoonsgegevens van de klanten worden bijgehouden.

Doordat A bij advisering van haar klanten gebruik maakt van persoonlijke gegevens van de klanten, is het van belang dat de privacy van deze mensen gewaarborgd is. Het gaat namelijk om gegevens die klanten graag privé houden. Binnen A staat integriteit dan ook hoog in het vaandel. Al haar werknemers hebben een geheimhoudingsverklaring, een integriteitsverklaring en een Verklaring Omtrent het Gedrag (VOG). Omdat het waarborgen van de privacy van haar klanten zo belangrijk is voor A, wil zij dit graag duidelijker aan haar klanten laten blijken en ervoor zorgen dat zij bekend staat om haar integriteit.

Om de gegevens van klanten te beschermen, is bij inschakeling van derde partijen in de contracten met hen opgenomen dat ook op hen een geheimhoudingsplicht rust. Daarnaast is voor het CRM-systeem C van B een bewerkersovereenkomst gesloten tussen A en B. Bij de digitale omgevingen die C ondersteunen is naast de licentieovereenkomst geen bewerkingsovereenkomst gesloten.

De gegevens die worden verwerkt bij A zijn aan te merken als persoonsgegevens[[9]](#footnote-9). Dit houdt in dat het gaat om informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. Aan de verwerking van persoonsgegevens zijn door de overheid regels gesteld. Deze zijn te vinden in de Algemene Verordening Gegevensbescherming (hierna te noemen AVG) welke op 24 mei 2016 in werking is getreden. Omdat het aanpassen van de bedrijfsvoering enige tijd behelst, is een termijn van twee jaar aangehouden voordat de AVG op 25 mei 2018 van toepassing is. Door de komst van de AVG moet een consistent niveau van bescherming worden geboden in de hele Europese Unie en zal worden voorkomen dat niet-consistente toepassing leidt tot belemmering van het vrije verkeer op de interne markt.[[10]](#footnote-10) Daarnaast heeft de verordening tot doel dat rechtszekerheid[[11]](#footnote-11) en transparantie[[12]](#footnote-12) wordt geboden aan de bevolking door dezelfde rechten aan natuurlijke personen toe te kennen en dezelfde verplichtingen en verantwoordelijkheden op verwerkingsverantwoordelijken en verwerkers te laten rusten.[[13]](#footnote-13) Om dit te kunnen bereiken worden de regels voor de verwerking van persoonsgegevens aangescherpt.

Het van toepassing worden van de AVG en daarmee samenhangende wijzingen die A moet doorvoeren om aan de AVG te voldoen, zijn aanleiding voor dit onderzoek. A wil in kaart gebracht hebben aan welke regels zij zich moet houden bij het verwerken van persoonsgegevens van klanten. Omdat de periode van onderzoek niet toereikend is om de gehele bedrijfsvoering door te lichten, beperkt dit onderzoek zich tot C en Adviesbox bij het verlenen van hypotheekadvies. Omdat alle klantgegevens eerst worden verzameld door middel van het invullen van fysieke formulieren alvorens de gegevens in C en Adviesbox worden ingevoerd, is het van belang dat de privacy van klanten ook wordt gewaarborgd voordat de gegevens zijn ingevoerd in de systemen. In dit onderzoek zal daarom ook aandacht worden besteed aan beveiliging van fysieke dossiers. Na oplevering van dit onderzoek moet het voor A duidelijk zijn in welke mate zij reeds voldoet aan de AVG, op welke gebieden zij nog stappen dient te zetten om aan de AVG te voldoen en op welke wijze een privacybeleid kan worden vormgegeven.

## 1.3 Centrale vraag

Welke aanbevelingen voor een privacybeleid en de werkwijze met betrekking tot de verwerking van persoonsgegevens van klanten in fysieke dossiers en de systemen C en Adviesbox in het kader van hypotheekadvisering kunnen worden gegeven aan A, afgeleid uit een toetsing van de huidige werkwijze aan de AVG?

## 1.4 Doelstelling

Op maandag 8 januari 2018 zal dit onderzoeksrapport met aanbevelingen worden opgeleverd aan de heer X, algemeen directeur van A. Uit dit rapport blijkt welke aspecten van de verwerking van persoonsgegevens van klanten in fysieke dossiers, C en Adviesbox verbeterd dienen te worden om te voldoen aan de AVG, alsmede op welke wijze A een privacybeleid kan vormgeven ter waarborging van de privacy van klanten zodat A haar werkwijze en beleid kan aanpassen overeenkomstig de AVG.

## 1.5 Deelvragen

1. Wat is het huidige beleid, de communicatie hieromtrent en de visie van A met betrekking tot de verwerking van persoonsgegevens van klanten in het kader van hypotheekadvisering?
2. Op welke wijze verwerkt A momenteel de persoonsgegevens van klanten in het kader van hypotheekadvisering in fysieke dossiers, C en Adviesbox?
3. Welke verplichtingen vloeien voort uit de Algemene Verordening Gegevensbescherming met betrekking tot het verwerken van persoonsgegevens van klanten voor A?
4. Welke verbeterpunten met betrekking tot de verwerking van persoonsgegevens van klanten in het kader van hypotheekadvisering kunnen worden geformuleerd als gevolg van een toetsing van de huidige werkwijze en het huidige beleid aan de verplichtingen uit de Algemene Verordening Gegevensbescherming?
5. Op welke wijze kan A een privacybeleid vormgeven gelet op de Algemene Verordening Gegevensbescherming?

## 1.6 Onderzoeksstrategieën, bronnen, methoden en methodische verantwoording

Onderstaand is per deelvraag aangegeven van welke onderzoeksstrategie, bronnen en methoden er gebruik is gemaakt om de deelvragen te kunnen beantwoorden. Vervolgens is per deelvraag verantwoord waarom gekozen is voor die strategie, bronnen en methode. Een uitgebreidere beschrijving van de onderzoeksstrategieën, bronnen, methoden en methodische verantwoording is te vinden in bijlage 1.

***1.6.1 Deelvraag 1:***

*Wat is het huidige beleid, de communicatie hieromtrent en de visie van A met betrekking tot de verwerking van persoonsgegevens van klanten in het kader van hypotheekadvisering?*

De onderzoeksstrategie die ter beantwoording van deze deelvraag is gebruikt is casestudy. Aan de hand van interviews met algemeen directeur de heer X, operationeel directeur de heer X en commercieel directeur de heer x is in kaart gebracht wat het huidige beleid is en welke visie A heeft omtrent bescherming van persoonsgegevens van klanten. Ook is een interview afgenomen met zzp’er mevrouw X (financieel adviseur bij A) om in kaart te brengen in hoeverre A haar ideeën omtrent privacy communiceert met werknemers. De directeuren zijn geïnterviewd omdat zij de oprichters zijn van A en zij bepalen welk beleid wordt aangehouden en op welke wijze dit wordt nageleefd.

De methode die gebruikt wordt is het houden van interviews waarbij telkens één persoon tegelijk wordt geïnterviewd. De vorm van deze interviews is semigestructureerd, er wordt aangesloten bij het boommodel. Dit houdt in dat vooraf het hoofdonderwerp is vastgesteld (de stam van de boom) en dat daarna verschillende onderwerpen worden behandeld waarover vooraf open vragen zijn geformuleerd (de takken van de boom). Ter ondersteuning van het interview is een gespreksleidraad, ook wel bekend als conversatiehulp worden opgesteld. Daarnaast zijn de interviews uitgewerkt in de vorm van een transscript.

Het hoofdstuk heeft de titel ‘huidige vormgeving privacybescherming’ gekregen, omdat verschillende aspecten die samenhangen met een privacybeleid worden behandeld.

***1.6.2. Deelvraag 2:***

*Op welke wijze verwerkt A momenteel de persoonsgegevens van klanten in het kader van hypotheekadvisering in fysieke dossiers, C en Adviesbox?*

Deze deelvraag is beantwoord aan de hand van de strategie casestudy. Door middel van observaties en documentanalyse is in kaart gebracht welke klantgegevens en op welke wijze klantgegevens door A worden verwerkt in fysieke dossiers, C en Adviesbox. De documenten die zijn bekeken zijn de door A opgemaakte fysieke dossiers met klantgegevens in het kader van hypotheekadvisering. De dossiers bestaan uit ingevulde inventarisatieformulieren, kopieën van legitimatiebewijzen, aantekeningen, kopieën van salarisstroken, taxatierapport en kopieën van verzekeringspolissen. Door middel van observatie van personen is in kaart worden gebracht op welke wijze de persoonsgegevens van klanten in het kader van hypotheekadvisering worden verwerkt in C en Adviesbox. De personen die hiervoor zijn geobserveerd, zijn dhr. X en dhr. X. Zij leveren informatie over het proces van verwerking van persoonsgegevens van klanten in voornoemde systemen en zijn daarom aan te merken als informant. Om ervoor te zorgen dat de documentanalyse en observaties betrouwbaar zijn, is nauwkeurig vastgelegd welke documenten uit de dossiers zijn geanalyseerd en op welke wijze en gedurende welke termijn deze dossiers worden bewaard. Daarnaast is een gedetailleerd waarnemingsschema opgenomen dat leidraad vormt voor de observaties zodat navolgbaar is op welke wijze de observaties zijn uitgevoerd. Verder zijn verslagen van observaties opgenomen indien aanvulling van dit waarnemingsschema vereist is. Omdat deze observaties gepaard gaan met het voeren van gesprekken en het bestuderen van documenten is er sprake van triangulatie. Er wordt namelijk gebruik gemaakt van meerdere methoden en bronnen.

Daarnaast is de bewerkingsovereenkomst met B betreffende C geanalyseerd. Vervolgens brengt deze deelvraag in kaart of A verwerker of verwerkingsverantwoordelijke is afgeleid uit de bewerkersovereenkomst met B inzake C, de AVG en een advies van groep gegevensbescherming artikel 29. Hiervoor is gebruik gemaakt van literatuuronderzoek. Aan de hand van deze bronnen is het mogelijk te bepalen of A met betrekking tot de fysieke dossiers, C en Adviesbox is aan te merken als verwerker of verwerkingsverantwoordelijke. Dit is mogelijk door de betreffende bepalingen uit de AVG en het advies van groep gegevensbescherming artikel 29 te vergelijken met de wijze waarop A de klantgegevens in het kader van hypotheekadvisering verwerkt in fysieke dossiers en voornoemde systemen. Doordat de AVG en het advies van groep gegevensbescherming artikel 29 aan te merken zijn als betrouwbare bronnen, is op vakkundige wijze bepaald wat de hoedanigheid van A is ten opzichte van voornoemde systemen.

***1.6.3. Deelvraag 3:***

*Welke verplichtingen vloeien voort uit de Algemene Verordening Gegevensbescherming met betrekking tot het verwerken van persoonsgegevens van klanten voor A?*

Deze deelvraag is beantwoord aan de hand van een onderzoek van rechtsbronnen en een literatuuronderzoek. De AVG is geanalyseerd en geïnterpreteerd waarna in deze deelvraag inzichtelijk is gemaakt welke bepalingen voor A van belang zijn bij de verwerking van persoonsgegevens van klanten in fysieke dossiers, C en Adviesbox in het kader van hypotheekadvisering. De rechtsbronnen waarvan hiervoor gebruik is gemaakt, zijn de AVG en relevante jurisprudentie. Voor de interpretatie van voornoemde rechtsbronnen zijn verschillende boeken geraadpleegd. Ook is gebruik gemaakt van media. Bij beantwoording van deze deelvraag zijn namelijk websites geraadpleegd.

Naast onderzoek van rechtsbronnen en literatuur is door middel van casestudy in kaart gebracht op welke wijze digitale omgevingen kunnen worden beschermd zodat de privacy van klanten gewaarborgd is in overeenstemming met de AVG. Hiervoor is externe IT specialist de heer K. van Dijck geïnterviewd. De keuze om de heer Van Dijck te interviewen is gemaakt omdat hij deskundig is op het gebied van beveiliging van digitale omgevingen.

Het interview heeft plaatsgevonden in de vorm van een tweegesprek. Het interview is semigestructureerd opgezet en er is aansluiting gezocht bij het boommodel (zie voorgaande uitleg). Ter ondersteuning van het interview is een gespreksleidraad, ook wel bekend als conversatiehulp opgesteld. Daarnaast is het interview uitgewerkt in de vorm van een transscript.

***1.6.4. Deelvraag 4:***

*Welke verbeterpunten met betrekking tot de verwerking van persoonsgegevens van klanten in het kader van hypotheekadvisering kunnen worden geformuleerd als gevolg van een toetsing van de huidige werkwijze en het huidige beleid aan de verplichtingen uit de Algemene Verordening Gegevensbescherming?*

Ter beantwoording van deze vraag, zijn deelvraag één en twee aan deelvraag drie getoetst. Doordat met deelvraag één en twee in kaart is gebracht wat het huidige beleid en de huidige werkwijze is van A, kan een toetsing plaatsvinden aan de AVG. De AVG is namelijk geanalyseerd in de derde deelvraag.

Er is een schema gemaakt waarin alle relevante verplichtingen voor A met betrekking tot verwerking van klantgegevens in de fysieke dossiers, C en Adviesbox afgeleid uit deelvraag drie zijn opgenomen. Vervolgens is in dit schema ingevuld of in de huidige situatie aan deze verplichting is voldaan en op welke wijze is voldaan. Wanneer niet voldaan is aan de verplichting zal worden toegelicht waarom er niet voldaan is aan de verplichting. Om te bepalen of aan de verplichtingen is voldaan, zullen de eerste en tweede deelvraag worden bekeken en naast het schema worden gelegd. De keuze om de deelvraag aan de hand van deze methode te beantwoorden, is gemaakt omdat door middel van een schema kort en krachtig inzichtelijk wordt voor A waaraan zij voldoet en waar zij nog niet aan voldoet. De toelichting op dit schema geeft dan verduidelijking waarom wel of niet aan de verplichting is voldaan. Doordat gewerkt wordt vanuit een schema, is in één oogopslag duidelijk hoe A ervoor staat.

***1.6.5.Deelvraag 5:***

*Op welke wijze kan A een privacybeleid vormgeven gelet op de Algemene Verordening Gegevensbescherming?*

Deze deelvraag wordt beantwoord door middel van een literatuuronderzoek in combinatie met het raadplegen van de bevindingen van deelvraag drie. Met behulp van deze literatuur kan worden bepaald of alle onderwerpen die in een privacybeleid horen ook daadwerkelijk zijn opgenomen. Het boek dient hierbij als controlemiddel.

## 1.7 Leeswijzer

In dit onderzoeksrapport is in het tweede hoofdstuk weergegeven wat het huidige beleid is dat A voert met betrekking tot de verwerking van persoonsgegevens van klanten in het kader van hypotheekadvisering. Door middel van interviews is dit in kaart gebracht. In hoofdstuk drie is opgenomen op welke wijze A de persoonsgegevens van klanten momenteel verwerkt in het kader van hypotheekadvisering. Hierbij is een onderscheid gemaakt tussen fysieke dossiers en de systemen C en Adviesbox. Vervolgens is in hoofdstuk vier opgenomen welke verplichtingen voortvloeien uit de AVG voor A met betrekking tot het verwerken van persoonsgegevens van klanten. In het vijfde hoofdstuk is inzichtelijk gemaakt op welke punten A zich moet verbeteren blijkens een toetsing van de huidige werkwijze aan de AVG. In hoofdstuk zes is weergegeven op welke wijze A een beleid kan vormgeven zodat zij voldoet aan haar verplichtingen afgeleid uit de AVG. Tot slot zijn in hoofdstuk zeven de conclusies en aanbevelingen gegeven van dit onderzoek. Hiermee wordt de centrale vraag van dit onderzoek beantwoord.

# Hoofdstuk 2. Huidige vormgeving privacybescherming

*In dit hoofdstuk is in kaart gebracht wat het huidige beleid van A is met betrekking tot de bescherming van persoonsgegevens van klanten in het kader van hypotheekadvisering. Dit is in kaart gebracht aan de hand van interviews die zijn afgenomen met de heer X(operationeel directeur), de heer X (algemeen directeur) en de heer X (commercieel directeur). Ook is een interview gehouden met mevrouw Smit (financieel adviseur, zzp’er) om in kaart te brengen op welke wijze het huidige beleid van A met medewerkers wordt gecommuniceerd. Tot slot is de visie met betrekking tot privacybescherming in kaart gebracht.*

## 2.1 Huidige beleid

Momenteel heeft A geen beleid opgesteld wat betreft de bescherming van persoonsgegevens van klanten.[[14]](#footnote-14) Op de website van A is dan ook geen privacyreglement of privacyverklaring geplaatst.[[15]](#footnote-15) Ondanks dat A niets heeft opgesteld, geeft zij aan dat privacy hoog in het vaandel staat.[[16]](#footnote-16)

## 2.2 Communicatie met de klant

Uit de interviews is gebleken dat er niet of nauwelijks aan de klant wordt medegedeeld op welke wijze A omgaat met de gegevens die zij van hen ontvangen.[[17]](#footnote-17) Ook is op de website niet aangegeven dat privacy bij A hoog in het vaandel staat en dat zij integer omgaat met de verstrekte gegevens. Bij een intakegesprek worden enkele documenten aan de klant overhandigd waaruit de klant kan afleiden dat integer wordt omgegaan met de klantgegevens. De documenten die overhandigd worden en zaken die besproken worden, zijn vastgesteld in een door de eigenaren opgestelde routing[[18]](#footnote-18). Tijdens dit gesprek worden onder andere algemene voorwaarden aan de klant overhandigd. Hierin is beschreven op welke wijze A persoonsgegevens van klanten beschermt. In art. 10 van de Algemene voorwaarden[[19]](#footnote-19) is bepaald dat A verstrekte persoonsgegevens niet zal verstrekken aan derden en niet zal gebruiken voor andere doeleinden dan voor het uitvoeren van de opdracht. De wijze waarop A omgaat met de privacy wordt momenteel dus niet expliciet aan de klant vermeld. Eén van de adviseurs geeft aan op de privacy in te haken wanneer hij merkt dat de klant zich ongemakkelijk voelt bij het verstrekken van de persoonlijke informatie.[[20]](#footnote-20) Hij geeft aan de klant dan gerust te stellen door aan de klant uit te leggen waarom bepaalde gegevens vereist zijn. Ook geeft hij aan dat hij merkt dat de jongere generatie, waarmee hij starters en doorstarters op de woningmarkt bedoelt, steeds bewuster bezig is met het bewaken van zijn en/of haar privacy.[[21]](#footnote-21)

## 2.3 Uitgangspunt

Omdat A werkzaam is op de financiële markt, dient zij bij haar dienstverlening aan enkele verplichtingen uit de Wet financieel toezicht (Wft), Besluit markttoegang financiële ondernemingen Wft (BMfo) en Besluit gedragstoezicht financiële ondernemingen (Bgfo) te voldoen die samenhangen met integere behandeling van klantgegevens. De Autoriteit Financiële Markten (hierna te noemen AFM) controleert deze verplichtingen. De verplichtingen die voortvloeien uit voornoemde regelgeving zien op de betrouwbaarheid, de vakbekwaamheid, integere en beheerste bedrijfsvoering, de zorgplicht en transparantie van A. A volgt het beleid van de AFM hierbij.[[22]](#footnote-22) Om aan te kunnen tonen aan de AFM dat A voldoet aan deze verplichtingen, heeft zij enkele verklaringen aangevraagd en formulieren ingevuld.[[23]](#footnote-23) Hierbij gaat het onder andere om door A verkregen integriteitsverklaringen en betrouwbaarheidsverklaringen van de AFM.[[24]](#footnote-24)

## 2.4 Informering en instruering personeel

De wijze waarop A het huidige beleid en de visie communiceert met werknemers respectievelijk de zzp’er is ook in kaart gebracht. Uit de interviews blijkt dat er met zzp’er mevrouw Smit niet diepgaand gesproken is over de wijze waarop zij de privacy van klanten moet bewaken bij haar werkzaamheden voor A.[[25]](#footnote-25) Alle adviseurs geven aan dat zij er vertrouwen in hebben dat zij integer te werk gaat ondanks dat hierover geen concrete afspraken zijn gemaakt. Het uitgangspunt dat A hanteert met betrekking tot het beschermen van klantgegevens, is wel met de zzp’er gecommuniceerd. Haar is verteld dat de uitgangspunten van A aansluiten bij de verplichtingen waarop de AFM controleert. Dit is dan ook reden dat zij een betrouwbaarheidsformulier heeft moeten tekenen, een eed van verklaring heeft afgelegd en een VOG heeft moeten overleggen.[[26]](#footnote-26) Hieruit blijkt dat het beschermen van de privacy van klanten voor A van belang is.

Ter controle van de wijze waarop communicatie met de zzp’er heeft plaatsgevonden, is ook een interview bij haar afgenomen. Blijkens dit interview is er niet uitgebreid gesproken over het idee dat A nastreeft met betrekking tot het bewaken van de privacy van klanten en op welke wijze dit terug te zien moet zijn in haar werkwijze.[[27]](#footnote-27) Het is haar duidelijk dat A zelf de fijne lijnen van het beleid niet voor ogen heeft en dat hierover in de toekomst uitgebreider gecommuniceerd moet worden.[[28]](#footnote-28)

## 2.5 Visie

De visie voor de toekomst is een beleid conform de AVG dat ook daadwerkelijk wordt nageleefd. Uit dit beleid moet blijken dat de klantgegevens bij A goed beveiligd zijn en dat er zo integer als mogelijk wordt omgegaan met de klantgegevens. Eén van de adviseurs geeft aan dat hij de bewaking van de privacy van klanten door A als Unique Selling Point (USP) zou willen zien.[[29]](#footnote-29)

## 2.6 Samenvatting

Uit het voorgaande blijkt dat A geen beleid heeft opgesteld en dat zij niet met de klant communiceert dat privacy bij A hoog in het vaandel staat. Verder blijkt dat het personeel van A onvoldoende op de hoogte wordt gesteld van de wijze waarop zij dienen te handelen bij de verwerking van persoonsgegevens.

# Hoofdstuk 3. Huidige werkwijze

*In dit hoofdstuk is in kaart gebracht wat de huidige werkwijze van A is met betrekking tot de verwerking van persoonsgegevens van klanten in het kader van hypotheekadvisering. Allereerst is de werkwijze met betrekking tot fysieke dossiers geanalyseerd. Vervolgens is aan de hand van observaties in kaart gebracht wat de werkwijze van A is met betrekking tot C en Adviesbox. Hierbij zijn de heer X en de heer X geobserveerd aan de hand van een waarnemingsschema[[30]](#footnote-30). Dit schema is uitgewerkt in een observatieverslag dat als bijlage aan dit onderzoek is toegevoegd.[[31]](#footnote-31) Dit hoofdstuk bevat ook een analyse van de bewerkersovereenkomst met B inzake C. Daarnaast is in dit hoofdstuk beschreven op welke wijze A de juistheid van gegevens controleert, of zij gegevens wist, of zij de huidige werkwijze controleert, welke beveiligingsmaatregelen A heeft genomen en of A aan te merken is als verwerker of verwerkingsverantwoordelijke.*

## 3.1 Fysieke dossiers

### *3.1.1 Verwerkte gegevens en kwalificatie*

Wanneer een klant contact opneemt met A wordt direct een fysiek dossier aangemaakt. Bij het eerste gesprek wordt de nodige informatie vergaard door middel van het invullen van een inventarisatieformulier.[[32]](#footnote-32) Dit formulier wordt in het dossier geplaatst. Tijdens het eerste gesprek wordt ook een kopie gemaakt van het legitimatiebewijs, de salarisstrook en van polissen van verzekeringen. Deze documenten worden in het dossier geplaatst. Verder in het proces zullen ook een taxatierapport, een bouwkundig rapport, een energierapport en een adviesrapport van het aan te kopen pand aan de dossiers worden toegevoegd. Soms maakt de adviseur tussentijds aantekeningen naar aanleiding van contact met geldverstrekkers, verzekeraars of de klant. Deze aantekeningen worden ook in het dossier geplaatst. De inhoud van voornoemde documenten is beschreven in het observatieverslag.[[33]](#footnote-33)

De klantgegevens die door A verwerkt worden, kunnen worden gekwalificeerd als persoonsgegevens of bijzonder persoonsgegevens. Een persoonsgegeven geeft informatie over een geïdentificeerde of identificeerbare natuurlijke persoon.[[34]](#footnote-34) Het gaat hierbij dus om alle gegevens die iets vertellen over de klant waardoor de klant kan worden geïdentificeerd. Persoonsgegevens worden als bijzonder aangemerkt als zij informatie verschaffen waaruit ras, etniciteit, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, lidmaatschap van een vakbond, genetische gegevens, biometrische gegevens, gezondheidsgegevens of gegevens over seksueel gedrag dan wel seksuele gerichtheid blijken.[[35]](#footnote-35) Niet alle gegevens die A verwerkt zijn aan te merken als persoonsgegeven of bijzonder persoonsgegeven omdat er ook gegevens worden verwerkt die er niet voor zorgen dat de klant kan worden geïdentificeerd.

*3.1.1.1 Inventarisatieformulier[[36]](#footnote-36)*

Door middel van het inventarisatieformulier brengen de adviseurs van A in kaart hoe de financiële situatie van de klant eruitziet. Alle aspecten die hierop van invloed zijn, worden behandeld in dit document. Het document bevat persoonlijke gegevens van de klant, juridische gegevens van de klant en indien de klant kinderen heeft, worden ook enkele gegevens van de kinderen genoteerd. Verder bevat dit document bankgegevens, inkomensgegevens, gegevens omtrent sparen en financiële verplichtingen die op de klant rusten. Daarnaast zijn het in bezit hebben van een woning, een hypotheek die reeds loopt en reeds afgesloten verzekeringen van invloed op de financiële situatie van de klant. Naast voornoemde gegevens, brengt dit formulier gegevens in kaart omtrent de aan te kopen woning, blijkt of de klant een overbrugging nodig heeft door latere verkoop van de eigen woning dan aankoop van de nieuwe woning en wordt bekeken op welke wijze de werkgever arbeidsongeschiktheid heeft geregeld. Tot slot blijkt uit dit formulier of de klant een aanvullende verzekering heeft afgesloten voor arbeidsongeschiktheid en hoe de pensioensituatie van de klant eruit ziet.

Uit de analyse van dit inventarisatieformulier is gebleken dat dit document gevoelige gegevens bevat die niet aan te merken zijn als persoonsgegeven, dat dit document persoonsgegevens bevat en dat dit document bijzondere persoonsgegevens bevat. Een concrete opsomming van de verwerkte gegevens en uitgebreide kwalificatie van deze gegevens is te vinden in het observatieverslag.[[37]](#footnote-37)

*3.1.1.2 Kopie legitimatiebewijs, kopie salarisstrook en kopie verzekeringen*

In het fysieke dossier is ook een kopie opgenomen van het legitimatiebewijs of de legitimatiebewijzen van de klant(en). Het gaat hierbij om kopieën van identiteitskaarten en paspoorten. De kopie is in kleur en is voorzien van een handtekening en de term kopie. Bij de handtekening is vermeld dat het originele bewijs gezien is evenals de datum waarop het origineel gezien is. Blijkens een analyse van dit document bevat deze kopie persoonsgegevens en bijzondere persoonsgegevens.[[38]](#footnote-38)

Om aan te tonen bij een bank dat de voorgenomen hypotheeklast gedragen kan worden door de klant, moet de klant een kopie van zijn of haar salarisstrook aandragen. Deze salarisstrook bevat blijkens inhoudsanalyse persoonsgegevens van de klant. Naast persoonsgegevens van de klant, bevat het document gevoelige klantgegevens.[[39]](#footnote-39) In het algemeen vinden mensen het niet prettig wanneer salarisgegevens voor anderen bekend zijn. Daarom behoeft de verwerking van deze gegevens extra bescherming.[[40]](#footnote-40)

In aanvulling op het inventarisatieformulier wordt in het dossier ook een kopie opgenomen van de polis of polissen die de klant heeft afgesloten bij een verzekeraar. Deze documenten bevatten vaak veel informatie over de afgesloten polis en bevatten weinig informatie over de klant. Enkele gegevens vermeld in de polis zijn aan te merken als persoonsgegeven.[[41]](#footnote-41)

*3.1.1.3 Taxatierapport, bouwkundig rapport en energierapport*

Naarmate het proces met betrekking tot de aankoop van een woning vordert, wordt er een taxatierapport opgesteld voor de aan te kopen woning. Dit rapport wordt toegevoegd aan het fysieke dossier en bevat voornamelijk gegevens over de aan te kopen woning. In het rapport zijn enkele gegevens vermeld van de klant. Deze gegevens zijn aan te merken als persoonsgegevens.[[42]](#footnote-42)

Het bouwkundig rapport bevat een overzicht van technische mankementen aan het pand. Door middel van dit rapport wordt inzichtelijk gemaakt welke kosten gemaakt moeten worden om het pand in orde te maken. Verder zijn in dit rapport enkele gegevens van de klant opgenomen welke aan te merken zijn als persoonsgegevens.[[43]](#footnote-43)

Het energierapport bevat tips en tricks om te zorgen voor een energiezuiniger huis en hierin wordt bepaald wat het energielabel van het pand is. Naast tips en tricks wordt beschreven ten behoeve van wie het rapport is opgesteld. Dit onderdeel van het rapport bevat persoonsgegevens van de klant.[[44]](#footnote-44)

*3.1.1.4 Adviesrapport*

Op basis van het inventarisatieformulier en het klantprofiel (dat is uitgewerkt in *3.3.1 verwerkte gegevens en kwalificatie*) dat gemaakt wordt in het programma Adviesbox, wordt een adviesrapport opgemaakt. Dit rapport benoemt eerder genoemde gegevens behandeld onder ‘*3.1.1.1* *Inventarisatieformulier’* en bevat dus persoonsgegevens. De gegevens die informatie verstrekken zoals bedoeld bij een bijzonder persoonsgegeven, worden niet in dit rapport opgenomen.

### *3.1.2 Opslag en inzage[[45]](#footnote-45)*

De fysieke dossiers waarin niet direct actie moet worden ondernomen, zijn opgeborgen in dossierkasten. Deze kasten kunnen op slot, maar dat gebeurt in de praktijk niet. Dossiers waarin direct werkzaamheden moeten worden verricht, liggen op het bureau van of op de grond bij de adviseur die het dossier in behandeling heeft. Aan het einde van de dag worden de dossiers waarin werkzaamheden zijn verricht niet teruggeplaatst in de kasten en worden de kasten niet afgesloten. De ruimte waarin de dossiers aanwezig zijn, wordt afgesloten als er niemand aanwezig is in de ruimte en aan het einde van de dag. Soms komt het voor dat een adviseur één of meerdere besprekingen heeft bij de klant thuis. De adviseur neemt dan de betreffende dossiers mee naar de besprekingen in zijn of haar tas. Als de adviseur na een bespreking bij een klant naar huis gaat, neemt hij of zij het dossier of de dossiers mee naar binnen bij hem of haar thuis.

De documenten geplaatst in de dossiermappen kunnen worden ingezien door alle adviseurs. Doordat de dossiers niet altijd opgeborgen zijn in de daartoe bestemde kasten, kan het voorkomen dat een klant of derde partij die de ruimte betreedt een glimp opvangt van een dossier waaraan gewerkt wordt. Een van de adviseurs gaf aan dat hij tijdens een afspraak een stapel dossiers heeft liggen op zijn bureau. Deze dossiers zijn gesloten en het bovenste dossier draait hij om.

### *3.1.3 Archief[[46]](#footnote-46)*

Gesloten fysieke dossiers worden opgeborgen in niet afgesloten, kartonnen dozen welke geplaatst zijn onder een bureau. Over het bureau hangt een spandoek van A waardoor de dozen niet zichtbaar zijn. De dozen bevinden zich in de algemene ruimte waarin ook de adviseurs werkzaam zijn. Als de adviseurs niet aanwezig zijn, is de ruimte afgesloten. Ook de ramen van het kantoor zijn dan gesloten. Eens in het jaar worden de dozen naar een professionele partij gebracht die de dossiers vernietigt. Na vernietiging ontvangt A een bewijs van vernietiging.

## 3.2 C

C is een softwareprogramma ontworpen door B waarin alle voor hypotheekadvies benodigde informatie wordt opgeslagen door A. In dit programma bevinden zich de digitale dossiers van klanten. Daarnaast fungeert dit programma als portaal om informatie door te geven aan de geldverstrekker. De geldverstrekker kan door het doorsturen van een stukkenlijst aangeven welke documenten A dient door te sturen vanuit C. Documenten die A in C plaatst, worden doorgezonden naar geldverstrekkers zonder dat deze geldverstrekkers inzage hebben in het programma. Zij ontvangen slechts door A geselecteerde en doorgestuurde documenten.

### *3.2.1 Verwerkte gegevens en kwalificatie*

Aan de hand van het fysieke dossier en Adviesbox (uitgewerkt in 3.3 Adviesbox) worden de velden ingevuld van het systeem C. In dit programma wordt gebruik gemaakt van een mappenstructuur. Er zijn vijf mappen: advies, belasting, hypothecaire lening, levensverzekering en schadeverzekeringen. In elke map, behalve onder belasting en hypothecaire lening, worden documenten geplaatst. Deze documenten bevatten persoonsgegevens. Daarnaast bestaat C uit een stukkenlijst. Deze lijst bestaat uit documenten die de geldverstrekker dient te ontvangen van de klant. A levert deze documenten namens de klant aan bij de geldverstrekker.

*3.2.1.1 Map advies*

De map ‘advies’ bestaat uit facturen, de opdracht tot dienstverlening, het klantprofiel en algemene voorwaarden van de geldverstrekker. Daarnaast bevinden zich in deze map het bouwkundige onderzoek (mits uitgevoerd) en het energierapport en -label van de aan te kopen woning. Tot slot bevat de map advies de dienstenwijzer van A en de berekeningen van de adviseur. Voornoemde documenten bevatten gegevens die zijn aan te merken als persoonsgegevens.[[47]](#footnote-47) De documenten bevatten geen gegevens die zijn aan te merken als bijzondere persoonsgegevens.

*3.2.1.2 Map levensverzekeringen*

In deze map worden documenten opgenomen inzake een overlijdensrisicoverzekering. Deze verzekering wordt vaak tegelijk met het vestigen van een hypotheek afgesloten. Een van de documenten in de map is het aanvraagformulier voor de overlijdensrisicoverzekering. Naast het aanvraagformulier, is een offerte voor de geadviseerde verzekering(en) opgenomen. Het laatste onderdeel in deze map, is de aan de klant geadviseerde polis of zijn de aan de klant geadviseerde polissen. Hierin zijn dezelfde gegevens opgenomen als op het aanvraagformulier.

Uit observaties is gebleken dat de documenten in deze map klantgegevens bevatten die aan te merken zijn als persoonsgegevens.[[48]](#footnote-48) Het aanvraagformulier bevat zowel persoonsgegevens als bijzondere persoonsgegevens.

*3.2.1.3 Map schadeverzekeringen*

Deze map bevat een pakketpolis waarin meerdere schadeverzekeringen zijn opgenomen. Uit observatie is gebleken dat in dit document gegevens van de klant zijn opgenomen om aan te duiden wie de verzekeringnemer is. Deze gegevens zijn aan te merken als persoonsgegevens.[[49]](#footnote-49)

*3.2.1.4 Stukkenlijst*

De stukkenlijst is een lijst met documenten die de geldverstrekker nodig heeft alvorens een hypotheek kan worden gevestigd. Deze documenten dienen door A te worden geüpload in C. C fungeert als doorgeefportaal van informatie aan de geldverstrekker. De geldverstrekker vraagt enkele verplichte documenten aan A. In sommige gevallen vraagt de geldverstrekker aanvullende documenten, dit is afhankelijk van de persoonlijke situatie van de klant.

*Verplichte documenten*

De stukken die de geldverstrekker in elk geval opvraagt bij A zijn de koopakte van het pand, een kopie van het legitimatiebewijs, een recente en originele werkgeversverklaring en een door de klant ondertekend renteaanbod. Daarnaast dient A een SEPA machtiging voor automatische afschrijving van de rekening van de klant, een recente salarisstrook van de klant en een recent opgemaakt origineel taxatierapport van het aan te schaffen pand door een erkende taxateur te uploaden in C. Verder dient een kopie van de koopovereenkomst van de door de klant aan te kopen woning, de financieringsopzet van A en een kopie van een recent bankafschrift op naam van de klant(en) van elke rekening waarvoor de klant een SEPA machtiging afgeeft, te zijn geplaatst. Tot slot dient een bewijs van eigen middelen van de klant aangeleverd te worden via C. Deze documenten bevatten klantgegevens welke kunnen worden aangemerkt als persoonsgegevens en bijzondere persoonsgegevens.[[50]](#footnote-50)

*Optionele documenten*

Naast de voorgaande documenten, kan de geldverstrekker om aanvullende documenten vragen als dit noodzakelijk is gezien de persoonlijke situatie van de klant. Hierbij kan het gaan om een echtscheidingsconvenant, -beschikking en/of –akte. Ook kan, indien de klant al een woning bezit, gevraagd worden om een schuldrestopgave van de bestaande hypotheek en een taxatierapport of ondertekende verkoopovereenkomst van de eigen woning van de klant om te bepalen of een overbrugging noodzakelijk is. Als de klant al een eigen woning bezit, vraagt de geldverstrekker ook om een kopie van de opdracht tot verkoop van de huidige woning van de klant. Als de eigen woning later verkocht wordt dan aankoop van de nieuwe woning plaatsvindt, dient de klant een bewijs van eigen middelen te overleggen waaruit blijkt dat gedurende twaalf maanden dubbele lasten gedragen kunnen worden. Deze documenten bevatten klantgegevens welke kunnen worden aangemerkt als persoonsgegevens.[[51]](#footnote-51)

### *3.2.2 Opslag en inzage[[52]](#footnote-52)*

Voornoemde documenten worden opgeslagen in het systeem C van B. Het programma is geïnstalleerd op de laptop en wordt geopend vanaf het bureaublad. Voordat gewerkt kan worden in C, dienen de adviseurs met een wachtwoord in te loggen in het programma. De gegevens die worden opgeslagen in dit programma, worden opgeslagen op de harde schijf van de laptop.

De documenten geplaatst in C kunnen worden ingezien door de adviseurs van A en medewerkers van B.[[53]](#footnote-53) De medewerkers van B dienen hiertoe geen inzageverzoek te sturen en kunnen te allen tijde op hoofdlijnen inzien wat er in C geplaatst is. Zij kunnen zien dat er documenten geplaatst zijn in het systeem, maar deze kunnen zij niet openen. Geldverstrekkers kunnen de gegevens uit C slechts inzien wanneer de adviseur het document geselecteerd heeft en doorstuurt naar de geldverstrekker. De geldverstrekker kan dus niet inloggen in C, maar krijgt via C documenten doorgestuurd.

### *3.2.3 Bewerkersovereenkomst*

Voor de verwerking van klantgegevens in C, heeft A met B een bewerkersovereenkomst gesloten. Uit de overeenkomst blijkt dat bij verwerking van persoonsgegevens dient te worden voldaan aan de AVG. Verder bepaalt de overeenkomst het onderwerp, de duur, de aard en het doel van de overeenkomst. Daarnaast bevat de overeenkomst bepalingen omtrent betrokken gegevens, categorieën van betrokkenen en de functionaris voor gegevensbescherming. Ook zijn uitvoeringsregels opgenomen voor de verwerking, is beschreven op welke wijze invulling wordt gegeven aan beveiliging van persoonsgegevens en op welke wijze dit gecontroleerd wordt. Een ander onderwerp dat uitgewerkt is in de overeenkomst is de wijze waarop incidentmanagement is ingevuld en hoe wordt omgegaan met datalekken. Naast voornoemde onderwerpen bevat de overeenkomst ook bepalingen omtrent een gegevensbeschermingseffectbeoordeling, privacy by design en bij aanstelling van onderaannemers. Tot slot zijn in de overeenkomst bepalingen opgenomen omtrent aansprakelijkheid, bewaartermijnen, teruggave van persoonsgegevens, vernietiging van persoonsgegevens en is beschreven dat Nederlands recht van toepassing is op de overeenkomst.

De strekking van de overeenkomst is dat B beveiligingsmaatregelen neemt ter uitvoering van de verwerking van de persoonsgegevens overeenkomstig de door A bepaalde doelen en dat melding wordt gemaakt aan A op het moment dat sprake is van een inbreuk op de beveiliging. Ook blijkt uit de overeenkomst dat de gegevens die A in C verwerkt, worden bewerkt, gerangschikt en opgeslagen. B verleent ook onderhoudsdiensten op de software en geeft ondersteuning bij het gebruik van C.

Verder is bepaald dat A aan B bekend dient te maken welke categorieën van gegevens worden verwerkt, om welke categorieën van betrokkenen het gaat en gegevens betreffende de functionaris van gegevensbescherming van A. Daarnaast is opgenomen dat een grondslag aanwezig is voor de verwerking van de persoonsgegevens en dat het gaat om een rechtmatige verwerking.

Wat betreft de uitvoering van de verwerking is bepaald dat B gegevens uitsluitend verwerkt op een wijze die noodzakelijk is voor de dienstverlening. Overige verwerkingen door B zullen slechts gedaan worden na expliciete opdracht van A of als daartoe een wettelijke verplichting bestaat. De gegevens die B ontvangt van A zullen niet voor eigen doeleinden of doeleinden van derden worden verwerkt. B zal de gegevens ook niet opslaan in of doorgeven aan derde landen, behoudens bij voorafgaande uitdrukkelijke, schriftelijke toestemming van A. In de overeenkomst verklaart B ook dat zij geen persoonsgegevens aan enige derde toont, verstrekt of anderszins ter beschikking stelt, tenzij dit nodig of toegestaan is voor de dienstverlening of wanneer hiervoor uitdrukkelijke, schriftelijke toestemming van A voor is verkregen. Naast voornoemde bepalingen, verklaart B dat zij bijstand verleent aan A bij het inwilligen van verzoeken van klanten gebaseerd op hun rechten.

Een ander onderwerp waaraan de overeenkomst invulling geeft is de beveiliging van persoonsgegevens en de controle daarop. Uit deze bepalingen blijkt dat B technische en organisatorische beveiligingsmaatregelen neemt die gezien de huidige stand der techniek en de daarmee gemoeide kosten overeenstemmen met de aard van de te verwerken persoonsgegevens. Als A vermoed dat er privacy- of informatie-incidenten plaats hebben gevonden, kan zij verzoeken om in overleg te treden waarna het beveiligingsbeleid van B zal worden aangepast. B verklaart voortdurend te evalueren op eigen werkwijze en indien nodig haar maatregelen te verscherpen, aanvullen of verbeteren. Mocht er toch een incident plaatsvinden met de persoonsgegevens, dan is bepaald dat B A hieromtrent direct in kennis stelt evenals informatie verschaft betreffende de aard van het incident, het risico dat gegevens onrechtmatig verwerkt zijn of kunnen worden en welke maatregelen getroffen zijn of getroffen kunnen worden om de schade zo veel mogelijk te beperken. Verder verklaart B redelijk te verwachten ondersteuning te bieden aan A bij de uitvoering van haar onderzoek naar het incident en verklaart betrokkenen, autoriteiten en derden enkel over incidenten te informeren voor zover hiertoe een wettelijke verplichting bestaat.

Nog een onderwerp dat wordt uitgewerkt in de overeenkomst is privacy by design en privacy by default. B verklaart de gegevens te beschermen door ontwerp en door standaardinstellingen. Naast privacy by design en by default, verklaart B dat zij de verwerking niet uitbesteedt aan een derde partij zonder dat daarvoor voorafgaand schriftelijke toestemming voor is gegeven door A en dat in het geval dat gebruik wordt gemaakt van een onderaannemer B de verantwoordelijkheid draagt voor het naleven van deze overeenkomst.

Tot slot is in de overeenkomst bepaald in welke gevallen B aansprakelijk kan worden gesteld en welke regels gelden omtrent bewaartermijnen, teruggave en vernietiging van persoonsgegevens. Zo is bepaald dat persoonsgegevens door B niet langer dan strikt noodzakelijk en niet na beëindiging van de bewerkersovereenkomst worden bewaard tenzij een afwijkende bewaartermijn is overeengekomen met A. Er is met B geen afwijkende bewaartermijn overeengekomen. De gegevens die B bezit zullen op schriftelijk verzoek van A worden teruggegeven en worden vernietigd. Vernietiging vindt plaats binnen vier weken na het verzoek en er zal een bewijs worden overlegd van vernietiging of verwijdering van de gegevens door B.

Na beëindiging van de overeenkomst blijven bepalingen omtrent geheimhouding en aansprakelijkheid van kracht.

## 3.3 Adviesbox

Adviesbox is het softwareprogramma waarin het inventarisatieformulier dat uitgeprint in de fysieke dossiers zit, digitaal wordt ingevuld. De onderwerpen die in dit programma worden uitgewerkt, zijn dezelfden als eerder genoemd in ‘*3.1.1.1 Inventarisatieformulier’*. Verder wordt in dit programma een klantprofiel uitgewerkt.

### *3.3.1 Verwerkte gegevens en kwalificatie*

De persoonsgegevens die verwerkt worden in Adviesbox zijn hetzelfde als de gegevens die verwerkt worden in het inventarisatieformulier uit het fysieke dossier. Het inventarisatieformulier dat eerder is beschreven, is namelijk een uitdraai van het programma Adviesbox. Adviesbox is hetzelfde inventarisatieformulier maar dan in digitale vorm. Het gaat hierbij, zoals eerder geconstateerd, om gevoelige gegevens welke niet als persoonsgegevens zijn aan te merken, persoonsgegevens en bijzondere persoonsgegevens. Het klantprofiel beschrijft de financiële doelen van de klant en bevat de voor- en achternaam van de klant. Deze gegevens zijn aan te merken als persoonsgegeven.[[54]](#footnote-54)

### *3.3.2 Opslag en inzage*

De gegevens die worden verwerkt in Adviesbox worden opgeslagen in dit programma. Dit programma is geïnstalleerd op de laptop en wordt geopend vanaf het bureaublad. Voordat gewerkt kan worden in Adviesbox, dienen de adviseurs met een wachtwoord in te loggen in het programma. De gegevens die worden opgeslagen in dit programma, worden opgeslagen op de harde schijf van de laptop.

De opgeslagen gegevens in Adviesbox kunnen worden ingezien door de adviseurs van A en door de medewerkers van Adviesbox.[[55]](#footnote-55) De medewerkers van Adviesbox kunnen echter niet te allen tijde inzien wat de adviseurs van A in het systeem onderbrengen. Zij kunnen dan ook slechts op hoofdlijnen ondersteunen bij het gebruik van dit programma. Als zich een probleem voordoet met het programma, kan A contact opnemen met de support afdeling van Adviesbox. Zij sturen dan een inzageverzoek naar de adviseur dat dient te worden geaccepteerd alvorens zij inzage hebben in de verwerkte gegevens. Zodra de inzagesessie wordt verbroken, vervalt de mogelijkheid voor de medewerkers van Adviesbox om kennis te nemen van de verwerkte gegevens door A.

## 3.4 Juistheid gegevens en gegevenswissing[[56]](#footnote-56)

Op dit moment controleren de adviseurs van A de juistheid van de gegevens slechts op het moment dat werkzaamheden worden verricht in het dossier. Nadat de financiering rond is, worden de gegevens van de klanten niet meer gecontroleerd. A vraagt haar klanten niet om haar te informeren over wijzigingen in de persoonlijke situatie of met betrekking tot contactgegevens. Er vindt dus geen actualisering plaats van de gegevens.

De door A verwerkte gegevens in de fysieke dossiers worden na ongeveer één jaar vernietigd door een gecertificeerd bedrijf. Hiervan ontvangt A een bewijsstuk. Wat betreft de gegevens van klanten in digitale omgevingen als C en Adviesbox is geen bewaartermijn vastgesteld. Momenteel bewaart A alle digitale dossiers en vernietigt zij of laat zij geen klantgegevens verwijderen of vernietigen.

## 3.5 Controle werkwijze[[57]](#footnote-57)

Momenteel controleert A niet of adviseurs op de juiste en integere wijze met gegevens van klanten omgaan. Hierdoor is het voor A niet inzichtelijk of er een inbreuk wordt gemaakt op het recht op bescherming van persoonsgegevens. Er is geen protocol opgesteld wat betreft het melden van datalekken aan de toezichthoudende autoriteit en betrokkenen. Binnen de organisatie is er niemand aangesteld om toe te zien op een integere werkwijze. De rol van een functionaris voor gegevensbescherming wordt momenteel dus niet vervuld.

## 3.6 Beveiliging

De beveiligingsmaatregelen die A heeft genomen bij de verwerking van klantgegevens, zijn op te delen in twee categorieën: organisatorische maatregelen en technische maatregelen. De organisatorische maatregelen zien onder andere toe op de bescherming van fysieke dossier door de wijze waarop adviseurs met de dossiers omgaan. Momenteel worden de fysieke dossiers waarin werkzaamheden worden verricht niet in kasten geplaatst en worden deze kasten niet afgesloten. Het archief van fysieke dossiers bevindt zich ook niet in afgesloten kasten. Deze dossiers zijn namelijk in kartonnen, niet gesloten dozen geplaatst onder een bureau. Aan het einde van de dag worden de ramen en deuren op kantoor afgesloten. Het pand van A is niet beveiligd met een alarmsysteem.

De technische maatregelen hebben betrekking op de beveiliging van laptops, het netwerk en programma’s. De adviseurs van A werken via laptops. Deze laptops zijn beveiligd met één wachtwoord. Op kantoor hangt een memo met de wachtwoorden en gebruikersnamen van de adviseurs zodat de adviseurs te allen tijde kunnen inloggen op de laptop van een collega die niet aanwezig is. Naast het wachtwoord, zijn de laptops voorzien van een virusscanner, een firewall en een anti-spam-oplossing. A werkt niet door middel van een ingeplugde UTP-kabel in de laptop om een beveiligde internetverbinding tot stand te brengen. Zij werkt uitsluitend via een eigen WiFi-netwerk. Dit netwerk wordt niet alleen gebruikt door de adviseurs in het kader van hun dienstverlening, maar ook door klanten. Er is dus geen gescheiden netwerk.

De programma’s C en Adviesbox worden geopend met een wachtwoord en inlognaam vanaf het bureaublad van de laptop. Na het inloggen in C en Adviesbox kunnen de adviseurs alle opgeslagen informatie openen. Het is namelijk niet zo dat de accounts specifiek toegewezen rechten hebben die de toegang tot bepaalde gegevens regelen. Bestanden die A opstelt voor hypotheekadviseringen in bijvoorbeeld Word, PowerPoint of Excel worden opgeslagen op de harde schijf van de laptop. Ook hetgeen A opslaat in C en Adviesbox wordt bewaard op de harde schijf van de laptop. De harde schijf is niet beveiligd en kan bij diefstal worden uitgelezen als deze wordt gekoppeld aan een andere computer of laptop. Van de gegevens op de laptops c.q. harde schijven van de laptops worden niet consequent back-ups gemaakt. Enkele adviseurs maken eens in de zoveel tijd een back-up van de harde schijf van de laptop op een externe harde schijf. Deze schijf bewaren ze in een kluis bij hen thuis. De back-ups zijn niet volledig omdat deze niet consequent en niet door alle adviseurs gemaakt worden.

## 3.7 Verwerker of verwerkingsverantwoordelijke

Met de komst van de AVG wordt de toepassing van de begrippen verwerkingsverantwoordelijke en verwerker steeds gecompliceerder. Dit geeft onduidelijkheden wat betreft verantwoordelijkheden en de werkingssfeer van relevante nationale wetgeving en kan de naleving en effectiviteit van regels omtrent gegevensbescherming nadelig beïnvloeden. Richtsnoeren en uitleg van deze begrippen zorgen voor een samenhangende en geharmoniseerde benadering waardoor gegevensbescherming wordt gewaarborgd. Deze richtsnoeren en uitleg zijn gegeven door groep gegevensbescherming artikel 29.[[58]](#footnote-58)

*Verwerkingsverantwoordelijke*

Een partij is aan te merken als verwerkingsverantwoordelijke als deze partij voor de verwerking verantwoordelijk is en ook verantwoordelijk kan worden gehouden voor de naleving van de verplichtingen uit de AVG. Het gaat hierbij om de partij die de doelen en middelen voor de verwerking vaststelt. Door te beoordelen wie bepaalt waarom de desbetreffende specifieke verwerking plaatsvindt, welke partij de verwerking initieert en de mate waarin een partij vrijheid heeft bij de verwerking wordt bepaald of een partij doelen en middelen vaststelt. De mate van vrijheid wordt bepaald door te bekijken welke partij aanwijzingen voor de verwerking geeft of ontvangt. Hierbij speelt ook een rol wie de termijn voor verwerking bepaalt en vrijheid heeft bij het geven van toegang tot de verwerking. De feitelijke gang van zaken geeft hierbij doorslag. [[59]](#footnote-59) De bevoegdheid tot het vaststellen van doelen en middelen blijkt uit een uitdrukkelijke juridische bevoegdheid, een impliciete bevoegdheid of uit feitelijke invloed.

*Verwerker*

Een partij is aan te merken als verwerker als het gaat om een partij die een aparte rechtspersoon is, die losstaat van de verwerkingsverantwoordelijke en persoonsgegevens verwerkt ten behoeve van een verwerkingsverantwoordelijke. Deze partij kan dus meerdere verwerkingen tegelijk verrichten in het belang van verschillende verwerkingsverantwoordelijken. Hierbij heeft de verwerkende partij geen invloed op de vast te stellen doelen van of middelen voor verwerking. Bij delegatie door verwerkingsverantwoordelijke kan de verwerker handelingsvrijheid hebben voor de wijze waarop de belangen van de verwerkingsverantwoordelijke het beste kunnen worden gediend. Het is ook mogelijk dat de verwerkingsverantwoordelijke meerdere verwerkers inschakelt of dat de verwerker één of meerdere onderaannemers aanstelt. Als een persoon of partij geen specifieke legitimiteit of bevoegdheid heeft bij de verwerking van persoonsgegevens, is deze aan te merken als derde.

### *3.4.1 Fysieke dossiers*

A is de organisatie die verwerking van persoonsgegevens initieert en bepaalt wat het doel van en de middelen voor de verwerking zijn. Het vaststellen hiervan doet A op basis van feitelijke invloed. A heeft veel vrijheid bij de bepaling van de doelen en middelen. Zij ontvangt hierbij geen aanwijzingen van een andere partij, bepaalt zelf gedurende welke termijn de gegevens worden verwerkt en is vrij te bepalen wie toegang krijgt tot de fysieke dossiers. A is dus verantwoordelijk voor de verwerking en naleving van de verplichtingen van de AVG wat betreft de fysieke dossiers. Zij deelt deze verantwoordelijkheid niet met een andere partij of andere partijen aangezien geen andere partij invloed heeft op de doelen en middelen van deze verwerking.

### *3.4.2 C en Adviesbox*

A initieert de verwerking van persoonsgegevens en bepaalt het doel en de middelen voor de verwerking. De vaststelling van de doelen en middelen geschied op basis van feitelijke invloed. Dit blijkt uit contractuele verhoudingen tussen B, Adviesbox en A. Bij het vaststellen van de doelen en middelen heeft A veel vrijheid. Zij bepaalt zonder dat anderen daar invloed op hebben haar doelen van de verwerking en middelen die zij inzet voor de verwerking. Zij heeft gekozen om te werken met de softwareprogramma’s C en Adviesbox. A heeft geen invloed op de velden die gevuld moeten worden in deze programma’s. Uit contact met B en Adviesbox is gebleken dat hun programmavelden op nationaal niveau worden gevormd via Hypotheken Data Netwerk (hierna te noemen HDN) en dat B en Adviesbox nauwelijks invloed kunnen uitoefenen op de velden in hun programma’s. Blijkens contact met HDN worden de eisen die zij aan programma’s stellen niet door hen geformuleerd, maar door de financieringsmaatschappijen. Er is geen sprake van een geheel van verwerkingen met een gezamenlijk doel of gebruikmaking van gezamenlijk vastgestelde middelen. Daarom zijn voornoemde partijen niet aan te merken als gezamenlijke verwerkingsverantwoordelijken. A is aan te merken als verwerkingsverantwoordelijke. De diensten van B betreffende C en Adviesbox zijn ten behoeve van A. Zij zijn daarom aan te merken als verwerker.

## 3.8 Samenvatting

Uit dit hoofdstuk blijkt dat in fysieke dossiers gevoelige gegevens, persoonsgegevens en bijzondere persoonsgegevens van klanten te vinden zijn. De dossiers worden niet opgeborgen in kasten en de kasten waarin dossiers geplaatst zijn, worden niet afgesloten. Het archief van de fysieke dossiers bevindt zich niet in een afgesloten kast, maar in kartonnen dozen welke onder een bureau zijn geplaatst. Doordat de dossiers niet worden opgeborgen, is het voor velen mogelijk kennis te nemen van de inhoud van de dossiers. In het systeem C worden ook gevoelige gegevens, persoonsgegevens en bijzondere persoonsgegevens verwerkt. C is geïnstalleerd op de laptop en wordt geopend vanaf het bureaublad door in te loggen in het programma. De documenten die de adviseurs in dit programma uploaden kunnen door alle adviseurs en door medewerkers van C worden ingezien, zonder dat de medewerkers van C hiertoe een inzageverzoek moeten indienen. A heeft met B een bewerkersovereenkomst gesloten inzake C waarin beschreven is dat bij de verwerking dient te worden voldaan aan de AVG en toekomstige privacywetgeving. Wat betreft Adviesbox is gebleken dat in dit systeem gevoelige gegevens, persoonsgegevens en bijzondere persoonsgegevens worden verwerkt en dat deze gegevens worden opgeslagen in het systeem. Dit systeem is geïnstalleerd op de laptop en kan worden geopend door het invoeren van een wachtwoord vanuit het bureaublad. De gegevens die in dit systeem zijn opgeslagen zijn zichtbaar voor de adviseurs van A en medewerkers van Adviesbox na goedkeuring van een inzageverzoek. Verder is uit dit hoofdstuk gebleken dat de juistheid van persoonsgegevens enkel wordt gecontroleerd als adviseurs werkzaamheden verrichten in het dossier en worden digitale dossiers niet verwijderd. Uit dit hoofdstuk blijkt ook dat A niet controleert of adviseurs op integere wijze omgaan met klantgegevens en dat er nauwelijks technische en organisatorische maatregelen zijn genomen om de persoonsgegevens van klanten te beschermen. Tot slot blijkt uit dit hoofdstuk dat A aan te merken is als verwerkingsverantwoordelijke ten opzichte van de fysieke dossiers en de systemen C en Adviesbox.

# Hoofdstuk 4. De Algemene verordening gegevensbescherming

*In dit hoofdstuk is in kaart gebracht wat de Algemene verordening gegevensbescherming (hierna te noemen AVG) inhoudt. Allereerst is beschreven wanneer de verordening bekend is gemaakt en in werking is getreden. Vervolgens zijn de geschiedenis van privacywetgeving en het toepassingsgebied van de AVG beschreven. Daarna is beschreven wat de doelstelling van de AVG is, welke verwerkingsregels gelden op grond van de AVG en welke verplichtingen rusten op een verwerkingsverantwoordelijke blijkens de AVG. Hierbij is beschreven op welke wijze digitale omgevingen kunnen worden beschermd zodat voldaan is aan de AVG en is een koppeling gemaakt naar relevante bepalingen in de Wet financieel toezicht (hierna Wft) en de Wet ter voorkoming van witwassen en financieren van terrorisme (hierna Wwft). Tot slot is in dit hoofdstuk opgenomen welke autoriteit toezicht houdt op de AVG en welke bevoegdheden zij hierbij heeft.*

## 4.1 Bekendmaking en inwerkingtreding[[60]](#footnote-60)

De AVG, opgesteld door het Europees Parlement en de Raad van de Europese Unie, is ondertekend op 27 april 2016 en is gepubliceerd op 4 mei 2016. Vervolgens is de verordening aangenomen op 24 mei 2016 en zal deze van toepassing worden op 25 mei 2018. Omdat er voor (sommige) ondernemingen grote organisatorische en/of technische wijzigingen moeten plaatsvinden om aan de AVG te voldoen, is een termijn ingebouwd van twee jaar voordat de verordening van toepassing is.

## 4.2 Geschiedenis

De AVG gaat de Europese richtlijn bescherming persoonsgegevens 95/46/EG (hierna richtlijn bescherming persoonsgegevens) opgesteld door de Europese Raad en het Parlement vervangen. De strekking van deze richtlijn is omgezet in de wet bescherming persoonsgegevens (Wbp) en moet de bescherming van persoonsgegevens waarborgen zonder dat het vrije verkeer op de interne markt van de Europese Unie met betrekking tot deze gegevens wordt belemmerd.

Door snelle technologische ontwikkelingen, globalisering en een significante stijging van de mate waarin persoonsgegevens worden verzameld en gedeeld, biedt de Wbp niet meer voldoende zekerheid dat persoonsgegevens beschermd zijn.[[61]](#footnote-61) Hierbij speelt ook een rol dat steeds meer natuurlijke personen hun persoonsgegevens wereldwijd bekend maken.[[62]](#footnote-62) Er is dus een krachtiger en coherenter kader voor gegevensbescherming vereist dat meer rechtszekerheid en praktische zekerheid biedt. Hiervoor is aanscherping van de doelstellingen en beginselen van richtlijn bescherming persoonsgegevens om meer rechtszekerheid te bieden vereist zonder dat een belemmering van het vrije verkeer van persoonsgegevens ontstaat. Met de aanscherping en aanvulling moet een gelijkwaardig, consistent en hoog beschermingsniveau worden gewaarborgd en dienen belemmeringen van het vrije verkeer van persoonsgegevens te worden opgeheven. Hiertoe zal een nadere omschrijving en versterking van de rechten van betrokkenen en plichten van verwerkers en verwerkingsverantwoordelijken noodzakelijk zijn.

## 4.3 Toepassingsgebied

Om te bepalen of de AVG van toepassing is, wordt gekeken naar de inhoud (materieel) en naar het grondgebied (territoriaal) waar de situatie zich voordoet. Het materiële toepassingsgebied is technologieneutraal geformuleerd en betreft de geheel of gedeeltelijke geautomatiseerde verwerking en verwerking van persoonsgegevens in een bestand of gegevens die bestemd zijn om hierin op te nemen.[[63]](#footnote-63) Hiervan is sprake als ICT-middelen en/of internet bij de verwerking van gegevens wordt gebruikt. Wat betreft de territoriale toepasselijkheid is bepaald dat de AVG van toepassing is op verwerkers en verwerkingsverantwoordelijken binnen de Europese Unie (hierna: EU) en op verwerkingen door organisaties buiten de EU die gegevens verwerken van personen die zich binnen de EU bevinden. Hierbij gaat het om het aanbieden van goederen of diensten of om het monitoren van gedrag.

## 4.4 Doelstelling

Het doel van de AVG is een krachtig en coherenter kader voor gegevensbescherming in de EU dat wordt gesteund door strenge handhaving zodat de interne markt ontwikkelt doordat de digitale economie voldoende vertrouwen en rechtszekerheid krijgt.[[64]](#footnote-64) Om dit te bereiken zijn in de AVG regels vastgesteld betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van persoonsgegevens.[[65]](#footnote-65) Door deze bepalingen wordt zorg gedragen voor een goede werking van de interne markt binnen de Europese Unie en wordt voorkomen dat een verbod of beperking op de verwerking van persoonsgegevens hierop een belemmering vormt.

## 4.5 Verwerkingsregels

In de AVG is opgenomen op welke wijze verwerking van persoonsgegevens dient te geschieden. Hiervoor zijn algemene regels, regels voor verwerkers en regels voor verwerkingsverantwoordelijken opgesteld. Deze regels zijn afgestemd op de doelen en beginselen die gelden voor de verwerking van persoonsgegevens. Belangrijke beginselen die blijken uit de verwerkingsregels, zijn dat de verwerking behoorlijk, rechtmatig en transparant moet zijn. Dit houdt in dat het voor betrokkenen inzichtelijk moet zijn in hoeverre en op welke manier er persoonsgegevens worden verwerkt. Dit is mogelijk door te zorgen voor begrijpelijk geformuleerde en toegankelijke communicatie. Deze eisen zijn niet alleen gesteld aan de verwerking zelf, maar gelden bijvoorbeeld ook bij een verzoek om inzage[[66]](#footnote-66) of bij het afhandelen van bezwaren[[67]](#footnote-67). Met rechtmatigheid wordt bedoeld dat de handelswijze met betrekking tot persoonsgegevens niet in strijd is met het ongeschreven recht.[[68]](#footnote-68) Er is sprake van een rechtmatige verwerking als de betrokkene toestemming heeft gegeven voor de verwerking van zijn persoonsgegevens voor een specifiek doel of specifieke doeleinden.[[69]](#footnote-69) Onder toestemming wordt verstaan een vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene aanvaardt dat zijn persoonsgegevens worden verwerkt.[[70]](#footnote-70) Deze toestemming moet actief worden gegeven op een duidelijk en begrijpelijk geformuleerde vraag naar de toestemming.[[71]](#footnote-71) Er is ook sprake van rechtmatigheid als aan het noodzakelijkheidscriterium voldaan is of dat op verzoek van de betrokkene maatregelen worden genomen voor verwerking alvorens de overeenkomst is gesloten.[[72]](#footnote-72) Er is sprake van noodzakelijkheid als de overeenkomst niet goed kan worden nagekomen zonder verwerking van de persoonsgegevens. De verwerking is per definitie noodzakelijk als de verwerking plaats dient te vinden in het kader van een wettelijke verplichting die rust op de verwerkingsverantwoordelijke of wanneer de verwerking vitale belangen van de betrokkene of van een andere natuurlijke persoon beschermt.[[73]](#footnote-73) Ook is er sprake van noodzakelijke verwerking wanneer de gegevens door de verwerkingsverantwoordelijke verwerkt moeten worden ter vervulling van een taak van algemeen belang of in de uitoefening van het openbaar gezag.[[74]](#footnote-74) Tot slot is voldaan aan het noodzakelijkheidscriterium wanneer verwerking nodig is voor behartiging van gerechtvaardigde belangen van de verwerkingsverantwoordelijke of een derde.[[75]](#footnote-75) Voornoemde verwerking is niet noodzakelijk wanneer de belangen of grondrechten en fundamentele vrijheden van de betrokkene zwaarder wegen dan de belangen van de verwerkingsverantwoordelijke of derde.

Naast dat de verwerking behoorlijk, rechtmatig en transparant moet zijn, bepaalt de AVG dat verwerking van persoonsgegevens slechts mogelijk is voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden (beginsel van doelbinding).[[76]](#footnote-76) Deze doeleinden moeten voorafgaand aan de verwerking zijn vastgesteld en beschreven.[[77]](#footnote-77) Een doel is gerechtvaardigd als er geen sprake is van strijd met de wet en als de inperking van het grondrecht op privacy een goede reden heeft blijkens een belangenafweging tussen de betrokkene en de verwerkingsverantwoordelijke. [[78]](#footnote-78) Persoonsgegevens mogen slechts verder verwerkt worden met een ander doel dan waarvoor zij verzameld zijn als deze verdere verwerking verenigbaar is met het aanvankelijke doel van de verzameling van de gegevens.[[79]](#footnote-79)

Nog een eis die de AVG stelt aan de verwerking is dat de verwerking toereikend, ter zake dienend en beperkt tot de noodzakelijke verwerking moet zijn. [[80]](#footnote-80) Hieruit blijkt het beginsel van minimale gegevensverwerking. Dit principe zorgt ervoor dat slechts de voor het doel noodzakelijke verwerking plaats mag vinden en dat de persoonsgegevens zo snel mogelijk moeten worden gewist of onherkenbaar moeten worden gemaakt.[[81]](#footnote-81) Onherkenbaar maken is mogelijk door te anonimiseren. Uit dit principe vloeit tevens voort dat persoonsgegevens alleen mogen worden verwerkt als het doel niet op een andere wijze kan worden verwezenlijkt.[[82]](#footnote-82)

De volgende eis waaraan de verwerking moet voldoen, is dat maatregelen moeten worden genomen om onjuiste persoonsgegevens gelet op de doeleinden onverwijld te wissen of de rectificeren.[[83]](#footnote-83) De gegevens moeten dus ook worden geactualiseerd zodat zij juist zijn. De verwerkingsverantwoordelijke heeft een vergaande inspanningsplicht om de juistheid te waarborgen en mag niet afwachten tot betrokkenen gaan klagen over onjuistheid van gegevens.[[84]](#footnote-84) Als gegevens onjuist of achterhaald zijn moeten zij namelijk worden gewist.

De volgende eis die gesteld wordt aan de verwerking van persoonsgegevens, is dat de gegevens niet langer mogen worden bewaard dan noodzakelijk is voor de verwerking.[[85]](#footnote-85) Deze eis is ook wel bekend als het beginsel van opslagbeperking. De AVG verlangt van de verwerkingsverantwoordelijke dat deze een termijn vaststelt voor het wissen van gegevens of voor een periodieke toetsing. Er hoeft door verwerkingsverantwoordelijken geen concreet tijdstip te worden vastgesteld, maar de verwerkingstermijn moet wel een duidelijk vast te stellen einde hebben.[[86]](#footnote-86) Wanneer gegevens gedurende langere tijd moeten worden bewaard op grond van een wettelijke bepaling, is voornoemde bepaling niet aan de orde.[[87]](#footnote-87) Een andere uitzondering op het beginsel van opslagbeperking is wanneer de persoonsgegevens langere tijd worden bewaard ten behoeve van archivering in het algemeen belang, historisch onderzoek of statistische doeleinden. Voor deze uitzonderingen wat betreft de bewaartermijn moeten passende waarborgen genomen ter beveiliging van de persoonsgegevens.[[88]](#footnote-88)

Daarnaast bepaalt de AVG dat bij de verwerking van persoonsgegevens passende technische of organisatorische maatregelen moeten worden genomen zodat een passende beveiliging is gewaarborgd.[[89]](#footnote-89) Door deze maatregelen moeten de persoonsgegevens beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking, tegen onopzettelijk verlies, vernietiging of beschadiging. Hieruit blijkt het beginsel van integriteit en vertrouwelijkheid. Deze beginselen zijn in de AVG terug te vinden onder afdeling twee van hoofdstuk vier.[[90]](#footnote-90) Deze afdeling beschrijft op welke wijze de verwerking dient te worden beveiligd en dat een meldplicht geldt bij het lekken van data. De melding dient te worden gemaakt door de verwerkingsverantwoordelijke bij de toezichthoudende autoriteit binnen 72 uur na kennisname van het lek tenzij het onwaarschijnlijk is dat de inbreuk een risico met zich meebrengt voor de rechten en vrijheden van natuurlijke personen.[[91]](#footnote-91) Voor de verwerker geldt de plicht om de verwerkingsverantwoordelijke in kennis te stellen van het lek zodra hij hiervan kennis heeft genomen.[[92]](#footnote-92) In sommige gevallen dient het datalek ook gemeld te worden aan de betrokkene als de inbreuk een hoog risico inhoudt voor de rechten en vrijheden van die persoon of van natuurlijke personen.[[93]](#footnote-93) Melding aan de betrokkene is niet vereist als de verwerkingsverantwoordelijke aantoonbaar passende technische en organisatorische maatregelen heeft toegepast, de verwerkingsverantwoordelijke achteraf maatregelen heeft genomen om het hoge risico voor de betrokkene af te wenden, als de mededeling dusdanig zware inspanningen vereist van de verwerkingsverantwoordelijke dat dit redelijkerwijs niet van hem gevraagd kan worden en als er een wettelijke uitzondering bestaat voor de melding aan de betrokkene.[[94]](#footnote-94) Voor financiële dienstverleners geldt een wettelijke uitzondering op de meldingsplicht aan betrokkenen.[[95]](#footnote-95)

Als een verwerkingsverantwoordelijke bijzondere persoonsgegevens verwerkt, is het van essentieel belang dat deze gegevens op een goede wijze beschermd worden. Hierbij gaat het om persoonsgegevens die informatie geven over bijvoorbeeld ras, politieke opvattingen, genetische gegevens, seksuele gerichtheid.[[96]](#footnote-96) Verwerking van deze gegevens is niet toegestaan onder de AVG tenzij een uitzondering geldt. De eerste uitzondering doet zich voor als er door de betrokkene toestemming voor is verleend.[[97]](#footnote-97) Deze toestemming is in de vorm van een expliciete wilsuiting gericht op het geven van toestemming. Verwerking is ook toegestaan als dit nodig is ter uitvoering van wettelijke plichten of rechten op het gebied van arbeidsrecht, socialezekerheidsrecht en socialebeschermingsrecht.[[98]](#footnote-98) Daarnaast mogen bijzondere persoonsgegevens verwerkt worden ter bescherming van vitale belangen van de betrokkene of een natuurlijk persoon als deze niet in staat is toestemming te verlenen.[[99]](#footnote-99) Dit doet zich bijvoorbeeld voor als iemand bewusteloos is in een spoedgeval en toegang tot het medisch dossier wordt verstrekt. Ook geldt een uitzondering als er sprake is van verwerking door politieke, religieuze en levensbeschouwelijke organisaties en vakbonden voor zover dit nodig is voor beheer van contactgegevens van leden en oud-leden.[[100]](#footnote-100) Hiervoor zijn passende waarborgen vereist. Nog een andere uitzondering doet zich voor als het gegevens betreft die de betrokkene zelf openbaar heeft gemaakt.[[101]](#footnote-101) Denk hierbij aan het publiceren van gegevens op bijvoorbeeld een sociale netwerkdienst als Facebook. Daarnaast is de verwerking uitgezonderd die noodzakelijk is voor gerechtelijke procedures.[[102]](#footnote-102) De gegevens gelden dan als bewijsstuk. Ook is verwerking van bijzondere gegevens toegestaan in het kader van een zwaarwegend algemeen belang met wettelijke grondslag.[[103]](#footnote-103) Verder geldt een uitzondering wanneer de verwerking noodzakelijk is voor medische redenen in verband met arbeid.[[104]](#footnote-104) Nog een uitzondering geldt voor de verwerking van bijzondere persoonsgegevens ter bescherming van ernstige grensoverschrijdende gevaren voor gezondheid.[[105]](#footnote-105) Daarnaast doet zich een uitzondering voor als bijzondere persoonsgegevens verwerkt worden voor archivering in het algemeen belang, voor wetenschappelijk of historisch onderzoek of voor statistische doeleinden.[[106]](#footnote-106) Tot slot is bepaald dat verwerking van bijzondere persoonsgegevens op basis van een wettelijke grondslag een uitzondering vormt op het verwerkingsverbod.[[107]](#footnote-107)

Onder het regime van de wet bescherming persoonsgegevens (hierna te noemen Wbp) is gebleken dat enkele zaken worden aangemerkt als bijzonder persoonsgegeven. Hieronder valt een foto blijkens een uitspraak van de Hoge Raad in het kader van identificatie.[[108]](#footnote-108) Ook merkt de Wbp een Burgerservicenummer aan als bijzonder persoonsgegeven.[[109]](#footnote-109) Onder het regime van de AVG is dit niet meer het geval voor het Burgerservicenummer.[[110]](#footnote-110)

## 4.6 Verplichtingen verwerkingsverantwoordelijke

In het vorige hoofdstuk is geconcludeerd dat A aan te merken is als verwerkingsverantwoordelijke. In de AVG is bepaald dat een verwerkingsverantwoordelijke zich bij de verwerking van persoonsgegevens moet houden aan voornoemde verwerkingsregels en dat op de verwerkingsverantwoordelijke enkele verplichtingen rusten.

Zo blijkt uit de AVG dat de verwerkingsverantwoordelijke technische en organisatorische maatregelen moet nemen gelet op de aard, de omvang, de context en het doel van de verwerking om de naleving te waarborgen. Deze maatregelen zijn gebaseerd op de waarschijnlijkheid en de ernst van de risico’s die de verwerking met zich meebrengt voor de rechten en vrijheden van natuurlijke personen. Om aan te tonen dat deze maatregelen passend zijn, kan worden aangedragen dat deze zijn opgesteld in overeenstemming met door de Autoriteit Persoonsgegevens goedgekeurde gedragscodes of certificeringen. Wat betreft passende technische beveiligingsmaatregelen, blijkt uit een interview met de heer K. van Dijck dat het werken vanuit een Cloud omgeving, het gebruik maken van een firewall en een anti-spamoplossing, het beperken van de inzagerechten van medewerkers en het beveiligen van e-mailverkeer aan te merken zijn als passende technische beveiligingsmaatregelen.[[111]](#footnote-111) Naast voornoemde maatregelen, moet de verwerkingsverantwoordelijke de computer of laptop beveiligen door middel van meerdere lange wachtwoorden en versleuteling van de harde schijf. Tot slot draagt de heer Van Dijck aan dat passende technische beveiligingsmaatregelen enkel zorg dragen voor een goede bescherming als het personeel goed geïnstrueerd is omtrent het gebruik van deze maatregelen.

Naast het nemen van deze maatregelen is het de verwerkingsverantwoordelijke verplicht om aan te tonen dat de verwerking is toegestaan gelet op de AVG. Een middel dat hiervoor gebruikt kan worden is een gegevensbeschermingsbeleid waarin beschreven staat hoe een organisatie omgaat met gegevensbescherming en op welke wijze invulling is gegeven aan de beginselen privacy by design en privacy by default. Hiermee wordt bedoeld dat er bij de ontwikkeling van nieuwe producten en diensten en/of een nieuw beleid aandacht dient te worden besteed aan maatregelen die privacyverhogend zijn en dat er niet meer gegevens worden verzameld dan noodzakelijk.[[112]](#footnote-112) Privacy by default houdt in dat de genomen maatregelen als standaard gelden en de privacy maximaal waarborgen.[[113]](#footnote-113) Ter actualisering

van het beleid dient het periodiek geëvalueerd te worden en waar nodig aangepast.[[114]](#footnote-114)

Een andere verplichting die blijkt uit de AVG, is dat een verwerkersovereenkomst op moet worden gesteld tussen de verwerkingsverantwoordelijke en de verwerker. In deze overeenkomst moet worden opgenomen wat de duur, de aard en het doel van de verwerking zijn. Tevens moet worden opgenomen om welk soort persoonsgegevens het gaat, om welke categorie betrokkenen het gaat en welke verplichtingen op de verwerkingsverantwoordelijke rusten en welke rechten zij heeft.[[115]](#footnote-115)

Nog een verplichting die rust op de verwerkingsverantwoordelijke, is het bijhouden van een register van de verwerkingsactiviteiten van haar organisatie. Dit register draagt bij aan de verantwoordingsplicht doordat hiermee kan worden aangetoond dat de AVG wordt nageleefd. Het register heeft een schriftelijke vorm, waaronder ook elektronische geschriften worden verstaan. Om aan deze registratieplicht te voldoen, moet de verwerkingsverantwoordelijke de volgende zaken opnemen in dit register[[116]](#footnote-116):

* de naam en contactgegevens van de verwerkingsverantwoordelijke en/of diens vertegenwoordiger en gegevens van de functionaris voor gegevensbescherming;
* de verwerkingsdoeleinden;
* een beschrijving van de categorieën betrokkenen en van de categorieën van persoonsgegevens;
* categorieën van ontvangers van persoonsgegevens;
* doorgiften van persoonsgegevens aan een derde land of internationale organisaties indien van toepassing;
* de beoogde termijnen waarbinnen verschillende categorieën van persoonsgegevens moeten worden gewist;
* indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen die zijn genomen.

Deze registratieplicht geldt niet voor ondernemingen met minder dan 250 personen in dienst, tenzij het gaat om verwerkingen die een risico meebrengen voor de rechten en vrijheden van betrokkenen, de verwerking niet incidenteel is of als het gaat om de verwerking van bijzondere persoonsgegevens of gegevens in verband met strafrechtelijke veroordelingen en strafbare feiten.[[117]](#footnote-117)

Naast de registratieplicht, rust op de verwerkingsverantwoordelijke een informatieplicht aan betrokkenen betreffende de verwerking van hun gegevens en de rechten die zij hierbij hebben. Wat betreft de verwerking van de gegevens dient de verwerkingsverantwoordelijke aan de betrokkene informatie te verschaffen over de volgende zaken[[118]](#footnote-118):

* de identiteit van de verwerkingsverantwoordelijke (statutaire naam, adres, telefoonnummer en e-mailadres);
* contactgegevens van de functionaris voor gegevensbescherming;
* de verwerkingsdoeleinden waarvoor de persoonsgegevens zijn bestemd en de rechtsgrond voor de verwerking;
* ontvangers of categorieën van ontvangers van de persoonsgegevens;
* het voornemen om persoonsgegevens door te geven aan een derde land of internationale organisatie;
* welke bewaartermijn wordt gehanteerd en waarom deze termijn wordt aangehouden
* dat de betrokkene toestemming voor de verwerking te allen tijde kan intrekken zonder terugwerkende kracht;
* dat het verstrekken van persoonsgegevens nodig is om te voldoen aan een wettelijke verplichting of noodzakelijk zijn om de overeenkomst na te komen;
* of er sprake is van geautomatiseerde besluitvorming.

Wat betreft de rechten van de betrokkene is bepaald dat de verwerkingsverantwoordelijke de betrokkene moet informeren over de rechten die hij of zij heeft bij de verwerking van zijn of haar persoonsgegevens, wat deze rechten inhouden en op welke wijze deze rechten kunnen worden ingeroepen.[[119]](#footnote-119) De rechten die betrokkenen hebben op grond van de AVG zijn het recht op inzage, het recht op rectificatie en gegevenswissing en het recht op beperking van de verwerking.[[120]](#footnote-120) Naast deze rechten beschrijft de AVG dat betrokkenen recht hebben op gegevensoverdraagbaarheid, bezwaar en het recht om niet aan uitsluitend geautomatiseerde gegevensverwerking te worden onderworpen.[[121]](#footnote-121)

Het recht op inzage houdt in dat de betrokkene zijn of haar verwerkte persoonsgegevens kosteloos mag inzien en dat de betrokkene kan verzoeken om een kopie van deze gegevens.[[122]](#footnote-122) De opgevraagde persoonsgegevens moeten worden aangeleverd in een gestructureerde, gangbare en machinaal leesbare vorm.[[123]](#footnote-123) De inzage strekt slechts tot de persoonsgegevens en niet tot interne werkdocumenten of notities.[[124]](#footnote-124) Wat betreft het recht op rectificatie en gegevenswissing bepaalt de AVG dat de betrokkene het recht heeft om zijn of haar persoonsgegevens te laten corrigeren of aanvullen. Dit recht is in lijn met het beginsel van juistheid van persoonsgegevens en is bedoeld om evidente fouten of omissies te herstellen bij op eenvoudige en objectieve wijze vast te stellen onjuistheden.[[125]](#footnote-125) Dit recht is niet bedoeld als extra inhoudelijke toets van de gegevens en is ook van toepassing op archieven.[[126]](#footnote-126) Na elke aanpassing van gegevens moet de verwerkingsverantwoordelijke hiervan melding maken aan de betrokkene.[[127]](#footnote-127) Wat betreft het recht op wissing van persoonsgegevens is bepaald dat gegevens welke niet of niet meer nodig zijn voor verwerking dienen te worden gewist.[[128]](#footnote-128) Onder het wissen van persoonsgegevens wordt verstaan het zorgdragen dat de gegevens feitelijk niet meer aanwezig zijn.[[129]](#footnote-129) Ook is bepaald dat dit wissen zonder onredelijke vertraging en kosteloos dient te geschieden.[[130]](#footnote-130) In beginsel is deze termijn een maand.[[131]](#footnote-131) Een verzoek tot wissing van persoonsgegevens heeft betrekking op elke koppeling naar, kopie of reproductie van de gegevens.[[132]](#footnote-132) Het wissen van gegevens door de verwerkingsverantwoordelijke is niet mogelijk voor zover op de verwerkingsverantwoordelijke een wettelijke verwerkingsverplichting rust.[[133]](#footnote-133)

Het recht op beperking van de verwerking houdt in dat de betrokkene aangeeft tijdelijk de verwerking van zijn of haar persoonsgegevens te willen stopzetten. Dit is mogelijk als de juistheid van de gegevens wordt betwist en hiernaar controle is ingesteld, als gegevens onrechtmatig worden verwerkt, als bezwaar is gemaakt op de verwerking en als de verwerkte gegevens nodig zijn bij het instellen, uitvoeren of onderbouwen van een rechtsvordering.[[134]](#footnote-134) Een ander recht dat de AVG beschrijft is het recht op gegevensoverdraagbaarheid. Dit recht houdt in dat betrokkenen door middel van een verzoek zijn of haar persoonsgegevens moet ontvangen van de verwerkingsverantwoordelijke in een gestructureerde, gangbare en machinaal leesbare vorm.[[135]](#footnote-135) De persoonsgegevens die de verwerkingsverantwoordelijke moet verstrekken zijn gegevens van de betrokkene zelf alsmede gepseudonimiseerde gegevens en gegevens van derden die aan de betrokkene kunnen worden gelinkt.[[136]](#footnote-136) Om deze overdraagbaarheid te waarborgen heeft Artikel 29 Werkgroep hieromtrent richtlijnen opgesteld. Uit deze richtlijnen blijkt dat de betrokkene zelf direct gegevens moet kunnen downloaden en dat hiervoor geen kosten in rekening mogen worden gebracht. Wat betreft het recht op bezwaar is bepaald dat de betrokkene de verwerkingsverantwoordelijke nogmaals kan vragen om een belangenafweging te maken voor de verwerking van de gegevens gelet op de specifieke situatie van de betrokkene. De betrokkene draagt dan specifieke omstandigheden aan.[[137]](#footnote-137) Als dit recht wordt ingeroepen moet de verwerkingsverantwoordelijke de verwerking van de persoonsgegevens van de betrokkene staken, tenzij de belangen van de verwerkingsverantwoordelijke zwaarder wegen. Dit recht moet de verwerkingsverantwoordelijke uitdrukkelijk onder de aandacht brengen van betrokkenen.[[138]](#footnote-138)

Tot slot is bepaald dat een betrokkene het recht heeft om niet te worden onderworpen aan een uitsluitend geautomatiseerde verwerking waaruit een besluit voortvloeit dat rechtsgevolgen heeft voor hem of haar.[[139]](#footnote-139) De mededeling omtrent geautomatiseerde verwerking omvat in elk geval uitleg over de onderliggende logica, belang en de verwachte gevolgen van de verwerking voor de betrokkene.[[140]](#footnote-140) Er kan geen beroep op dit recht worden gedaan als de verwerking noodzakelijk is voor totstandkoming of uitvoering van een overeenkomst tussen de verwerkingsverantwoordelijke en de betrokkene, als het gaat om een besluit dat is toegestaan bij een Europese of nationale wet en hierbij is voorzien in beschermingsmaatregelen voor de betrokkene. Een beroep op dit recht is ook niet mogelijk als de betrokkene uitdrukkelijke toestemming heeft gegeven voor geautomatiseerde gegevensverwerking.[[141]](#footnote-141) Wat betreft bijzondere persoonsgegevens is bepaald dat deze nooit aan geautomatiseerde verwerking mogen worden onderworpen tenzij hiervoor uitdrukkelijke toestemming is verleend of het gaat om een besluit in het algemeen belang.[[142]](#footnote-142) Hiervoor zullen dan specifieke maatregelen genomen moeten worden.

Een uitgebreide uitwerking van voornoemde rechten is als bijlage toegevoegd aan dit onderzoek.[[143]](#footnote-143)

Naast de plicht om betrokkenen te informeren inzake hun rechten bij de verwerking van hun persoonsgegevens, rust op de verwerkingsverantwoordelijke de plicht om een beoordeling op te stellen betreffende haar verwerkingsactiviteiten. In het kader van de zorgvuldigheid bij verwerking van persoonsgegevens, is het in sommige gevallen voor de verwerkingsverantwoordelijke verplicht om een gegevensbeschermingseffectbeoordeling uit te voeren. Dit is het geval als de verwerking een hoog risico met zich meebrengt voor rechten en vrijheden van de betrokkene. Indien er een functionaris voor gegevensbescherming is aangesteld moet de verwerkingsverantwoordelijke advies bij hem inwinnen voor de beoordeling.[[144]](#footnote-144) In de beoordeling dient blijkens de AVG aan enkele zaken uitwerking te worden gegeven.[[145]](#footnote-145) Er moet namelijk beschreven worden welke verwerkingen voor welke doelen plaatsvinden en er moet worden beoordeeld of de verwerking noodzakelijk en evenredig is in verhouding tot het doel van de verwerking. Daarnaast moet worden beschreven welke risico’s er kunnen ontstaan, wanneer er een verhoogde kans is dat deze risico’s optreden en er dient opgenomen te worden welke maatregelen worden genomen om de risico’s terug te dringen. Een gegevensbeschermingseffectbeoordeling is niet altijd vereist. Als het gaat om verwerkingen blijkens een wettelijke plicht of verwerking in het algemeen belang of in de uitoefening van het openbare gezag, mag dit achterwege blijven mits eerder een privacyoverweging is gemaakt en de wettelijke plicht geldt voor alle verwerkte persoonsgegevens.[[146]](#footnote-146)

Tot slot verplicht de AVG een verwerkingsverantwoordelijke in sommige gevallen om een functionaris voor gegevensbescherming (hierna te noemen functionaris) aan te stellen. Dit is een onafhankelijke, deskundige persoon binnen de organisatie van de verwerker of verwerkingsverantwoordelijke. Zijn taak is te informeren en adviseren over de omgang met persoonsgegevens en is aanspreekpunt voor medewerkers, verwerkers, betrokkenen en de toezichthoudende autoriteit. In sommige situaties is het verplicht een functionaris aan te stellen.[[147]](#footnote-147) Het aanstellen van een functionaris is verplicht als het gaat om een verwerking door een overheidsinstantie of een overheidsorgaan, als er regelmatige, stelselmatige, grootschalige observaties vereist zijn voor de verwerkingen of als het gaat om een grootschalige verwerking van bijzondere persoonsgegevens, persoonsgegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten.

## 4.7 Controlerende autoriteit

Een onafhankelijke toezichthoudende autoriteit controleert of de AVG wordt nageleefd. In Nederland is de Autoriteit Persoonsgegevens (hierna te noemen de autoriteit) de toezichthoudende autoriteit.[[148]](#footnote-148) Aan deze autoriteit zijn bevoegdheden toegekend ter controle en handhaving van de AVG.[[149]](#footnote-149) Het gaat hierbij om onderzoeksbevoegdheden, corrigerende bevoegdheden en adviserende bevoegdheden.[[150]](#footnote-150) De autoriteit is bevoegd om boetes op te leggen. De boete die zij kan opleggen bij overtreding van regels met betrekking tot doelbinding, grondslag, bijzondere persoonsgegevens, rechten van betrokkenen en doorgifte naar derde landen, bedragen maximaal 20 miljoen euro of vier procent van de wereldwijde jaaromzet.[[151]](#footnote-151) Bij overtreding van regels met betrekking tot passende technische en organisatorische maatregelen en de verantwoordingsplicht, kunnen boetes worden opgelegd van maximaal tien miljoen euro of twee procent van de wereldwijde jaaromzet.[[152]](#footnote-152)

## 4.8 Samenvatting

Uit dit hoofdstuk blijkt dat de verwerkingsverantwoordelijke bij de verwerking van persoonsgegevens aan enkele beginselen moet voldoen: het beginsel van behoorlijke, transparante en rechtmatige verwerking, het beginsel van doelbinding, het beginsel van minimale gegevensverwerking, het beginsel van juistheid van gegevens en het beginsel van opslagbeperking. Naast deze beginselen, blijkt dat op de verwerkingsverantwoordelijke enkele plichten rusten bij de verwerking van persoonsgegevens: het nemen van passende technische en organisatorische maatregelen, een verantwoordingsplicht, een plicht tot het sluiten van overeenkomsten met verwerkers, een registratieplicht, een informatieplicht, het uitvoeren van een gegevensbeschermingseffectbeoordeling en het aanstellen van een functionaris voor gegevensbescherming. Tot slot beschrijft dit hoofdstuk dat de Autoriteit Persoonsgegevens controleert of de AVG wordt nageleefd en dat de autoriteit boetes op kan leggen.

# Hoofdstuk 5. Toetsing aan AVG

*In dit hoofdstuk is in kaart gebracht welke punten met betrekking tot het verwerken van persoonsgegevens van klanten in het kader van hypotheekadvisering verbetering behoeven gelet op de AVG. Om te bepalen of de huidige werkwijze van A met betrekking tot fysieke dossiers, C en Adviesbox in het kader van hypotheekadvisering voldoet aan de AVG, is de werkwijze aan de AVG getoetst. Omdat in het tweede hoofdstuk is geconcludeerd dat er geen beleid is opgesteld door A, kan dit beleid ook niet getoetst worden aan de AVG. Deze toetsing is vormgegeven door middel van drie schema’s.*

In het eerste schema (schema 1) is weergegeven of bij de verwerking van klantgegevens aan de beginselen is voldaan en of aan de verplichtingen die gelden voor een verwerkingsverantwoordelijke is voldaan. Uit hoofdstuk drie blijkt namelijk dat A aan te merken is als verwerkingsverantwoordelijke. In het tweede schema (schema 2) is weergegeven of er sprake is van een rechtmatige verwerking van persoonsgegevens van klanten. Het derde schema (schema 3) beschrijft of de bewerkersovereenkomst met B inzake C alle vereiste aspecten bevat gelet op de AVG. Deze overeenkomst is getoetst aan de eisen die de AVG stelt aan een overeenkomst tussen een verwerker en een verwerkingsverantwoordelijke. De schema’s bevatten een toelichting waarin verduidelijkt wordt waarom wel of niet aan de betreffende verplichting is voldaan.

## 5.1 Beginselen en verplichtingen

In onderstaand schema zijn de beginselen en verplichtingen zoals beschreven in hoofdstuk vier, getoetst aan de AVG.

|  |
| --- |
| **Schema 1 Beginselen en verplichtingen** |
| **Rood = niet voldaan** |  | **Groen = voldaan** |
| Beginsel/verplichting AVG | Voldaan? | Toelichting |
| Beginsel van doelbinding: Welbepaald, uitdrukkelijk en gerechtvaardigd(§ 4.5) | Nee | A heeft geen specifieke doeleinden vastgesteld en omschreven alvorens de persoonsgegevens worden verwerkt. De verwerking is wel gerechtvaardigd omdat er geen sprake is van strijd met de wet. De persoonsgegevens die A verwerkt zijn noodzakelijk voor het naar behoren nakomen van de overeenkomst met de klant. De verwerking is noodzakelijk omdat deze plaatsvindt in het kader van een wettelijke verplichting die A moet nakomen: de identificatieplicht[[153]](#footnote-153) blijkens de WWFT. |
| Beginsel van minimale gegevensverwerking: toereikend, ter zake dienend en beperkt tot de noodzakelijke verwerking(§ 4.5) | Ja | A verwerkt slechts de persoonsgegevens die noodzakelijk zijn om de financiële situatie van de klant te bepalen. Dit is noodzakelijk voor het geven van een passend hypotheekadvies. |
| Beginsel van juistheid van gegevens(§ 4.5) | Nee  | A heeft geen maatregelen genomen om onjuiste gegevens te rectificeren of wissen en wacht tot de klant aangeeft dat gegevens niet kloppen alvorens zij inspanningen verricht om juistheid te waarborgen. |
| Beginsel van opslagbeperking(§ 4.5) | Ja | A heeft geen bewaartermijn vastgesteld en wist persoonsgegevens niet. De opgeslagen persoonsgegevens worden ook niet aan een periodieke toetsing onderworpen. Echter bepaalt art. 33 lid 4 WWFT dat een bewaartermijn geldt van vijf jaar. Hierdoor handelt A niet in strijd met dit beginsel. |
| Passende technische en organisatorische maatregelen ter waarborging van passende beveiliging. Deze verplichting hangt samen met het beginsel van integriteit en vertrouwelijkheid.(§ 4.5 en § 4.6) | Nee | A heeft nauwelijks maatregelen genomen ter bescherming van persoonsgegevens voor een ongeoorloofde of onrechtmatige verwerking, tegen onopzettelijk verlies, vernietiging of beschadiging. A heeft de fysieke dossiers, laptops, C en Adviesbox op dit moment namelijk niet voorzien van voldoende beveiliging. Fysieke dossiers liggen niet in afgesloten kasten, laptops zijn slechts beveiligd met één wachtwoord. C en Adviesbox zijn op de laptop geïnstalleerd en wachtwoorden van laptops zijn aangeplakt op kantoor op een memo. De harde schijf van de laptop is niet beveiligd en er wordt niet gewerkt door middel van een beveiligd netwerk. Vele gegevens waaronder persoonsgegevens ontvangt A via e-mailverkeer. Daarnaast maken adviseurs niet vaak genoeg en onvolledig een back-up van de laptop. Wat betreft de mogelijkheid tot kennisname van persoonsgegevens heeft A ook onvoldoende maatregelen genomen. Alle adviseurs kunnen alle mappen inzien en fysieke dossiers kunnen door iedereen die het kantoor betreedt worden bekeken. Tot slot heeft A geen interne werkinstructie, is geen privacybeschermingsbeleid en geen protocol voor datalekken opgesteld. Verder sluit A niet aan bij gedragscodes en heeft zij geen certificeringen in het kader van bescherming van persoonsgegevens. |
| Verantwoordingsplicht(§ 4.6) | Nee | A kan niet aantonen dat zij de in § 4.5 en § 4.6 beschreven beginselen en verplichtingen voldoet bij haar verwerking. Zij heeft hiertoe namelijk geen documenten opgesteld. |
| Overeenkomstenplicht (§ 4.6) | Nee | A heeft enkel met B een bewerkersovereenkomst gesloten. Wat betreft Adviesbox is geen bewerkers- of verwerkersovereenkomst opgesteld. |
| Registratieplicht(§ 4.6) | Nee | A houdt geen register bij van haar verwerkingsactiviteiten. Ondanks dat A minder dan 250 personen in dienst heeft, dient zij dit register toch op te stellen omdat zij bijzondere persoonsgegevens verwerkt. |
| Informatieplicht aan betrokkenen inzake hun rechten en inzake de verwerking. Deze verplichting hangt samen met het beginsel van behoorlijke, rechtmatige en transparante verwerking.(§ 4.6) | Nee | A verstrekt klanten geen informatie over de rechten die zij hebben, op welke wijze zij hun rechten kunnen inroepen en welke gevolgen het inroepen van een bepaald recht met zich meebrengt. Met name het recht op bezwaar dient uitdrukkelijk onder de aandacht te worden gebracht bij de klant en hierover vertellen de adviseurs niets aan de klant.Daarnaast communiceert niet met klanten in hoeverre en op welke manier hun persoonsgegevens worden verwerkt. |
| Gegevensbeschermingseffect-beoordeling(§ 4.6) | Nee  | A verwerkt gegevens waarbij een hoog risico bestaat voor de rechten en vrijheden van de klant. Er worden namelijk vele persoonsgegevens en bijzondere persoonsgegevens verwerkt. Hiervoor is het uitvoeren van een beoordeling van belang. Omdat A de gegevens verwerkt op basis van een wettelijke plicht, mag een gegevensbeschermingseffectbeoordeling achterwege blijven. Echter is er niet eerder een privacyoverweging gemaakt en geldt de wettelijke plicht niet voor alle verwerkte persoonsgegevens. De beoordeling dient daarom te worden uitgevoerd. |
| Aanstellen functionaris voor gegevensbescherming(§ 4.6) | Nee | A verwerkt grootschalig bijzondere persoonsgegevens maar heeft geen persoon aangewezen als functionaris voor gegevensbescherming. Er is niemand binnen de organisatie aangesteld die alle partijen informeert en adviseert omtrent de naleving van de AVG, overige privacywetgeving en het interne beleid. Er is ook niemand die fungeert als aanspreekpunt voor betrokkenen en de Autoriteit Persoonsgegevens. |

## 5.2 Verwerkte persoonsgegevens en grondslag

In dit schema zijn de verwerkte persoonsgegevens door A getoetst aan de grondslagen voor verwerking blijkens de AVG. Hieruit blijkt of A de persoonsgegevens mag verwerken.

|  |
| --- |
| **Schema 2 Verwerkte persoonsgegevens en grondslag** |
| **Rood = geen grondslag** |  | **Groen = wel grondslag** |
| Verwerkt persoonsgegeven | Grondslag blijkens AVG | Toelichting |
| Voornaam/voornamenAchternaamGeboortedatumAdresWoonplaatsBurgerservicenummer (BSN)Aard van legitimatie (ID/paspoort)Nummer document ter identificatiePlaats uitgifte document identificatieDatum uitgifte document identificatie | Art. 6 lid 1 sub c  | A mag deze persoonsgegevens verwerken op basis van art. 33 lid 1 sub a onder 1 WWFT omdat door middel van deze gegevens aan de identificatieplicht die rust op financiële dienstverleners wordt voldaan.Art. 44 Uitvoeringswet AVG bepaalt dat een BSN slechts verwerkt mag worden gebaseerd op een wettelijke grondslag. Hierbij gaat het om de grondslag zoals voornoemd. |
| Nationaliteit Burgerlijke staatGeslachtVoornamen kinderenAchternaam kinderenGeboortedatum kinderenRekeningnummer lopende rekeningOpleidingsniveauTenaamstelling lopende rekeningRekeningnummer spaarrekeningTenaamstelling spaarrekeningHypotheeknummerPolisnummer verzekeringenTelefoonnummerE-mailadresWerknemersnummerOffertenummer SEPA machtiging | Art. 6 lid 1 sub b | De verwerking van deze gegevens door A is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene, de klant, partij is. Als A deze gegevens niet verwerkt kan de overeenkomst niet goed worden nagekomen. Er is dus sprake van een noodzaak. |
| Kopie legitimatiebewijs(achternaam, voornaam/voornamen, geslacht, nationaliteit, geboortedatum, datum afgifte legitimatiebewijs, datum verloop legitimatiebewijs, documentnummer, geboorteplaats, instantie die het bewijs heeft uitgegeven, Burgerservicenummer, lengte, handtekening en foto) | Art. 6 lid 1 sub c | A mag deze gegevens verwerken omdat zij wettelijk verplicht is haar klanten te identificeren.[[154]](#footnote-154) Het is binnen de financiële dienstverlening toegestaan om een kopie te maken van een identiteitsbewijs of paspoort blijkens de CBP richtsnoeren waarnaar Autoriteit Persoonsgegevens verwijst op haar website.[[155]](#footnote-155) Doordat er sprake is van een wettelijke grondslag voor de verwerking van identiteitsbewijzen, is de verwerking van deze bijzondere persoonsgegevens toegestaan.[[156]](#footnote-156) |

## 5.3 Bewerkersovereenkomst B

In dit schema is de inhoud van de bewerkersovereenkomst die A gesloten heeft met B inzake C getoetst aan de AVG. De AVG stelt namelijk, zoals beschreven in hoofdstuk vier, inhoudelijke eisen aan overeenkomsten tussen verwerkers en verwerkingsverantwoordelijken.

|  |
| --- |
| **Schema 3 Bewerkersovereenkomst B** |
| **Rood = niet opgenomen** |  | **Groen = opgenomen** |
| Verplichte onderdelen overeenkomst[[157]](#footnote-157) | Opgenomen? | Toelichting |
| Duur van de overeenkomst | Ja | Art. 1 van de overeenkomst geeft aan dat de duur van de overeenkomst gelijk is aan de periode dat B leverancier is aan A. |
| Aard van de overeenkomst | Ja | Art. 2.2 van de overeenkomst bepaalt dat B software aanbiedt en de gegevens die A invoert, bewerkt, rangschikten opslaat met de software. Verder bepaalt dit artikel dat B onderhoudsdiensten op de software en ondersteuning bij het gebruik van de software verleent. |
| Doel van de verwerking | Ja | In art. 2.1 van de overeenkomst is bepaald dat A de doeleinden waarvoor de persoonsgegevens verwerkt worden bepaalt.  |
| Soort persoonsgegevens | Ja | Art. 3.1 van de overeenkomst beschrijft dat A een uittreksel van haar verwerkingsregister of overzicht van de aard van de gegevens die worden verwerkt, verstrekt aan B. |
| Categorieën van betrokkenen | Ja | In art. 3.1 van de overeenkomst is beschreven dat A B op de hoogte stelt van de categorieën betrokkenen bij de verwerking. |
| Rechten en plichten verwerkingsverantwoordelijke | Ja | De rechten die A heeft op basis van deze overeenkomst zijn beschreven in art. 4 t/m 10 van deze overeenkomst. Hierin staat beschreven wat A van B mag verwachten bij de uitvoering van de verwerking, wat betreft beveiliging van persoonsgegevens en controle daarop en wat zij mag verwachten op het gebied van incidentenmanagement en datalekken. Verder is beschreven dat A bijstand krijgt bij het uitvoeren van een gegevensbeschermingseffectbeoordeling en dat er gewerkt wordt vanuit privacy by design en privacy by default. Tot slot is in deze artikelen bepaald wat A mag verwachten bij het aanstellen van onderaannemers, in welke gevallen B aansprakelijk is en wat A mag verwachten wat betreft bewaartermijnen, teruggave en vernietiging van persoonsgegevens.Wat betreft de verplichtingen die rusten op A bepaalt de overeenkomst dat zij informatie moet verstrekken aan B betreffende de aard van de te verwerken gegevens, de categorieën betrokkenen, de functionaris van gegevensbescherming, sectorspecifieke regelgeving indien relevant en tot slot moet A zorg dragen voor een rechtmatige verwerking van persoonsgegevens. |

## 5.4 Samenvatting

Uit de toetsing blijkt dat niet voldaan is aan enkele beginselen en verplichtingen uit de AVG. Deze punten behoeven verbetering om te voldoen aan de AVG. Uit deze toetsing blijkt dat niet aan het beginsel van doelbinding is voldaan en dat de juistheid van gegevens op dit moment niet voldoende wordt gewaarborgd. Daarnaast blijkt uit de toetsing dat dat A onvoldoende passende technische en organisatorische maatregelen heeft genomen en dat zij deze maatregelen dient aan te scherpen om aan de AVG te voldoen. Verder blijkt uit de toetsing dat A niet kan voldoen aan haar verantwoordingsplicht, dat zij geen bewerkers- of verwerkersovereenkomsten heeft opgesteld en dat zij niet voldoet aan de registratieplicht. Tot slot blijkt uit de toetsing dat A geen gegevensbeschermingseffectbeoordeling heeft uitgevoerd terwijl dit voor haar verplicht is en dat geen functionaris voor gegevensbescherming is aangesteld terwijl dit voor A verplicht is. Naast de aspecten waaraan A niet voldoet blijkens deze toetsing, is ook gebleken dat zij voldoet aan het beginsel van minimale gegevensverwerking en het beginsel van opslagbeperking. Daarnaast blijkt dat A de persoonsgegevens verwerkt overeenkomstig een grondslag conform de AVG en dat de bewerkersovereenkomst met B alle verplichte aspecten van een overeenkomst tussen een verwerker en verwerkingsverantwoordelijke behandelt.

# Hoofdstuk 6. Privacybeleid

*In dit hoofdstuk wordt in kaart gebracht op welke wijze een privacybeleid voor de klant door A kan worden vormgegeven. Zoals in het vierde hoofdstuk beschreven, dient het privacybeleid in begrijpelijke taal geformuleerd te zijn. Dit draagt bij aan de transparantie die A aan haar klanten moet bieden. Dit hoofdstuk maakt inzichtelijk welke aspecten moeten worden uitgewerkt in een privacybeleid en op welke wijze deze aspecten kunnen worden uitgewerkt.*

## 6.1 Inhoud

Door middel van een privacybeleid wordt aan de klant aangegeven wat hij of zij van A mag verwachten. Het is daarom van belang dat in dit beleid alle aspecten van de informatieplicht zoals vermeld in hoofdstuk vier worden behandeld.[[158]](#footnote-158) Allereerst moet in het beleid zijn opgenomen wie de verwerkingsverantwoordelijke is. Daarnaast moet zijn opgenomen tot wie klanten zich kunnen wenden als zij vragen hebben omtrent de bescherming van hun privacy. Verder moet in het beleid zijn opgenomen welke specifieke doeleinden gelden voor de verwerking van de persoonsgegevens door de verwerkingsverantwoordelijke. Nog een onderdeel dat dient te zijn opgenomen, is of klantgegevens worden gedeeld met derden. Hierbij gaat het om verwerkers die samenwerken met A of doorgiften aan landen buiten Europa. Als de verwerkingsverantwoordelijke het voornemen heeft om de gegevens door te geven aan een derde land of internationale organisatie, dient dit te zijn benoemd in het beleid. Verder moet in het beleid worden opgenomen op welke wijze de gegevens van de klant worden verzameld en wat de bewaartermijn van de gegevens is. Nog een onderdeel van het beleid is het beschrijven van de rechten die de betrokkene heeft en op welke wijze zij deze rechten kunnen inroepen. Daarnaast moet uit het beleid blijken wat de grondslag is voor de verwerking van de persoonsgegevens door de verwerkingsverantwoordelijke en of er bij de verwerking van persoonsgegevens gebruik gemaakt wordt van geautomatiseerde besluitvorming. Naast de eisen die blijken uit deze informatieplicht, kan vermeld worden wat de aard is van de te verwerken gegevens, op welke wijze A handelt op het moment dat een incident plaatsvindt met betrekking tot de klantgegevens, op welke wijze een geschil met A dient te worden afgehandeld en wat er gebeurt als de klant zijn of haar persoonsgegevens niet verstrekt.

## 6.2 Vormgeving

Door in de kop- of voettekst van het document de contactgegevens van A te plaatsen, is het voor de klant duidelijk dat het privacybeleid de verwerking van klantgegevens door A betreft. Het adres, de postcode, de woonplaats, het telefoonnummer, het e-mailadres, KVK-nummer en Kifid-nummer van A zijn vermeld in de kop- of voettekst van het beleid. Om te zorgen voor een begrijpelijk geformuleerd beleid waarin de klant inzicht krijgt in alle voornoemde aspecten, kan het beleid worden vormgegeven door de volgende vraag en antwoord structuur:

*Waarom verwerkt A uw gegevens?*

Om te kunnen komen tot een passend hypotheekadvies is het noodzakelijk om uw financiële situatie in kaart te brengen. Om dit te kunnen doen vragen wij financiële en persoonlijke gegevens van u. Het doel van de verwerking van uw gegevens door A, is financiële diensten verlenen, deze financiële diensten factureren, gegevens bewaren en verantwoording voor de verwerking afleggen. A is een financiële dienstverlener en om onze diensten te mogen verlenen moeten wij aan wettelijke verplichtingen voldoen. De gegevens die wij aan u vragen worden gevraagd in

het kader van de identificatieplicht. Overige gegevens worden van u gevraagd omdat het zonder deze gegevens niet mogelijk is de overeenkomst met u na te komen.

*Hoe en gedurende welke termijn verwerkt A uw gegevens?*

A gebruikt uitsluitend gegevens die u ons verstrekt. De bewaartermijn die voor deze gegevens geldt is wettelijk vastgesteld op vijf jaar. Dit blijkt uit art. 33 lid 4 wet ter voorkoming witwassen en financiering van terrorisme (WWFT). Sommige van uw gegevens zijn ook nodig om te kunnen voldoen aan de wettelijk vastgelegde fiscale administratieplicht. Deze verplichting blijkt uit art. 52 lid 4 Algemene wet Rijksbelastingen (AWR). Uit deze bepaling blijkt dat uw gegevens gedurende zeven jaar bewaard moeten blijven.

*Welke gegevens verwerkt A waardoor u kunt worden geïdentificeerd?*

Onder deze gegevens worden alle gegevens verstaan die informatie over u geven evenals alle gegevens die indirect informatie over u geven. Het gaat om informatie die naar u leidt of kan leiden. Deze gegevens worden aangemerkt als persoonsgegevens.

De gegevens die door A verwerkt worden waardoor u kunt worden geïdentificeerd, zijn:

* Voornaam/voornamen
* Achternaam
* Geboortedatum
* Adres
* Woonplaats
* Burgerservicenummer (BSN)
* Legitimatiebewijs (achternaam, voornaam/voornamen, geslacht, nationaliteit, geboortedatum, datum afgifte legitimatiebewijs, datum verloop legitimatiebewijs, documentnummer, geboorteplaats, instantie die het bewijs heeft uitgegeven, Burgerservicenummer, lengte, handtekening en foto)
* Kinderen: voornaam/voornamen, achternaam, geboortedatum
* Rekeningnummers en tenaamstelling lopende rekening en spaarrekening
* Hypotheeknummer
* Polisnummer verzekeringen
* Werknemersnummer
* Offertenummer SEPA machtiging
* Telefoonnummer
* E-mailadres

Enkele van deze gegevens zijn aan te merken als bijzondere persoonsgegevens. Dat houdt in dat het persoonsgegeven A informatie geeft over uw ras/etniciteit. Hieronder valt de pasfoto op het identiteitsbewijs en de nationaliteit in combinatie met de voor- en achternaam en de geboorteplaats.

*Welke gegevens verwerkt A waardoor u niet kunt worden geïdentificeerd?*

Naast persoonsgegevens verwerkt A ook andere gegevens van u die noodzakelijk zijn voor het in kaart brengen van uw financiële situatie, namelijk informatie betreffende:

* Beroep
* Inkomensgegevens
* Beleggingen
* Financiële verplichtingen
* Eigen woning
* Bestaande hypotheek
* Verzekeringen
* Aan te kopen woning
* Pensioen
* Alimentatie
* Schenkingen

*Deelt A uw gegevens?*

Ter berekening van uw hypotheek en het aanvragen van de hypotheek werkt A samen met softwareleveranciers. Deze softwareleveranciers zijn gehouden aan privacywetgeving en hebben hieromtrent een verwerkersovereenkomst met A gesloten. A deelt uw gegevens niet met instanties in landen buiten Europa.

*Welke rechten heeft u met betrekking tot uw gegevens?*

Omdat privacy een grondrecht is, moet de privacy van u bij de verwerking van uw persoonsgegevens zo goed mogelijk worden gewaarborgd. Om uw privacy te beschermen zijn in privacywetgeving de volgende rechten opgenomen die u kunt inroepen ten aanzien van A. Deze rechten kunt u inroepen door een aangetekende brief te sturen aan de in dit beleid beschreven functionaris voor gegevensbescherming.

Recht op inzage

U heeft het recht uw verwerkte persoonsgegevens in te zien en u kunt verzoeken om een kopie van deze gegevens. Voordat A u inzage geeft, moet u zich identificeren. Als A u inzage geeft in uw persoonsgegevens, levert A uw gegevens aan in gestructureerde, gangbare en machinaal leesbare vorm. Voor deze inzage en eventueel een kopie van uw persoonsgegevens, brengt A geen kosten in rekening.

Recht op rectificatie en gegevenswissing

U heeft het recht om uw gegevens te laten aanvullen of corrigeren. Dit recht strekt ook tot onjuiste gegevens in archieven. Soms duurt het een tijd voordat de gegevens verbeterd of gewist worden. A heeft hier enige tijd voor nodig omdat voordat de gegevens gerectificeerd worden een controle wordt uitgevoerd door A. Na elke aanpassing van gegevens zal A hiervan een melding maken aan u. Wat betreft de wissing van uw persoonsgegevens is bepaald dat de gegevens gewist worden zodra de bewaartermijn van zeven jaar is verstreken. A zorgt ervoor dat uw gegevens zonder redelijke vertraging en kosteloos na het verstrijken van de bewaartermijn feitelijk niet meer aanwezig zijn. Uw gegevens zullen met het inroepen van dit recht ook worden verwijderd door partijen waarmee A samenwerkt.

Recht op beperking van de verwerking

U heeft het recht om de verwerking van uw persoonsgegevens te beperken. Dit is mogelijk als u de juistheid van de verwerkte gegevens betwijfelt en u A in staat heeft gesteld om te controleren of uw gegevens juist zijn. Ook kunt u dit recht inroepen als uw gegevens niet verwerkt mogen worden en u liever uw gegevensverwerking beperkt dan uw gegevens laat wissen. Daarnaast kunt u dit recht inroepen als uw persoonsgegevens nodig zijn om een rechtsvordering in te stellen, uit te oefenen of te onderbouwen. Dit is bijvoorbeeld het geval als u aangifte doet tegen A. Tot slot kunt u dit recht inroepen als u bezwaar heeft gemaakt tegen de verwerking en in afwachting bent van de beslissing van A op dit bezwaar.

Recht op gegevensoverdraagbaarheid

U heeft het recht om uw persoonsgegevens te ontvangen van A in een gestructureerde gangbare en machinaal leesbare vorm. Dit houdt in dat u uw gegevens kunt downloaden. Hiervoor rekent A geen kosten.

Recht op bezwaar

U heeft het recht om bezwaar te maken tegen de verwerking van uw persoonsgegevens. Dit kunt u doen als u wilt dat A nogmaals bekijkt of uw gegevens verwerkt moeten worden gelet op uw specifieke situatie. Om dit recht in te roepen moet u specifieke omstandigheden aandragen bij A. Als u dit recht inroept wordt de verwerking van uw persoonsgegevens gestaakt tenzij de belangen van A in de specifieke situatie zwaarder wegen.

Recht op niet uitsluitend geautomatiseerde gegevensverwerking

Dit recht houdt in dat een werkwijze waarbij geen menselijke tussenkomst is en waarbij de verwerking gevolgen heeft voor uw rechten en vrijheden, niet is toegestaan. A werkt niet uitsluitend geautomatiseerd maar verwerkt uw gegevens gedeeltelijk geautomatiseerd. Adviseurs van A werken namelijk met laptops en software om u te kunnen voorzien van passend hypotheekadvies.

*Wie is uw aanspreekpunt voor zaken die gaan over privacy?*

A heeft een functionaris voor gegevensbescherming aangesteld. Als u vragen heeft omtrent uw persoonsgegevens of uw rechten bij de verwerking van uw persoonsgegevens, kunt u contact opnemen met:

De heer X

Adres

Telefoonnummer

*Wat onderneemt A als zich een incident voordoet met uw gegevens?*

Mocht het onverhoopt voorkomen dat een inbreuk is gemaakt op uw privacy doordat een onbevoegde kennis heeft genomen van uw gegevens, er sprake is van diefstal, er onrechtmatige gegevensverwerking, vernietiging of beschadiging heeft plaatsgevonden, dan neemt A maatregelen om de gevolgen voor u zo veel mogelijk in te perken. Indien nodig meldt A het incident bij de toezichthoudende autoriteit (Autoriteit Persoonsgegevens).

*Wat te doen als er een geschil is ontstaan met A?*

A is aangesloten bij het Klachteninstituut Financiële Dienstverlening (hierna Kifid). Als u een klacht heeft over de financiële dienst van A kunt u hiervan melding maken bij het Kifid. Kifid heeft een bemiddelende rol en probeert overeenstemming te bereiken tussen partijen. Voordat andere instanties benaderd worden, moeten partijen een bemiddelingstraject doorlopen hebben bij Kifid.

Als u bezwaar heeft gemaakt tegen de verwerking door A, kunt u na afwijzing van dit bezwaar een schriftelijk verzoek indienen bij de rechtbank om aan A te bevelen om uw verzoek over één of meerdere van uw rechten in te willigen. Dit verzoekschrift kunt u binnen zes weken na ontvangst van het antwoord van A op uw bezwaar indienen. Binnen de voornoemde termijn kunt u ook contact opnemen met de Autoriteit persoonsgegevens en haar verzoeken om te bemiddelen of adviseren over het geschil met A.

*Wat gebeurt er als u uw benodigde gegevens niet verstrekt aan A?*

Zoals eerder in dit beleid beschreven zijn de gegevens die A van u vraagt noodzakelijk voor het uitvoeren van de overeenkomst of heeft A de gegevens nodig in het kader van de identificatieplicht waaraan zij moet voldoen. Als u de benodigde gegevens niet verstrekt, kan A geen passend advies opstellen en kan zij niet voldoen aan haar zorgplicht. Als zij uw gegevens niet kan controleren of niet op de hoogte is van bepaalde gegevens, kan A haar berekeningen en advies niet of onvoldoende onderbouwen. Dat A haar adviezen moet kunnen onderbouwen wordt opgelegd door de Autoriteit Financiële Markten (AFM). Als u uw gegevens niet verstrekt, voorziet A u dan ook niet van hypotheekadvies.

## 6.3 Samenvatting

Uit dit hoofdstuk blijkt dat het privacybeleid de klant inzicht moet geven in de verwerking, welke rechten de klant heeft bij de verwerking van persoonsgegevens, op welke wijze een geschil moet worden afgehandeld en wat er gebeurt bij het niet verstrekken van de benodigde gegevens. Dit beleid kan worden vormgegeven door een vraag en antwoord structuur.

# Hoofdstuk 7. Conclusies en aanbevelingen

*In dit hoofdstuk is antwoord gegeven op de centrale vraag van dit onderzoek: Welke aanbevelingen voor een privacybeleid en de werkwijze met betrekking tot de verwerking van persoonsgegevens van klanten in fysieke dossiers en de systemen C en Adviesbox in het kader van hypotheekadvisering kunnen worden gegeven aan A, afgeleid uit een toetsing van de huidige werkwijze aan de AVG? Dit hoofdstuk beschrijft de beginselen en verplichtingen waaraan A blijkens een toetsing aan de AVG niet voldoet alsmede welke aanbevelingen kunnen worden gegeven zodat zij hier wél aan voldoet. Daarnaast beschrijft dit hoofdstuk op welke wijze een privacybeleid kan worden vormgegeven zodat aan de AVG is voldaan.*

## 7.1 Beginsel van doelbinding

Een aspect dat in de toekomst verbeterd moet worden bij de verwerking van persoonsgegevens, is het opstellen van welbepaalde, uitdrukkelijke en gerechtvaardigde doeleinden. A dient ervoor te zorgen dat zij doeleinden formuleert die aan deze eisen voldoen. Uit hoofdstuk drie is gebleken dat A in elk geval persoonsgegevens verwerkt om financiële diensten te verlenen, om te kunnen factureren voor deze financiële diensten, om de gegevens te bewaren overeenkomstig hoofdstuk vier en om te verantwoording voor de verwerking af te kunnen leggen. Uit de toetsing in hoofdstuk vijf is gebleken dat A geen specifieke doeleinden heeft vastgesteld en omschreven alvorens de persoonsgegevens worden verwerkt.

## 7.2 Juistheid en gegevenswissing

Een ander aspect dat in de toekomst verbeterd dient te worden, is de wijze waarop A de juistheid van gegevens bewaakt. Daarnaast dient zij de gegevens van klanten, behoudens voor zover deze nodig zijn voor archieven en de eis van reproduceerbaarheid, te wissen. Dit blijkt uit hoofdstuk drie en hoofdstuk vijf. Hiertoe kan A eens per jaar een bericht sturen aan de klant waarin wordt aangegeven dat er gegevenscontrole plaatsvindt en of de klant contact op kan nemen indien gegevens zijn gewijzigd sinds hun laatste contact met A. Wat betreft het wissen van gegevens dient A haar klanten een bericht te sturen dat zij de gegevens zal verwijderen bij het verstrijken van de bewaartermijn. Om de gegevens terug over te kunnen dragen naar de klant, kan A het dossier alvorens wissing nogmaals een week ter beschikking kunnen stellen aan de klant door middel van een SharePoint. Dat hieraan momenteel niet voldaan wordt, blijkt uit de afgenomen interviews met de heer X, de heer X en de heer X.

## 7.3 Passende technische en organisatorische maatregelen

## *7.3.1 Technische maatregelen*

In de toekomst dient A ook haar laptops beter te beveiligen, te gaan werken vanuit een beveiligde digitale omgeving, dienen back-ups te worden gemaakt en dient op andere wijze te worden omgegaan met e-mail. Dit is gebleken uit het interview met dhr. K. van Dijk van IT Support Groep.

### *Laptops*

Ter beveiliging van de laptops dienen lange wachtwoorden met bijzondere tekens te worden gebruikt. Hulpmiddelen die A kan gebruiken om de wachtwoorden te onthouden en in te vullen zijn LastPass en een passwordgenerator. Deze tools kunnen worden gezien als een digitale kluis die na ontgrendelen de wachtwoorden in alle portalen automatisch aanvult. Hiermee wordt ook kostbare tijd bespaard. Ook dienen de laptops te worden voorzien van een virusscanner en een anti-spamoplossing van bijvoorbeeld Intronis of Barracuda. Verder kan de harde schijf van de laptop door middel van Bitlocker geëncrypt worden waardoor informatie op de schijf niet zichtbaar is wanneer deze aangesloten wordt op een andere computer. Nog een middel dat A zou kunnen inzetten is het inloggen op een laptop door middel van een gezichtsscan (biometrie). Hierdoor is de harde schijf ook vergrendeld wanneer de laptop aan staat maar er niet is ingelogd.

### *C en Adviesbox*

Om te zorgen dat C en Adviesbox goed beveiligd zijn, dient A vanuit de Cloud te werken. Hierbij kan worden gekozen voor office 365. Ook dient zij te zorgen dat een goede firewall wordt geïnstalleerd op de laptops. Verder kan zij de toegang tot gegevens beperken waardoor niet elke medewerker alle informatie kan inzien. Slechts de relevante informatie voor de uitoefening van zijn of haar functie is dan toegankelijk. Ook dient A gebruik te maken van een twee-authenticatiesysteem om in te loggen op deze Cloudomgeving. Hierdoor is de kans dat onbevoegden kennis nemen van gevoelige informatie flink ingeperkt.

### *Back-up*

In de toekomst dient A een back-up te maken of te laten maken. A kan de data op een versleutelde harde schijf plaatsen waarna de schijf in een kluis wordt geplaatst. Deze back-up dient dagelijks te worden gemaakt. Een andere mogelijkheid is dat A het maken van een back-up uitbesteedt. Dit kan bijvoorbeeld door middel van Intronis of via IT Support Groep.

### *Klantpagina en klantennetwerk*

Om een veilige toegang tot de klantpagina te creëren, dient A hierop een twee-authenticatiesysteem toe te passen. Op deze wijze wordt vooraf vastgesteld of de gegevens van de klant ook daadwerkelijk door de klant worden ingezien. Als dit niet het geval is wordt geen toegang tot de pagina verleend. Daarnaast is het van belang gescheiden netwerken te verzorgen. Eén voor gasten en één voor de dienstverlening. Zo verklein je het risico dat iemand ongeoorloofd uit weet te komen bij bepaalde gegevens.

### *E-mail*

Wat betreft e-mail dient A geen bijlagen meer te verzenden en/of ontvangen welke persoonsgegevens of bijzondere persoonsgegevens bevatten. Daarnaast dient belangrijke informatie, zoals een gebruikersnaam en wachtwoord, zo veel mogelijk gescheiden verzonden te worden. Om mailverkeer nog meer te beschermen, kan A ervoor kiezen de e-mails te encrypten.

### *Personeel*

Om ervoor te zorgen dat deze digitale middelen altijd op juiste wijze ingesteld zijn en gebruikt worden, is het A aan te raden alle werknemers te laten werken vanaf een laptop of computer van A. Om deze reden is het ook van belang werknemers op te leiden hoe zij om moeten gaan met laptops, computers, wachtwoorden, digitale omgevingen en e-mail. Als zij zich bewust zijn van de gevaren en gevolgen zullen zij voorzichtiger omgaan met deze zaken.

### *7.3.2 Organisatorische maatregelen*

Een ander punt dat A dient aan te pakken, is de wijze waarop wordt omgegaan met de fysieke dossiers blijkens de toetsing uit hoofdstuk vijf. Allereerst dient een uniforme handelswijze te worden geformuleerd door middel van een interne werkinstructie. Deze is momenteel niet opgesteld blijkens hoofdstuk vijf. Daarnaast moeten dossiers opgeruimd worden in een kast met een slot erop. Aan het einde van de werkdag gaan deze kasten op slot met alle dossiers erin opgeborgen. De sleutel van deze kasten wordt in een kluis geplaatst. Gedurende de dag mag een stapeltje dossiers waarin de adviseur werkt op de werkplek aanwezig zijn, maar dan wel op een wijze waardoor geen gegevens uit dossiers zichtbaar zijn voor niet-medewerkers. Wanneer een adviseur een afspraak heeft, dienen er geen dossiers, aantekeningen of memo’s met informatie voor of over een klant zichtbaar te zijn. Deze kunnen in een kast geplaatst worden. Deze aanbevelingen zijn gebaseerd op hoofdstuk vijf van dit onderzoek.

## 7.4 Overeenkomstenplicht

In de toekomst dient A met partijen die ten behoeve van haar gegevens van klanten verwerken verwerkersovereenkomsten op te stellen. Deze overeenkomsten moeten voldoen aan de eisen beschreven in hoofdstuk vier. In hoofdstuk vijf is geconstateerd dat A niet voldoet aan de verplichting om verwerkersovereenkomsten op te stellen met alle partijen die ten behoeve van A verwerken. Er is namelijk slechts met B een bewerkersovereenkomst opgesteld

## 7.5 Registratieplicht

In de toekomst dient A een register bij te gaan houden van haar verwerkingsactiviteiten. In dit register moeten de aspecten zoals beschreven in hoofdstuk vier worden opgenomen. Uit hoofdstuk vijf blijkt namelijk dat A niet aan deze verplichting voldoet.

## 7.6 Informatieplicht

In de toekomst dient A haar klanten beter te informeren over de wijze waarop zij de persoonsgegevens van klanten verwerkt evenals de rechten die de klanten hebben bij deze verwerking. Momenteel zijn betrokkenen niet op de hoogte van de doelen van de verwerking en van de rechten die zij hebben. Dit blijkt uit de toetsing in hoofdstuk vijf en interviews met de heer X, de heer X en de heer X. De klanten kunnen geïnformeerd worden door aan de klanten vóór verwerking een privacybeleid ter beschikking te stellen welke in begrijpelijke taal is opgesteld. Dit beleid kan aan de klanten worden toegezonden, kan worden afgegeven bij het eerste gesprek en kan op de website worden geplaatst zodat deze ook online raadpleegbaar is. Idealiter wordt deze verklaring geplaatst in een bestandsvorm die na het openen kan worden opgeslagen zodat de klant het document later nogmaals kan raadplegen. A zou hiertoe het beleid beschreven in hoofdstuk zes kunnen hanteren.

## 7.7 Gegevensbeschermingseffectbeoordeling

A dient in de toekomst een gegevensbeschermingseffectbeoordeling uit te voeren aangezien zij gegevens verwerkt waarbij een hoog risico bestaat voor de rechten en vrijheden voor de klant. Dit blijkt uit hoofdstuk vijf van dit onderzoek. Zij verwerkt namelijk vele bijzondere persoonsgegevens van de klant. A moet in de toekomst in kaart gaan brengen wat de risico’s zijn van de verwerking, wanneer er een verhoogde kans bestaat dat de risico’s van de verwerking optreden en welke maatregelen in welke gevallen kunnen worden genomen.

## 7.8 Functionaris voor gegevensbescherming

Gelet op de aard van de gegevens die verwerkt worden voor de dienstverlening van A, dient A een functionaris voor gegevensbescherming aan te stellen. Op dit moment is hiervoor niemand aangesteld blijkens de toetsing in hoofdstuk vijf.

## 7.9 Beleid

A dient blijkens de toetsing in hoofdstuk vijf haar klanten beter te informeren. Hiertoe kan een privacybeleid worden opgesteld dat aan de klant wordt overhandigd en dat geplaatst wordt op de website van A blijkens hoofdstuk vier. Door middel van dit beleid moet het de klant duidelijk worden wat zij bij de verwerking van haar persoonsgegevens mag verwachten van A. Door het beleid vorm te geven als in hoofdstuk zes, is er sprake van een beleid in begrijpelijke taal. Het is dan ook aan te bevelen om dit beleid te hanteren.

#

# Bronnenlijst

**Literatuur**

**Berkvens & Vinken 2016.**

J. Berkvens & S. Vinken, *Checklist privacy: privacbeleid in 30 checklists,* Amsterdam: Berghauser Pont Publishing 2016.

**Boeije, Scheepers & Tobi 2016.**

H. Boeije, P. Scheepers & H. Tobi, *Onderzoeksmethoden,* Amsterdam: Boom Uitgevers 2016.

**Engelfriet, Kager & Meij 2017.**

A. Engelfriet, P. Kager & L. Meij, *De AVG artikelsgewijs commentaar,* Amsterdam: Ius Mentis 2017.

**Evers 2015**

J. Evers, *Kwalitatief interviewen: kunst én kunde,*  Amsterdam: Boom Lemma Uitgevers 2015.

**Krijgsman, Terstegge & Vermissen 2017.**

N. Krijgsman, J. Terstegge & K. Vermissen, *Grip op de AVG,* Deventer: Wolters Kluwer 2017.

**Personen**

Interview X

Interview X

Interview X

Interview X

Interview K. van Dijck

Observatie X

Observatie X

**Publicaties**

Article 29 Data protection working party 13 december 2016, *Guidelines on the right to data portability*, ec.europa.eu.

**CBP richtsnoeren: identificatie en verificatie van persoonsgegevens gebruik van kopietje paspoort in private sector**

*Identificatie en verificatie van persoonsgegevens gebruik van kopietje paspoort in private sector (*CBP Richtsnoeren*),* Den Haag: Autoriteit Persoonsgegevens 2012 (online publiek).

Opinion 1/2010 of article 29 Data protection working party (16 februari 2010) on the concepts of ‘controller’ and ‘processor’, ec.europa.eu.

**Jurisprudentie**

HR 23 maart 2010, ECLI:NL:PHR:2010:BK6331

Hof ’s-Hertogenbosch 25 mei 2009, ECLI:NL:GHSHE:2009:B16357.

Rb. Rotterdam 2 juni 2008, ECLI:NL:RBROT:2008:BM0412.

RvS 3 februari 2010, ECLI:NL:RVS:2010:BL1852.

SWIFT-zaak

**Elektronische bronnen**

[www.autoriteitpersoonsgegevens.nl](http://www.autoriteitpersoonsgegevens.nl)

[www.eur-lex.europa.eu](http://www.eur-lex.europa.eu)

www.europadecentraal.nl

1. Art. 14 Uitvoeringswet. [↑](#footnote-ref-1)
2. Art. 4 lid 6 Verordening (EU) 679/2016. [↑](#footnote-ref-2)
3. Art. 1 sub f Wbp. [↑](#footnote-ref-3)
4. Art. 9 lid 1 Verordening (EU) 679/2016. [↑](#footnote-ref-4)
5. Art. 4 lid 1 Verordening (EU) 679/2016. [↑](#footnote-ref-5)
6. Art. 4 lid 8 Verordening (EU) 679/2016. [↑](#footnote-ref-6)
7. Art. 4 lid 2 Verordening (EU) 679/2016. [↑](#footnote-ref-7)
8. Art. 4 lid 7 Verordening (EU) 679/2016. [↑](#footnote-ref-8)
9. Art. 4 onder 1 Verordening (EU) 679/2016. [↑](#footnote-ref-9)
10. Overweging 13 Verordening (EU) 679/2016. [↑](#footnote-ref-10)
11. Overweging 13 Verordening (EU) 679/2016. [↑](#footnote-ref-11)
12. Overweging 13 jo. art. 5 lid 1 sub a Verordening (EU) 679/2016. [↑](#footnote-ref-12)
13. Overweging 13 Verordening (EU) 679/2016. [↑](#footnote-ref-13)
14. Bijlage 4,5,6 Transcript interview X, X en X. [↑](#footnote-ref-14)
15. Bijlage 5 Transcript interview X, alinea 4 p.2. [↑](#footnote-ref-15)
16. Bijlage 5 Transcript interview X, alinea 8 p.2. [↑](#footnote-ref-16)
17. Bijlage 4 en 6: Transcript interview X en X. [↑](#footnote-ref-17)
18. Bijlage 8, Routing. [↑](#footnote-ref-18)
19. Bijlage 9, Algemene voorwaarden A. [↑](#footnote-ref-19)
20. Bijlage 6 Transcript interview X, p. 3. [↑](#footnote-ref-20)
21. Bijlage 6 Transcript interview X, alinea 1 p. 4. [↑](#footnote-ref-21)
22. Bijlage 5 Transcript interview X, alinea 6 p. 1. [↑](#footnote-ref-22)
23. Bijlage 10 Handboek en Checklist Wft SVC Compliance B.V.. [↑](#footnote-ref-23)
24. Bijlage 11 Vergunningen AFM. [↑](#footnote-ref-24)
25. Bijlage 6 Transcript interview X, alinea 13 p.6. [↑](#footnote-ref-25)
26. Bijlage 5 Transcript interview X, alinea 11 p. 4. [↑](#footnote-ref-26)
27. Bijlage 7 Transcript interview X, alinea 12 p. 1. [↑](#footnote-ref-27)
28. Bijlage 7 Transcript interview X, alinea 5 p. 2. [↑](#footnote-ref-28)
29. Bijlage 6 Transcript interview X, alinea 3 p. 4. [↑](#footnote-ref-29)
30. Bijlage 12 Waarnemingsschema. [↑](#footnote-ref-30)
31. Bijlage 13 Observatieverslag. [↑](#footnote-ref-31)
32. Bijlage 14 Inventarisatieformulier. [↑](#footnote-ref-32)
33. Bijlage 13 Observatieverslag, *fysieke dossiers*. [↑](#footnote-ref-33)
34. Art. 4 lid 1 Verordening (EU) 679/2016. [↑](#footnote-ref-34)
35. Art. 9 lid 1 Verordening (EU) 679/2016. [↑](#footnote-ref-35)
36. Bijlage 14 Inventarisatieformulier. [↑](#footnote-ref-36)
37. Bijlage13 Observatieverslag, *Inventarisatieformulier*. [↑](#footnote-ref-37)
38. Bijlage 13 Observatieverslag, *Kopie legitimatiebewijs.* [↑](#footnote-ref-38)
39. Bijlage 13 Observatieverslag, *Kopie salarisstrook.* [↑](#footnote-ref-39)
40. Krijgsman, Terstegge & Vermissen 2017, p. 67. [↑](#footnote-ref-40)
41. Bijlage 13 Observatieverslag, *Kopie verzekeringen.* [↑](#footnote-ref-41)
42. Bijlage 13 Observatieverslag, *Taxatierapport.* [↑](#footnote-ref-42)
43. Bijlage 13 Observatieverslag, *Bouwkundig rapport.*  [↑](#footnote-ref-43)
44. Bijlage 13 Observatieverslag, *Energierapport.* [↑](#footnote-ref-44)
45. Bijlage 13 Observatieverslag, O*pslag en inzage.* [↑](#footnote-ref-45)
46. Bijlage 13 Observatieverslag, *Archief.*  [↑](#footnote-ref-46)
47. Bijlage 13 Observatieverslag, *Map advies.* [↑](#footnote-ref-47)
48. Bijlage 13 Observatieverslag, *Map levensverzekeringen.* [↑](#footnote-ref-48)
49. Bijlage 13 Observatieverslag, *Map schadeverzekeringen.* [↑](#footnote-ref-49)
50. Bijlage 13 Observatieverslag, *Verplichte documenten.* [↑](#footnote-ref-50)
51. Bijlage 13 Observatieverslag, *Optionele documenten.* [↑](#footnote-ref-51)
52. Bijlage 13 Observatieverslag, O*pslag en inzage.* [↑](#footnote-ref-52)
53. Bijlage 18 Gespreksverslag X. [↑](#footnote-ref-53)
54. Bijlage 13 Observatieverslag, *Klantprofiel.* [↑](#footnote-ref-54)
55. Bijlage 18 Gespreksverslag X. [↑](#footnote-ref-55)
56. Bijlage 18 Gespreksverslag X. [↑](#footnote-ref-56)
57. Bijlage 18 Gespreksverslag X. [↑](#footnote-ref-57)
58. Opinion 1/2010 of article 29 Data protection working party (16 februari 2010) on the concepts of ‘controller’ and ‘processor’, ec.europa.eu. [↑](#footnote-ref-58)
59. SWIFT-zaak. [↑](#footnote-ref-59)
60. [www.eur-lex.europa.eu](http://www.eur-lex.europa.eu) (zoek op algemene verordening gegevensbescherming). [↑](#footnote-ref-60)
61. Overweging 6 Verordening (EU) 679/2016. [↑](#footnote-ref-61)
62. Overweging 6 Verordening (EU) 679/2016. [↑](#footnote-ref-62)
63. Art. 2 lid 1 Verordening (EU) 679/2016 jo. Chew-Meij, Engelfriet & Kager 2017, p.15. [↑](#footnote-ref-63)
64. Overweging 7 Verordening (EU) 679/2016. [↑](#footnote-ref-64)
65. Art. 1 lid 1 Verordening (EU) 679/2016. [↑](#footnote-ref-65)
66. Art. 15 Verordening (EU) 679/2016. [↑](#footnote-ref-66)
67. Art. 21 Verordening (EU) 679/2016. [↑](#footnote-ref-67)
68. Chew-Meij, Engelfriet & Kager 2017, p.40. [↑](#footnote-ref-68)
69. Art. 6 lid 1 sub a Verordening (EU) 679/2016. [↑](#footnote-ref-69)
70. Art. 4 lid 11 Verordening (EU) 679/2016. [↑](#footnote-ref-70)
71. Art. 7 lid 2 Verordening (EU) 679/2016. [↑](#footnote-ref-71)
72. Art. 6 lid 1 sub b Verordening (EU) 679/2016. [↑](#footnote-ref-72)
73. Art. 6 lid 1 sub d Verordening (EU) 679/2016. [↑](#footnote-ref-73)
74. Art. 6 lid 1 sub e Verordening (EU) 679/2016. [↑](#footnote-ref-74)
75. Art. 6 lid 1 sub f Verordening (EU) 679/2016. [↑](#footnote-ref-75)
76. Art. 5 lid 1 sub b Verordening (EU) 679/2016. [↑](#footnote-ref-76)
77. Chew-Meij, Engelfriet & Kager 2017, p.40. [↑](#footnote-ref-77)
78. Chew-Meij, Engelfriet & Kager 2017, p.40. [↑](#footnote-ref-78)
79. Art. 6 lid 4 Verordening (EU) 679/2016. [↑](#footnote-ref-79)
80. Art. 5 lid 1 sub c Verordening (EU) 679/2016. [↑](#footnote-ref-80)
81. Chew-Meij, Engelfriet & Kager 2017, p.41. [↑](#footnote-ref-81)
82. Chew-Meij, Engelfriet & Kager 2017, p.41. [↑](#footnote-ref-82)
83. Art. 5 lid 1 sub d Verordening (EU) 679/2016. [↑](#footnote-ref-83)
84. Chew-Meij, Engelfriet & Kager 2017, p.41 jo art. 83 lid 5 sub a Verordening (EU) 679/2016. [↑](#footnote-ref-84)
85. Art. 5 lid 1 sub e jo. art. 89 li 1 Verordening (EU) 679/2016. [↑](#footnote-ref-85)
86. Chew-Meij, Engelfriet & Kager 2017, p.42. [↑](#footnote-ref-86)
87. Art. 6 lid 1 sub c Verordening (EU) 679/2016. [↑](#footnote-ref-87)
88. Art. 89 lid 1 Verordening (EU) 679/2016. [↑](#footnote-ref-88)
89. Art. 5 lid 1 sub f Verordening (EU) 679/2016. [↑](#footnote-ref-89)
90. Art. 32 jo. 33 jo. 34 Verordening (EU) 679/2016. [↑](#footnote-ref-90)
91. Art.33 lid 1 Verordening (EU) 679/2016. [↑](#footnote-ref-91)
92. Art. 33 lid 2 Verordening (EU) 679/2016. [↑](#footnote-ref-92)
93. Art. 34 lid 1 Verordening (EU) 679/2016. [↑](#footnote-ref-93)
94. Art. 34 lid 3 Verordening (EU) 679/2016. [↑](#footnote-ref-94)
95. Art. 42 Uitvoeringswet AVG. [↑](#footnote-ref-95)
96. Art. 9 lid 1 Verordening (EU) 679/2016. [↑](#footnote-ref-96)
97. Art. 9 lid 2 sub a jo. 6 lid 1 sub a Verordening (EU) 679/2016. [↑](#footnote-ref-97)
98. Art. 9 lid 2 sub b jo. 6 lid 1 sub c Verordening (EU) 679/2016. [↑](#footnote-ref-98)
99. Art. 9 lid 2 sub c jo. 6 lid 1 sub d Verordening (EU) 679/2016. [↑](#footnote-ref-99)
100. Art. 9 lid 2 sub d jo. 6 lid 1 sub f Verordening (EU) 679/2016. [↑](#footnote-ref-100)
101. Art. 9 lid 2 sub e Verordening (EU) 679/2016. [↑](#footnote-ref-101)
102. Art. 9 lid 2 sub f jo. 6 lid 1 sub f Verordening (EU) 679/2016. [↑](#footnote-ref-102)
103. Art. 9 lid 2 sub g jo. 6 lid 1 sub e Verordening (EU) 679/2016. [↑](#footnote-ref-103)
104. Art. 9 lid 2 sub h jo. 6 lid 1 sub b en c Verordening (EU) 679/2016. [↑](#footnote-ref-104)
105. Art. 9 lid 2 sub i jo. 6 lid 1 sub e Verordening (EU) 679/2016. [↑](#footnote-ref-105)
106. Art. 9 lid 2 sub j jo. 6 lid 1 sub e Verordening (EU) 679/2016. [↑](#footnote-ref-106)
107. [www.eruopadecentraal.nl](http://www.eruopadecentraal.nl) (zoek op kopiëren van ID), *geraadpleegd op 10-11-2017.* [↑](#footnote-ref-107)
108. HR 23 maart 2010, ECLI:NL:PHR:2010:BK6331 jo. Rb. Rotterdam 2 juni 2008, ECLI:NL:RBROT:2008:BM0412. [↑](#footnote-ref-108)
109. Autoriteit Persoonsgegevens 20 juni 2017, ‘*Blijft BSN straks een bijzonder persoonsgegeven?’,* www.autoriteitpersoonsgegevens.nl. [↑](#footnote-ref-109)
110. Chew-Meij, Engelfriet & Kager 2017, p.293. [↑](#footnote-ref-110)
111. Bijlage 19 Transcript interview Kevin van Dijck. [↑](#footnote-ref-111)
112. [www.autoriteitpersoonsgegevens.nl](http://www.autoriteitpersoonsgegevens.nl) (zoek op privacy by design), *geraadpleegd op 27-11-2017.* [↑](#footnote-ref-112)
113. [www.autoriteitpersoonsgegevens.nl](http://www.autoriteitpersoonsgegevens.nl) (zoek op privacy by default), *geraadpleegd op 27-11-2017.* [↑](#footnote-ref-113)
114. Art. 24 lid 1 Verordening (EU) 679/2016. [↑](#footnote-ref-114)
115. Art. 28 lid 2 Verordening (EU) 679/2016. [↑](#footnote-ref-115)
116. Art. 30 lid 1 Verordening (EU) 679/2016. [↑](#footnote-ref-116)
117. Art. 30 lid 5 Verordening (EU) 679/2016. [↑](#footnote-ref-117)
118. Art. 13 lid 1 jo. lid 2 Verordening (EU) 679/2016. [↑](#footnote-ref-118)
119. Art. 12 Verordening (EU) 679/2016. [↑](#footnote-ref-119)
120. Art. 15 jo. 16 jo. 17 jo. 18 Verordening (EU) 679/2016. [↑](#footnote-ref-120)
121. Art. 20 jo. 21 jo. 22 Verordening (EU) 679/2016. [↑](#footnote-ref-121)
122. Art. 12 lid 5 Verordening (EU) 679/2016. [↑](#footnote-ref-122)
123. Art. 20 lid 1 Verordening (EU) 679/2016. [↑](#footnote-ref-123)
124. Chew-Meij, Engelfriet & Kager 2017, p.86 jo art. 15 lid 4 Verordening (EU) 679/2016. [↑](#footnote-ref-124)
125. Art. 5 lid 1 sub d Verordening (EU) 679/2016 jo. Hof ’s-Hertogenbosch 25 mei 2009, ECLI:NL:GHSHE:2009:B16357. [↑](#footnote-ref-125)
126. RvS 3 februari 2010, ECLI:NL:RVS:2010:BL1852. [↑](#footnote-ref-126)
127. Art. 19 Verordening (EU) 679/2016. [↑](#footnote-ref-127)
128. Art. 17 lid 1 Verordening (EU) 679/2016. [↑](#footnote-ref-128)
129. Chew-Meij, Engelfriet & Kager 2017, p. 91. [↑](#footnote-ref-129)
130. Art. 12 lid 3 Verordening (EU) 679/2016. [↑](#footnote-ref-130)
131. Chew-Meij, Engelfriet & Kager 2017, p.91 jo. art. 12 lid 3 Verordening (EU) 679/2016. [↑](#footnote-ref-131)
132. Art. 17 lid 2 Verordening (EU) 679/2016. [↑](#footnote-ref-132)
133. Art. 17 lid 3 sub b Verordening (EU) 679/2016. [↑](#footnote-ref-133)
134. Art. 18 lid 1 Verordening (EU) 679/2016. [↑](#footnote-ref-134)
135. Chew-Meij, Engelfriet & Kager 2017, p.99. [↑](#footnote-ref-135)
136. Article 29 Data protection working party 13 december 2016, *Guidelines on the right to data portability*, ec.europa.eu. [↑](#footnote-ref-136)
137. Chew-Meij, Engelfriet & Kager 2017, p.103. [↑](#footnote-ref-137)
138. Art. 21 lid 4 Verordening (EU) 679/2016. [↑](#footnote-ref-138)
139. Art. 22 lid 1 Verordening (EU) 679/2016. [↑](#footnote-ref-139)
140. Art. 13 lid 2 sub f jo. art. 14 lid 2 sub g Verordening (EU) 679/2016. [↑](#footnote-ref-140)
141. Art. 22 lid 2 sub a jo. sub b jo. 22 lid 3 Verordening (EU) 679/2016. [↑](#footnote-ref-141)
142. Art. 22 lid 4 Verordening (EU) 679/2016. [↑](#footnote-ref-142)
143. Bijlage 17 Overzicht rechten betrokkenen. [↑](#footnote-ref-143)
144. Art. 35 lid 2 Verordening (EU) 679/2016. [↑](#footnote-ref-144)
145. Art. 35 lid 7 Verordening (EU) 679/2016. [↑](#footnote-ref-145)
146. Art. 35 lid 10 Verordening (EU) 679/2016. [↑](#footnote-ref-146)
147. Art.37 lid 1 Verordening (EU) 679/2016. [↑](#footnote-ref-147)
148. Art. 14 Uitvoeringswet. [↑](#footnote-ref-148)
149. Art. 57 lid 1 sub a Verordening (EU) 679/2016. [↑](#footnote-ref-149)
150. Art. 58 lid 1 jo lid 2 jo lid 3 Verordening (EU) 679/2016. [↑](#footnote-ref-150)
151. Krijgsman, Terstegge & Vermissen 2017, p.91. [↑](#footnote-ref-151)
152. Krijgsman, Terstegge & Vermissen 2017, p.91. [↑](#footnote-ref-152)
153. Art. 33 lid 1 sub a WWFT. [↑](#footnote-ref-153)
154. Art. 33 lid 1 sub a onder 1 en 2 WWFT. [↑](#footnote-ref-154)
155. [www.autoriteitpersoonsgegevens.nl](http://www.autoriteitpersoonsgegevens.nl) (zoek op kopie paspoort) jo. CBP richtsnoeren: identificatie en verificatie van persoonsgegevens gebruik van kopietje paspoort in private sector – juli 2012. [↑](#footnote-ref-155)
156. Chew-Meij, Engelfriet & Kager 2017, p.56 jo. [www.europadecentraal.nl](http://www.europadecentraal.nl) (zoek op kopiëren ID), *geraadpleegd op 3-12-2017*. [↑](#footnote-ref-156)
157. Art. 28 lid 2 Verordening 679/2016. [↑](#footnote-ref-157)
158. Berkvens, Vinken, Wiegerinck & Wolters 2016, p. 47-50. [↑](#footnote-ref-158)