Privacy bij de notaris?

Een praktijkgericht juridisch onderzoek naar de gevolgen van de huidige en toekomstige privacywetgeving voor Daamen de Kort van Tuijl Notarissen

DAAMEN
DE KORT
VAN TUIJL
NOTARISSEN

T.C.M. (Tom) Oerlemans
Tilburg, mei 2017

Privacy bij de notaris?

Een praktijkgericht juridisch onderzoek naar de gevolgen van de huidige en toekomstige privacywetgeving voor Daamen de Kort van Tuijl Notarissen

Auteur	T.C.M. (Tom) Oerlemans
Studentnummer	2081239
Afstudeerorganisatie	Daamen de Kort van Tuijl Notarissen
Afstudeermentor	Dhr. mr. J.A. Beijsens
Afstudeerperiode	februari 2017 t/m mei 2017
Onderwijsinstelling	Juridische hogeschool Avans-Fontys
Opleiding	HBO-Rechten
Locatie	Tilburg
Eerste afstudeerdocent	Mevr. mr. M.E.R. van Remortel
Tweede afstudeerdocent	Mevr. mr. L.A. Hopmans

Tilburg, mei 2017

Voorwoord

Het onderzoeksrapport dat voor u ligt is geschreven ter afsluiting van mijn opleiding HBO-Rechten aan de Juridische Hogeschool Avans-Fontys en is het eindproduct van het onderzoek dat ik gedurende vier maanden bij Daamen de Kort van Tuijl Notarissen (DKT) heb mogen uitvoeren. Samen met DKT is er gekozen voor een onderwerp op het gebied van privacyrecht. Hoewel dit niet een van de rechtsgebieden is waarin het kantoor zich heeft gespecialiseerd, heeft het kantoor er indirect wel dagelijks mee te maken. Er worden namelijk persoonsgegevens van cliënten verwerkt om de notariële diensten te kunnen verlenen. Met de verandering van de privacywetgeving in zicht, werd dit als een goed moment gezien om de gang van zaken binnen DKT te analyseren en evalueren. Met dit onderzoek heb ik getracht DKT handvatten te bieden om de bedrijfsvoering met betrekking tot persoonsgegevens in lijn te brengen met zowel de huidige als de toekomstige wetgeving.

Ik wil hierbij graag enkele personen bedanken die mij geholpen hebben bij de totstandkoming van deze scriptie. Ten eerste wil ik mijn begeleider binnen DKT, mr. Jeroen Beijsens, bedanken voor zijn inhoudelijke feedback op het onderzoek en voor de inzichten die hij mij heeft gegeven in het beroep van notaris. Ook wil ik drs. Ruud Nijnens bedanken voor het regelmatig van gedachten wisselen omtrent privacy binnen DKT. Daarnaast wil ik Monique Hamers-Massuger, Charlotte Maat, Lauran van Hoof en Mariska Donders bedanken voor hun medewerking aan de observaties die gedurende dit onderzoek zijn verricht. Het laatste woord van dank gaat uit naar alle medewerkers van DKT, met name Ingrid Houkes, die deze afstudeerperiode tot niet alleen een leerzame maar ook een leuke tijd hebben gemaakt.

Tom Oerlemans

Tilburg, mei 2017

Inhoudsopgave

Samenvatting

Lijst van gebruikte afkortingen

Begrippenlijst

Hoofdstuk 1: Inleiding 11

§ 1.1 Organisatiebeschrijving 11

§ 1.2 Probleembeschrijving 11

§ 1.3 Centrale vraag 12

§ 1.4 Doelstelling 12

§ 1.5 Deelvragen 12

§ 1.6 Onderzoeksmethoden en verantwoording 13

§ 1.7 Leeswijzer 14

Hoofdstuk 2: Wet bescherming persoonsgegevens 15

§ 2.1 Toepassingsgebied en betrokken partijen 15

§ 2.2 Vereisten aan verwerking 15

§ 2.3 Meldplicht bij verwerking 16

§ 2.3.1 Vrijstelling meldplicht verwerking 16

§ 2.4 Informatieplicht 17

§ 2.5 Bewaren van persoonsgegevens 17

§ 2.5.1 De notaris en de bewaartermijn uit de Wbp 18

§ 2.6 Rechten van betrokkene 19

§ 2.7 Beveiliging van persoonsgegevens 19

§ 2.8 De bewerker 20

§ 2.8.1 De bewerkersovereenkomst 21

§ 2.9 Meldplicht datalekken 21

§ 2.9.1 Definitie datalek 21

§ 2.9.2 Melding aan de AP 22

§ 2.9.3 Melding aan de betrokkene 22

§ 2.9.4 Onverwijld 23

§ 2.9.5 Registratie datalek 24

§ 2.10 Sancties 24

Hoofdstuk 3: Het huidige beleid en de huidige werkwijze van DKT 26

§ 3.1 Aanvaarding van de opdracht 26

§ 3.2 Inhoud en verloop van een dossier 26

§ 3.4 Bewaren van dossiers 28

§ 3.5 Beveiliging 28

§ 3.5.1 Organisatorische beveiligingsmaatregelen 28

§ 3.5.2 Technische beveiligingsmaatregelen 29

§ 3.6 Bewerkers 30

§ 3.7 Meldplicht datalekken 30
§ 3.7.1 Datalekken binnen DKT 31
Hoofdstuk 4: Algemene Verordening Gegevensbescherming 32
§ 4.1 Toepassingsgebied en betrokken partijen 32
§ 4.1.1 Functionaris voor de gegevensbescherming 32
§ 4.2 Vereisten aan verwerking 32
§ 4.2.1 Verantwoordingsplicht 33
§ 4.2.2 Privacy by design en privacy by default 33
§ 4.3 Registratieplicht 34
§ 4.4 Informatieplicht 34
§ 4.5 Bewaren van persoonsgegevens 35
§ 4.5.1 De notaris en de bewaartermijn uit de AVG 35
§ 4.6 Rechten van betrokkene 36
§ 4.7 Beveiliging van persoonsgegevens 37
§ 4.7.1 Privacy Impact Assessment 37
§ 4.8 De bewerker 37
§ 4.8.1 De bewerkersovereenkomst 38
§ 4.9 Meldplicht datalekken 38
§ 4.9.1 Definitie datalek 39
§ 4.9.2 Melding aan de AP 39
§ 4.9.3 Melding aan de betrokkene 39
§ 4.9.4 Onverwijld 40
§ 4.9.5 Registratie datalek 40
§ 4.10: Sancties 40
Hoofdstuk 5: DKT en de Wbp 42
§ 5.1 Toepassingsgebied en betrokken partijen 42
§ 5.2 Vereisten aan verwerking 42
§ 5.3 Meldplicht bij verwerking en vrijstelling 43
§ 5.4 Informatieplicht 43
§ 5.5 Bewaren van persoonsgegevens 44
§ 5.6 Beveiliging van persoonsgegevens 44
§ 5.7 De bewerker en de bewerkersovereenkomst 45
§ 5.8 Meldplicht datalekken 46
§ 5.9 Sancties 46
Hoofdstuk 6: DKT en de AVG 48
§ 6.1 Toepassingsgebied en betrokken partijen 48
§ 6.2 Vereisten aan verwerking 48
§ 6.3 Registratieplicht verwerkingsactiviteiten 49
§ 6.4 Informatieplicht 49

§ 6.5 Bewaren van persoonsgegevens....49
§ 6.6 Beveiliging van persoonsgegevens....50
§ 6.7 De bewerker en de bewerkersovereenkomst....51
§ 6.8 Meldplicht datalekken....51
§ 6.9 Sancties....52
Hoofdstuk 7: Conclusies en aanbevelingen....53
Literatuurlijst....58

Samenvatting

Daamen de Kort van Tuijl Notarissen (hierna: DKT) is een van de grotere notariskantoren in Nederland, met vestigingen in Tilburg, Rijen en Udenhout. Bij het leveren van notariële diensten verwerkt DKT veel persoonsgegevens van cliënten. De wet- en regelgeving omtrent deze persoonsgegevens is de laatste jaren aan veranderingen onderhevig. Zo is de huidige Wet bescherming persoonsgegevens (hierna: Wbp) in 2016 aangevuld met een meldplicht datalekken. Op 25 mei 2018 wordt de huidige Wbp vervangen door de Algemene verordening gegevensbescherming (hierna: AVG). Deze veranderingen zijn reden geweest om een kritische blik te werpen op de huidige omgang met persoonsgegevens van cliënten binnen DKT. Gedurende dit onderzoek heeft de volgende vraag centraal gestaan: 'Welke aanbevelingen kunnen aan DKT worden gedaan over de omgang met persoonsgegevens van cliënten, gelet op een analyse van de Wet bescherming persoonsgegevens en de Algemene verordening gegevensbescherming?'

Om deze vraag te beantwoorden, zijn de Wbp en de AVG geanalyseerd. Daaruit is gebleken dat de AVG veel verplichtingen uit de Wbp aangescherpt. De AVG eist ook dat naleving van deze verplichtingen kan worden aangetoond. De sanctiemogelijkheden van de Autoriteit Persoonsgegevens (hierna: AP) worden uitgebreid. Ook is de huidige gang van zaken met betrekking tot persoonsgegevens binnen DKT geanalyseerd aan de hand van observaties, interviews en documentenonderzoek. De resultaten van deze analyse zijn vervolgens getoetst aan de Wbp en de AVG. Hieruit blijkt dat DKT op verschillende punten nog niet aan de Wbp voldoet. Cliënten worden niet volledig geïnformeerd over de verwerking van hun persoonsgegevens en de wettelijke bewaartermijnen worden overschreden. Hoewel er voldoende technische beveiligingsmaatregelen zijn genomen, schieten de organisatorische beveiligingsmaatregelen tekort. Zo zijn de papieren dossiers enkel beveiligd met het alarmsysteem van het pand en is er geen procedure om het beveiligingsniveau regelmatig te evalueren. Ook zijn er geen deugdelijke bewerkersovereenkomsten gesloten met BB Diensten en Box B.V., twee bewerkers die betrokken zijn bij de papieren dossiervoering. Ten aanzien van datalekken is er niet altijd onverwijld gemeld en is er in het beleid een verkeerde meldingstermijn opgenomen. DKT voldoet tevens niet aan de aangescherpte eisen uit de AVG betreffende de informatieplicht, de bewaartermijn en bewerkersovereenkomsten. Met betrekking tot datalekken wijkt het huidige beleid van DKT af van de AVG. Daarnaast heeft het kantoor onvoldoende vastgelegd om naleving van de AVG aan te kunnen tonen.

Aanbevolen wordt om middels een privacyverklaring meteen aan de informatieplicht uit de AVG te voldoen. Ten aanzien van de bewaartermijn moet DKT, zolang de Wbp nog geldt, de verwerking van persoonsgegevens melden aan de AP omdat de bewaartermijn uit het Vrijstellingsbesluit Wbp wordt overschreden. Het huidige beleid om dossiers met daarin persoonsgegevens voor onbepaalde tijd te bewaren is tevens in strijd met de strikte bewaartermijn uit de AVG en moet worden herzien. Op het gebied van beveiliging wordt aanbevolen om een extra laag beveiliging in te stellen voor de papieren dossiervoering, bijvoorbeeld door het gebruik van afsluitbare dossierkasten. Ook moet er een procedure worden ingesteld om het beveiligingsniveau regelmatig te evalueren en eventueel te testen. Met Box B.V. en BB Diensten moeten bewerkersovereenkomsten worden gesloten, die aan de eisen uit de AVG voldoen. Ten aanzien van datalekken moet het beleid omtrent het onverwijld melden van een datalek worden aangepast om zowel aan de Wbp als de AVG te voldoen. Onder de Wbp moet DKT nog situaties melden waarin de onrechtmatige verwerking van persoonsgegevens niet redelijkerwijs kan worden uitgesloten. Onder de AVG is dit niet langer vereist, maar is de registratie van alle beveiligingsincidenten verplicht. Na het van toepassing worden van de AVG moet hier het beleid op worden aangepast. Tenslotte moet DKT een register van verwerkingsactiviteiten gaan bijhouden, wat tevens kan helpen bij het voldoen aan de verantwoordingsplicht van de AVG. Door de genoemde aanbevelingen op te volgen, worden hoge boetes en andere ingrijpende sancties, zoals een verwerkingsbeperking of -verbod, voorkomen.

Lijst van gebruikte afkortingen

AP	Autoriteit Persoonsgegevens
AVG	Algemene Verordening Gegevensbescherming
AW	Archiefwet
Awb	Algemene wet bestuursrecht
Awr	Algemene wet inzake rijksbelastingen
BRP	Basisregistratie personen
BSN	Burgerservicenummer
DIN	Deutschen Institut für Normung
DKT	Daamen de Kort van Tuijl Notarissen
FG	Functionaris voor de gegevensbescherming
ISO	International Standardization Organization
Jo.	Juncto
PIA	Privacy Impact Assessment
Sr.	Wetboek van Strafrecht
Wbp	Wet bescherming persoonsgegevens
Wna	Wet op het notarisambt
Wwft	Wet ter voorkoming van witwassen en financiering van terrorisme

Begrippenlijst

Autoriteit Persoonsgegevens
De Autoriteit Persoonsgegevens, voorheen het College Bescherming Persoonsgegevens genoemd, is de Nederlandse toezichthouder op het gebied van privacywetgeving.[1]

Bestand
Het begrip bestand wordt gedefinieerd als elk gestructureerd geheel van persoonsgegevens dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen.[2] Hierbij kan gedacht worden aan een systeem met gestructureerde digitale of fysieke dossiers.[3]

Betrokkene
De betrokkene is de natuurlijke persoon op wie een persoonsgegeven betrekking heeft.[4] Wanneer persoonsgegevens van een betrokkene worden verwerkt, kan hij zich op verschillende rechten beroepen.

Bewerker
Degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, maar niet onder zijn rechtstreeks gezag is onderworpen, wordt bewerker genoemd.[5] De bewerker staat buiten de organisatie van de verantwoordelijke, maar handelt wel onder zijn verantwoordelijkheid. Dit is vaak een externe dienstverlener, zoals een bedrijf dat wordt ingeschakeld om de boekhouding te doen. Daarbij is het niet uitgesloten dat de bewerker bepaalde zeggenschap heeft over de te gebruiken middelen zonder dat hij wordt aangemerkt als verantwoordelijke.[6]

Persoonsgegeven
Een persoonsgegeven is elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.[7] Naast tekst omvat het begrip ook beeld en geluid.[8] Wanneer gegevens over een zaak indirect ook wat vertellen over een natuurlijke persoon en deze in zijn maatschappelijke positie kunnen raken, bijvoorbeeld gegevens uit het Kadaster, worden ook de gegevens over de zaak aangemerkt als persoonsgegevens.[9] De gegevens moeten betrekking hebben op een natuurlijke persoon die geïdentificeerd is of waarvan de identiteit redelijkerwijs kan worden vastgesteld.[10] Wanneer een gegeven geen betrekking heeft op een natuurlijke persoon of de natuurlijke persoon niet kan worden geïdentificeerd, wordt het gegeven niet aangemerkt als persoonsgegeven.

Sub-bewerker
Een sub-bewerker is een bewerker die door een andere bewerker wordt ingeschakeld voor het in opdracht van de verantwoordelijke verwerken van persoonsgegevens. Sub-bewerkerschap doet zich bijvoorbeeld voor wanneer de verantwoordelijke een externe partij inschakelt om de salarisadministratie te verzorgen, die op zijn beurt een IT bedrijf inschakelt om de salarisadministratie te kunnen verzorgen. Het IT bedrijf is in dat geval de sub-bewerker.

---

[1] Artikel 1 sub k Wbp jo. artikel 51 Wbp.
[2] Artikel 1 sub c Wbp.
[3] Sauerwein & Linnemann 2002, p. 15.
[4] Artikel 1 sub f Wbp.
[5] Artikel 1 sub e Wbp.
[6] Kranenborg & Verhey 2011, p. 78-79.
[7] Artikel 1 sub a Wbp.
[8] *Kamerstukken II* 1997/98, 25892, 3, p. 50.
[9] *Kamerstukken II* 1997/98, 25892, 9, p. 1; zie ook Hooghiemstra & Nouwt 2007, p. 34.
[10] *Kamerstukken II* 1997/98, 25892, 3, p. 47.

Verantwoordelijke
De verantwoordelijke is de natuurlijke persoon, de rechtspersoon, het bestuursorgaan of ieder ander die, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.[11] Zoals het begrip impliceert, is de verantwoordelijke verantwoordelijk voor de verwerking van persoonsgegevens. Primair is dit degene die formeel-juridisch bevoegd is het doel en de middelen vast te stellen, niet degene die feitelijk de beslissing neemt. Dit is bijvoorbeeld de rechtspersoon.

Verwerking
Onder de verwerking van persoonsgegevens valt elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval 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.[12] Dit is een niet-limitatieve opsomming en ook andere handelingen met betrekking tot persoonsgegevens moeten als verwerking van persoonsgegevens worden aangemerkt. Feitelijke macht over de gegevens is hierbij vereist.[13]

[11] Artikel 1 sub d Wbp.
[12] Artikel 1 sub b Wbp.
[13] Sauerwein & Linnemann 2002, p. 14.

Hoofdstuk 1: Inleiding

In dit hoofdstuk wordt het raamwerk voor dit onderzoek uiteengezet. Allereerst wordt er kort aandacht besteed aan DKT als organisatie. Daarna wordt het probleem omschreven dat bij DKT speelt. Vervolgens komen de daarop gebaseerde centrale vraag, doelstelling en deelvragen aan bod, waarna er wordt ingegaan op methoden en technieken die zijn gebruikt bij het uitvoeren van dit onderzoek. Tenslotte wordt in een leeswijzer weergegeven wat in welk hoofdstuk wordt besproken.

§ 1.1 Organisatiebeschrijving

DKT is een notariskantoor gevestigd in Tilburg, Rijen en Udenhout. Het is een van de grotere notariskantoren in Nederland, het grootste van Noord-Brabant. Het kantoor streeft ernaar de laagdrempeligheid en persoonlijke benadering van een klein kantoor te combineren met de ervaring en specialismen van een groot kantoor. DKT biedt diensten aan op het gebied van onder andere personen- en familierecht, estate planning, ondernemingsrecht en onroerend goed.

§ 1.2 Probleembeschrijving

Om hun werkzaamheden binnen het notariaat te kunnen verrichten, hebben de (kandidaat-) notarissen, notarisklerken en notarieel medewerkers van DKT veel informatie over hun cliënten nodig. Deze informatie wordt onder andere verzameld om een notariële akte op te stellen, om cliënten te kunnen adviseren, om met hen te corresponderen en om te factureren voor de verrichte werkzaamheden. Bij deze informatie kan gedacht worden aan de adresgegevens en identiteitsbewijzen van de betrokken partijen, een inzage in de Basisregistratie Personen (hierna: BRP), het Centraal Curatele- en bewindregister of het huwelijksgoederenregister. Afhankelijk van wat voor zaak het betreft kunnen er aanvullende gegevens worden opgevraagd. Zo wordt er bij de overdracht van een woning ook recherche gedaan naar de kadastrale gegevens van de woning, wordt er bij het behandelen van een testament inzage gedaan in het Centraal Testamentenregister en worden er bij een statutenwijziging van een rechtspersoon gegevens opgevraagd bij de Kamer van Koophandel (hierna: KvK). Om al haar diensten aan te kunnen bieden, werkt DKT in de dagelijkse praktijk veel met persoonsgegevens van cliënten. Deze persoonsgegevens worden zowel fysiek als digitaal opgenomen in dossiers.

De voornoemde gegevens over cliënten die door DKT worden ingezien en gebruikt, zijn vooral persoonlijk. Cliënten willen deze informatie dan ook privé houden. De notaris en degenen die onder hem of haar werkzaam zijn, hebben een geheimhoudingsplicht ten aanzien van deze informatie op basis van artikel 22 van de Wet op het notarisambt (hierna: Wna). Naast deze geheimhoudingsplicht bestaat er specifieke wetgeving over een bepaald soort gegevens, de persoonsgegevens. Een persoonsgegeven is elk gegeven over een geïdentificeerd of identificeerbaar persoon. Regels over persoonsgegevens zijn vastgelegd in de Wet bescherming persoonsgegevens (hierna: Wbp). Elke handeling of geheel van handelingen met betrekking op deze gegevens valt onder de Wbp wanneer de handeling geheel of gedeeltelijk geautomatiseerd verloopt. De Wbp is ook van toepassing wanneer de persoonsgegevens niet geautomatiseerd verwerkt worden met als doel ze op te nemen in een bestand. Omdat DKT bij het verrichten van notariële werkzaamheden persoonsgegevens verwerkt, dient het kantoor zich aan de Wbp te houden. In 2016 is het wetsvoorstel Meldplicht Datalekken in werking getreden. Hiermee werd de Wbp uitgebreid met de verplichting om datalekken te melden en kreeg de Autoriteit Persoonsgegevens (hierna: AP) een grotere boetebevoegdheid.

De wetgeving omtrent de persoonsgegevens gaat echter nogmaals veranderen. In 2012 heeft de Europese Commissie een start gemaakt met de Algemene Verordening

Gegevensbescherming[14] (hierna: AVG), waar de Europese Commissie uiteindelijk op 14 april 2016 mee heeft ingestemd. De verordening is op 4 mei 2016 gepubliceerd in het Publicatieblad van de Europese Unie, waarna de verordening 20 dagen later in werking is getreden. Vervolgens zal de AVG op 25 mei 2018 van toepassing worden. Deze ruimte van twee jaar is ingebouwd om bedrijven, organisaties en overheden de kans te bieden zich voor te bereiden op de AVG. De bescherming van persoonsgegevens wordt namelijk verder aangescherpt. Er worden onder andere veranderingen doorgevoerd in de meldplicht voor datalekken en de regels over bewerkersovereenkomsten. Daarnaast wordt er een registratieplicht ingevoerd, worden de rechten van betrokkenen uitgebreid en kunnen bedrijven worden verplicht om een functionaris voor de gegevensbescherming aan te stellen of een *privacy impact assessment* uit te voeren. De Europese verordening zal de Nederlandse Wbp, net als de privacywetten in de andere lidstaten, vervangen.

Naar aanleiding van de invoering van het wetsvoorstel Meldplicht Datalekken in 2016 en het van toepassing worden van de AVG in 2018 wil DKT weten welke gevolgen dit heeft voor het kantoor. DKT werkt immers dagelijks met persoonsgegevens van cliënten. Om deze reden is dit onderzoek gericht op de persoonsgegevens van cliënten en niet die van eigen medewerkers. DKT zal tot 25 mei 2018 moeten voldoen aan de Wbp, waarna het kantoor zich aan de AVG zal moeten houden. Door dit onderzoek moet het voor DKT duidelijk worden in hoeverre er aan de huidige en toekomstige privacywetgeving wordt voldaan en welke stappen er nog gezet moeten worden om hier volledig aan te voldoen. Het doel is het kantoor op het gebied van privacy klaar te stomen voor de toekomst.

§ 1.3 Centrale vraag

Welke aanbevelingen kunnen aan DKT worden gedaan over de omgang met persoonsgegevens van cliënten, gelet op een analyse van de Wet bescherming persoonsgegevens en de Algemene verordening gegevensbescherming?

§ 1.4 Doelstelling

Op 29 mei 2017 wordt een onderzoeksrapport opgeleverd aan de heer mr. J.A. Beijsens, notaris en estate planner bij DKT, met daarin een analyse van de omgang met persoonsgegevens van cliënten binnen DKT aan de hand van de Wet bescherming persoonsgegevens met de daarin opgenomen meldplicht datalekken en de vanaf 25 mei 2018 geldende Algemene Verordening Gegevensbescherming, alsmede concrete, op deze analyse gebaseerde aanbevelingen ter verbetering van de omgang met persoonsgegevens van cliënten.

§ 1.5 Deelvragen

1. Wat is het huidig juridisch kader met betrekking tot de omgang met persoonsgegevens?
2. Wat is het huidige beleid en de huidige werkwijze van DKT met betrekking tot de omgang met persoonsgegevens van cliënten?
3. Welke veranderingen in het juridisch kader met betrekking tot de omgang met persoonsgegevens brengt het van toepassing worden van de Algemene Verordening Gegevensbescherming met zich mee?
4. In welke mate wijkt het huidige beleid en de huidige werkwijze van DKT met betrekking tot de omgang met persoonsgegevens van cliënten af van de Wet bescherming persoonsgegevens en de Algemene Verordening Gegevensbescherming?

[14] Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (*PbEU* 2016, L 119/1).

§ 1.6 Onderzoeksmethoden en verantwoording
In deze paragraaf wordt per deelvraag behandeld welke onderzoeksstrategie, bronnen en methoden er zijn gebruikt bij de beantwoording hiervan.

- Wat is het huidig juridisch kader met betrekking tot de omgang met persoonsgegevens?
- Welke veranderingen in het juridisch kader met betrekking tot de omgang met persoonsgegevens brengt het van toepassing worden van de Algemene Verordening Gegevensbescherming met zich mee?

Om de bovenstaande deelvragen met betrekking tot het juridisch kader te beantwoorden, is er gebruik gemaakt van een rechtsbronnen- en literatuuronderzoek. Er zijn gedurende het onderzoek verschillende rechtsbronnen bestudeerd, waarbij de Wbp en de AVG centraal hebben gestaan. Ook zijn er kamerstukken en verschillende beleidsdocumenten van de AP geanalyseerd, die de wettekst verder inkleuren. Bij het analyseren van de Wbp is er tevens gebruik gemaakt van verschillende boeken. Over de AVG is er minder literatuur beschikbaar, aangezien de verordening pas relatief kort een definitieve vorm heeft gekregen. Daarom is er bij de analyse van de AVG en vergelijking met de Wbp meer gebruik gemaakt van internetpublicaties, waarbij informatie hieruit altijd is getoetst aan de definitieve versie van de AVG. Er zijn namelijk ook oudere publicaties over de AVG, die gebaseerd zijn op een oudere versie van de verordening. Bij het uitwerken van het juridisch kader is tevens aandacht besteed aan de raakvlakken met wetgeving omtrent het notariaat. Om hier verdere invulling aan te geven is er gebruik gemaakt van jurisprudentie en verschillende artikelen over digitalisering binnen het notariaat.

- Wat is het huidige beleid en de huidige werkwijze van DKT met betrekking tot de omgang met persoonsgegevens van cliënten?

Het antwoord op de tweede deelvraag is geformuleerd aan de hand van een casestudy. Om de huidige omgang met persoonsgegevens in kaart te brengen, zijn er half-gestructureerde interviews afgenomen met kantoordirecteur drs. R. Nijnens en notaris mr. J.A. Beijsens. Zij houden zich, naast hun reguliere werkzaamheden binnen DKT, ook bezig met privacy binnen het kantoor. Ook zijn er drie medewerkers geobserveerd bij het aanmaken en inboeken van dossiers. Bij deze vrije observatie is er gekeken naar welke gegevens er worden verzameld en op welke manier deze worden opgeslagen. Verschillende documenten die daarbij worden gebruikt, zoals procedurelijsten, zijn geanalyseerd**.** Ook is er een vrije observatie uitgevoerd bij de administratie, om de financiële afhandeling van een dossier in kaart te brengen. Daarnaast zijn er interne beleidsdocumenten geanalyseerd met betrekking tot het opslaan van dossiers, de technische beveiliging en het beleid omtrent datalekken. Ook zijn er overeenkomsten geanalyseerd die DKT heeft gesloten met partijen die bij de omgang met persoonsgegevens van cliënten zijn betrokken.

- In welke mate wijkt het huidige beleid en de huidige werkwijze van DKT met betrekking tot de omgang met persoonsgegevens van cliënten af van de Wet bescherming persoonsgegevens en de Algemene Verordening Gegevensbescherming?

Bij beantwoording van deze deelvraag zijn de resultaten uit de voorgaande drie deelvragen samengebracht. Het huidige beleid en de huidige werkwijze van DKT omtrent persoonsgegevens van cliënten is vergeleken met de twee juridische kaders die in de eerste en derde deelvraag zijn vastgesteld. Bij deze vergelijking zijn verschillende onderwerpen verder aangevuld om verbinding te kunnen maken tussen DKT als notariskantoor en de privacywetgeving. Aan de hand van deze vergelijking is vastgesteld

op welke punten de huidige werkwijze en het huidig beleid van DKT voldoet aan de Wbp en de AVG. Ook is er vastgesteld op welke punten DKT tekortschiet.

§ 1.7 Leeswijzer

In hoofdstuk 2 wordt de huidige privacywetgeving in de vorm van de Wbp behandeld. Hierin worden de verschillende kernpunten van de Wbp benoemd die in het onderzoek meerdere malen zullen terugkomen. Hoofdstuk 3 gaat over het huidige beleid en de huidige werkwijze van DKT met betrekking tot de omgang met persoonsgegevens van cliënten. Nadat zowel het huidige juridisch kader als de huidige situatie is geschetst, wordt er in hoofdstuk 4 gekeken naar de veranderingen die de AVG teweeg zal brengen. Daarbij wordt er ingegaan op dezelfde kernpunten die zijn behandeld in het tweede hoofdstuk. In hoofdstuk 5 wordt de Wbp vergeleken met DKT. Hoofdstuk 6 maakt dezelfde vergelijking, maar dan op basis van de AVG. In het laatste hoofdstuk worden de conclusies en aanbevelingen van het onderzoek gegeven, waarmee antwoord wordt gegeven op de centrale vraag.

Hoofdstuk 2: Wet bescherming persoonsgegevens

Dit hoofdstuk behandelt het huidig juridisch kader met betrekking tot persoonsgegevens. Dit kader, hoofdzakelijk bestaande uit de Wbp, wordt vastgesteld om uiteindelijk de vergelijking te kunnen maken met het toekomstig juridisch kader, de AVG. Er zal onder andere worden ingegaan op de verwerking en beveiliging van persoonsgegevens en de hieraan verbonden meldplicht. Ook zal de in 2016 ingevoerde Meldplicht Datalekken aan bod komen. Bij het vaststellen van het huidig juridisch kader zal er op bepaalde punten aandacht worden besteed aan de voor de notaris relevante aspecten.

§ 2.1 Toepassingsgebied en betrokken partijen

De Wbp is van toepassing op de (gedeeltelijk) geautomatiseerde verwerking van persoonsgegevens, bijvoorbeeld het opslaan van persoonsgegevens in een computersysteem. De Wbp is ook van toepassing op de niet geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn of worden opgenomen.[15] Onder verwerking valt elke handeling of geheel van handelingen met betrekking op persoonsgegevens, vanaf het moment van verzameling tot het moment van vernietiging.[16] Een belangrijke partij hierbij is de verantwoordelijke, aan wie de Wbp verschillende verplichtingen oplegt. Aan de betrokkene, degene waarop de gegevens betrekking hebben, worden door de Wbp verschillende rechten toegekend.[17]

§ 2.2 Vereisten aan verwerking

Aan de verwerking van persoonsgegevens worden verschillende vereisten gesteld.
De verantwoordelijke dient er zorg voor te dragen dat aan deze vereisten wordt voldaan.[18] Zo moeten persoonsgegevens in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze worden verwerkt.[19] Een belangrijk begrip is doelbinding, dat stelt dat de persoonsgegevens alleen verzameld mogen worden voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden.[20] Vervolgens mogen de persoonsgegevens alleen verwerkt worden op een manier die met deze doeleinden verenigbaar is.[21] Daarnaast mogen de persoonsgegevens alleen verwerkt worden voor zover deze, gelet op de doeleinden, toereikend, ter zake dienend en niet bovenmatig zijn. Daarbij dienen de persoonsgegevens juist en nauwkeurig te zijn.[22] De verantwoordelijke moet ervoor zorgen dat de gegevens niet langer worden bewaard dan noodzakelijk voor de verwerkelijking van het doel waarvoor zij verzameld worden.[23] Hierop wordt verder ingegaan in paragraaf 2.5. Daarnaast is een passend beveiligingsniveau vereist, dat in paragraaf 2.7 aan bod komt.[24]

Tenslotte geeft de Wbp een limitatieve opsomming van zes situaties waarin de verwerking van persoonsgegevens rechtmatig is.[25] Deze grondslagen voor de verwerking zijn:

- de ondubbelzinnige toestemming van de betrokkene;
- het uitvoeren van een overeenkomst waarbij de betrokkene partij is;
- het nakomen van een wettelijke verplichting;
- het vrijwaren van een vitaal belang van de betrokkene;
- de goede vervulling van een publiekrechtelijke taak;
- het behartigen van een gerechtvaardigd belang van de verantwoordelijke of derde aan wie de gegevens worden verstrekt.

[15] Artikel 2 lid 1 Wbp.
[16] Artikel 1 sub b Wbp; zie ook Kranenborg & Verhey 2011, p. 65.
[17] De begrippen genoemd in deze paragraaf zijn ter verduidelijking opgenomen in de begrippenlijst.
[18] Artikel 15 Wbp.
[19] Artikel 6 Wbp.
[20] Artikel 7 Wbp; zie ook Kranenborg & Verhey 2011, p. 93.
[21] Artikel 9 Wbp.
[22] Artikel 11 Wbp.
[23] Artikel 10 Wbp.
[24] Artikel 13 Wbp.
[25] Artikel 8 Wbp.

De verwerking van bijzondere persoonsgegevens, bijvoorbeeld gegevens over ras of het burgerservicenummer (hierna: BSN), is enkel bij uitzondering toegestaan.[26] Ras is een breed begrip en omvat ook huidskleur, afkomst en nationale of etnische afstamming. Een foto van een persoon op een identiteitsbewijs wordt ook als rasgegeven gezien.[27] Een gegeven over ras mag alleen verwerkt worden met het oog op identificatie en slechts voor zover dit voor dit doel onvermijdelijk is.[28] Het BSN mag enkel verwerkt worden indien dit wettelijk is geregeld.[29] Tenslotte mogen degenen die handelen onder het gezag van de verantwoordelijke de persoonsgegevens alleen in opdracht van de verantwoordelijke verwerken. Daarbij geldt een geheimhoudingsplicht, voor zover deze niet reeds geldt op basis van ambt, beroep of wettelijk voorschrift.[30]

§ 2.3 Meldplicht bij verwerking

Wanneer er persoonsgegevens worden verwerkt, moet de verantwoordelijke dit in principe melden aan de AP. De melding omvat gegevens zoals de naam en het adres van de verantwoordelijke, het doel van de verwerking en een beschrijving van de gegevens die worden verwerkt. Ook moet er vermeld worden van welke categorieën betrokkenen er gegevens worden verwerkt, of deze gegevens buiten de EU worden gebracht en in hoeverre er beveiligingsmaatregelen zijn genomen.[31] Deze melding aan de AP is verplicht, tenzij de verantwoordelijke een beroep kan doen op een vrijstelling.

§ 2.3.1 Vrijstelling meldplicht verwerking

Het Vrijstellingsbesluit Wbp stelt bepaalde verwerkingen van persoonsgegevens vrij van melding aan de AP.[32] Dit moet ervoor zorgen dat meldingen van verwerkingen waarvan het nodig is dat deze in kaart worden gebracht, niet worden bedolven onder meldingen van verwerkingen die overduidelijk nodig zijn.[33] Per vrijstelling wordt vastgesteld voor welke doeleinden de verwerking mag plaatsvinden, welke gegevens er van welke partijen verwerkt mogen worden, aan wie deze verstrekt mogen worden en hoe lang deze bewaard mogen worden. De verwerking van persoonsgegevens die buiten deze grenzen valt, moet aan de AP gemeld worden.

Er bestaat een vrijstelling voor juridische en financiële dienstverleners, die op de dossiervorming en de daaraan verbonden kaartsystemen van notarissen, advocaten en andere rechtshulpverleners ziet.[34] Hieraan zijn verschillende eisen verbonden. Zo mogen de gegevens voor een beperkt aantal doelen verwerkt worden, waarbij juridische of financiële dienstverlening en advisering de belangrijkste is. Hieronder vallen allerlei juridische handelingen, zoals dossiervorming en het opstellen van akten. Ook wordt gespecificeerd welke gegevens onder de vrijstelling vallen, zoals de naam, het adres, het bankrekeningnummer en de contactgegevens van de cliënt, de wederpartij en derden. Gegevens vereist voor de behandeling van de zaak vallen ook onder de vrijstelling. De persoonsgegevens mogen alleen worden verstrekt aan degenen die belast zijn of leiding geven aan het doel van de verwerking. Alleen in specifieke gevallen mogen de gegevens ook aan anderen verstrekt worden. Daarbij moeten geheimhoudingsplichten in acht worden genomen.[35] Tenslotte moeten de persoonsgegevens na twee jaar verwijderd

[26] Artikel 16 Wbp.
[27] *Kamerstukken II* 1997/98, 25892, 3, p. 104-105.
[28] Artikel 18 Wbp.
[29] Artikel 24 lid 1 Wbp.
[30] Artikel 12 Wbp.
[31] Artikel 27 Wbp jo. artikel 28 Wbp.
[32] Artikel 29 Wbp.
[33] *Kamerstukken II* 1997/98, 25892, 3, p. 140.
[34] Artikel 15 Vrijstellingsbesluit Wbp.
[35] Besluit van 7 mei 2001, houdende aanwijzing van verwerkingen van persoonsgegevens die zijn vrijgesteld van de melding bedoeld in artikel 27 van de Wet bescherming persoonsgegevens (Vrijstellingsbesluit Wbp), *Stb.* 2001, 250, p. 61-62.

worden, behoudens een bewaartermijn op basis van beroepsregels of een wettelijke bewaarplicht. Paragraaf 2.5 gaat verder op de bewaartermijn in.

§ 2.4 Informatieplicht

Naast meldplicht aan de AP moet de verantwoordelijke rekening houden met de informatieplicht aan de betrokkene. De verantwoordelijke is verplicht de betrokkene op de hoogte te stellen van de verwerking van persoonsgegevens.[36] Daarbij moet in ieder geval de identiteit van de verantwoordelijke en de verwerkingsdoeleinden kenbaar worden gemaakt. Extra informatie om tegenover de betrokkene een zorgvuldige verwerking te garanderen, wordt indien nodig bijgevoegd. De informatie moet op zodanige wijze worden verstrekt dat de betrokkene er daadwerkelijk beschikking over krijgt. Een algemene verwijzing naar informatie die ergens anders verkrijgbaar is, is dus niet voldoende.[37] De informatieplicht vervalt als de betrokkene reeds op de hoogte is van de vereiste informatie.

Omdat verantwoordelijke en betrokkene vaak ongelijke partijen zijn, bijvoorbeeld een bedrijf en een consument, mag de verantwoordelijke niet zomaar aannemen dat de betrokkene op de hoogte is van de bovenstaande informatie. Het feit dat de betrokkene redelijkerwijs kan weten dat zijn persoonsgegevens worden verwerkt, is onvoldoende grond om aan te nemen dat hij hier daadwerkelijk van op de hoogte is.[38] Het op de hoogte zijn van de betrokkene mag worden aangenomen wanneer de vereiste informatie aan de betrokkene is overhandigd of toegezonden. Ook kunnen bepaalde gedragingen van de betrokkene aanleiding geven tot een gerechtvaardigd vermoeden dat deze op de hoogte is van vereiste informatie. Zo mag een reisbureau er vanuit gaan dat degene die een reis boekt, weet dat er gegevens worden verwerkt om de reis te boeken en dit financieel af te wikkelen. De betrokkene die de verantwoordelijke zelf benadert, is in de meeste gevallen op de hoogte zijn van diens identiteit.[39] In dat geval moet de verantwoordelijke nog wel het concrete doel en eventueel aanvullende informatie meedelen aan de betrokkene.

§ 2.5 Bewaren van persoonsgegevens

Nadat de persoonsgegevens zijn verzameld, worden ze vaak opgeslagen en voor een bepaalde tijd bewaard, wat ook onder verwerken valt. De Wbp zelf geeft geen concrete bewaartermijn. Persoonsgegevens mogen, in een vorm die identificatie van de betrokkene mogelijk maakt, in principe niet langer bewaard worden dan nodig is om het vastgestelde doel van de verzameling of verwerking van de persoonsgegevens te bereiken.[40] Als er bijvoorbeeld persoonsgegevens zijn verwerkt met als doel een overeenkomst te sluiten, mogen deze gegevens na het sluiten van de overeenkomst niet langer bewaard worden. Als er gebruik wordt gemaakt van een vrijstelling voor de meldplicht, behandeld in paragraaf 2.3.1, is de bewaartermijn concreter. De vrijstelling voor juridische en financiële dienstverlening stelt dat persoonsgegevens verwijderd moeten worden nadat de bewaartermijn op grond van toepasselijke gedrags- en beroepsregels is verstreken. Mocht deze ontbreken dan geldt een termijn van uiterlijk twee jaren na beëindiging van de behandeling van de zaak, tenzij de persoonsgegevens op basis van een wettelijke plicht bewaard moeten worden.[41] In geval van een wettelijke bewaarplicht mogen de persoonsgegevens waartoe de bewaarplicht zich uitstrekt niet langer worden bewaard dan dat de plicht vereist.[42]

---

[36] Artikel 33 Wbp jo. artikel 34 Wbp.
[37] Sauerwein & Linnemann 2002, p. 35.
[38] *Kamerstukken II* 1997/98, 25892, 3, p. 150.
[39] *Kamerstukken II* 1997/98, 25892, 3, p. 151.
[40] Artikel 10 lid 1 Wbp.
[41] Artikel 15 lid 5 Vrijstellingsbesluit Wbp.
[42] Besluit van 7 mei 2001, houdende aanwijzing van verwerkingen van persoonsgegevens die zijn vrijgesteld van de melding bedoeld in artikel 27 van de Wet bescherming persoonsgegevens (Vrijstellingsbesluit Wbp), *Stb.* 2001, 250, p. 50.

§ 2.5.1 De notaris en de bewaartermijn uit de Wbp

Omdat de werkzaamheden van een notaris onder juridische en financiële dienstverlening vallen, kan hij gebruik maken van de vrijstelling voor het melden van de verwerking van persoonsgegevens aan de AP.[43] Daarmee is de notaris gebonden aan de verschillende eisen uit deze vrijstelling, waaronder de concretere bewaartermijn van uiterlijk twee jaren na beëindiging van de behandeling van de zaak, behoudens gedrags- of beroepsregels of een bewaarplicht. Voor notarissen is er in gedrags- of beroepsregels geen bewaartermijn vastgesteld, maar zij zijn wel gebonden aan verschillende bewaarplichten. Zo moet de notaris op basis van de Wet ter voorkoming van witwassen en financiering van terrorisme (hierna: Wwft) een cliëntenonderzoek uitvoeren, waarbij de identiteit van de cliënten wordt vastgesteld en geverifieerd.[44] Daarbij moet er ofwel een kopie van een identiteitsbewijs met een persoonsidentificerend nummer (zoals het BSN), ofwel de naam, geboortedatum en het adres van de cliënt worden geregistreerd. Ook moeten de aard, het nummer, de datum en plaats van uitgifte van het identiteitsbewijs en de aard van de dienstverlening worden vastgelegd. Deze gegevens moeten tot vijf jaar na het uitvoeren van de transactie, bijvoorbeeld de overdracht van een woning, worden bewaard.[45] Daarnaast moet de notaris de facturen die hij aan cliënten verstuurd voor de verrichte werkzaamheden, met daarop adres- en financiële gegevens, op basis van de Algemene wet inzake rijksbelastingen (hierna: Awr) zeven jaar bewaren.[46]

Ten aanzien van het notarieel protocol, bestaande uit de originele notariële akten, notariële verklaringen, registers, afschriften, repertoria en de kaartsystemen van de notaris geldt er een eeuwige bewaarplicht.[47] In het repertorium worden dagelijks de door de notaris gepasseerde akten digitaal ingeschreven.[48] De kaartsystemen, met daarin gegevens over cliënten en verwijzingen naar zaken met betrekking tot de cliënt, zijn vandaag de dag voornamelijk digitaal. De notaris is verplicht zijn protocol ordelijk en op een tegen brand en andere gevaren beveiligde plaats te bewaren. Het protocol mag alleen in uitzonderlijke gevallen uit handen worden gegeven, bijvoorbeeld wanneer de notaris defungeert of overlijdt.[49] In dat geval wordt het protocol en eventueel de overige notariële bescheiden overgedragen aan een andere notaris. Afhankelijk van de 'leeftijd' van delen van het protocol, moeten deze naar archiefbewaarplaatsen worden gebracht.[50]

De eeuwige bewaarplicht van de notaris is strikt begrensd tot het protocol, zo blijkt uit een uitspraak van het Gerechtshof Amsterdam uit 2014.[51] Het Hof stelt in rechtsoverweging 5.8 vast dat de bewaarplicht alleen geldt voor het notarieel protocol, niet voor overige notariële bescheiden. Overige notariële bescheiden zijn stukken die samen met het protocol moeten worden overgedragen, zoals kopieën van successiememories, kladrepertoria en de notariële (kantoor)boekhouding.[52] Uit de Wna en daarop gebaseerde regelgeving vloeit geen verplichting voort om naast het protocol andere geschriften met betrekking tot de werkzaamheden van een notaris te bewaren. De overige notariële bescheiden moeten wel worden overgedragen, indien en voor zover deze nog voorhanden zijn. Daarbij moet worden opgemerkt dat in het geval er een notariële akte is opgesteld, de notaris ook rekening moet houden met de Archiefwet (hierna: AW). De notaris wordt in onder de AW als overheidsorgaan gezien.[53] Op basis van een selectielijst geldt dat bescheiden, die uit het voorbereiden en afhandelen van authentieke akten zijn

[43] Artikel 15 Vrijstellingsbesluit Wbp.
[44] Artikel 1 sub a onder 12 Wwft jo. artikel 3 Wwft.
[45] Artikel 33 lid 1 Wwft jo. artikel 33 lid 4 Wwft.
[46] Artikel 52 lid 4 Awr.
[47] Artikel 12 Wna jo. artikel 1 onder f Wna jo. artikel 1 onder d Wna.
[48] Artikel 7 Registratiewet 1970.
[49] Artikel 15 Wna.
[50] Artikel 58 Wna jo. artikel 59 Wna.
[51] Hof Amsterdam 1 april 2014, ECLI:NL:GHAMS:2014:972.
[52] Artikel 15 lid 1 Wna; zie ook *Kamerstukken II* 1993/94, 23706, 3, p. 23.
[53] Artikel 1 sub b AW; zie ook Van der Woude & Sleeking, *WPNR* 2015/7073, p. 716.

voortgekomen, pas na 20 jaar vernietigd mogen worden. In geval van milieuzaken is dit 30 jaar.[54] Deze bescheiden kunnen ook persoonsgegevens bevatten.

Er kan zich een situatie voordoen waarin de notaris bepaalde bescheiden met daarin persoonsgegevens langer wil bewaren dan een bewaarplicht of het Vrijstellingsbesluit Wbp voorschrijft. Het op basis van deze bescheiden verifieerbaar houden van de notariële werkzaamheden kan hiervoor een reden zijn, helemaal nu de verjaringstermijn in het notarieel tuchtrecht wordt versoepeld.[55] De notaris draagt namelijk een exclusieve zorg en verantwoordelijkheid voor zijn protocol, die zonder overige notariële bescheiden niet kan worden gedragen.[56] De notaris kan bepaalde bescheiden nodig hebben om verantwoording af te kunnen leggen over zijn handelen en zich tegen eventuele klachten of aanspraken te kunnen verweren.[57] Bij overschrijding van de termijn die het Vrijstellingsbesluit Wbp of een bewaarplicht voorschrijft, wordt er niet voldaan aan alle eisen van de vrijstelling voor juridische en financiële dienstverlening en moet de verwerking alsnog gemeld worden aan de AP.

§ 2.6 Rechten van betrokkene

Wanneer er van een betrokkene persoonsgegevens worden verwerkt, heeft deze het recht op inzage, correctie en verzet.[58] Dit houdt in dat de betrokkene het recht heeft te weten of er van hem persoonsgegevens worden verwerkt en zo ja, op verbetering, aanvulling, verwijdering of afscherming van deze gegevens wanneer ze bijvoorbeeld feitelijk onjuist blijken te zijn. Ook kan de betrokkene zich in bepaalde gevallen tegen verwerking verzetten. Een situatie waarin de betrokkene zich op zijn rechten beroept, zal zich bij de notaris niet vaak voordoen. De verwerking door de notaris geschiedt namelijk op basis van toestemming van de betrokkene of omdat de betrokkene partij is bij een overeenkomst, waardoor de betrokkene van de verwerking afweet. Daarbij is de notaris gehouden tot de grootst mogelijke zorgvuldigheid bij het uitvoeren van zijn taak en is hij in bepaalde gevallen gebonden aan een bewaartermijn (zie paragraaf 2.5.1).[59] In die gevallen verwerkt de notaris de persoonsgegevens op basis van een wettelijke verplichting en zal hij bijvoorbeeld niet in kunnen gaan op een verzoek tot verwijdering van persoonsgegevens. Om deze redenen zal dit onderzoek niet dieper ingaan op de rechten van betrokkenen.

§ 2.7 Beveiliging van persoonsgegevens

De verantwoordelijke is verplicht passende technische en organisatorische maatregelen te nemen tegen verlies of enige vorm van onrechtmatige verwerking van persoonsgegevens. Hierbij wordt rekening gehouden met de stand van de techniek en de uitvoeringskosten, om zo een passend beveiligingsniveau te garanderen.[60] Aan het begrip passend beveiligingsniveau kunnen geen vaste maatregelen worden gekoppeld. De te nemen maatregelen moeten worden afgestemd op de risico's die de onrechtmatige verwerking en de aard van de te beschermen gegevens met zich meebrengen.[61] Naarmate de persoonsgegevens gevoeliger van aard zijn, of gezien hun context waarin zij gebruikt worden een groter risico voor de persoonlijke levenssfeer van betrokkene

[54] Artikel 5 AW; zie ook Vaststelling selectielijst neerslag handelingen Koninklijke Notariële Beroepsorganisatie beleidsterrein Notariaat periode na 1975 van 9 augustus 2005, *Stcrt*. 2005, 212.
[55] F. de Smeth, 'Notarissen opgepast: de verjaringstermijn voor tuchtklachten wordt versoepeld', *Boekel* 22 februari 2016, Boekel.co.uk. De huidige driejaarstermijn blijft van kracht, maar indien het klachtwaardige handelen pas ná die termijn wordt ontdekt (en redelijkerwijs niet eerder had kunnen worden ontdekt), kan binnen één jaar na ontdekking alsnog een klacht worden ingediend.
[56] Spanjaart, *Notariaat Magazine* 2016, editie 6, p. 27.
[57] Van der Woude & Sleeking, *WPNR* 2015/7073, p. 715.
[58] Artikel 35 Wbp jo. artikel 36 Wbp jo. artikel 40 Wbp.
[59] Artikel 17 Wna.
[60] Artikel 13 Wbp.
[61] *Kamerstukken II* 1999/00, 25892, 92c, p. 15.

vormen, moeten er zwaardere eisen aan de beveiliging worden gesteld.[62] Met de ontwikkelende techniek moet er periodiek een nieuwe afweging worden gemaakt over het beveiligingsniveau. Daarom adviseert de AP het gebruik van een plan-do-check-act cyclus in de dagelijkse praktijk.[63] De verwerkingsrisico's moeten worden vastgesteld en op basis daarvan kunnen er gericht beveiligingsmaatregelen worden getroffen.

Bij de beoordeling van de beveiliging van persoonsgegevens neemt de AP verschillende beveiligingsmaatregelen die in veel gevallen noodzakelijk zijn als uitgangspunt.[64] De AP noemt onder andere het hanteren van een op bestuurlijk niveau goedgekeurd beleidsdocument voor informatiebeveiliging waar alle medewerkers van op de hoogte zijn, het creëren van beveiligingsbewustzijn door middel van training en het loggen en controleren van activiteiten met betrekking tot persoonsgegevens. Andere voorbeelden zijn het gebruik van encryptie, alsmede procedures om toegang tot informatiesystemen te verlenen en onbevoegde toegang te voorkomen. Continuïteitsbeheer wordt genoemd, waarbij er voor gezorgd wordt dat persoonsgegevens niet verloren gaan, ondanks bijvoorbeeld uitval van apparatuur. Ook de fysieke beveiliging van IT-voorzieningen en juiste afhandeling van datalekken zijn van belang. Met betrekking tot persoonsgegevens op papier noemt de AP het gebruik van afgesloten dossierkasten en papierversnipperaars of afsluitbare containers, waarvan de inhoud vernietigd wordt door een gespecialiseerd bedrijf.[65] Er moet regelmatig worden geëvalueerd of de maatregelen leiden tot een passend beveiligingsniveau, waarna er indien nodig verdere maatregelen moeten worden doorgevoerd.

§ 2.8 De bewerker

In de praktijk komt het vaak voor dat niet alleen de verantwoordelijke, maar ook een bewerker persoonsgegevens verwerkt. Een bewerker verwerkt persoonsgegevens voor de verantwoordelijke maar valt niet onder zijn rechtstreeks gezag.[66] De verantwoordelijke blijft echter verantwoordelijk voor de verwerking en moet bij het inschakelen van een bewerker verschillende afspraken maken.[67] Ten eerste moet hij ervoor zorgen dat de bewerker alleen in opdracht van de verantwoordelijke persoonsgegevens verwerkt.[68] Daarbij is de bewerker en iedereen die onder zijn gezag handelt tot geheimhouding verplicht, voor zover er al geen geheimhoudingsplicht geldt op basis van ambt, beroep of wettelijk voorschrift. De verantwoordelijke moet ook zorgen dat de bewerker een passend beveiligingsniveau hanteert ten aanzien van de persoonsgegevens die hij gaat verwerken (zie paragraaf 2.7).[69] Tenslotte zorgt de verantwoordelijke ervoor dat de bewerker maatregelen treft ten aanzien van het melden van een datalek, behandeld in paragraaf 2.9, zodat de verantwoordelijke aan zijn meldplicht datalekken kan voldoen.[70] In veel gevallen zal de bewerker namelijk als eerste op de hoogte zijn van een datalek en moet hij verantwoordelijke op tijd en adequaat hierover informeren.[71] De verantwoordelijke moet erop toezien dat de genomen maatregelen met betrekking tot het beveiligingsniveau en de meldplicht datalekken worden nageleefd. Onvoldoende transparantie over de beveiliging en beveiligingsincidenten vanuit de bewerker kan ertoe leiden dat de verantwoordelijke niet voldoet aan zijn plicht om te zorgen voor een passend beveiligingsniveau.[72]

[62] Beveiliging van persoonsgegevens 2013, p. 10.
[63] Beveiliging van persoonsgegevens 2013, p. 2.
[64] Beveiliging van persoonsgegevens 2013, p. 22-24.
[65] Beveiliging van persoonsgegevens 2013, p. 27.
[66] Artikel 1 onder e Wbp.
[67] Artikel 14 Wbp.
[68] Artikel 14 lid 3 sub a Wbp jo. artikel 12 Wbp.
[69] Artikel 14 lid 3 sub b Wbp jo. artikel 13 Wbp.
[70] Artikel 14 lid 3 sub c Wbp.
[71] Beleidsregels voor toepassing van artikel 34a van de Wbp 2015, p. 16.
[72] Beveiliging van persoonsgegevens 2013, p. 30.

§ 2.8.1 De bewerkersovereenkomst

De uitvoering van de verwerking door een bewerker moet geregeld worden in een overeenkomst of op basis van een andere rechtshandeling waardoor er een verbintenis tussen de verantwoordelijke en de bewerker ontstaat. Daarnaast moeten de afspraken over de bescherming van de persoonsgegevens, beveiligingsmaatregelen en het naleven van de meldplicht datalekken schriftelijk of in een andere, gelijkwaardige vorm worden vastgelegd.[73] In de praktijk resulteert dit in een bewerkersovereenkomst die tussen verantwoordelijke en bewerker wordt gesloten. Deze overeenkomst moet gericht zijn op de gegevensverwerking en mag niet betrekking hebben op een vorm van dienstverlening waar de verwerking uit voortvloeit.[74] De bewerkersovereenkomst dient dus een losse overeenkomst te zijn, niet slechts een onderdeel van bijvoorbeeld een overeenkomst tot dienstverlening.

De AP heeft in een persbericht bevestigd dat er een aparte bewerkersovereenkomst moet zijn.[75] Als aanvulling op de eisen uit de Wbp wordt aangegeven dat de verplichtingen over en weer duidelijk in de overeenkomst moeten zijn vastgelegd, waarbij informatie zoals de soort gegevens, de verwerkingsdoeleinden, de duur van de opslag en genomen beveiligingsmaatregelen moet worden opgenomen. Ook moet er een geheimhoudingsplicht voor de bewerker worden opgenomen en moet worden vastgelegd hoe de verantwoordelijke gaat toezien op de naleving van de getroffen maatregelen gericht op beveiliging en datalekken. Wanneer er sprake is van sub-bewerkerschap, de situatie waarin de bewerker een andere bewerker inschakelt, moeten bepalingen daarover worden opgenomen. Tenslotte adviseert de AP verschillende concrete afspraken te maken over de meldplicht datalekken, bijvoorbeeld over de manier waarop en wanneer de verantwoordelijke over een datalek wordt ingelicht en welke partij hiervan melding maakt.[76] Deze eisen zijn schematisch opgenomen in een checklist, in bijlage A.

§ 2.9 Meldplicht datalekken

Naar aanleiding van een groot aantal incidenten waarbij er persoonsgegevens vrijkwamen als gevolg van een inbreuk op de beveiliging is in 2013 het wetsvoorstel meldplicht datalekken ingediend. Met dit wetsvoorstel werd vooruitgelopen op de AVG, die zich destijds in de conceptfase bevond.[77] Op 26 mei 2015 is het voorstel aangenomen door de Eerste Kamer en op 1 januari 2016 is de Meldplicht Datalekken in werking getreden en opgenomen in de Wbp.

§ 2.9.1 Definitie datalek

Een datalek doet zich voor wanneer er bij een inbreuk op de beveiliging persoonsgegevens verloren zijn gegaan, of niet redelijkerwijs kan worden uitgesloten dat persoonsgegevens onrechtmatig zijn verwerkt. Onder onrechtmatige verwerking vallen aantasting, onbevoegde kennisneming, wijziging, of verstrekking van persoonsgegevens.[78] Hierbij zijn verschillende situaties denkbaar, waarin er bijvoorbeeld een database met persoonsgegevens (waar geen actuele back-up van beschikbaar) wordt vernietigd of versleuteld door een hacker die zegt de gegevens tegen betaling te zullen ontsleutelen.[79] Ook meer eenvoudige situaties, zoals iemand die een USB-stick verliest of documenten met persoonsgegevens die bij het oud papier worden gezet, worden aangemerkt als datalek.

---

[73] Artikel 14 lid 2 Wbp jo artikel 14 lid 5 Wbp.
[74] *Kamerstukken II* 1997/98, 25892, 3, p. 99.
[75] 'AP eist betere afspraken over digitaliseren patiëntdossiers', *Autoriteit Persoonsgegevens* 17 mei 2016, Autoriteitpersoonsgegevens.nl.
[76] Beleidsregels voor toepassing van artikel 34a van de Wbp 2015, p. 16-17.
[77] *Kamerstukken II* 2012/13, 33662, 3, p. 3.
[78] Beleidsregels voor toepassing van artikel 34a van de Wbp 2015, p. 19-21.
[79] Aan de Stegge, *Notariaat Magazine* 2016, editie 5, p. 26.

§ 2.9.2 Melding aan de AP

Het datalek moet gemeld worden aan de AP wanneer het leidt tot (de aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van persoonsgegevens.[80] Om dit vast te stellen wordt er gekeken naar de aard van de persoonsgegevens en de aard en omvang van de inbreuk.[81] Als er persoonsgegevens van gevoelige aard zijn gelekt, moet er standaard melding van worden gemaakt bij de AP. Dit zijn persoonsgegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene, financiële schade, gezondheidsschade of (identiteits)fraude. Hieronder vallen in ieder geval bijzondere persoonsgegevens, zoals besproken in paragraaf 2.2. Ook informatie over de financiële of economische situatie van de betrokkene, bijvoorbeeld over (problematische) schulden, is van gevoelige aard. Bij gegevens die kunnen leiden tot (identiteits)fraude kan gedacht worden aan het BSN of kopieën van identiteitsbewijzen. Tenslotte worden ook persoonsgegevens die onder een bijzondere, wettelijk bepaalde geheimhoudingsplicht of beroepsgeheim vallen als gevoelig aangemerkt.[82]

Wanneer de gelekte persoonsgegevens niet van gevoelige aard zijn, kunnen de aard en omvang van het datalek toch reden zijn tot melding aan de AP. Dit is weer afhankelijk van de omvang van de verwerking, de beslissingen die normaal op basis van de persoonsgegevens worden genomen en of de persoonsgegevens in een keten worden gedeeld.[83] De omvang van de verwerking kan de persoonsgegevens interessant maken voor het criminele circuit. Daarnaast wordt de impact van het datalek groter naarmate de beslissingen die op basis van de gelekte persoonsgegevens gemaakt worden ingrijpender zijn. Als persoonsgegevens tenslotte in een keten met veel partijen worden gedeeld, zoals bij de overheid, kunnen gevolgen van een datalek in de gehele keten optreden. Dit maakt het voor de betrokkene lastiger om deze gevolgen te overzien. Als aan de hand van deze drie factoren alsnog wordt vastgesteld dat er sprake is van (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van persoonsgegevens, moet het datalek aan de AP gemeld worden.

§ 2.9.2.1 Inhoud melding aan de AP

In de melding aan de AP moet in ieder geval de aard van de inbreuk zijn opgenomen, samen met de instanties waar meer informatie over het datalek kan worden verkregen en de aanbevolen maatregelen om de negatieve gevolgen van de inbreuk te beperken.[84] Een algemene omschrijving van de inbreuk zal vaak volstaan. Zo noemt het webformulier, waarmee de melding aan de AP kan worden gedaan, onder andere persoonsgegevens bij het oud papier zetten en versturen aan de verkeerde ontvanger.[85] Ook moeten de geconstateerde en vermoedelijke gevolgen van de inbreuk voor de verwerking van persoonsgegevens worden beschreven en de verantwoordelijke moet aangeven welke maatregelen hij wil treffen of heeft getroffen om deze gevolgen te verhelpen.[86]

§ 2.9.3 Melding aan de betrokkene

Het datalek moet ook aan de betrokkene worden gemeld wanneer het waarschijnlijk ongunstige gevolgen zal hebben voor zijn persoonlijke levenssfeer, zoals identiteitsfraude.[87] Als er persoonsgegevens van gevoelige aard zijn gelekt, moet er vanuit worden gegaan dat het datalek waarschijnlijk ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van de betrokkene en moet het datalek aan hem gemeld

[80] Artikel 34a lid 1 Wbp.
[81] Beleidsregels voor toepassing van artikel 34a van de Wbp 2015, p. 24.
[82] Beleidsregels voor toepassing van artikel 34a van de Wbp 2015, p. 26-27.
[83] Beleidsregels voor toepassing van artikel 34a van de Wbp 2015, p. 27-28.
[84] Artikel 34a lid 3 Wbp.
[85] *Kamerstukken II* 2012/13, 33662, 3, p. 21; zie ook Autoriteit Persoonsgegevens, *'Een nieuwe melding doen'*, datalekken.autoriteitpersoonsgegevens.nl
[86] Artikel 34a lid 4 Wbp.
[87] Artikel 34a lid 2 Wbp.

worden. In alle andere situaties dient de verantwoordelijke een afweging te maken op basis van de omstandigheden van het geval.[88]

In bepaalde situaties kan van deze melding worden afgezien. Als de gelekte persoonsgegevens door encryptie of andere technische beschermingsmaatregelen onbegrijpelijk of ontoegankelijk zijn voor degenen die geen recht hebben hiervan kennis te nemen, kan de melding achterwege worden gelaten.[89] Voorbeelden van andere technische beschermingsmaatregelen zijn het op afstand wissen van gegevensdragers of pseudonimiseren van persoonsgegevens.[90] Als de beveiligingsmaatregelen tekort schieten, kan er alsnog van melding worden afgezien wanneer het onwaarschijnlijk is dat de inbreuk ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van de betrokkene. Dit is aan de verantwoordelijke om te bepalen, met uitzondering van de gevallen waarin er persoonsgegevens van gevoelige aard zijn gelekt. In die gevallen moet, zoals eerder vermeld, worden aangenomen dat ongunstige gevolgen voor de persoonlijke levenssfeer zich zullen voordoen. Als de beschermingsmaatregelen tekort schieten én het datalek waarschijnlijk ongunstige gevolgen voor de betrokkene zal hebben, resteren enkel zwaarwegende redenen om de betrokkene niet te informeren, zoals staatsveiligheid en vervolging van strafbare feiten.[91]

Bij de melding van het datalek aan de AP wordt ook aangegeven of er melding zal worden gemaakt aan de betrokkene. Als de verantwoordelijke op basis van de beveiligingsmaatregelen, de waarschijnlijkheid van ongunstige gevolgen of zwaarwegende redenen besluit om geen melding te maken aan de betrokkene, kan de AP dit alsnog opleggen. De AP zal deze melding verplichten wanneer zij meent dat het datalek waarschijnlijk ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van de betrokkene.[92]

§ 2.9.3.1 Inhoud melding aan de betrokkene

De betrokkene moet net als de AP op de hoogte worden gebracht van de aard van de inbreuk, de instanties met meer informatie over het datalek en de aanbevolen maatregelen om negatieve gevolgen te beperken.[93] De betrokkene kan zo vragen stellen aan de betrokkene en zelf stappen zetten om negatieve gevolgen te voorkomen. De melding aan betrokkene moet voor een behoorlijke en zorgvuldige informatievoorziening zorgen. Hierbij moet rekening worden gehouden met de aard van de inbreuk, de geconstateerde en feitelijke gevolgen daarvan voor de verwerking van persoonsgegevens, de kring van betrokkenen en uitvoeringskosten. Vaak volstaat het individueel informeren van betrokkenen, maar bij grotere datalekken kan er gekozen worden voor een combinatie van algemene voorlichting en individueel contact.[94]

§ 2.9.4 Onverwijld

Zowel de melding aan de AP als de betrokkene dient onverwijld te geschieden.[95] Wat onverwijld is, hangt af van de omstandigheden van het geval.[96] De AP heeft het begrip onverwijld verder geconcretiseerd, gebaseerd op de conceptversie van de Algemene Verordening Gegevensbescherming.[97] De verantwoordelijke moet een datalek zonder onnodige vertraging en zo mogelijk niet later dan 72 uur na ontdekking melden aan de AP. Als binnen 72 uur niet alle informatie is verzameld, moet er melding worden gemaakt

[88] Beleidsregels voor toepassing van artikel 34a van de Wbp 2015, p. 39.
[89] Artikel 34a lid 6 Wbp.
[90] Beleidsregels voor toepassing van artikel 34a van de Wbp 2015, p. 38-39.
[91] Artikel 43 Wbp.
[92] Artikel 34a lid 7 Wbp.
[93] Artikel 34a lid 3 Wbp.
[94] Beleidsregels voor toepassing van artikel 34a van de Wbp 2015, p. 43.
[95] Artikel 34a lid 1 Wbp jo. artikel 34a lid 2 Wbp.
[96] *Kamerstukken II* 2012/13, 33662, 6, p. 16.
[97] Beleidsregels voor toepassing van artikel 34a van de Wbp 2015, p. 31.

op basis van de gegevens waarover de verantwoordelijke op dat moment beschikt. Een verlate melding moet worden gemotiveerd. Voor de melding aan de betrokkene geldt enkel de eis dat deze onverwijld moet geschieden, zonder de concrete grens van 72 uur. Er mag enige tijd worden genomen voor verder onderzoek zodat de betrokkene behoorlijk en zorgvuldig wordt geïnformeerd. Daarbij moet rekening worden gehouden met de maatregelen die de betrokkene mogelijk zelf moet nemen. Hoe eerder de betrokkene op de hoogte is van het datalek, hoe eerder hij hierop actie kan ondernemen.[98]

§ 2.9.5 Registratie datalek

Als het datalek aan de AP gemeld moet worden, moet het ook geregistreerd worden.[99] Daarbij moeten in ieder geval de feiten en gegevens over de aard van de inbreuk worden vastgelegd. Als de betrokkene wordt geïnformeerd, moet de tekst van de kennisgeving worden opgenomen. De AP geeft aan dat de registratie van het datalek minimaal één jaar bewaard moet worden, gerekend vanaf de laatste melding die aan betrokkene is gedaan. Als het datalek niet aan de betrokkene wordt gemeld op basis van zwaarwegende redenen of omdat de verantwoordelijke heeft geoordeeld dat de beschermingsmaatregelen voldoende bescherming bieden, wordt de termijn verlengd naar minimaal drie jaar. Er moet dan minimaal jaarlijks geëvalueerd worden of het datalek alsnog aan de betrokkene moet worden gemeld.[100] Dit kan nodig zijn wanneer er bijvoorbeeld nieuwe kwetsbaarheden worden ontdekt in de gebruikte encryptie.

§ 2.10 Sancties

Met de invoering van de Meldplicht Datalekken werd tevens de boetebevoegdheid van de AP uitgebreid. Daarvoor kon de AP, naast een last onder bestuursdwang en een last onder dwangsom[101], een bestuurlijke boete van slechts €4500 opleggen voor het niet voldoen aan de meldplicht van verwerking van persoonsgegevens. Sinds 1 januari 2016 kan de AP in meer gevallen boetes opleggen, die daarnaast hoger kunnen uitvallen. De maximaal mogelijke hoogte van een boete opgelegd door de AP op grond van de Wbp is €820.000 of 10% van de jaaromzet van de rechtspersoon, mocht de €820.000 geen passende straf zijn.[102] Voordat de AP boetes oplegt, zal er in de meeste gevallen een bindende aanwijzing aan de verantwoordelijke worden opgelegd.[103] Daarmee krijgt de verantwoordelijke de kans om de overtreding te herstellen. Als deze aanwijzing niet wordt opgevolgd kan de AP alsnog overgaan tot het opleggen van boetes. Als de overtreding opzettelijk is gepleegd of het gevolg is van ernstige verwijtbare nalatigheid zal de AP direct een boete opleggen.[104]

De hoogte van de boete wordt vastgesteld aan de hand van Boetebeleidsregels Autoriteit Persoonsgegevens 2016. Hierin zijn drie boetemaxima vastgelegd, die vervolgens elk zijn opgedeeld in drie categorieën met minimum- en maximumbedragen. In de bijlagen van de boetebeleidsregels is opgenomen onder welk boetemaximum en welke categorie een overtreding valt. Zo valt bijvoorbeeld het in strijd handelen met de wettelijke bewaartermijn of de informatieplicht onder de tweede categorie van het boetemaximum van €820.000.[105] In dat geval zal de AP een basisboete tussen de €120.000 en €500.000 vaststellen, waarna het boetebedrag op basis van factoren zoals de duur van de overtreding en de mate van verwijtbaarheid naar boven of naar beneden wordt bijgesteld.[106] Als de voorgeschreven boetecategorie geen passende straf biedt, dan kan de AP een categorie

[98] Beleidsregels voor toepassing van artikel 34a van de Wbp 2015, p. 45.
[99] Artikel 34a lid 8 Wbp.
[100] Beleidsregels voor toepassing van artikel 34a van de Wbp 2015, p. 46.
[101] Artikel 65 Wbp jo. artikel 5:32 lid 1 Awb.
[102] Artikel 66 lid 2 Wbp jo. artikel 23 lid 3 Sr. jo. artikel 23 lid 7 Sr.
[103] Artikel 66 lid 3 Wbp jo. artikel 1 sub q Wbp jo. artikel 1 sub r Wbp.
[104] Artikel 66 lid 4 Wbp.
[105] Artikel 2 Boetebeleidsregels Autoriteit Persoonsgegevens 2016.
[106] Artikel 5 Boetebeleidsregels Autoriteit Persoonsgegevens 2016 jo. artikel 6 Boetebeleidsregels Autoriteit Persoonsgegevens 2016.

daaronder of daarboven hanteren. Als de hoogste boetecategorie is voorgeschreven maar deze niet volstaat, kan er een boete worden opgelegd van maximaal 10% van de jaaromzet van de overtreder.[107] Bij het vaststellen van het uiteindelijke boetebedrag houdt de AP ook nog rekening met boeteverhogende en boeteverlagende omstandigheden, zoals het belemmeren van het onderzoek van de AP of het schadeloos stellen van degene die door de overtreding schade lijdt.

[107] Artikel 7 Boetebeleidsregels Autoriteit Persoonsgegevens 2016 jo. artikel 23 lid 7 Sr.

Hoofdstuk 3: Het huidige beleid en de huidige werkwijze van DKT

In dit hoofdstuk wordt beschreven wat voor beleid en welke werkwijze DKT hanteert met betrekking tot de omgang met persoonsgegevens van cliënten. Het op schrift gestelde beleid en de werkwijze in de praktijk worden geanalyseerd om dit uiteindelijke te kunnen toetsen aan het huidig en toekomstig juridisch kader. Eerst worden de fases die persoonsgegevens van de cliënten doorlopen chronologisch behandeld, waarna andere belangrijke aspecten, zoals beveiliging van persoonsgegevens en de meldplicht datalekken aan bod zullen komen. Het beleid en de werkwijze worden vastgesteld aan de hand van observaties, interviews en de analyse van interne documenten. Vanwege de gevoeligheid van verschillende interne documenten, zoals checklists, documentatie omtrent beveiliging en datalekken, overeenkomsten met externe partijen en het overzicht van alle bewerkers van DKT, zijn deze niet opgenomen in de bijlagen. Deze informatie is toegankelijk op het interne netwerk van DKT.

§ 3.1 Aanvaarding van de opdracht

Het behandelen van een zaak start met de aanvaarding van een opdracht door DKT. Dit gebeurt middels een opdrachtbevestiging, wanneer een cliënt op zijn verzoek gemaakte ontwerpakte of persoonlijk advies in ontvangst neemt of wanneer DKT een koopovereenkomst ontvangt waarin is bepaald dat het kantoor de leveringsakte zal verlijden en hiervoor de benodigde werkzaamheden zijn gestart.[108] Naast cliënten zelf kunnen ook andere partijen opdrachten aanleveren, zoals makelaars of accountants. De opdrachtbevestiging wordt meestal voorafgegaan door een bespreking met een notaris, kandidaat-notaris of notarisklerk.[109] De klanten maken hiervoor een afspraak. In de afspraakbevestiging door het kantoor wordt een indicatie van de kosten gegeven en wordt aangegeven welke gegevens de cliënt dient mee te nemen.[110] Tijdens de bespreking worden er gespreksaantekeningen gemaakt of wordt er een checklist ingevuld. Een checklist is, zoals de naam al suggereert, een lijst waarop precies kan worden aangevinkt en ingevuld wat de wensen van de cliënt zijn omtrent de op te stellen akte. Deze checklists of gespreksaantekeningen bevatten ook uiteenlopende gegevens over de cliënt zelf, zoals informatie over de burgerlijke staat en de financiële situatie. Deze informatie vormt uiteindelijk de basis voor de op te stellen akte. Na afloop van de bespreking tekent de cliënt een opdrachtbevestiging met daarop een omschrijving van de opdracht en wordt de zaak in behandeling genomen.[111] Als een opdracht binnenkomt via een koopovereenkomst wordt de zaak gelijk in behandeling genomen en wordt er een opdrachtbevestiging aan zowel de koper als de verkoper verstuurd.[112] Daarin wordt aangegeven dat DKT overdracht zal behandelen en wordt de cliënt geïnformeerd over de werkzaamheden die zullen worden uitgevoerd. De cliënten worden tevens verzocht om bepaalde informatie aan te leveren.[113] In beide gevallen ontvangt de cliënt een kopie van de algemene voorwaarden.

§ 3.2 Inhoud en verloop van een dossier

Na acceptatie van de opdracht wordt er een dossier aangemaakt aan de hand van een procedurelijst. Elk type zaak heeft een andere procedurelijst, waarop precies staat aangegeven welke werkzaamheden er verricht moeten worden en welke informatie nodig is om het dossier af te wikkelen.[114] In ieder geval wordt er ter identificatie een kopie van het identiteitsbewijs van de betrokken cliënt(en) verzameld. Daarnaast wordt er, afhankelijk van het type zaak, inzage gedaan in verschillende registers, zoals in de BRP,

[108] Zie bijlage K: Algemene voorwaarden DKT.
[109] Zie bijlage C: Interview mr. J.A. Beijsens.
[110] Zie bijlage G: Afspraakbevestiging.
[111] Zie bijlage H: Opdrachtbevestiging.
[112] Zie bijlage I: Opdrachtbevestiging en inlichtingenformulier onroerend goed.
[113] Zie bijlage J: Overzicht gebruikelijke en extra werkzaamheden levering en hypotheek.
[114] Een selectie van procedurelijsten is opgenomen in bijlage L.

het huwelijksgoederenregister, het Centraal Insolventieregister, het Centraal Curatele- en bewindregister, het Kadaster, het handelsregister van de KvK en het Centraal (Levens-)Testamentenregister. Uit deze documenten komen verschillende persoonsgegevens van de cliënt voort, waaronder:

- de naam, het adres en de woonplaats, inclusief oude adressen;
- de geboortedatum en -plaats en de nationaliteit;
- het geslacht;
- het BSN;
- informatie over een huwelijk of geregistreerd partnerschap;
- informatie over mogelijke schuldsanering, ondercuratelestelling of beschermingsbewind;
- informatie over het eigendom van en de hypotheek rustende op onroerend goed;
- informatie over de rechtspersoon waar de cliënt bestuurder is;
- de locatie van een (levens)testament, indien opgesteld.

In de inzage in het BRP staan tevens persoonsgegevens van de partner, ouders en kinderen van degene waarop de inzage betrekking heeft, zoals de naam, het BSN en de geboortedatum- en plaats. Naast inzage in de verschillende registers worden ook andere, voor het dossier relevante documenten en informatie in het dossier opgenomen. Hierbij kan gedacht worden een e-mailadres, maar ook aan het testament van een overleden partij die bij het dossier is betrokken, de koopovereenkomst van het huis dat wordt overgedragen of een hypotheekopdracht voor de hypotheek die op dat huis moet worden gevestigd. Indien nodig wordt ook het bankrekeningnummer van cliënten verzameld. Als er een bespreking heeft plaatsgevonden worden de gespreksaantekeningen of de ingevulde checklist ook in het dossier opgenomen. Ook de opdrachtbevestiging wordt opgenomen. Naarmate de zaak vordert wordt het dossier aangevuld met zaken zoals correspondentie en een nota van afrekening of declaratie.

Nadat de benodigde informatie is verzameld, wordt er een concept-akte opgesteld. Dit concept wordt naar de cliënten gestuurd, via e-mail of via post. Cliënten kunnen aan de hand van het concept vragen stellen en kijken of alles duidelijk is. Vervolgens wordt er een passeerafspraak gemaakt, waar de akte met de notaris wordt doorgenomen en ondertekend. Na deze passeerafspraak zal de notaris indien nodig zorgen voor de verzending van de akte, bijvoorbeeld aan het Kadaster bij de overdracht van onroerend goed of aan de KvK bij de oprichting van een rechtspersoon.

3.3 Digitale en fysieke dossiervoering

Dossiers worden zowel digitaal als fysiek aangemaakt.[115] Digitale dossiers worden aangemaakt met het computerprogramma Assyst, dat automatisch inzage kan doen in bepaalde registers, zoals de BRP, het Kadaster en de KvK. In Assyst wordt een digitaal dossier aangemaakt en hierbij wordt aangegeven wat voor type zaak het betreft en bij welke notaris de akte zal passeren. Gegevens over de cliënten (zoals de naam, het adres, de woonplaats, contactgegevens en gegevens over het identiteitsbewijs) worden opgenomen in cliëntkaarten, die vervolgens aan het digitale dossier worden gekoppeld. Ook andere betrokken partijen, zoals tussenpersonen, hypotheekverstrekkers, accountants of makelaars worden aan het dossier gekoppeld. Wanneer de zaak een registergoed betreft, wordt ook dit gekoppeld aan het dossier.

Naast de digitale dossiervoering wordt er ook een fysiek dossier aangemaakt en bijgehouden. In beginsel bevat dit papieren dossier dezelfde informatie als het digitale dossier. Het wordt verder aangevuld met zaken zoals een afdruk van de digitale cliëntkaart en een voorblad met daarop informatie over partijen, de betrokken notaris en de geplande passeerdatum. Als gegevens op papier worden aangeleverd, worden deze

[115] Zie bijlage E: Observaties aanmaken van dossiers.

gescand en opgeslagen in het digitale dossier. Na het scannen krijgt het papieren document de stempel 'GEARCHIVEERD'. Als er een document wordt geprint dat uiteindelijk onnodig of onjuist blijkt te zijn, komt het terecht in een specifieke bak die geleegd wordt in een afgesloten container van Box. B.V. (zie paragraaf 3.5.1). Het papieren dossier ligt, afhankelijk van de fase waarin het dossier zich bevindt, bij notariële ondersteunende staf of bij een (kandidaat-)notaris.

§ 3.4 Bewaren van dossiers

Nadat de zaak is gepasseerd, krijgt de ondertekende akte een repertoriumnummer en wordt de akte onderdeel van het protocol van de notaris die de akte heeft gepasseerd. Het protocol van de notaris wordt bewaard op de vestiging van DKT waar hij of zij werkzaam is. Dit kan Tilburg Centrum, Tilburg Reeshof, Rijen of Udenhout zijn. De akten komen in een kluis terecht en komen daar in principe niet meer uit. De facturering voor de verrichte werkzaamheden wordt afgehandeld door de administratie, waarna de factuur 7 jaar wordt bewaard. Daarna wordt de factuur vernietigd.[116]

De rest van het papieren dossier wordt aan de hand van een instructie geschoond en gescand.[117] Alle documenten die al in het digitale dossier zijn opgenomen, zoals documenten met de stempel 'GEARCHIVEERD' of een geprinte digitale inzage, worden niet gescand maar kunnen meteen worden vernietigd. De overgebleven inhoud van het dossier wordt dan op volgorde gelegd en gescand naar een enkel PDF bestand. Dit digitale dossier wordt bewaard om de werkzaamheden, bijvoorbeeld de opgestelde akte, op een later moment te kunnen verantwoorden.[118] Stukken gemarkeerd met 'bewaren' worden daarnaast fysiek bewaard, maar in principe wordt het hele dossier gedigitaliseerd en de papieren versie vernietigd. Na het scannen komt de papieren versie in een container van Box B.V. terecht, die deze container ophaalt en de inhoud vernietigd. Deze vorm van digitalisering is relatief nieuw vergeleken met de 'leeftijd' van de dossiers die DKT heeft behandeld. DKT heeft op meerdere vestigingen een archief van papieren dossiers van voordat digitalisering de norm was, dat tientallen jaren teruggaat.[119] Uit inzage in dit archief blijkt dat dossiers in het archief nog persoonsgegevens bevatten, zoals kopieën van identiteitsbewijzen en informatie uit verschillende registers genoemd in paragraaf 3.2. Een gedeelte van het archief staat extern opgeslagen bij BB Diensten. Dit is het archief van Daamen Notarissen, het kantoor dat in 2015 samen met de Kort van Tuijl Notarissen DKT heeft gevormd.

§ 3.5 Beveiliging

Zoals hierboven beschreven verwerkt DKT een grote hoeveelheid aan persoonsgegevens. Het kantoor heeft zowel organisatorische als technische beveiligingsmaatregelen getroffen om de verwerking van persoonsgegevens van cliënten te beschermen.

§ 3.5.1 Organisatorische beveiligingsmaatregelen

Alle vestigingen van het kantoor zijn uitgerust met een beveiligingssysteem en beschikken over een kluis waarin het protocol van de notarissen wordt opgeslagen. Dossiers die in behandeling zijn, liggen op plekken waar geen cliënten komen. De kamers van de notarissen zijn hierop een uitzondering. Naast dat er in die kamers aan dossiers wordt gewerkt, worden er ook besprekingen met cliënten gevoerd. Mocht de notaris de ruimte verlaten, dan hebben medewerkers bij bepaalde ruimtes zicht op de cliënten.[120] Dit is echter niet bij alle ruimtes mogelijk.

[116] Zie bijlage F: Observatie administratie.
[117] Zie bijlage M: Instructie voor het schonen en scannen van dossiers.
[118] Zie bijlage C: Interview mr. J.A. Beijsens.
[119] Zie bijlage D: Interview drs. R. Nijnens.
[120] Zie bijlage C: Interview mr. J.A. Beijsens.

Specifiek gericht op bescherming van papieren persoonsgegevens is het gebruik van een container van Box B.V, een dienstverlener op het gebied van archief- en datavernietiging.[121] Per ongeluk of onjuist afgedrukte documenten met persoonsgegevens worden apart gehouden en komen uiteindelijk in de container van Box B.V. terecht. Hetzelfde geldt voor de papieren versie van een gepasseerd dossier. Elke vestiging van DKT beschikt over een container van Box B.V. De containers wordt met een speciaal ingericht inzamelvoertuig opgehaald, waarna de gegevens binnen 24 uur door speciaal opgeleid personeel onder videobewaking worden vernietigd tot niet te reconstrueren snippers. Box B.V. is ISO 9001:2008 en DIN-32757-1 gecertificeerd. ISO staat voor International Organization for Standardization en DIN staat voor Deutsches Institut für Normung. Dit zijn twee organisaties die zich bezighouden met het vaststellen van standaardnormen. Zo is de hierboven genoemde ISO norm gericht op kwaliteitsmanagement ten aanzien van archiefpapier en de DIN norm op archief- en datavernietiging.

Dossiers die zijn gepasseerd voordat digitalisering hiervan de norm werd, zijn opgeslagen in het archief. Het archief in beheer van DKT is beveiligd met het alarmsysteem van de panden waar dit archief is opgeslagen. Het archief van Daamen Notarissen is opgeslagen bij BB Diensten in Tilburg. Dit archief staat in een met alarm beveiligde loods, in een afgesloten deel dat alleen voor DKT toegankelijk is. De cijfersloten zijn door een notaris van DKT zelf ingesteld, buiten de aanwezigheid van medewerkers van BB Diensten. Er wordt een logboek van bezoekers bijgehouden en er wordt geen toegang tot de ruimte verleend, tenzij een bezoek door DKT is aangekondigd. Als dit iemand anders is dan gebruikelijk, moet deze persoon zich legitimeren.

§ 3.5.2 Technische beveiligingsmaatregelen

DKT heeft in samenwerking met ICT Concept technische beveiligingsmaatregelen getroffen. ICT Concept verzorgt de cloud-omgeving waarin DKT werkt en is ISO 27001 gecertificeerd, een certificering op het gebied van informatiebeveiliging.[122] Een omschrijving van de automatisering en beveiliging binnen het kantoor is opgenomen in het kantoorboek. Uit een analyse van deze omschrijving komt het volgende over de technische beveiliging voort.

Alle gegevens en programma's waar DKT mee werkt, staan in een cloud-omgeving. Deze cloud-omgeving draait op beveiligde servers in een datacenter in Nederland. De verbinding tussen het kantoor en dit datacenter is versleuteld. DKT neemt van ICT Concept het Connectivity Pack af, dat onder andere een gatekeeper en noodstroomvoorziening omvat. Bij het gebruik van een gatekeeper verloopt al het dataverkeer via een firewall, proxy of versleutelde VPN verbinding. Alle inkomende e-mail en data wordt tevens gecontroleerd op virussen en spyware. Tenslotte zijn de servers van ICT Concept niet direct via het internet te bereiken. Om de continuïteit te waarborgen zijn er verschillende maatregelen getroffen. Zo is elke server meervoudig uitgevoerd, wat inhoudt dat er gebruik wordt gemaakt van dubbele voedingen, dubbele harde schijven met een reserveschijf en dubbele netwerkverbindingen. Firewalls en netwerkcomponenten zijn dubbel tot driedubbel uitgevoerd. Als een van de componenten uitvalt, kan DKT dankzij deze dubbele componenten toch bij de gegevens en programma's. Er wordt dagelijks een back-up gemaakt van alle data en e-mail naar een beveiligde server in een tweede datacenter, op een geografisch andere locatie. Deze back-ups worden regelmatig op integriteit getest en 30 dagen bewaard. De datacenters worden 24 uur per dag bewaakt, hebben een meervoudig uitgevoerde stroomvoorziening met dieselgeneratoren als back-up en beschikken over systemen voor klimaatbeheersing en branddetectie.

[121] Box B.V., '*Archief- en datavernietiging'*, boxbv.nl/archief-en-datavernietiging.
[122] ICT Concept, *'ICT Concept tot 2019 gecertificeerd conform ISO 27001'* ict-concept.nl/over-ons.

Ook aan de kantoorzijde zijn er technische beveiligingsmaatregelen getroffen. Zo heeft elke medewerker een persoonlijk account om in te loggen op de cloud-omgeving, beveiligd met een wachtwoord dat iedere drie maanden gewijzigd wordt. Dit wachtwoord moet een minimaal aantal karakters lang zijn en verschillende bijzondere tekens bevatten. Aanmelden vanuit een thuislocatie is ook mogelijk middels een authenticatie applicatie op de mobiele telefoon, waarbij er naast de reguliere inloggegevens ook een wisselende code moet worden ingevoerd. Aan elke account zijn specifieke rechten toegewezen. Zo zijn er schijfstations waar slechts bepaalde medewerkers toegang tot hebben of aanpassingen in kunnen doen. De gegevens van cliënten worden opgeslagen op een schijfstation waar iedere medewerker toegang tot heeft. Rechten ten aanzien van cliëntgegevens worden in Assyst toegekend. Deze rechten zijn onderverdeeld in de categorieën notaris, kandidaat-notaris, ondersteunende staf, P&O en boekhouding. De ICT-managers hebben hier beheerrechten en kunnen toegangsrechten toewijzen of intrekken, bijvoorbeeld bij uitdiensttreding of wijziging van functie. Ieder kwartaal wordt gecontroleerd of de juiste rechten nog steeds zijn toegewezen aan de juiste medewerker.

§ 3.6 Bewerkers

Zoals uit het voorgaande al blijkt, werkt DKT bij het verwerken van persoonsgegevens van cliënten samen met verschillende bewerkers. Zo wordt het programma Assyst geleverd door Devoon en wordt er gewerkt in een cloudomgeving van ICT Concept. Met behulp Assyst worden verschillende inzages gedaan en gegevens digitaal opgeslagen. De boekhouding werkt met het Profit programma, dat gegevens uit Assyst gebruikt. Daarnaast staat het archief van Daamen Notarissen opgeslagen bij BB Diensten en zorgt Box B.V. voor de vernietiging van papieren dossiers.[123] Met Devoon en ICT Concept zijn, naast de overeenkomst van opdracht, ook bewerkersovereenkomsten gesloten. Met Box B.V. is een overeenkomst tot opdracht gesloten. Tussen BB Diensten en DKT is een huurcontract afgesloten.

§ 3.7 Meldplicht datalekken

Ten aanzien van de meldplicht datalekken heeft DKT verschillende stappen genomen. Mevrouw O. Javornik, destijds bij DKT werkzaam als ICT manager, heeft in december 2015 de notitie meldplicht datalekken opgesteld.[124] Hierin worden de hoofdlijnen van de meldplicht datalekken behandeld, zoals wanneer en hoe er gemeld moet worden. De notitie geeft voorbeelden van datalekken en stelt dat er binnen twee werkdagen gemeld moet worden aan de AP. Ook wordt geadviseerd om een privacy-administratie aan te leggen om zo accountable en auditable te zijn. De administratie bestaat op dit moment uit deze notitie, een overzicht van bewerkers van persoonsgegevens en de eerder genoemde beschrijving van de automatisering en beveiliging. In het overzicht van bewerkers is vastgelegd welke gegevens er verwerkt worden, welke diensten hiervoor worden gebruik, wie deze diensten levert en of hiermee een bewerkersovereenkomst is gesloten. Ook het risico bij een datalek is geïnventariseerd. DKT houdt een register van datalekken bij, met daarin per datalek de melding aan de AP en de betrokkene en andere relevante correspondentie. In een Excel document wordt de datum en de aard van het datalek vastgelegd, samen met de datum van de melding en aan welke partijen melding is gemaakt. Tenslotte is het kantoor in geval van een datalek verzekerd tegen boetes en kosten voor bijvoorbeeld calamiteitenmanagement.[125]

Naast de privacy-administratie beschikt het kantoor sinds kort over een procedure voor datalekken. Op 20 januari 2017 is er door de mr. J.A. Beijsens en drs. R. Nijnens, respectievelijk notaris en kantoordirecteur bij DKT, een e-mail over datalekken verstuurd aan alle medewerkers. Daarin wordt kort toegelicht wat een datalek is, wanneer er gemeld

[123] Zie bijlage D: Interview drs. R. Nijnens.
[124] Zie bijlage N: Notitie meldplicht datalekken.
[125] Zie bijlage D: Interview drs. R. Nijnens.

moet worden en welke procedure er wordt gevolgd.[126] Er moet contact worden opgenomen met kantoordirecteur drs. R. Nijnens, de coördinator op het gebied van datalekken, die samen met de betrokken medewerker melding zal maken bij de AP en een vervolgaanpak zal bepalen. Deze e-mail is gebaseerd op de notitie datalekken en noemt een uiterlijke termijn van twee werkdagen om het datalek te melden. Een deadline voor de melding aan de betrokkene wordt niet vermeld. Sinds het rondsturen van deze e-mail wordt er door drs. R. Nijnens gewerkt aan beleid voor DKT met betrekking tot persoonsgegevens, dat op dit moment nog steeds in ontwikkeling is.

§ 3.7.1 Datalekken binnen DKT

Sinds de notitie datalekken en de invoering van de meldplicht datalekken heeft DKT een aantal keer melding gemaakt van een datalek dat zich op het kantoor heeft voorgedaan. Het datalek van 10 januari 2017 was het ernstigst. Op die dag werd er een doos met daarin oude dossiers en documenten van de vestiging Udenhout naar Tilburg Centrum gebracht, om daar weggegooid te worden. De vestiging Udenhout had destijds namelijk nog geen eigen Box B.V. container. De doos met documenten werd echter niet in de container van Box B.V., maar in de reguliere papiercontainer gegooid. Deze papiercontainer werd op 16 januari geleegd en op 23 januari besefte men dat er een fout was gemaakt. Hoewel de papiercontainer was geleegd, kon niet worden uitgesloten dat er persoonsgegevens waren gelekt. Op 23 januari 2017 is er melding gemaakt aan de AP, die vervolgens op 26 januari 2017 is aangevuld. Beide keren is er gebruik gemaakt van webformulieren, die zijn opgeslagen in het register. Omdat ondanks inspanning vanuit DKT niet kon worden achterhaald op welke personen deze informatie betrekking had, is er afgezien van een melding aan de betrokkenen. Uiteindelijk zijn er wel maatregelen genomen in de vorm van een instructie aan nieuwe medewerkers over de verwerking van oud papier en het plaatsen van een Box B.V. container op de vestiging in Udenhout.

Uit een analyse van het register van datalekken blijkt dat DKT consequent gebruik maakt van het webformulier om datalekken te melden bij de AP. Afgezien van het bovenstaande geval zijn datalekken altijd gemeld aan de betrokkene. Meestal is dit schriftelijk gebeurd, in een enkel geval mondeling. Aan de betrokkene is telkens gemeld hoe het datalek heeft kunnen gebeuren. Van elk datalek is het webformulier, relevante correspondentie en de melding aan de betrokkene opgeslagen in het systeem van DKT. Daarnaast zijn relevante gegevens van ieder datalek, zoals de aard, datum van ontdekking en datum van melding, apart geregistreerd in een Excel bestand.

Vermeldenswaardig is dat het eigen beleid om datalekken binnen twee werkdagen aan de AP te melden in een enkel geval niet is gevolgd. In dat geval werd het datalek 18 dagen na ontdekking aan de AP gemeld. De betrokkene werd een week na ontdekking van dit datalek geïnformeerd. Bij het ene datalek dat zich daarvoor had voorgedaan, werd er op tijd gemeld aan de AP maar werd de betrokkene pas een maand na ontdekking volledig geïnformeerd over het datalek. De betrokkene had dit datalek zelf opgemerkt en aan DKT gemeld, waarna het kantoor actie heeft ondernomen. Er werd echter pas een maand later een bericht verstuurd met daarin de aard van het datalek en de genomen maatregelen. Na de e-mail over datalekken aan alle medewerkers lijkt deze situatie te verbeteren. Dit blijkt uit het meest recente incident, dat zich buiten de schuld van DKT om heeft voorgedaan. Een medewerker van het kantoor heeft een envelop met daarin een of meerdere akte(n) naar het juiste adres verzonden. Deze envelop is echter na twee weken nog niet bij de cliënt aangekomen en het wordt aangenomen dat er iets is misgegaan bij de postdiensten. Omdat DKT niet kan uitsluiten dat de envelop in verkeerde handen is gevallen, heeft het kantoor één dag na ontdekking hiervan melding gemaakt aan de AP en aan de betrokkene.

[126] Zie bijlage O: E-mail verplicht melden datalekken.

Hoofdstuk 4: Algemene Verordening Gegevensbescherming

Door snelle technologische ontwikkelingen en globalisering zijn er nieuwe uitdagingen voor de bescherming van persoonsgegevens ontstaan, die een krachtig en coherent kader voor gegevensbescherming vereisen. Daarom wordt er sinds 2012 gewerkt aan de vervanger van de richtlijn waarop de Wbp is gebaseerd, de Europese Privacyrichtlijn uit 1995.[127] Dit resulteerde uiteindelijk in Algemene Verordening Gegevensbescherming. De AVG is op 24 mei 2016 in werking getreden en wordt op 25 mei 2018 van toepassing. Hiermee wijzigen verschillende onderdelen van het juridisch kader omtrent persoonsgegevens, die in dit hoofdstuk behandeld zullen worden. Ook zal er in dit hoofdstuk op bepaalde punten aandacht worden besteed aan de voor de notaris relevante aspecten.

§ 4.1 Toepassingsgebied en betrokken partijen

De AVG is net als de Wbp van toepassing op de (gedeeltelijk) geautomatiseerde verwerking van persoonsgegevens en op de niet geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn of worden opgenomen. Het territoriaal toepassingsgebied verandert echter wel. De AVG zal namelijk gelden in alle lidstaten van de EU. Sommige partijen betrokken bij de verwerking van persoonsgegevens veranderen van naam. Zo wordt de verantwoordelijke in de AVG de verwerkingsverantwoordelijke genoemd en wordt de bewerker als verwerker aangeduid.[128] Omdat er aan de inhoud van de begrippen niets wordt gewijzigd, worden in de rest van dit onderzoek gemakshalve de termen verantwoordelijke en bewerker gehanteerd.

§ 4.1.1 Functionaris voor de gegevensbescherming

Een betrokken partij die in de AVG een grotere rol krijgt, is de functionaris voor de gegevensbescherming (hierna: FG). Onder de Wbp kan de verantwoordelijke reeds vrijwillig een onafhankelijke natuurlijke persoon aanstellen als FG, die toeziet op de naleving van de wet en waaraan de verantwoordelijke de verwerking van persoonsgegevens kan melden (zie paragraaf 2.3).[129] De taken en positie van de FG worden in de AVG uitgebreid met het adviseren en informeren van werknemers en bewerkers. De FG wordt ook het contactpunt voor de AP en betrokkenen. Ook moet de verantwoordelijke de FG betrekken bij alles gerelateerd aan de bescherming van persoonsgegevens en de FG ondersteunen bij het uitvoeren van zijn taken. De FG is tot geheimhouding verplicht en mag ook andere taken vervullen, mits dit niet tot een belangenconflict leidt.[130] Onder de AVG wordt het aanstellen van een FG in drie gevallen verplicht, namelijk wanneer[131]:

- de verwerking wordt verricht door een overheidsinstantie of -orgaan;
- de verwerking regelmatige en stelselmatige observatie op grote schaal van betrokkenen vereist;
- er op grote schaal hoofdzakelijk bijzondere persoonsgegevens of persoonsgegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten worden verwerkt.

§ 4.2 Vereisten aan verwerking

Qua strekking komen de vereisten die de AVG aan de verwerking stelt grotendeels overeen met de Wbp, net als de gronden voor verwerking (paragraaf 2.2).[132] De AVG voegt aan de vereisten echter een verantwoordingsplicht toe. Waar de Wbp alleen het

[127] Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (*PbEG* 1995, L 281).
[128] Artikel 4 lid 7 AVG jo. artikel 4 lid 8 AVG.
[129] Artikel 62 Wbp jo. artikel 63 Wbp jo. artikel 64 Wbp.
[130] Artikel 38 AVG jo. artikel 39.
[131] Artikel 37 lid 1 AVG.
[132] Artikel 5 AVG jo. artikel 6 AVG.

voldoen aan deze vereisten voorschrijft, eist de AVG daarnaast dat dit aantoonbaar is (zie paragraaf 4.2.1).[133] De bewaartermijn wordt aangescherpt en komt in paragraaf 4.5 aan bod.

De verwerking van bijzondere persoonsgegevens is opnieuw alleen bij uitzondering toegestaan, bijvoorbeeld wanneer de betrokkene toestemming heeft gegeven of de verwerking noodzakelijk is voor de uitvoering van verplichtingen van de verantwoordelijke.[134] Overweging 52 van de AVG stelt tevens dat er van het verbod kan worden afgeweken als er een wettelijke grondslag is en er passende waarborgen worden geboden ter bescherming van persoonsgegevens. De regeling over het verwerken van een nationaal identificerend persoonsnummer, in Nederland het BSN, wordt geheel aan de lidstaten van de EU overgelaten. Ter uitvoering van de AVG is het wetsvoorstel Uitvoeringswet Algemene verordening gegevensbescherming opgesteld. In dit wetsvoorstel is er gekozen voor een beleidsneutrale uitvoering van de AVG.[135] Dit houdt in dat de uitzondering voor het BSN wordt gehandhaafd en dit alleen verwerkt mag worden wanneer dit wettelijk geregeld is.[136]

§ 4.2.1 Verantwoordingsplicht

De AVG voert een verantwoordingsplicht voor de verantwoordelijke in. Dit houdt in dat de verantwoordelijke aan moet kunnen tonen dat aan de vereisten aan de verwerking, behandeld in paragraaf 4.2, is voldaan.[137] Ook moet verantwoordelijke passende technische en organisatorische maatregelen treffen om te waarborgen en tevens aan te kunnen tonen dat de gehele verwerking van persoonsgegevens voldoet aan de eisen van de AVG.[138] Daarbij moet gelet worden op de aard, omvang, context en het doel van de verwerking, evenals de waarschijnlijkheid en ernst van de risico's voor de rechten van de betrokkenen. Hieronder valt, wanneer dit in verhouding staat tot de verwerkingsactiviteiten, het opstellen van een gegevensbeschermingsbeleid. De maatregelen moeten regelmatig geëvalueerd en indien nodig geactualiseerd worden. Het voldoen aan de nieuwe registratieplicht (zie paragraaf 4.3) kan helpen aantonen dat de AVG wordt nageleefd.[139] Ook aansluiting bij goedgekeurde gedragscodes of certificeringsmechanismen kan hiervoor worden gebruikt.

§ 4.2.2 Privacy by design en privacy by default

Privacy by design en privacy by default, in het Nederlands gegevensbescherming door ontwerp en door gebruik van standaardinstellingen genoemd, zijn twee beginselen die de verantwoordelijke expliciet in acht moet nemen.[140] Privacy by design houdt in dat er bij de ontwikkeling van nieuw beleid of nieuwe diensten, met betrekking tot de verwerking van persoonsgegevens, aandacht wordt besteed aan privacyverhogende maatregelen zoals pseudonimisering. Privacy by default betekent dat de hoogst mogelijke mate van privacybescherming de standaard moet zijn. Dit betekent dat de verantwoordelijke standaard alleen persoonsgegevens verwerkt die noodzakelijk zijn voor het specifieke verwerkingsdoel. Deze verplichting geldt voor de hoeveelheid persoonsgegevens die verzameld worden, maar ook voor de bewaartermijn die wordt gehanteerd en wie toegang heeft tot deze gegevens. Een minimale gegevensverwerking moet de standaard zijn, zodat de inbreuk op de persoonlijke levenssfeer zo klein mogelijk wordt gehouden.[141]

---

[133] Artikel 5 lid 2 AVG.
[134] Artikel 9 lid 2 sub b AVG.
[135] Wetsvoorstel en toelichting Uitvoeringswet Algemene verordening gegevensbescherming, p. 40-41.
[136] Artikel 44 wetsvoorstel Uitvoeringswet Algemene verordening gegevensbescherming.
[137] Artikel 5 lid 2 AVG.
[138] Artikel 24 AVG.
[139] *Anticiperen op de Algemene verordening gegevensbescherming: Tien stappen voor een goede voorbereiding,* Den Haag: Ministerie van Veiligheid en Justitie 2017 (online publiek).
[140] Artikel 25 AVG.
[141] Wetsvoorstel en toelichting Uitvoeringswet Algemene verordening gegevensbescherming, p. 60-61.

§ 4.3 Registratieplicht

Onder de AVG wordt de verplichting om de verwerking van persoonsgegevens te melden aan de AP vervangen door een registratieplicht. De verwerkingsactiviteiten die onder de verantwoordelijkheid van de verantwoordelijke plaatsvinden, moeten gedocumenteerd worden om naleving van de verordening aan te tonen.[142] Het register moet in schriftelijke vorm, waaronder elektronisch, worden opgesteld.[143] Als de verantwoordelijke minder dan 250 personen in dienst heeft, geldt de registratieplicht in principe niet. Dit criterium van 250 personen vervalt echter als de verwerking waarschijnlijk een risico inhoudt voor de rechten en vrijheden van betrokkenen, de verwerking niet incidenteel is, of als er persoonsgegevens in verband met strafrechtelijke veroordelingen en strafbare feiten worden verwerkt.[144] De verantwoordelijke moet verschillende gegevens opnemen in het register, namelijk:

- de naam en contactgegevens van de verantwoordelijke en in voorkomend geval de FG;
- de verwerkingsdoeleinden;
- een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens;
- de categorieën van ontvangers van persoonsgegevens;
- doorgiften van persoonsgegevens aan landen buiten de EU of internationale organisaties;
- indien mogelijk, de beoogde termijn waarbinnen de verschillende categorieën gegevens moeten worden gewist;
- indien mogelijk, een algemene beschrijving van de genomen technische en organisatorische beveiligingsmaatregelen.

§ 4.4 Informatieplicht

De informatieplicht van de verantwoordelijke ten opzichte van de betrokkene wordt in de AVG uitgebreid.[145] Het informeren van de betrokkene over de identiteit van de verantwoordelijke en de verwerkingsdoeleinden is niet langer voldoende. Daarnaast overweegt de AVG specifiek dat als de verantwoordelijke de persoonsgegevens verwerkt voor een ander doel dan waarvoor zij zijn verzameld, hij de betrokkene ook over dit andere doel moet informeren. Naast de identiteit van de verantwoordelijke en de verwerkingsdoeleinden eist de AVG dat de betrokkene ook wordt geïnformeerd over:

- de contactgegevens van de verantwoordelijke en in voorkomend geval van de FG;
- de rechtsgrond van de verwerking;
- in voorkomend geval, het gerechtvaardigd belang van de verantwoordelijke waarop de verwerking is gebaseerd;
- in voorkomend geval, de ontvangers of categorieën van ontvangers van de persoonsgegevens;
- in voorkomend geval, dat het voornemen bestaat persoonsgegevens door te geven aan ontvangers in landen buiten de EU of een internationale organisatie en welke waarborgen hiervoor zijn getroffen;
- de bewaartermijn van de persoonsgegevens of de criteria op basis waarvan deze wordt vastgesteld;
- de rechten die de betrokkene heeft (zie paragraaf 2.6 en 4.6);
- de mogelijkheid om zonder terugwerkende kracht de toestemming tot de verwerking van persoonsgegevens in te trekken;
- de mogelijkheid tot het indienen van een klacht bij de AP;
- of de verstrekking van de persoonsgegevens wettelijk of contractueel verplicht is dan wel noodzakelijk is om een overeenkomst te sluiten en wat de gevolgen zijn wanneer de gegevens niet worden verstrekt;

[142] Artikel 30 lid 1 AVG; zie ook overweging 82 AVG.
[143] Artikel 30 lid 3 AVG.
[144] Artikel 30 lid 5 AVG.
[145] Artikel 13 AVG.

- of er sprake is van geautomatiseerde besluitvorming, wat de onderliggende logica hiervan is en de verwachte gevolgen voor de betrokkene van die verwerking zijn.

Als de persoonsgegevens niet van de betrokkene worden verkregen maar uit een andere bron voortkomen, moet de bovenstaande informatie aan de betrokkene worden meegedeeld, behalve of de verstrekking wettelijk of contractueel verplicht is dan wel noodzakelijk is om een overeenkomst te sluiten. In plaats daarvan moet betrokkene geïnformeerd worden over:

- de betrokken categorieën van persoonsgegevens;
- de bron van deze gegevens en of deze bron openbaar is.[146]

Al deze informatie dient kosteloos in een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal verstrekt te worden.[147] Als de persoonsgegevens bij de betrokkene worden verzameld, vervalt deze informatieplicht alleen als de betrokkene reeds over deze informatie beschikt.[148] Als de persoonsgegevens niet van de betrokkene zelf afkomen, komt de informatieplicht daarnaast te vervallen wanneer het verstrekken onmogelijk blijkt of onevenredig veel inspanning zou vergen, het verkrijgen van de persoonsgegevens uitdrukkelijk wettelijk is verplicht of de persoonsgegevens vertrouwelijk moeten blijven op basis van een geheimhoudingsplicht.[149]

§ 4.5 Bewaren van persoonsgegevens

Net als in de Wbp wordt de bewaartermijn in de AVG gekoppeld aan de verwerkingsdoeleinden.[150] Persoonsgegevens, in een vorm die identificatie mogelijk maakt, mogen niet langer bewaard worden dan noodzakelijk is voor het bereiken van de verwerkingsdoeleinden.[151] Overweging 39 van de AVG scherpt deze termijn verder aan en stelt dat de opslagperiode van de persoonsgegevens tot een strikt minimum moet worden beperkt. Waar de Wbp de bewaartermijn in bepaalde gevallen concretiseert en hier uitzonderingen op maakt (zie paragraaf 2.3.1 en 2.5.1), doet de AVG dit niet. De enige concrete uitzondering op de strikt minimale bewaartermijn wordt gemaakt voor archivering ten behoeve van het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden. De bewaartermijn voor persoonsgegevens onder de AVG blijft dus afhankelijk van de verwerkingsdoeleinden.

§ 4.5.1 De notaris en de bewaartermijn uit de AVG

De strikt minimale bewaarperiode uit de AVG botst met de verschillende bewaarplichten waaraan de notaris gebonden is. Omdat de AVG de strikt minimale bewaarperiode niet verder invult en geen concrete uitzondering biedt voor bewaarplichten, moet deze uitzondering gezocht worden in de formulering van deze bewaarperiode. Artikel 5 lid 1 sub e AVG stelt dat de persoonsgegevens, in een vorm die identificatie mogelijk maakt, slechts bewaard mogen worden zolang dit noodzakelijk is voor de verwerkingsdoeleinden. ‘Noodzakelijk voor de verwerkingsdoeleinden’ zijn de sleutelwoorden.

De notaris die op basis van het Vrijstellingsbesluit Wbp geen melding maakt van de verwerking aan de AP, is door de vrijstelling niet alleen gebonden aan een maximale bewaartermijn van twee jaar (met daarin een uitzondering voor bewaartermijnen en -plichten), maar ook aan bepaalde verwerkingsdoeleinden. Zowel deze meldplicht als de vrijstelling vervalt met het van kracht worden van de AVG. Dit betekent dat de uitzondering voor de bewaarplichten van de notaris wegvalt, maar ook dat de notaris niet

[146] Artikel 14 lid 1 sub d AVG jo. artikel 14 lid 2 sub f AVG.
[147] Artikel 12 lid 1 AVG jo. artikel 12 lid 5 AVG.
[148] Artikel 13 lid 4 AVG.
[149] Artikel 14 lid 5 AVG.
[150] Artikel 10 Wbp.
[151] Artikel 5 lid 1 sub e AVG.

langer gebonden is aan vastgestelde doeleinden. De notaris zal zijn verwerkingsdoeleinden, voor zover ze te rechtvaardigen zijn, zelf kunnen vaststellen.

De verwerking van persoonsgegevens hangt vaak samen met meerdere doelen. Zo zal een webwinkel gegevens verzamelen om een product te leveren, maar deze vervolgens bewaren om een mogelijke retournering of non-conformiteitsclaim af te handelen.[152] Ook de notaris verwerkt persoonsgegevens van cliënten voor verschillende doeleinden. In beginsel is de verwerking noodzakelijk om het primaire verwerkingsdoel, het leveren van notariële diensten zoals het opstellen van een akte of adviseren van een cliënt, te bereiken. Als dit het enige verwerkingsdoel zou zijn, zou dit onder de AVG betekenen dat de verzamelde gegevens na het passeren van de akte verwijderd zouden moeten worden. Er geldt echter een bewaarplicht voor documenten zoals de akten, identiteitsbewijzen en verstuurde facturen. De notaris moet deze documenten na het passeren bewaren om hieraan te voldoen. Het voldoen aan de bewaarplichten is dus ook een verwerkingsdoel. Voor dit verwerkingsdoel is het noodzakelijk dat de documenten met daarin persoonsgegevens zo lang worden bewaard als de bewaarplichten voorschrijven. Op deze manier is er ook in de AVG ruimte voor de bewaarplichten waaraan de notaris gebonden is. Tevens stelt overweging 65 van de AVG, in het kader van het recht op vergetelheid (zie paragraaf 4.6), dat het ondanks dit recht rechtmatig dient te zijn persoonsgegevens langer te bewaren wanneer dat noodzakelijk is voor de nakoming van bijvoorbeeld een wettelijke verplichting. De bewaarplichten van de notaris zijn wettelijk geregeld en gaan daarmee voor op de strikt minimale bewaarperiode uit de AVG. De notaris kan ook bepaalde gegevens willen bewaren om zijn werkzaamheden verifieerbaar te houden. Het verifieerbaar houden van de notariële werkzaamheden is in dat geval het verwerkingsdoel. Op basis van dit verwerkingsdoel kan de notaris ook gegevens bewaren die niet onder een bewaarplicht vallen, indien deze noodzakelijk zijn om zijn werkzaamheden verifieerbaar te houden. Dit geldt ook voor persoonsgegevens waarvan de bewaarplicht is verstreken.

Als persoonsgegevens worden verwerkt voor een ander doel dan dat waarvoor zij oorspronkelijk zijn verzameld, zoals hierboven beschreven, moet gekeken worden of dit andere doel verenigbaar is met het oorspronkelijke doel.[153] Daarbij wordt onder andere rekening gehouden met het verband tussen de doeleinden, het kader waarin de persoonsgegevens zijn verzameld, de mogelijke gevolgen van de verdere verwerking voor de betrokkene en de genomen beveiligingsmaatregelen. Ook de aard van de persoonsgegevens is van belang, met name of het bijzondere persoonsgegevens betreft. Wanneer de doelen verenigbaar blijken, moet worden bepaald hoe lang het noodzakelijk is de persoonsgegevens voor deze doelen te bewaren. Deze termijn zal tot een strikt minimum beperkt moeten blijven, maar het vaststellen en documenteren van dit strikte minimum wordt aan de verantwoordelijke overgelaten.

§ 4.6 Rechten van betrokkene

Ook onder de AVG heeft de betrokkene de in paragraaf 2.6 besproken rechten op inzage, correctie en verzet (in de AVG het recht op bezwaar genoemd).[154] Daarnaast wordt het recht op correctie verder uitgewerkt met het recht op gegevenswissing en wordt het recht op dataportabiliteit ingevoerd.[155] Zo moet de verantwoordelijke die persoonsgegevens openbaar heeft gemaakt op basis van het recht op gegevenswissing nu ook andere verantwoordelijken die de gegevens hebben verwerkt, zoals een zoekmachine, inlichten over ontvangen verzoeken tot gegevenswissing. Het recht op dataportabiliteit geeft de betrokkene de mogelijkheid om de door hem verstrekte persoonsgegevens op te vragen

[152] A. Engelfriet, 'Bewaren van persoonsgegevens: het mag niet maar het moet wel!', *Ius Mentis* 4 november 2013, blog.iusmentis.com.
[153] Artikel 6 lid 4 AVG.
[154] Artikel 15 AVG jo. artikel 16 AVG jo. artikel 21 AVG.
[155] Artikel 17 AVG jo. artikel 20 AVG.

en mee te nemen naar een andere verantwoordelijke. Ook onder de AVG zal de notaris niet snel te maken krijgen met deze rechten van de cliënt. Zo stelt de AVG in overweging 65 dat als er een verzoek tot gegevenswissing is gedaan, het rechtmatig moet zijn gegevens langer te bewaren om een wettelijke verplichting na te komen. De verschillende bewaarplichten van notaris (zie paragraaf 2.5.1) vormen hier een beperking. De notaris zal bijvoorbeeld niet in kunnen gaan op een verzoek tot gegevenswissing wanneer dit een akte betreft, omdat de hij juist verplicht is deze akte te bewaren. Ook ligt het niet voor de hand dat de cliënt van de notaris zijn persoonsgegevens opvraagt om deze vervolgens bij een andere verantwoordelijke onder te brengen. Omdat de nieuwe rechten de notaris in zijn klassieke rol niet snel zullen deren, wordt hier niet verder op ingegaan.[156]

§ 4.7 Beveiliging van persoonsgegevens

De verantwoordelijke moet ook onder de AVG passende technische en organisatorische maatregelen nemen om een op de risico's voor de rechten en vrijheden van personen afgestemd, oftewel een passend, beveiligingsniveau te waarborgen. Dit blijft een relatief begrip waarbij rekening moet worden gehouden met factoren zoals de stand van de techniek, de uitvoeringskosten, de verwerkingsdoeleinden en risico's die de verwerking met zich meebrengt.[157] De maatregelen die de AVG voorstelt zijn onder andere de versleuteling van persoonsgegevens en het vermogen om bij een fysiek of technisch incident de beschikbaarheid en toegang tot de persoonsgegevens tijdig te herstellen. In de praktijk vertaalt dit zich in een actuele back-up van de persoonsgegevens. Ook een procedure om de technische en organisatorische beveiligingsmaatregelen op vaste tijdstippen te testen kan bijdragen aan het beveiligingsniveau. In het kader van de verantwoordingsplicht moet de verantwoordelijke aan kunnen tonen dat hij een passend beveiligingsniveau handhaaft, wat onder andere mogelijk is door middel van certificering of aansluiting bij een goedgekeurde gedragscode.[158] Om een passend beveiligingsniveau te bereiken, kan er gebruik worden gemaakt van dezelfde richtsnoeren als besproken in paragraaf 2.7. Bij het opstellen hiervan is er namelijk zoveel mogelijk rekening gehouden met de AVG, die zich destijds nog in conceptfase bevond. In de toekomst zal de AP de richtsnoeren herzien, zodat deze volledig zullen aansluiten op de AVG.[159]

§ 4.7.1 Privacy Impact Assessment

De AVG voert een gegevensbeschermingseffectbeoordeling of *Privacy Impact Assessment* (hierna: PIA) in.[160] Een PIA wordt gebruikt om voorafgaand aan een verwerking de privacyrisico's in kaart te brengen en om beschermingsmaatregelen ter beperking van deze risico's vast te stellen.[161] Een PIA is vereist wanneer het verwerken van persoonsgegevens, in het bijzonder waarbij nieuwe technologieën worden gebruikt, waarschijnlijk een hoog risico voor de betrokkene zal hebben. Hierbij wordt gelet op de aard, omvang, context en doeleinden van de verwerking. Een PIA is in ieder geval verplicht bij profilering van natuurlijke personen, grootschalige verwerking van bepaalde bijzondere persoonsgegevens of gegevens met betrekking tot het strafrecht, en stelselmatige en grootschalige monitoring van openbare ruimtes.[162] In de toekomst kan de AP lijsten opstellen van verwerkingen waarvoor wel of geen PIA vereist is.[163]

§ 4.8 De bewerker

De AVG scherpt de eisen verbonden aan het inschakelen van een bewerker aan. Zo mag de verantwoordelijke alleen beroep doen op verwerkers die voldoende garanties bieden

[156] Lekkerkerker & Van Ee *WPNR* 2015/7070, p. 626.
[157] Artikel 32 lid 1 AVG jo artikel 32 lid 2 AVG.
[158] Artikel 32 lid 3 AVG.
[159] Beveiliging van persoonsgegevens 2013, p. 5.
[160] Artikel 35 AVG.
[161] Privacy Impact Assessment: introductie, handreiking en vragenlijst 2015, p. 9.
[162] Artikel 35 lid 3 AVG.
[163] Artikel 35 lid 4 AVG jo. artikel 35 lid 5 AVG.

met betrekking tot het nemen van technische en organisatorische maatregelen, zodat de verwerking voldoet aan de eisen van de verordening en de bescherming van de rechten van de betrokkene is gewaarborgd.[164] Aansluiting bij een goedgekeurde gedragscode of certificering kan gebruikt worden als element om dit aan te tonen.[165] Net als onder de Wbp mag de bewerker alleen persoonsgegevens verwerken wanneer de verantwoordelijke hiertoe opdracht geeft.[166] Die bewerker mag vervolgens alleen een sub-bewerker inschakelen wanneer de verantwoordelijke hier schriftelijke toestemming voor geeft.[167] De eisen uit de bewerkersovereenkomst, met name de verplichting om technische en organisatorische maatregelen te nemen om aan de verordening te voldoen en de rechten van betrokkene te beschermen, moeten ook worden opgelegd aan de sub-bewerker.

§ 4.8.1 De bewerkersovereenkomst

De eisen die aan de bewerkersovereenkomst worden gesteld, worden onder de AVG uitgebreid. Daarbij zijn de eisen in de verordening opgenomen, in plaats van dat ze grotendeels voortvloeien uit beleidsregels of mededelingen van de AP. De overeenkomst moet in schriftelijke vorm, waaronder elektronisch, worden opgesteld.[168] In de bewerkersovereenkomst moet in ieder geval het onderwerp, de duur, de aard en het doel van verwerking, het soort persoonsgegevens, de categorieën van betrokkenen en de rechten en plichten van de verantwoordelijke worden omschreven.[169] Verder eist de AVG dat de overeenkomst met name bepaalt dat de bewerker:

- de persoonsgegevens alleen op schriftelijke instructie van de verantwoordelijke verwerkt;
- tot geheimhouding is verplicht, indien dit niet al wettelijk is geregeld;
- beveiligingsmaatregelen neemt om tot een passend beveiligingsniveau te komen;
- in het geval hij een sub-bewerker wil inschakelen, hij hiervoor schriftelijke toestemming van de verantwoordelijke nodig heeft en aan de sub-bewerker dezelfde verplichtingen over gegevensbescherming moet opleggen als uit deze bewerkersovereenkomst voortvloeien;
- de verantwoordelijke helpt bij het voldoen aan verzoeken die de betrokkene op basis van zijn rechten instelt;
- de verantwoordelijke helpt bij het waarborgen van een passend beveiligingsniveau, het voldoen aan de meldplicht datalekken en het uitvoeren van een PIA;
- na afloop van de verwerkingsdiensten alle persoonsgegevens wist of teruggeeft aan de verantwoordelijke en bestaande kopieën verwijdert;
- alle informatie benodigd om naleving van deze eisen aan te tonen ter beschikking stelt en meewerkt aan audits van de verantwoordelijke.

Deze eisen zijn schematisch weergegeven in een checklist, in bijlage B. De Europese Commissie en de AP kunnen standaard contractbepalingen opstellen om invulling van bewerkersovereenkomsten te vergemakkelijken.[170] Tenslotte is het vermeldenswaardig dat de bewerkersovereenkomst onder de AVG geen aparte overeenkomst meer hoeft te zijn.

§ 4.9 Meldplicht datalekken

De AVG vervangt de meldplicht datalekken uit de Wbp met een eigen meldplicht datalekken. In vergelijking met de Wbp zijn er verschillende overeenkomsten, maar ook een aantal belangrijke verschillen. Deze paragraaf gaat hier verder op in, waarbij dezelfde structuur als in paragraaf 2.9 wordt aangehouden.

[164] Artikel 28 lid 1 AVG.
[165] Artikel 28 lid 5 AVG.
[166] Artikel 29 AVG.
[167] Artikel 28 lid 2 AVG.
[168] Artikel 28 lid 9 AVG.
[169] Artikel 28 lid 3 AVG.
[170] Artikel 28 lid 7 AVG jo. artikel 28 lid 8 AVG.

§ 4.9.1 Definitie datalek

De AVG verandert de inhoud en de naam van het begrip datalek. De Wbp zelf definieert niet precies wat een datalek inhoudt, maar volgens de beleidsregels is er al sprake van een datalek wanneer er niet redelijkerwijs kan worden uitgesloten dat de persoonsgegevens onrechtmatig zijn verwerkt.[171] De AVG noemt een datalek een inbreuk in verband met persoonsgegevens. Dit wordt gedefinieerd als een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens.[172] Onder de AVG is er dus pas sprake van een datalek wanneer het lek zich daadwerkelijk heeft voorgedaan. De situatie waarin niet redelijkerwijs kan worden uitgesloten dat de persoonsgegevens onrechtmatig zijn verwerkt, wordt niet langer gezien als datalek.

§ 4.9.2 Melding aan de AP

Onder de AVG moet elk datalek in principe gemeld worden aan de AP, tenzij het niet waarschijnlijk is dat het datalek een risico inhoudt voor de rechten en vrijheden van de betrokkenen, zoals het recht op privacy.[173] Dit is een algemene uitzondering op de meldplicht aan de AP. Een dergelijke uitzondering komt niet voor in de Wbp, die enkel een uitzondering biedt voor de meldplicht aan de betrokkene.[174] Een ander verschil is dat de AVG de bewerker verplicht een datalek aan de verantwoordelijke te melden.[175] Dit lag voorheen niet expliciet vast, maar werd opgenomen in bewerkersovereenkomsten (zie paragraaf 2.8.1**)**

§ 4.9.2.1 Inhoud melding aan de AP

Net als in de Wbp moet in de melding aan de AP in ieder geval de aard van de inbreuk zijn opgenomen, samen met gegevens van het contactpunt waar meer informatie kan worden verkregen, de waarschijnlijke gevolgen van de inbreuk en de voorgestelde of genomen maatregelen om eventueel nadelige gevolgen te beperken. De AVG eist verder dat waar mogelijk de categorieën van betrokkenen en persoonsgegevens worden vermeld, samen met, bij benadering, het aantal betrokkenen en persoonsgegevens.[176] Hoewel deze punten niet in de Wbp worden genoemd, zijn deze wel opgenomen in het webformulier van de AP.[177]

§ 4.9.3 Melding aan de betrokkene

Wanneer het datalek waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van de betrokkene, moet de betrokkene hiervan onverwijld op de hoogte worden gesteld.[178] Dit zal met name het geval zijn wanneer er gevoelige persoonsgegevens zijn gelekt. De uitzonderingen hierop zijn onder de AVG anders dan onder de Wbp. Van de melding aan betrokkene kan worden afgezien wanneer de verantwoordelijke vooraf passende technische en organisatorische beschermingsmaatregelen heeft genomen of na de inbreuk maatregelen heeft getroffen ter voorkoming van het hoge risico. Wanneer de mededeling onevenredige inspanning vergt, wordt deze vervangen door een openbare mededeling waarbij betrokkenen net zo doeltreffend worden geïnformeerd.[179] Ook onder de AVG kan de AP, wanneer het datalek een hoog risico met zich meebrengt, de verantwoordelijke verplichten het datalek aan de betrokkene te melden.[180]

---

[171] Beleidsregels voor toepassing van artikel 34a van de Wbp 2015, p. 19.
[172] Artikel 33 lid 1 AVG jo. artikel 4 onder 12 AVG.
[173] Artikel 33 lid 1 AVG.
[174] Wetsvoorstel en toelichting Uitvoeringswet Algemene verordening gegevensbescherming, p. 63.
[175] Artikel 33 lid 2 AVG.
[176] Artikel 33 lid 3 AVG.
[177] Autoriteit Persoonsgegevens, *'Een nieuwe melding doen'*, datalekken.autoriteitpersoonsgegevens.nl.
[178] Artikel 34 lid 1 AVG.
[179] Artikel 34 lid 3 AVG.
[180] Artikel 34 lid 4 AVG.

§ 4.9.3.1 Inhoud melding aan de betrokkene

Vergeleken met de melding aan de betrokkene onder de Wbp blijft ook deze melding grotendeels gelijk. Ook onder de AVG moet de betrokkene worden geïnformeerd over de aard van de inbreuk, over gegevens van het contactpunt waar meer informatie kan worden verkregen en over maatregelen die de verantwoordelijke voorstelt om eventuele nadelige gevolgen te beperken. De AVG voegt hieraan toe dat de betrokkene op de hoogte moet worden gesteld van de waarschijnlijke gevolgen van het datalek en de maatregelen die de verantwoordelijke zelf heeft genomen.[181]

§ 4.9.4 Onverwijld

Net als de Wbp stelt de AVG dat zowel de melding aan de AP als de betrokkene onverwijld moet geschieden. Zoals besproken in paragraaf 2.9.4 heeft de AP in beleidsregels voor de meldplicht datalekken dit begrip verder geconcretiseerd, waarbij aansluiting is gezocht bij de conceptversie van de AVG. De uiteindelijke versie van de AVG brengt hier geen wijzigingen in aan. De AP moet zonder onredelijke vertraging en zo mogelijk binnen 72 uur op de hoogte worden gesteld van het datalek. Informatie over het datalek kan indien nodig ook in stappen worden verstrekt en overschrijding van de grens van 72 uur moet gemotiveerd worden. Deze harde grens geldt niet voor de melding aan de betrokkene, maar hij moet wel onverwijld op de hoogte worden gebracht.[182]

§ 4.9.5 Registratie datalek

De registratieplicht ten aanzien van datalekken wordt onder de AVG uitgebreid.[183] Alleen het bijhouden van meldingsplichtige inbreuken, zoals de Wbp voorschrijft, is niet langer voldoende. De registratieplicht uit de AVG geldt ten aanzien van elke inbreuk in verband met persoonsgegevens, ook de inbreuken waar geen meldingsplicht voor geldt.[184] De inhoud van de registratie wordt echter beperkt. De AVG spreekt namelijk niet over het bewaren van de kennisgeving aan de betrokkene. Alleen de feiten, de gevolgen en de genomen corrigerende maatregelen ten aanzien van het datalek moeten worden geregistreerd. Het bewaren van de kennisgeving ligt echter wel voor de hand. Tenslotte geeft de AVG geen duidelijkheid over een bewaartermijn voor deze registratie.

§ 4.10: Sancties

De AVG breidt de boetebevoegdheid van de AP nog verder uit.[185] De AVG heeft twee boetetarieven. Onder het eerste tarief kan de boete oplopen tot €10 miljoen of tot 2% van de totale wereldwijde jaaromzet als dit bedrag hoger is. Onder het tweede tarief kan de boete oplopen tot €20 miljoen of tot 4% van de totale wereldwijde jaaromzet als dit bedrag hoger is.[186] Het 'lagere' tarief wordt toegepast bij overtredingen met betrekking tot administratieve vereisten zoals het sluiten van bewerkersovereenkomsten, registreren van verwerkingen en melden van datalekken. Opvallend is dat op het niet hebben van een bewerkersovereenkomst nu wel een boete staat, waar dit onder de Wbp nog niet het geval was.[187] Het hogere tarief wordt onder andere gebruikt wanneer er in strijd wordt gehandeld met de basisbeginselen van de verwerking, zoals het hanteren van een minimale bewaarperiode en het verwerken voor welbepaalde en uitdrukkelijk omschreven gerechtvaardigde doeleinden. De boete moet doeltreffend en evenredig, maar ook afschrikkend zijn.[188] Bij het bepalen van de hoogte van de boete wordt er rekening gehouden met de omstandigheden van het geval, zoals de aard, ernst en duur van de

[181] Artikel 33 lid 3 AVG jo. artikel 34 lid 2 AVG.
[182] Artikel 33 lid 1 AVG jo. artikel 34 lid 1 AVG
[183] M. Jansen, 'Valkuil onder komend privacyrecht (AVG): voortaan alle beveiligingsinbreuken loggen, niet alleen de meldingsplichtige', *Dirkzwager Intellectuele eigendom & IT* 15 juni 2016, dirkzwagerieit.nl.
[184] Artikel 33 lid 5 AVG.
[185] Artikel 14 wetsvoorstel Uitvoeringswet Algemene verordening gegevensbescherming.
[186] Artikel 83 lid 4 jo. artikel 83 lid 5 AVG.
[187] Artikel 84 lid 4 onder a AVG; zie ook M. Jansen, 'Op het niet hebben van een bewerkersovereenkomst staat over twee jaar wel een boete', *Dirkzwager Intellectuele eigendom & IT* 31 mei 2016, dirkzwagerieit.nl.
[188] Artikel 83 lid 1 AVG.

overtreding en de betrokken categorieën van persoonsgegevens. Waar een boete onder de Wbp in de meeste gevallen pas volgt na een bindende aanwijzing, kan de AP onder de AVG direct overgaan tot het opleggen van een boete.

Naast boetes noemt het wetsvoorstel Uitvoeringswet Algemene verordening gegevensbescherming de bevoegdheid van de AP om ook onder de AVG een last onder bestuursdwang en een last onder dwangsom op te leggen, wat als effectief middel wordt gezien om overtredingen te beëindigen.[189] De AVG geeft de AP vervolgens aanvullende sanctiemogelijkheden. Zo kan de AP de verantwoordelijke berispen bij overtreding van de verordening en hem gelasten de verwerking in overeenstemming met de verordening te brengen.[190] Ook kan er een tijdelijke of definitieve verwerkingsbeperking of -verbod worden opgelegd. Op het niet naleven van een dergelijke corrigerende maatregel staat een boete op basis van het hoge tarief.[191]

[189] Artikel 17 wetsvoorstel Uitvoeringswet Algemene verordening gegevensbescherming jo. artikel 5:32 lid 1 Awb; zie ook Wetsvoorstel en memorie van toelichting Uitvoeringswet Algemene verordening gegevensbescherming, p. 78.
[190] Artikel 58 lid 2 AVG.
[191] Artikel 83 lid 5 sub e AVG jo artikel 83 lid 6 AVG.

Hoofdstuk 5: DKT en de Wbp

In dit hoofdstuk wordt de Wbp toegepast op het huidige beleid en de huidige werkwijze van DKT. Er wordt gekeken in hoeverre de gang van zaken binnen DKT, beschreven in hoofdstuk 3, op dit moment afwijkt van de wettelijke eisen die aan de omgang met persoonsgegevens worden gesteld zoals verwoord in hoofdstuk 2. Aan de hand van deze analyse worden uiteindelijk aanbevelingen aan DKT gedaan over de omgang met persoonsgegevens van cliënten onder de Wbp.

§ 5.1 Toepassingsgebied en betrokken partijen

Bij het behandelen van een dossier verzamelt DKT persoonsgegevens met behulp van Assyst. Dit programma kan gegevens uit verschillende registers halen en deze vervolgens samenbrengen in bijvoorbeeld een cliëntkaart. Ook leveren cliënten zelf informatie aan, die vervolgens in het dossier wordt opgenomen. Alle dossiers worden zowel fysiek als digitaal bijgehouden. Daarmee is er sprake van een gedeeltelijk geautomatiseerde verwerking van persoonsgegevens. Ook heeft DKT een archief met daarin oudere dossiers die voor deze digitalisatie zijn gepasseerd, doorzoekbaar op dossiernummer. Daarmee is er ook sprake van een niet geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen. De verwerking van persoonsgegevens van cliënten van DKT valt dus onder de Wbp (zie paragraaf 2.1). DKT bepaalt voor welke doelen en met welke middelen de persoonsgegevens van cliënten worden verwerkt en kan daarom worden aangemerkt als verantwoordelijke. De cliënten waarvan persoonsgegevens worden verwerkt zijn de betrokkenen.

§ 5.2 Vereisten aan verwerking

DKT moet er als verantwoordelijke voor zorgen dat de verwerking van persoonsgegevens aan de verschillende vereisten uit de Wbp voldoet (zie paragraaf 2.2). De juistheid en nauwkeurigheid van persoonsgegevens ligt in het verlengde van de plicht van een notaris om het ambt met de grootst mogelijke zorgvuldigheid uit te voeren.[192] DKT verwerkt persoonsgegevens van de cliënt om de opdracht van deze cliënt uit te voeren. Bepaalde documenten met daarin persoonsgegevens, zoals een akte, worden daarna bewaard om aan wettelijke bewaarplichten te voldoen. De verwerking van persoonsgegevens van cliënten door DKT is daarmee gebaseerd op het uitvoeren van een overeenkomst waarbij de betrokkene een partij is en het nakomen van wettelijk verplichtingen.

Een van de belangrijkste vereisten die de Wbp stelt, is dat persoonsgegevens alleen verzameld mogen worden voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. DKT heeft zelf geen verwerkingsdoeleinden vastgesteld. Omdat het kantoor de verwerking van persoonsgegevens op basis van de vrijstelling voor juridische en financiële dienstverleners niet aan de AP meldt (zie paragraaf 2.3), is DKT gebonden aan de doeleinden vastgelegd in deze vrijstelling.[193] DKT verzamelt persoonsgegevens van cliënten om akten op te stellen, cliënten te adviseren en om hiervoor te factureren. Vervolgens worden deze gegevens na het passeren van deze akten bewaard om te voldoen aan bewaarplichten en om de notariële werkzaamheden te kunnen verantwoorden. Dit valt binnen de doelen uit de vrijstelling. Vervolgens mogen persoonsgegevens alleen verwerkt worden voor zover zij, gelet op deze doeleinden toereikend, ter zake dienend en niet bovenmatig zijn. Het gebruik van procedurelijsten binnen DKT draagt hieraan bij. Op deze lijsten staat precies aangegeven welke informatie nodig is om de zaak te kunnen afhandelen. Er wordt dus alleen informatie verzameld die relevant is voor het dossier. Voor het opstellen van een leveringsakte wordt bijvoorbeeld een inzage gedaan in het Kadaster, iets wat bij een schenking in de vorm van geld niet relevant is en dus ook niet gebeurt.

[192] Artikel 17 Wna.
[193] *Kamerstukken II* 1997/98, 25892, 3, p. 79.

Bij uitvoering van deze opdrachten verwerkt DKT ook bijzondere persoonsgegevens. Er worden persoonsgegevens over ras verwerkt in de vorm van de foto op het identiteitsbewijs, alsmede de nationaliteit en geboorteplaats van de cliënt op dit identiteitsbewijs en uit de inzage in de BRP. Notarissen zijn verplicht hun cliënten te identificeren.[194] De verwerking van deze gegevens is daarbij onvermijdelijk en daarmee toegestaan. De inzage in de BRP en het identiteitsbewijs bevatten ook het BSN. DKT heeft toegang tot het BRP op basis van een autorisatiebesluit.[195] In de toelichting op dit autorisatiebesluit worden notarissen aangeduid als overheidsorgaan in de zin van de Wet basisregistratie personen. Het begrip overheidsorgaan komt uit Wet algemene bepalingen burgerservicenummer.[196] Deze wet biedt overheidsorganen, waaronder dus DKT, de ruimte om het BSN te verwerken voor het uitvoeren van hun taak.[197] De verwerking van het BSN door DKT is dus wettelijk geregeld en daarmee toegestaan.

§ 5.3 Meldplicht bij verwerking en vrijstelling

DKT maakt, zoals eerder vermeld, gebruik van de vrijstelling voor juridische en financiële dienstverleners en meldt de verwerking van persoonsgegevens niet aan de AP. Om dit te kunnen doen, moet het kantoor zich aan verschillende eisen houden. Zoals eerder gesteld vallen de doelen waarvoor DKT de persoonsgegevens verzamelt binnen de grenzen van de vrijstelling. De verschillende soorten persoonsgegevens die DKT verwerkt zijn ofwel specifiek opgenomen in de vrijstelling of vallen onder gegevens die met het oog op behandeling van de zaak verwerkt worden. Zo is er bijvoorbeeld een inzage in het Kadaster nodig om een leveringsakte op te stellen. DKT verstrekt de persoonsgegevens alleen aan partijen die noodzakelijk betrokken zijn bij de juridische dienstverlening, bijvoorbeeld aan de KvK om een rechtspersoon op te richten. De geheimhoudingsplicht van de notaris draagt bij aan de naleving van deze eis.[198] Tenslotte moet er aan een bewaartermijn worden voldaan, wat in het geval van DKT een probleem vormt. Dit wordt behandeld in paragraaf 5.5.

§ 5.4 Informatieplicht

DKT moet de cliënt als verantwoordelijke informeren over de identiteit van het kantoor, de verwerkingsdoeleinden en eventueel extra informatie om een zorgvuldige verwerking te garanderen, zoals besproken in paragraaf 2.4. In de meeste gevallen doen cliënten zelf een beroep op DKT. In die gevallen mag worden aangenomen dat de identiteit van het kantoor bij hen bekend is. Als de cliënt niet zelf een beroep op DKT doet, bijvoorbeeld de verkoper van een woning waarbij de koper DKT als notaris heeft aangewezen, wordt de identiteit van het kantoor middels een brief aan de cliënt gemeld. Het kantoor moet in beide gevallen nog wel de verwerkingsdoeleinden mededelen aan de cliënten. De cliënt wordt op dit moment echter niet duidelijk geïnformeerd over deze verwerkingsdoeleinden. In het eerste bericht aan de cliënten wordt aangegeven welke informatie zij moeten aanleveren, zoals het identiteitsbewijs. Er wordt niet vermeld waarvoor deze gegevens verzameld en vervolgens bewaard worden. Ook de opdrachtbevestiging spreekt niet over verwerkingsdoeleinden. Hoewel het mogelijk voor de hand ligt dat DKT de persoonsgegevens verwerkt om bijvoorbeeld een akte op te stellen en om hiervoor te factureren, mag niet worden aangenomen dat de cliënt ook weet dat zijn gegevens vervolgens voor onbepaalde tijd bewaard worden om bijvoorbeeld aan een wettelijke bewaarplicht te voldoen of om op een later tijdstip de notariële werkzaamheden te kunnen verantwoorden.

[194] Artikel 39 lid 1 Wna.
[195] Autorisatiebesluit Koninklijke Notariële Beroepsorganisatie, Rijksdienst voor Identiteitsgegevens van 25 maart 2014, *Stcrt.* 2016, 8781.
[196] *Kamerstukken II* 2011/12, 33219, 3, p. 30.
[197] Artikel 1 sub c Wet algemene bepalingen burgerservicenummer jo. artikel 10 Wet algemene bepalingen burgerservicenummer.
[198] Artikel 22 Wna.

§ 5.5 Bewaren van persoonsgegevens

Omdat DKT op basis van het Vrijstellingsbesluit Wbp geen melding maakt van de verwerking van persoonsgegevens, mag het kantoor de verzamelde persoonsgegevens in principe maximaal twee jaar bewaren. Er wordt echter een uitzondering gemaakt voor bewaarplichten, waar DKT als notariskantoor mee te maken heeft (zie paragraaf 2.5.1). In die gevallen mogen de gegevens niet langer worden bewaard dan dat de plicht vereist. Deze uitzondering geeft DKT de wettelijke ruimte om gepasseerde akten maar ook de cliëntkaarten met daarin persoonsgegevens als onderdeel van het protocol van de notarissen eeuwig te bewaren, zoals verplicht in de Wna. Daarnaast worden de facturen voor de geleverde diensten 7 jaar bewaard, zoals de bewaarplicht uit de Awr vereist. Daarna worden de facturen vernietigd.

Het huidig beleid omtrent het bewaren van persoonsgegevens binnen DKT conflicteert op verschillende punten met de Wbp. Onder de Wbp mag een identiteitsbewijs 5 jaar lang bewaard worden om aan de bewaarplicht uit de Wwft te voldoen. Indien er een notariële akte is opgesteld, mogen de bescheiden die zijn voortgekomen uit de voorbereiding en afhandeling hiervan 20 jaar worden bewaard. In geval van milieuzaken is dit 30 jaar. Indien er geen bewaarplicht geldt, mogen de persoonsgegevens onder het Vrijstellingsbesluit Wbp maximaal 2 jaar bewaard worden. Onder het huidige beleid van DKT wordt het complete dossier voor onbepaalde tijd digitaal bewaard om de notariële werkzaamheden te kunnen verantwoorden. Om diezelfde reden bewaart DKT een groot aantal papieren dossiers van voor de digitalisatie, in een archief dat tientallen jaren omvat. De verschillende wettelijke bewaartermijnen gelden ook voor de persoonsgegevens in dit archief, ondanks dat een gedeelte hiervan verzameld is voordat de Wbp in 2001 in werking trad.[199] Met het bewaren van deze persoonsgegevens is er op dit moment namelijk sprake van een verwerking die onder de Wbp valt. Door complete dossiers voor onbepaalde tijd fysiek of digitaal op te slaan, handelt DKT na het verstrijken van de bewaartermijnen in strijd met een van de eisen uit de vrijstelling besproken in paragraaf 5.3. Dit betekent dat DKT op het moment van overschrijding niet is vrijgesteld van de meldplicht en de verwerking moet melden aan de AP. Tot op heden is dit niet gedaan, hoewel dit gezien de omvang van het archief van DKT, wel had moeten gebeuren.

§ 5.6 Beveiliging van persoonsgegevens

Als verantwoordelijke moet DKT passende technische en organisatorische maatregelen nemen tegen verlies of enige vorm van onrechtmatige verwerking van persoonsgegevens, zoals besproken in paragraaf 2.7. Naarmate persoonsgegevens gevoeliger van aard zijn, moeten er zwaardere eisen aan de beveiliging worden gesteld. DKT verwerkt veel gevoelige persoonsgegevens, waaronder bijzondere persoonsgegevens zoals de pasfoto op het identiteitsbewijs alsmede de nationaliteit en het BSN van de cliënt. Het kopie van het identiteitsbewijs en het BSN kunnen tevens misbruikt worden voor (identiteits)fraude. Ook gegevens over de financiële situatie van de cliënt, bijvoorbeeld over nalatenschappen, zijn gevoelige persoonsgegevens. Daarnaast worden persoonsgegevens die onder een bijzondere, wettelijke bepaalde geheimhoudingsplicht of beroepsgeheim vallen, aangemerkt als gevoelig (zie paragraaf 2.9.2). De notarissen en medewerkers van DKT zijn gebonden aan de notariële geheimhoudingsplicht.[200] Dit betekent dat alle persoonsgegevens waarvan zij uit hoofde van hun werkzaamheden kennis nemen, in geval van DKT vastgelegd in bijvoorbeeld de checklist of gespreksaantekeningen, worden aangemerkt als gevoelig. Omdat deze gevoelige persoonsgegevens onlosmakelijk onderdeel zijn van de verwerking van persoonsgegevens binnen DKT, moeten aan deze gehele verwerking zwaardere beveiligingseisen worden gesteld.

[199] Besluit van 5 juli 2001, houdende vaststelling van het tijdstip van inwerkingtreding van de Wet bescherming persoonsgegevens, *Stb.* 2001, 337.
[200] Artikel 22 Wna.

Er zijn veel overeenkomsten tussen de beveiligingsmaatregelen die DKT heeft geïmplementeerd en de beveiligingsmaatregelen die de AP als uitgangspunt hanteert. Zo wordt er op dit moment gewerkt aan een beleidsdocument voor alle medewerkers over de omgang met persoonsgegevens binnen DKT en is er een procedure om datalekken af te handelen. Tevens zijn de IT-voorzieningen fysiek beveiligd. De digitale dossiers worden namelijk opgeslagen op servers in een datacenter dat 24 uur per dag wordt bewaakt en beschikt over een systeem voor branddetectie. Voor de verbinding tussen DKT en het datacenter wordt gebruik gemaakt van encryptie. Toegang tot de gegevens in het digitale systeem is op verschillende manieren beveiligd. Medewerkers loggen op het digitale systeem in met een persoonlijke account, die beveiligd is met een wachtwoord dat iedere drie maanden wordt gewijzigd. De rechten ten aanzien van de gegevens in het systeem worden per type medewerker toegekend, ieder kwartaal gecontroleerd en indien nodig aangepast. In het kader van continuïteitsbeheer wordt er dagelijks een back-up van alle data en e-mail gemaakt en opgeslagen in een tweede datacenter. Tevens zijn de voedingen, harde schijven en netwerkverbindingen in deze datacenters meervoudig uitgevoerd, zodat DKT ondanks uitval van componenten toch toegang blijft houden tot haar gegevens.

Wanneer een dossier in behandeling is, ligt de papieren versie bij de behandelende medewerker op het bureau. Na de werkdag wordt het dossier niet opgeborgen in bijvoorbeeld een afgesloten dossierkast, hoewel de AP dit wel als beveiligingsmaatregel aanhaalt. Cliënten hebben in de meeste gevallen geen toegang tot ruimtes waar zich dossiers bevinden. De kamers van de notarissen zijn een zwak punt, omdat daar ook cliënten komen. Er wordt wel aangegeven dat medewerkers zicht hebben op cliënten die binnenkomen en op verschillende ruimtes waarin zij worden ontvangen. Dit is echter niet bij iedere ruimte het geval. Na het passeren van het dossier wordt de akte opgeslagen in een kluis. De rest van het papieren dossier wordt na het passeren verwijderd en vernietigd door een gespecialiseerd bedrijf, namelijk Box B.V. Dit gebeurt ook met documenten die bijvoorbeeld tijdens het aanmaken van een dossier dubbel of onjuist worden afgedrukt. Box B.V. is een gespecialiseerd en gecertificeerd bedrijf, wat de AP specifiek als beveiligingsmaatregel aanhaalt. Het archief van oude dossiers die niet zijn gedigitaliseerd, is op de verschillende vestigingen beveiligd met het alarmsysteem van het pand. Het deel van het archief opgeslagen bij BB Diensten is beveiligd met een alarm en codesloten. Daarnaast moet een bezoek vooraf door DKT worden aangekondigd en wordt er een logboek van bezoekers bijgehouden.

DKT heeft dus zowel technische als organisatorische beveiligingsmaatregelen getroffen om de verwerking van persoonsgegevens te beschermen. Echter is er op dit moment binnen het kantoor geen procedure om regelmatig te evalueren of de genomen beveiligingsmaatregelen zorgen voor een passend beveiligingsniveau. Bij het vaststellen of DKT voor een passend beveiligingsniveau heeft gezorgd, zijn ook de bewerkers die in de volgende paragraaf worden besproken van belang.

§ 5.7 De bewerker en de bewerkersovereenkomst

Zoals blijkt uit paragraaf 3.6 werkt DKT bij het verwerken van persoonsgegevens van cliënten samen met verschillende bewerkers. De persoonsgegevens worden opgeslagen op servers van ICT Concept, met behulp van Assyst dat geleverd wordt door Devoon. De fysieke dossiers worden na passeren vernietigd door Box B.V. en een deel van het archief staat opgeslagen bij BB Diensten. Met ICT Concept en Devoon zijn specifieke bewerkersovereenkomsten gesloten. Uit een analyse aan de hand van de checklist uit bijlage A blijkt dat de overeenkomsten grotendeels aan de eisen uit de Wbp voldoen. De ingevulde checklists zijn opgenomen in bijlagen P en Q. Een enkel aandachtspunt is dat de soorten persoonsgegevens niet zijn opgenomen, maar hiervoor wordt verwezen naar

de onderliggende overeenkomst. Daarnaast wordt er niet specifiek gesproken over geheimhouding.

De checklist is ook ingevuld voor de overeenkomsten met Box B.V. en BB Diensten. Uit deze analyse, opgenomen in bijlagen R en S**,** blijkt dat er aan meerdere eisen niet wordt voldaan. Ten eerste zijn er geen afzonderlijke bewerkersovereenkomsten gesloten. Ook zijn er in beide overeenkomsten geen concrete afspraken gemaakt over de meldplicht datalekken en over toezicht op de naleving van de genomen beveiligingsmaatregelen door DKT. Tenslotte zijn er geen afspraken gemaakt over geheimhouding en kunnen sub-bewerkers zonder toestemming van DKT worden ingeschakeld. Dit kan leiden tot een gebrek aan transparantie over de beveiliging en beveiligingsincidenten, wat negatieve invloed heeft op het passend beveiligingsniveau waar DKT voor moet zorgen.

§ 5.8 Meldplicht datalekken

Wanneer het beleid en de werkwijze van DKT ten aanzien van datalekken wordt vergeleken met de Wbp, vallen er een aantal zaken op. Elke situatie waarin niet kan worden uitgesloten dat er persoonsgegevens onrechtmatig zijn verwerkt, wordt consequent gemeld aan de AP. Gezien de gevoelige aard van bepaalde persoonsgegevens in een dossier (zie paragraaf 3.2) is het kantoor hier ook tot verplicht. Omdat een datalek van deze gevoelige persoonsgegevens ongunstige gevolgen kunnen hebben voor de persoonlijke levenssfeer van de betrokkene, is in deze situaties ook een melding aan de betrokkene vereist. DKT heeft dit in alle gevallen gedaan, behalve bij het datalek omschreven in paragraaf 3.7.1 waar de betrokkenen niet achterhaald konden worden.

Voor de melding aan de AP wordt gebruik gemaakt van het webformulier, waardoor automatisch de aard van de inbreuk, de instanties met meer informatie, de vermoedelijke gevolgen en de aanbevolen en genomen tegenmaatregelen worden opgenomen. In de gevallen dat DKT een datalek aan de betrokkene heeft gemeld, is daarbij altijd de aard van de inbreuk vermeld. Aangezien alle datalekken bij DKT zelf zijn ontstaan, was het kantoor het contactpunt met meer informatie. Er werden echter geen maatregelen aanbevolen om negatieve gevolgen te voorkomen. DKT houdt wel zoals verplicht een registratie van de datalekken bij. Het webformulier, de melding aan de betrokkene en andere relevante correspondentie wordt hierin per datalek opgeslagen.

Ten aanzien van het onverwijld melden van een datalek zijn er binnen DKT twee problemen. Ten eerste spreekt het huidige beleid over een termijn van twee werkdagen voor een melding aan de AP. Deze termijn, waarschijnlijk afkomstig uit de conceptversie van de beleidsregels opgesteld door de AP, is onjuist.[201] Een datalek moet zonder onnodige vertraging aan de AP worden gemeld, en zo mogelijk niet later dan 72 uur. Ook de melding aan de betrokkene moet onverwijld geschieden, wat betekent dat er gemeld moet worden wanneer er voldoende informatie beschikbaar is om de betrokkene behoorlijk en zorgvuldig te informeren. Ten tweede blijkt uit een analyse van het register van datalekken van DKT dat noch het huidige beleid, noch de wettelijke regels over onverwijld melden altijd gevolgd worden door de medewerkers. Zo is er in twee gevallen te laat gemeld aan de betrokkene en bij een van deze gevallen ook te laat aan de AP. Sinds de e-mail over datalekken aan alle medewerkers lijkt dit te verbeteren, aangezien het meest recente datalek binnen 72 uur gemeld is aan zowel de AP als de betrokkene.

§ 5.9 Sancties

Zoals besproken in paragraaf 2.10 kan de AP sinds de invoering van de meldplicht datalekken hogere boetes opleggen voor het overtreden van de Wbp. DKT riskeert met handhaving van de huidige werkwijze en het huidige beleid verschillende boetes, mits de

[201] Peter Kager, 'Vijf misverstanden over de meldplicht datalekken', *ICTRecht.nl*, 30 december 2015.

AP niet eerst een bindende aanwijzing zal doen. Op het niet voldoen aan de informatieplicht en de beveiligingsplicht staat een basisboete van €120.000 tot €500.000. Deze basisboete kan ook worden opgelegd voor het overtreden van de maximale bewaartermijn of het niet voldoen aan de meldplicht datalekken. Op het niet melden van een verwerking van persoonsgegevens en het niet hebben van een deugdelijke bewerkersovereenkomst staat echter geen boete.

Hoewel DKT voor boetes ten aanzien van datalekken verzekerd is, kan de AP ook voor andere overtredingen een boete opleggen. Daarbij zal de AP hoogstwaarschijnlijk eerst een bindende aanwijzing opleggen voordat er tot beboeting wordt overgegaan. De AP is daarnaast niet terughoudend met het publiceren van informatie over overtreders.[202] Deze vorm van 'naming and shaming' kan leiden tot reputatieschade voor DKT. Dit kan ervoor zorgen dat potentiële cliënten voor een ander notariskantoor kiezen, met de financiële gevolgen van dien.

[202] M. Jansen, 'Wat het verleden ons kan leren over handhaving door de Autoriteit Persoonsgegevens', *Dirkzwager Intellectuele eigendom & IT* 24 april 2017, dirkzwagerieit.nl.

Hoofdstuk 6: DKT en de AVG

Dit hoofdstuk behandelt de AVG in relatie tot het huidige beleid en de huidige werkwijze van DKT. Er wordt gekeken in hoeverre de huidige gang van zaken binnen DKT voldoet aan de eisen die de AVG vanaf 25 mei 2018 aan de omgang met persoonsgegevens zal stellen. Deze vergelijking vormt de basis voor de aanbevelingen aan DKT over de omgang met persoonsgegevens van cliënten na het van toepassing worden van de AVG.

§ 6.1 Toepassingsgebied en betrokken partijen

Het materieel toepassingsgebied van de verordening is zoals besproken in paragraaf 4.1 hetzelfde als dat van de Wbp. De verwerking van persoonsgegevens door DKT valt dus ook onder de AVG en het kantoor blijft hierbij de verantwoordelijke. De cliënt is daarbij nog steeds de betrokkene. De FG krijgt in de AVG een grotere rol toebedeeld. De verantwoordelijke die een overheidsinstantie- of orgaan is, op grote schaal regelmatig en stelselmatig op grote schaal betrokkenen observeert of hoofdzakelijk bijzondere persoonsgegevens verwerkt, moet onder de AVG namelijk een FG aanstellen. Hoewel DKT bijvoorbeeld in de Wet basisregistratie personen onder het begrip overheidsorgaan valt (zie paragraaf 5.2) is het onduidelijk of dit ook in de AVG het geval is. De AVG geeft namelijk zelf geen definitie van het begrip. De Artikel 29 werkgroep, die bestaat uit de nationale privacytoezichthouders in de EU, noemt onder andere de rijksoverheid en instanties die zich bezighouden met het openbaar vervoer en water- en stroomvoorziening.[203] Als de notaris als overheidsorgaan in de zin van de AVG zou worden aangemerkt, zou dit betekenen dat ook notarissen die hun beroep solitair uitoefenen verplicht worden een FG aan te stellen. Hierop gelet zal de notaris niet onder het begrip overheidsorgaan zoals bedoeld in de AVG vallen en is DKT niet verplicht een FG aan te stellen.

§ 6.2 Vereisten aan verwerking

DKT moet als verantwoordelijke zorgen dat de verwerking van persoonsgegevens voldoet aan de vereisten uit de AVG. Deze vereisten komen grotendeels overeen met de vereisten uit de Wbp. Ten aanzien van de verwerkingsdoeleinden verandert er echter wat voor DKT. De welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden waar DKT de verwerking op baseert, komen uit het Vrijstellingsbesluit Wbp dat net als de Wbp met het van toepassing worden van de AVG zal vervallen.[204] Op dit moment heeft DKT zelf geen welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde verwerkingsdoeleinden vastgelegd.

De verwerking van bijzondere persoonsgegevens door DKT, namelijk de foto op het identiteitsbewijs, de nationaliteit en het BSN, is ook onder de AVG toegestaan. De verwerking van het identiteitsbewijs en de nationaliteit van de cliënt is namelijk noodzakelijk om hem of haar te identificeren, een wettelijke verplichting van de notaris.[205] Daarnaast blijft de uitzondering waaronder DKT het BSN mag verwerken, besproken in paragraaf 4.2 en 5.2, van kracht door de beleidsneutrale uitvoering van de AVG.

De AVG koppelt een verantwoordingsplicht aan de vereisten die aan de verwerking gesteld worden, zoals besproken in paragraaf 4.2.1. DKT moet aan kunnen tonen dat aan alle vereisten aan de verwerking van persoonsgegevens is voldaan. Groter is de verplichting om aan te kunnen tonen dat de gehele verwerking van persoonsgegevens aan de AVG voldoet, bijvoorbeeld door middel van een gegevensbeschermingsbeleid, aansluiting bij goedgekeurde gedragscodes of certificeringsmechanismen of het voldoen aan de registratieplicht die wordt behandeld in paragraaf 6.3. Binnen DKT wordt op dit moment gewerkt aan beleid gericht op persoonsgegevens, onder andere gericht op

[203] Richtlijnen voor functionarissen voor de gegevensbescherming (FG's) 2017, p. 5.
[204] Artikel 46 wetsvoorstel Uitvoeringswet Algemene verordening gegevensbescherming.
[205] Artikel 9 lid 2 sub b AVG jo. artikel 39 Wna.

datalekken en beveiliging. Ook is er een procedure voor datalekken en is de beveiliging van de digitale systemen vastgelegd. DKT is op dit moment niet aangesloten bij een gedragscode of certificeringsmechanisme ten aanzien van persoonsgegevens.

De begrippen privacy by design en privacy by default zijn ook voor DKT relevant. Met inachtneming van privacy by design zal DKT in de toekomst, bijvoorbeeld bij de ontwikkeling van nieuw beleid over het opstellen van en omgaan met dossiers, aandacht moeten besteden aan privacyverhogende maatregelen. Met het gebruik van de procedurelijsten zorgt het kantoor er nu al voor dat er zo min mogelijk persoonsgegevens worden verzameld. Dit moet volgens privacy by default de standaard zijn. Echter wordt deze dataminimalisatie niet doorgevoerd wanneer er wordt gelet op de bewaartermijn, die in paragraaf 6.5 aan bod komt.

§ 6.3 Registratieplicht verwerkingsactiviteiten

De plicht om de verwerking van persoonsgegevens te melden aan de AP wordt vervangen door een registratieplicht zoals besproken in paragraaf 4.3. Deze plicht geldt ook voor DKT, ondanks dat het kantoor geen 250 personen in dienst heeft. Dit criterium vervalt namelijk omdat de verwerking van persoonsgegevens door DKT niet incidenteel is. Bepaalde informatie die op grond van de registratieplicht moet worden vastgelegd, zoals de categorieën van persoonsgegevens en een omschrijving van technische beveiligingsmaatregelen, is al opgenomen in afzonderlijke documenten zoals procedurelijsten. Ook de naam en contactgegevens van de verantwoordelijke zijn logischerwijs voorhanden. Deze informatie wordt echter op dit moment niet samengebracht in een register. Er zijn ook gegevens die DKT nog niet heeft geregistreerd, zoals de verwerkingsdoeleinden, de categorieën van betrokkenen en de categorieën van ontvangers van persoonsgegevens. Ook ontbreekt een beoogde termijn waarbinnen de verschillende categorieën persoonsgegevens gewist moeten worden en zijn organisatorische beveiligingsmaatregelen niet vastgelegd.

§ 6.4 Informatieplicht

Wanneer de uitgebreide informatieplicht van de AVG wordt vergeleken met de informatie die DKT verstrekt aan cliënten, blijkt dat deze informatie grotendeels tekortschiet. De contactgegevens van de verantwoordelijke (het kantoor) worden verstrekt. Hoewel het gezien de verwerking van persoonsgegevens door DKT wel is vereist, wordt de cliënt niet geïnformeerd over:

- de verschillende verwerkingsdoeleinden, waaronder het opstellen van akten, het adviseren van cliënten, het voldoen aan bewaarplichten, de verantwoording van notariële werkzaamheden en de facturering;
- de rechtsgrond van de verwerking, namelijk het uitvoeren van een overeenkomst waarbij de betrokkene partij is en het voldoen aan wettelijke verplichtingen;
- de (categorieën van) ontvangers van de persoonsgegevens, zoals het Kadaster of de KvK;
- de bewaartermijn van de persoonsgegevens of de criteria op basis waarvan deze wordt vastgesteld;
- de rechten die hij of zij heeft (zie paragraaf 2.6 en 4.6);
- de mogelijkheid tot het indienen van een klacht bij de AP.

DKT verzamelt niet alleen persoonsgegevens bij de betrokkene zelf. Er worden ook andere bronnen geraadpleegd, zoals de BRP. Daarom moet het kantoor de betrokkene ook informeren over welke categorieën van persoonsgegevens uit deze bronnen wordt verwerkt, welke bronnen dit zijn en of deze openbaar zijn. Ook deze informatie wordt niet verstrekt.

§ 6.5 Bewaren van persoonsgegevens

Onder de AVG vervalt de verplichting om de verwerking van persoonsgegevens te melden aan de AP, de daaraan verbonden vrijstellingen en de daarin vastgelegde

bewaartermijn. In plaats daarvan zal DKT zich moeten houden aan de strikt minimale bewaartermijn die de AVG voorschrijft, zoals beschreven in paragraaf 4.5. Wat dit strikt minimum is, is afhankelijk van de verwerkingsdoeleinden die DKT op basis van de registratieplicht zelf moet vaststellen. Het kantoor verzamelt de persoonsgegevens in beginsel om akten op te stellen en cliënten te adviseren. Dit is het primaire doel van de verwerking. De persoonsgegevens worden daarna bewaard voor andere doeleinden, namelijk om te voldoen aan verschillende wettelijke bewaarplichten, om de notariële werkzaamheden verifieerbaar te houden en om de werkzaamheden in rekening te kunnen brengen (zie paragraaf 2.5.1 en 3.4). Gelet op het verband tussen deze doeleinden, het kader waarin de gegevens zijn verzameld en de beveiligingsmaatregelen die DKT heeft getroffen, kan worden gesteld dat deze andere doeleinden verenigbaar zijn met het primaire doel zoals de AVG eist.

Op basis van deze doeleinden moet DKT een strikt minimale bewaartermijn vaststellen voor de verschillende persoonsgegevens die worden verwerkt. Dit heeft het kantoor tot op heden niet gedaan. De strikte bewaartermijn uit de AVG geldt ook voor persoonsgegevens die voor het van toepassing worden van de verordening zijn verzameld. Net zoals besproken in paragraaf 5.5 is er op dat moment namelijk sprake van een verwerking die onder de AVG valt. Het ligt voor de hand dat de akte en de cliëntkaart eeuwig worden bewaard. Als onderdeel van het protocol van de notaris is dit namelijk wettelijk verplicht. Echter wordt onder het huidig beleid het gehele dossier voor onbepaalde tijd fysiek of digitaal opgeslagen. Dit staat per definitie haaks op de strikt minimale opslagperiode die de AVG voorschrijft.

§ 6.6 Beveiliging van persoonsgegevens

Net als de Wbp eist de AVG dat DKT voor een passend beveiligingsniveau zorgt. De punten genoemd in paragraaf 5.6 blijven dan ook onder de AVG relevant. De AVG geeft daarnaast zelf suggesties over beveiligingsmaatregelen. Vergeleken met de beveiliging van DKT zijn er verschillende overeenkomsten met deze suggesties te ontdekken. Onder ander is de verbinding tussen DKT en het datacenter versleuteld. Daarnaast heeft DKT, samen met ICT Concept, dankzij de meervoudig uitgevoerde servers en regelmatige back-ups, het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en toegang tot de persoonsgegevens te herstellen. Er zijn echter ook maatregelen die de AVG noemt die DKT (nog) niet heeft genomen. Zo is de verbinding tussen het kantoor en het datacenter wel versleuteld, maar de data op de servers niet. Ook is er geen procedure om op gezette tijdstippen de technische en organisatorische beveiligingsmaatregelen te testen, beoordelen en evalueren. Dit sluit aan bij het in paragraaf 5.6 vermelde feit dat DKT geen procedure heeft om regelmatig te evalueren of de huidige beveiligingsmaatregelen nog leiden tot een passend beveiligingsniveau.

Op basis van de verantwoordingsplicht moet DKT kunnen aantonen dat er sprake is van een passend beveiligingsniveau. Dit kan onder andere door middel van certificering en aansluiting bij een goedgekeurde gedragscode. Dit is nu nog geen optie voor DKT, maar mogelijk in de toekomst wel. Op dit moment wordt er namelijk door Stichting Rechtszekerheid Digitaal, een onafhankelijke stichting opgericht door de KNB, gewerkt aan de Baseline Informatiebeveiliging Notariaat.[206] Dit is een kwaliteitshandboek voor informatiebeveiliging binnen het notariaat, met daarin normen die zijn afgeleid van ISO standaarden voor informatiebeveiliging. Twee bewerkers van DKT zijn al wel gecertificeerd. Zo is ICT Concept gecertificeerd op het gebied van informatiebeveiliging en is Box B.V. gecertificeerd op het gebied van kwaliteitsmanagement ten aanzien van archiefpapier en op het gebied van archief- en datavernietiging. Net als onder de Wbp spelen de bewerkers ook onder de AVG een rol bij het bepalen of DKT voor een passend beveiligingsniveau heeft gezorgd.

[206] Van Almelo, *Notariaat Magazine* 2017, editie 1, p. 10-11.

Geheel nieuw is dat de AVG in bepaalde gevallen een PIA verplicht stelt (paragraaf 4.7.1). Dit zal niet gelden voor DKT. Het kantoor doet namelijk niet aan profilering, noch aan grootschalige verwerking van bijzondere persoonsgegevens of aan stelselmatige en grootschalige monitoring van openbare ruimtes.

§ 6.7 De bewerker en de bewerkersovereenkomst
Zoals beschreven in paragraaf 5.7 werkt DKT bij het verwerken van persoonsgegevens van cliënten samen met vier bewerkers. Met de bewerkers zijn overeenkomsten gesloten. In het geval van ICT Concept en Devoon zijn dit specifieke bewerkersovereenkomsten. Deze bewerkersovereenkomsten zijn geanalyseerd aan de hand van de checklist uit bijlage B. Uit deze analyse, opgenomen in bijlagen P en Q, blijkt dat de bewerkersovereenkomsten ook grotendeels aan de eisen van de AVG voldoen. De aandachtspunten uit paragraaf 5.7 met betrekking tot de soort persoonsgegevens en de geheimhoudingsplicht zijn ook hier van toepassing. Het enige nieuwe punt van aandacht dat naar voren komt, is het ontbreken van de categorieën van betrokkenen.

Uit de analyse van de overeenkomsten met Box B.V. en BB Diensten, opgenomen in bijlagen R en S, blijkt dat deze net als onder de Wbp grotendeels niet voldoen aan de wettelijke eisen. Ook in deze overeenkomsten wordt het soort persoonsgegevens en de categorieën van betrokkenen niet vermeld. Er wordt daarnaast niet gesproken over geheimhouding, een passend beveiligingsniveau wordt niet gegarandeerd en er zijn geen afspraken gemaakt over de meldplicht datalekken. Tevens zijn er geen of onvoldoende afspraken gemaakt over sub-bewerkers, het voldoen aan verzoeken van betrokkenen, het na afloop van de verwerking teruggeven van de persoonsgegevens en over de controle op naleving van deze afspraken. Net als onder de Wbp kan het ontbreken van deze afspraken leiden tot een gebrek aan transparantie ten aanzien van de verwerkingen die deze bewerkers verrichten, met negatieve invloed op het passend beveiligingsniveau tot gevolg.

§ 6.8 Meldplicht datalekken
Wanneer de AVG wordt toegepast op het beleid en de werkwijze van DKT met betrekking tot datalekken, vallen de volgende zaken op. Tot nu toe heeft DKT melding gemaakt van alle situaties waarin niet kon worden uitgesloten dat er persoonsgegevens onrechtmatig waren verwerkt. De AVG ziet deze situaties niet langer als datalek. Hoewel DKT op dit moment dergelijke situaties consistent meldt, hoeft het kantoor een datalek onder de AVG alleen te melden wanneer vaststaat dat het datalek zich daadwerkelijk heeft voorgedaan.

Onder de AVG kan van de melding aan de AP worden afgezien wanneer het niet waarschijnlijk is dat het datalek een risico inhoudt voor de rechten en vrijheden van de betrokkene.[207] Gezien de gevoelige aard van de gegevens die DKT verwerkt, zal een dergelijke situatie zich niet snel voordoen. Voor de melding aan de AP maakt DKT gebruik van het webformulier. Als het datalek waarschijnlijk een hoog risico vormt voor de rechten en vrijheden van de betrokkene, moet het datalek ook aan de betrokkene worden gemeld.[208] Opnieuw gelet op de gevoelige aard van de gegevens die DKT verwerkt, zal een datalek waarschijnlijk een hoog risico vormen voor bijvoorbeeld de privacy van de betrokkene. DKT zal in de meeste gevallen ook melding moeten doen aan de betrokkene, wat tot nu toe ook gedaan is. Een enkele keer, beschreven in paragraaf 3.7.1, heeft DKT geen melding gedaan aan betrokkenen, omdat niet achterhaald kon worden op welke cliënten de mogelijk gelekte informatie betrekking had. Als er onder de AVG wordt afgezien van de melding aan de betrokkene omdat dit onevenredige inspanning zou

[207] Artikel 33 lid 1 AVG.
[208] Artikel 34 lid 1 AVG.

vergen, is een openbare mededeling vereist.[209] Een dergelijke mededeling zou, helemaal gezien de bijzondere maatschappelijke positie van een notaris, voor reputatieschade kunnen zorgen.

Op basis van wettelijke eisen moet de melding aan de AP onder de AVG meer informatie bevatten dan de melding aan de AP onder de Wbp. Echter zal DKT door gebruik te maken van het webformulier ook aan deze eisen voldoen. Als DKT het datalek meldt aan de betrokkene, moeten onder de AVG ook de waarschijnlijke gevolgen van het datalek en de door het kantoor genomen maatregelen worden vermeld. Op dit moment wordt de betrokkene alleen geïnformeerd over de aard van het datalek en gegevens van een contactpunt met meer informatie. Ook de reeds onder de Wbp verplichte aanbevolen maatregelen worden niet vermeld.

Deze melding aan de betrokkene hoeft onder de AVG niet opgenomen te worden in de registratie van datalekken, hoewel dit wel voor de hand ligt. Deze registratieplicht omtrent datalekken wordt op een ander punt uitgebreid, wat betekent dat DKT ook de inbreuken op de beveiliging moet registreren die niet tot een melding leiden. Op dit moment worden alleen de door DKT gemelde datalekken geregistreerd. Tenslotte blijven de eisen omtrent onverwijld melden hetzelfde en het probleem beschreven in paragraaf 5.8 blijft dus bestaan.

§ 6.9 Sancties

Met het van toepassing worden van de AVG wordt de boetebevoegdheid van de AP nogmaals uitgebreid (zie paragraaf 4.10). Net als in paragraaf 5.9 riskeert DKT met handhaving van de huidige werkwijze en het huidige beleid verschillende boetes. Het in strijd handelen met de beginselen van de verwerking van persoonsgegevens, zoals het hanteren van een strikt minimale bewaartermijn, kan bestraft worden met een boete van maximaal €20.000.000 of 4% van de totale wereldwijde jaaromzet als dit bedrag hoger is. Dit geldt ook voor het niet voldoen aan de informatieplicht richting de betrokkene. De lagere boete, van maximaal €10.000.000 of 2% van de totale wereldwijde jaaromzet als dit bedrag hoger is, kan worden opgelegd voor het overtreden van bepalingen omtrent privacy by design en default, bewerkersovereenkomsten, de registratieplicht voor verwerkingsactiviteiten en de meldplicht datalekken. Hoewel bij het bepalen van deze boete ook rekening wordt gehouden met de omstandigheden van het geval, moet worden opgemerkt dat drempel om een boete op te leggen in de vorm van de bindende aanwijzing komt te vervallen. De AP kan onder de AVG direct overgaan tot het opleggen van boetes.

Naast boetes kan de AP ook corrigerende maatregelen opleggen, zoals een berisping, een last om de verwerking in overeenkomst met de AVG te brengen of een verwerkingsbeperking of -verbod. De mogelijkheid om een last onder bestuursdwang of dwangsom blijft tevens bestaan. Ook onder de AVG kan de AP overgaan tot ‘naming and shaming’ van overtreders van de verordening. Net zoals onder de Wbp kan dit gevolgen hebben voor de reputatie van DKT. De negatieve publiciteit kan financiële consequenties hebben, zoals potentiële cliënten die voor een notariskantoor kiezen dat niet negatief in het nieuws is. Een sanctie in de vorm van een verwerkingsbeperking of -verbod kan echter nog grotere gevolgen hebben voor DKT. Als gevolg van een dergelijk verbod of dergelijke beperking komt namelijk een gedeelte van de werkzaamheden binnen het kantoor stil te liggen.

[209] Artikel 34 lid 3 AVG.

Hoofdstuk 7: Conclusies en aanbevelingen

Welke aanbevelingen kunnen aan DKT worden gedaan over de omgang met persoonsgegevens van cliënten, gelet op een analyse van de Wet bescherming persoonsgegevens en de Algemene verordening gegevensbescherming? Deze vraag staat in dit onderzoek centraal. Als notariskantoor verwerkt DKT veel persoonsgegevens van cliënten bij het leveren van haar diensten. Gezien de gevoeligheid van sommige van deze persoonsgegevens is het belangrijk om de privacy van cliënten te waarborgen. Als verantwoordelijke moet DKT zich tot 25 mei 2018 aan de Wbp houden en daarna aan de eisen uit de AVG. Op basis van de vergelijking gemaakt in hoofdstuk 5 en 6 kunnen de volgende conclusies worden getrokken, aan de hand waarvan verschillende aanbevelingen kunnen worden gedaan. Eerst wordt ingegaan op de gevallen waarin DKT niet voldoet aan eisen uit de Wbp die onder de AVG verder worden aangescherpt. Dit zijn de eisen aan de informatieplicht, de bewaartermijn, de beveiliging van persoonsgegevens en aan de bewerkersovereenkomsten. Daarna komt de meldplicht datalekken aan bod, die niet wordt aangescherpt maar wordt gewijzigd. Vervolgens komen de aandachtspunten aan bod die specifiek voor de AVG gelden, namelijk het vaststellen van verwerkingsdoeleinden en het voldoen aan de verantwoordings- en registratieplicht.

Informeren van betrokkene

Op dit moment voldoet DKT niet aan de informatieplicht die in de Wbp is voorgeschreven. De cliënten worden namelijk niet geïnformeerd over de doeleinden waarvoor DKT hun persoonsgegevens verwerkt, terwijl dit wel is verplicht. Het opnemen van de verwerkingsdoeleinden in de eerste communicatie richting de cliënt, bijvoorbeeld de opdrachtbevestiging of eerste brief, zal tijd kosten. Omdat de AVG relatief snel van toepassing wordt, is het beter om de informatieverstrekking gelijk af te stemmen op de eisen uit de AVG.

De informatieplicht wordt in de AVG namelijk met meerdere elementen uitgebreid en de cliënten van DKT worden over het merendeel niet geïnformeerd. Om aan de informatieplicht uit de AVG te voldoen, moet DKT de cliënten informeren over de elementen besproken in paragraaf 6.4. De informatie moet kosteloos in een beknopte, duidelijke, begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal verstrekt worden. De cliënt moet over veel zaken omtrent de verwerking van zijn persoonsgegevens worden geïnformeerd, wat het lastig maakt om deze informatie op te nemen in bijvoorbeeld een eerste brief of opdrachtbevestiging. DKT kan het beste aan de informatieplicht voldoen middels een los document, bijvoorbeeld in de vorm van een privacyverklaring die net als de algemene voorwaarden aan de cliënt wordt verstrekt. Daarmee is DKT er zeker van dat de cliënt daadwerkelijk beschikking krijgt over deze informatie, iets wat bijvoorbeeld met een verwijzing naar een online privacyverklaring niet altijd het geval is. Tevens wordt daarmee voorkomen dat opdrachtbevestigingen en eerste brieven naar cliënten moeten worden aangepast.

Bewaartermijn herzien

DKT meldt op dit moment de verwerking van persoonsgegevens niet aan de AP op basis van de vrijstelling voor juridische en financiële dienstverleners. Om een beroep te kunnen doen op deze vrijstelling moet er aan verschillende eisen worden voldaan, waaronder een bewaartermijn die uitvoerig is besproken in paragraaf 2.5. DKT handelt op dit moment in strijd met deze bewaartermijn, aangezien alle persoonsgegevens in een dossier onder het huidige beleid ofwel digitaal ofwel fysiek voor onbepaalde tijd worden bewaard. DKT heeft hier twee opties. Het kantoor moet ofwel persoonsgegevens waarvan de bewaartermijn wordt overschreden verwijderen, ofwel de verwerking van persoonsgegevens melden aan de AP. Gezien de hoeveelheid dossiers en het feit dat de dossiers mogelijk op een later tijdstip nodig zijn om de notariële werkzaamheden te verantwoorden, is het melden van de verwerking aan de AP op de korte termijn de beste optie. Op de lange termijn, in aanloop

naar de AVG, zal het kantoor echter stappen moeten ondernemen om persoonsgegevens na een bepaalde termijn te gaan verwijderen.

Het huidig beleid van DKT ten aanzien van het bewaren van persoonsgegevens is namelijk ook in strijd met de AVG, aangezien het voor onbepaalde tijd bewaren van complete dossiers met daarin persoonsgegevens haaks staat op de strikt minimale bewaartermijn die de AVG voorschrijft. Ook is het in strijd met de minimale gegevensverwerking die door het begrip privacy by default wordt voorgeschreven. DKT moet op basis van de verwerkingsdoeleinden afwegen wat de strikt minimale bewaartermijn is voor de persoonsgegevens die het kantoor verzamelt. Als er voor een bepaald document met persoonsgegevens een wettelijke bewaarplicht geldt, is de strikt minimale bewaartermijn logischerwijs de duur van die bewaarplicht. Ten aanzien van gegevens waarvoor geen bewaarplicht (meer) geldt, moet DKT zich afvragen hoe lang het kantoor deze persoonsgegevens na het afhandelen van het dossier nog nodig heeft om de notariële werkzaamheden te verantwoorden. Deze afwegingen moeten op basis van de hierna besproken registratieplicht worden vastgelegd, zodat kan worden aangetoond dat er een strikt minimale bewaartermijn wordt aangehouden. Op basis van deze afwegingen moet DKT vaststellen welke persoonsgegevens in papieren of digitale vorm niet langer nodig zijn, om deze persoonsgegevens vervolgens te verwijderen. De dossiervoering is nu vooral digitaal en om het aanhouden van een minimale bewaartermijn in de toekomst te vergemakkelijken, kan er gezocht worden naar een softwarematige oplossing. Een voorbeeld hiervan is het toekennen van een bewaartermijn aan bepaalde documenten of een compleet dossier, waarna Assyst enkele dagen voor het einde van deze termijn hiervan melding maakt aan de medewerker of notaris die de zaak heeft behandeld. Vervolgens kan deze persoon, bijvoorbeeld op basis van de complexiteit van een zaak, het verwijderen van deze gegevens goed- of afkeuren.

Beveiliging aanscherpen en bewerkersovereenkomsten sluiten
Als verantwoordelijke moet DKT onder de Wbp zorgen voor een passend beveiligingsniveau. Het kantoor heeft samen met ICT Concept en Devoon uitgebreide technische beveiligingsmaatregelen getroffen. Met deze twee bewerkers zijn bewerkersovereenkomsten gesloten die aan bijna alle eisen uit de Wbp voldoen. De beveiliging schiet ten aanzien van de papieren dossiers echter tekort. De gepasseerde akten worden opgeslagen in een kluis maar de papieren dossiers zijn alleen beveiligd met het alarmsysteem van het pand. Met de twee bewerkers die bij de papieren dossiervoering betrokken zijn, Box B.V. en BB Diensten, zijn tevens geen goede bewerkersovereenkomst gesloten. Dit kan leiden tot een gebrek aan transparantie over bijvoorbeeld beveiligingsincidenten. Tenslotte heeft DKT geen procedure ingesteld om regelmatig te evalueren of de genomen beveiligingsmaatregelen zorgen voor een passend beveiligingsniveau. Dit alles maakt dat DKT op dit moment geen passend beveiligingsniveau hanteert. Om de beveiliging naar een passend niveau te tillen zal DKT verschillende maatregelen moeten treffen. Door papieren dossiers aan het eind van de werkdag op te bergen in afsluitbare dossierkasten wordt er een extra laag van beveiliging gecreëerd. Voorwaarde is wel dat de dossierkast wordt afgesloten wanneer de medewerker niet aanwezig is. Een andere optie is het afsluiten van de kantoorruimtes waar de dossiers zich bevinden. Ook moet er een procedure worden ingesteld om regelmatig te evalueren of alle genomen beveiligingsmaatregelen leiden tot een passend beveiligingsniveau. Tenslotte moet de samenwerking met Box B.V. en met BB Diensten geregeld worden middels kloppende bewerkersovereenkomsten. Gelet op de relatief korte periode tot het van toepassing worden van de AVG, is het voor DKT de beste optie om ervoor te zorgen dat deze overeenkomsten aan de eisen uit de AVG voldoen.

Net als bij de informatieplicht en de bewaartermijn scherpt de AVG namelijk ook de eisen aan de bewerkersovereenkomst aan. De beveiliging van persoonsgegevens moet opnieuw passend zijn. Hoewel de bewerkersovereenkomsten met ICT Concept en

Devoon grotendeels aan de eisen van de AVG voldoen en door DKT getroffen technische beveiligingsmaatregelen overeenkomsten vertonen met de maatregelen die de verordening noemt, blijft de papieren dossiervoering het zwakke punt. Daarnaast voldoen de overeenkomsten met Box B.V. en BB Diensten niet aan de eisen uit de AVG. Dit betekent dat DKT ook onder de AVG niet heeft gezorgd voor een passend beveiligingsniveau. Met BB Diensten en Box B.V. moeten bewerkersovereenkomsten gesloten worden die voldoen aan de eisen uit de AVG. Daarvoor kan gebruik worden gemaakt van de checklist in bijlage B. Daarmee zullen deze overeenkomsten ook op de lange termijn aan de wettelijke eisen voldoen. Naast de hierboven genoemde aanbevelingen ten aanzien van de beveiliging, zoals het instellen van een evaluatieprocedure en het gebruik van afgesloten dossierkasten, suggereert de AVG nog verdere beveiligingsmaatregelen. Zo kan de procedure om de beveiligingsmaatregelen te evalueren worden aangevuld met het op gezette tijdstippen testen en beoordelen van de beveiliging. Een dergelijke test, bijvoorbeeld in de vorm van een gesimuleerd beveiligingsincident, kan zwakke plekken in de beveiliging blootleggen en medewerkers bewuster maken van de gevolgen van een datalek en hoe zij hier mee om moeten gaan. Een andere mogelijke beveiligingsmaatregel is het versleutelen van digitale dossiers nadat deze zijn gepasseerd, wat de impact van een inbreuk op de digitale beveiliging kan beperken. Tenslotte kan de in paragraaf 6.6 genoemde Baseline Informatiebeveiliging Notariaat, nadat deze is gepubliceerd, als handboek worden gebruikt bij het beveiligen van de verwerking van persoonsgegevens binnen DKT.

Beleid meldplicht datalekken aanpassen
Met betrekking tot de meldplicht datalekken uit de Wbp is DKT tot nu toe consequent geweest in het melden aan de AP en wanneer mogelijk ook aan de betrokkene. DKT heeft grotendeels voldaan aan de inhoudelijke eisen die aan de meldingen worden gesteld. Er worden alleen geen maatregelen aan de betrokkene aanbevolen, wat wel wordt vereist. Zoals verplicht worden de meldingen opgenomen in een register, samen met alle relevante correspondentie. In enkele gevallen heeft DKT een datalek niet onverwijld gemeld. Ook het huidige beleid omtrent onverwijld melden, dat spreekt over een termijn van twee werkdagen voor de melding aan de AP en geen termijn noemt voor de melding aan de betrokkene, klopt niet. Desondanks is het meest recente datalek wel onverwijld gemeld aan zowel de betrokkene als de AP. Hoewel de werkwijze van DKT met betrekking tot datalekken grotendeels in lijn is met de Wbp, moet het beleid met betrekking tot het onverwijld melden van datalekken dus worden gewijzigd. De termijn voor de melding aan de AP moet worden aangepast naar 72 uur vanaf het moment van ontdekking. Daarnaast moet worden opgenomen dat de melding aan de betrokkene ook onverwijld moet geschieden, wat inhoudt dat er gemeld moet worden op het moment dat DKT voldoende informatie heeft om de betrokkene behoorlijk en zorgvuldig te informeren. Drs. R. Nijnens, kantoordirecteur en coördinator op het gebied van datalekken binnen DKT, zal op de naleving van deze termijnen moeten toezien. Indien mogelijk moet de betrokkene ook worden geïnformeerd over maatregelen die hij zelf kan treffen. Door de bovenstaande wijzigingen door te voeren en te volgen, zal DKT voldoen aan de meldplicht datalekken uit de Wbp.

De meldplicht datalekken wordt in de AVG niet zozeer aangescherpt, maar gewijzigd. Onder de AVG wordt het begrip datalek namelijk versmald naar situaties waarin vaststaat dat er persoonsgegevens zijn gelekt. Situaties waarin niet redelijkerwijs kan worden uitgesloten dat er persoonsgegevens zijn gelekt, worden niet langer als datalek gezien. Ter vervanging daarvan moet elke inbreuk op de beveiliging geregistreerd worden, onafhankelijk van het feit of hier melding van wordt gemaakt of niet. Ook moet er volgens de AVG meer informatie aan de AP en aan de betrokkene worden medegedeeld. De eisen omtrent onverwijld melden blijven hetzelfde. Als gevolg van deze wijzigingen zal DKT het beleid omtrent datalekken, na het van toepassing worden van de AVG, opnieuw moeten aanpassen. In het beleid moet worden opgenomen dat alleen situaties waarin

vaststaat dat er sprake is van een datalek gemeld moeten worden. DKT moet onder de AVG wel alle inbreuken op de beveiliging gaan registreren, onafhankelijk van het feit of deze inbreuk gemeld wordt of niet. In geval van een datalek zal de melding van DKT aan de AP door gebruik van het webformulier aan de inhoudelijke eisen voldoen. Als de betrokkene moet worden geïnformeerd moet er meer informatie verstrekt worden dan nu het geval is, zoals omschreven in paragraaf 6.8. Tenslotte betekent het begrip onverwijld melden in de AVG hetzelfde als in de Wbp, waardoor de eerdere genoemde wijziging op basis van de Wbp het beleid ook in lijn zal brengen met de AVG.

Vaststellen van verwerkingsdoeleinden
Net als onder de Wbp moet DKT onder de AVG de verwerking baseren op welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. De verwerking van DKT is onder de Wbp gebaseerd op de doeleinden uit het Vrijstellingsbesluit Wbp. Met het van toepassing worden van de AVG komt dit besluit, net als de Wbp waaraan het gekoppeld is, te vervallen. Voordat de AVG van toepassing wordt, moet DKT zelf verwerkingsdoeleinden vaststellen en -leggen. Dit kan bijvoorbeeld in het register van verwerkingsactiviteiten dat hieronder aan bod komt. Zoals eerder in dit onderzoek is benoemd, verwerkt DKT persoonsgegevens in ieder geval om notariële diensten te kunnen leveren, om hiervoor te kunnen factureren, om te voldoen aan wettelijke bewaarplichten en om de werkzaamheden op een later tijdstip te kunnen verantwoorden. De verwerkingsdoeleinden die DKT vaststelt, vormen zoals hiervoor besproken tevens de basis voor de bewaartermijn.

Voldoen aan de verantwoordings- en registratieplicht
DKT moet aan kunnen tonen dat de verwerking van persoonsgegevens van cliënten voldoet aan de AVG. Dit kan onder andere worden aangetoond door een gegevensbeschermingsbeleid op te stellen en door middel van aansluiting bij een goedgekeurde gedragscode of een certificeringsmechanisme. Ook het voldoen aan de registratieplicht kan helpen om naleving van de AVG aan te tonen. DKT werkt op dit moment aan een beleid over persoonsgegevens. Dit is echter nog niet af. Het kantoor is tevens niet aangesloten bij een gedragscode of certificeringsmechanisme gericht op persoonsgegevens. de verwerking van persoonsgegevens door DKT niet incidenteel is, wordt het bijhouden van een register van verwerkingsactiviteiten verplicht. Hoewel enkele verplichte elementen van dit register wel voorhanden zijn, is er geen register van de verwerkingsactiviteiten van DKT. Het bovenstaande maakt dat DKT op dit moment niet kan aantonen dat de verwerking van persoonsgegevens van cliënten voldoet aan de AVG.

DKT heeft verschillende mogelijkheden om aan deze verantwoordingsplicht te voldoen. Ten eerste is DKT verplicht een register van verwerkingsactiviteiten opstellen. Daarin moeten de elementen beschreven in paragraaf 4.3 zijn opgenomen, waaronder de verwerkingsdoeleinden en de daarop gebaseerde bewaartermijn die DKT onder de AVG zelf moet vaststellen. Daarbij moet worden vermeld dat deze registratie alle verwerkingsactiviteiten moet bevatten, bijvoorbeeld ook de verwerking van persoonsgegevens van medewerkers in het kader van de salarisadministratie of personeelszaken. Tevens kan het beleid over persoonsgegevens binnen DKT, nadat het is ingevoerd, helpen aantonen dat de verwerking van persoonsgegevens in lijn is met de AVG. Ook kan DKT, na publicatie van de Baseline Informatiebescherming Notariaat, de verwerking van persoonsgegevens afstemmen op de normen die hierin zijn opgenomen. Het voldoen aan deze Baseline kan als element worden gebruikt om aan te tonen dat de beveiliging van persoonsgegevens op orde is.

Slotconclusie
Zoals hierboven per onderdeel staat beschreven, moet DKT de volgende stappen zetten om aan zowel de huidige als toekomstige privacywetgeving te voldoen. Ten aanzien van de informatieplicht wordt aanbevolen om een privacyverklaring op te stellen en deze samen met de eerste brief of opdrachtbevestiging aan de cliënt te verstrekken. Gelet op de bewaartermijnen moet DKT de verwerking van persoonsgegevens onder de Wbp melden aan de AP. Onder de AVG moet er, op basis van verwerkingsdoeleinden die DKT zelf moet vaststellen, worden bepaald hoe lang bepaalde persoonsgegevens bewaard moeten worden. De persoonsgegevens die nu worden bewaard maar niet langer nodig zijn voor deze verwerkingsdoeleinden, moeten worden verwijderd. Daarnaast moet de beveiliging naar een passend niveau worden getild. Aanbevolen wordt om aan het eind van de werkdag papieren dossiers op te bergen in afgesloten dossierkasten of ruimtes met daarin dossiers af te sluiten. Ook moeten er met BB Diensten en Box B.V. bewerkersovereenkomsten worden gesloten die aan de eisen van de AVG voldoen. Om een passend beveiligingsniveau te waarborgen, wordt aanbevolen om de beveiliging regelmatig te testen en evalueren. In het beleid omtrent datalekken moet de termijn voor een melding aan de AP worden gewijzigd naar 72 uur. De betrokkene moet bij een datalek ook onverwijld worden geïnformeerd en moet tevens meer informatie ontvangen. Onder de Wbp moet DKT nog situaties melden waarin niet redelijkerwijs is uit te sluiten dat er persoonsgegevens zijn gelekt. Onder de AVG is dit niet langer vereist, maar moet DKT wel alle beveiligingsincidenten registreren. Tot slot moet DKT onder de AVG zoals eerder vermeld zelf verwerkingsdoeleinden vaststellen en voldoen aan de verantwoordings- en registratieplicht. Het register van verwerkingsactiviteiten dat DKT verplicht op moet stellen, zal helpen aantonen dat aan de AVG wordt voldaan. Hetzelfde geldt voor het invoeren van het beleid omtrent persoonsgegevens, dat op dit moment wordt ontwikkeld. Het voldoen aan de Baseline Informatiebeveiliging Notariaat kan helpen aantonen dat de beveiliging van persoonsgegevens op orde is.

Hoewel de AVG nog een jaar op zich laat wachten, moet DKT nu aan de slag met deze aanbevelingen om gedurende dit laatste jaar aan de Wbp te voldoen. Met het opvolgen van deze aanbevelingen is DKT tevens goed voorbereid op de AVG, wat erg belangrijk is. De boetebevoegdheid van de AP wordt namelijk uitgebreid van €820.000 naar maximaal €20.000.000 of 4% van de jaaromzet indien dit bedrag hoger is. Daarbij is de AP niet terughoudend in het publiceren van informatie over overtreders van de privacywetgeving. Dit kan tot reputatieschade leiden, met de financiële gevolgen van dien. Tenslotte zou een verwerkingsbeperking of -verbod, een sanctie die de AP onder de AVG kan opleggen, een gedeelte van de werkzaamheden van DKT stilleggen.

Literatuurlijst

Van Almelo, *Notariaat Magazine* 2017, editie 1, p. 10-11
L. van Almelo, 'Kwaliteitshandboek voor informatiebeveiliging in de maak', *Notariaat Magazine* 2017, editie 1, p. 10-11.

Beleidsregels voor toepassing van artikel 34a van de Wbp 2015
Beleidsregels voor toepassing van artikel 34a van de Wbp, Den Haag: Autoriteit Persoonsgegevens 2015 (online publiek).

Beveiliging van persoonsgegevens 2013
Beveiliging van persoonsgegevens (CBP Richtsnoeren), Den Haag: College bescherming persoonsgegevens 2013 (online publiek).

Hooghiemstra & Nouwt 2007
T.F.M. Hooghiemstra en J. Nouwt, *Tekst en toelichting Wet bescherming persoonsgegevens,* Den Haag: Sdu Uitgevers 2007.

Kranenborg & Verhey 2011
H.R. Kranenborg & L.F.M. Verhey, *Wet bescherming persoonsgegevens in Europees perspectief*, Deventer: Kluwer 2011.

Lekkerkerker & Van Ee, *WPNR* 2015/7070, p. 623-631
G.J.C. Lekkerkerker & J.W. van Ee, 'De notaris in een digitale wereld, twee invalshoeken', *Weekblad voor Privaatrecht Notariaat en Registratie* 2015/7070, p. 623-631.

Privacy Impact Assessment: introductie, handreiking en vragenlijst 2015
Privacy Impact Assessment: introductie, handreiking en vragenlijst, Amsterdam: Norea 2015 (online publiek)

Richtlijnen voor functionarissen voor de gegevensbescherming (FG's) 2017
Richtlijnen voor functionarissen voor de gegevensbescherming (FG's), Den Haag: Autoriteit Persoonsgegevens 2017 (online publiek).

Sauerwein & Linnemann 2002
L.B. Sauerwein & J.J. Linnemann, *Handleiding voor verwerkers van persoonsgegevens*, Den Haag: Ministerie van Justitie 2002.

Spanjaart, *Notariaat Magazine* 2016, editie 6, p. 26-27
J. Spanjaart, 'Vragen staat vrij: Protocollen', *Notariaat Magazine* 2016, editie 6, p. 26-27.

Aan de Stegge, *Notariaat Magazine* 2016, editie 5, p. 26-27
J. aan de Stegge, 'De noodzaak van goede internetbeveiliging - 'Help, we zijn gehackt!'', *Notariaat Magazine* 2016, editie 5, p. 26-27.

Van der Woude & Sleeking, *WPNR* 2015/7073, p. 715-721
F. van der Woude & O.A. Sleeking, 'Digitaal archiveren binnen het notariaat', *Weekblad voor Privaatrecht Notariaat en Registratie* 2015/7073, p. 715-721.