De notaris in een digitale wereld, twee invalshoeken

G.J.C. Lekkerkerker*
J.W. van Ee*

Inleiding

De notaris in een digitale wereld, het thema dat de KNB dit jaar koos voor haar jaarcongres, kan inspireren tot een veelheid van invalshoeken. Wij richten ons in deze bijdrage op twee aspecten: de beveiliging van cliëntgegevens en de notaris die 'vertrouwen', *trust* in het jargon van de digitale wereld, toevoegt aan het digitaal berichtenverkeer.
Onze eerste invalshoek ziet op de vraag in hoeverre de voortgaande digitalisering van alle berichtenverkeer nieuwe voorschriften nodig gaat maken ten behoeve van de beveiliging van de aan de notaris toevertrouwde persoonsgegevens. Wij denken dat dit het geval is en komen met enige suggesties.
Voor onze tweede invalshoek verlaten we het perspectief van regelgeving en toezicht en schetsen we een nieuwe mogelijkheid, zoals die thans voor de notaris in de markt lijkt te ontstaan. We beschrijven een invulling van de rol de notaris als hoeder van de integriteit van data, als bezorger van *trust*. Het betreft een mooi initiatief, een 'product' dat thans wordt ontwikkeld en dat naar wij denken nog een stuk extra potentie in zich heeft.
Tot slot geven wij nog enige overwegingen bij de mogelijkheden zoals die zich aandienen in het door ons geschetste scenario.

1. *De eerste invalshoek: de beveiliging van persoonsgegevens*

Wij menen dat voor de beroepsgroep de tijd nu gekomen is om serieus aandacht te geven aan het beveiligingsniveau van de cliëntgegevens in de digitale omgeving. De notaris heeft hier een staat op te houden en niet alleen de statuur van het beroep vraagt hierom, ook de op handen zijnde wetgeving. Aandacht voor bescherming van persoonsgegevens, voor de privacy, in een *online* omgeving is er al sinds de het laatste decennium van de vorige eeuw[1].

---

*G.J.C. Lekkerkerker is werkzaam bij de KNB en J.W. van Ee is oud notaris. Dit artikel is op persoonlijke titel geschreven.

[1] 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.

Maar de ontwikkelingen in de ICT zijn sindsdien snel gegaan. Er komen nieuwe wettelijke eisen en dit alles vraagt, ook voor het notariaat, om een nieuw bewustzijn van de *do's* en *dont's*[2].

Wij beschrijven in dit eerste onderdeel het wettelijk kader en wat er aan wetgeving op ons af komt. In de laatste paragraaf nemen we een voorschot op mogelijke voorschriften of richtsnoeren voor de beveiliging van persoonsgegevens waarvoor de notaris een verantwoordelijkheid heeft.

1.1. Het wettelijk kader: de Wet bescherming persoonsgegevens

Sinds 2000 kennen we de Wet bescherming persoonsgegevens (Wbp)[3]. De wet vereist 'passende technische en organisatorische maatregelen' teneinde persoonsgegevens[4] te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking[5]. Er worden regels gegeven voor het opslaan, verzamelen, verstrekken en combineren (kort gezegd: het verwerken) van deze persoonsgegevens. Belangrijke rollen zijn daarbij weggelegd voor 'verantwoordelijke' en 'bewerker'. De verantwoordelijke is degene die 'alleen of te zamen met anderen, het doel van en de middelen voor de verwerking van de persoonsgegevens vaststelt'[6]. De bewerker is 'degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen'[7]. Elk notariskantoor beschikt over bestanden met persoonsgegevens en binnen het notariële speelveld is de notaris de verantwoordelijke in de zin van de Wbp. Vaak is ook sprake van externe opslag van data, een bewerkersactiviteit.

De verantwoordelijke, in ons geval dus de notaris, is eindverantwoordelijk voor de 'passende technische en organisatorische maatregelen' ter beveiliging van de persoonsgegevens. De maatregelen moeten garant staan voor een 'passend beveiligingsniveau', rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging[8]. De verantwoordelijke moet er voor zorgen dat ook de bewerkers met betrekking tot de te verrichten bewerkingen

---

2. Men denke bijvoorbeeld aan de snel opkomende techniek van cloudcomputing, het op grote schaal gebruiken van persoonsgegevens als digitaal 'betaalmiddel' - het verdienmodel van veel internetdiensten – aan de schaal en omvang van het gebruik van persoonsprofielen voor commerciële doeleinden en daar tegenover, aan het groeiend besef dat de burger 'baas' hoort te zijn over zijn eigen persoonsgegevens en dat deze beter beschermd moeten worden.

3 Wet van 6 juli 2000, houdende regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens).

[4] Een persoonsgegeven wordt in art. sub a Wbp omschreven als 'elk gegeven betreffende een geïdentificeerde of identificeerbare persoon.

[5] Zie art. 13 Wbp.

[6] Art. 1 sub d. Wbp.

[7] Art. 1 sub e. Wbp.

[8] Art. 13 Wbp.

aan deze standaard voldoen[9]. Een bewerker bewerkt de gegevens immers 'slechts in opdracht van de verantwoordelijke, behoudens afwijkende wettelijke verplichting'[10].
Als bewerkers van de notariële persoonsgegevens zijn software leveranciers en hostingpartijen verplicht tot geheimhouding 'behoudens voor zover enig wettelijk voorschrift hen tot mededeling verplicht of uit hun taak de noodzaak tot mededeling voortvloeit'[11]. We mogen er van uit gaan dat de aard van hun relatie met het notariskantoor met zich brengt, dat het softwarehuizen en hostingpartijen niet is toegestaan om gegevens die onder het notarieel verschoningsrecht vallen, aan opsporingsinstanties of aan welke derden ook ter beschikking te stellen. Het ligt in de rede dat zij zich als bewerkers van persoonsgegevens die vallen onder het beheer van een verschoningsgerechtigde, kunnen beroepen op een (afgeleid) verschoningsrecht[12].
In beginsel dient iedere verwerking van persoonsgegevens in de zin van de wet te worden gemeld aan het College bescherming persoonsgegevens (hierna Cbp)[13]. Het notariaat valt hier onder de uitzonderingen[14].

1.2 Het wettelijk kader: een meldplicht voor datalekken en een uitbreiding van de bestuurlijke boetebevoegdheid voor het Cbp.

De Wet bescherming persoonsgegevens zal binnen afzienbare tijd worden aangevuld met een nieuwe verplichting. Er komt een meldplicht ingeval van een datalek, of beter, ingeval van een inbreuk op de beveiliging die kan leiden tot een datalek[15]. Er is sprake van een datalek, wanneer persoonsgegevens in handen vallen van derden die geen toegang tot deze gegevens zouden mogen hebben. Zo'n datalek is het gevolg van een beveiligingsprobleem. Dit hoeft niet perse te betekenen dat het beveiligingsprotocol, de beveiliging 'op papier', van onvoldoende niveau was. Het kan ook zijn dat er slordig mee werd omgegaan. Denk aan een kantoor dat weliswaar een beleid kent van regelmatig wisselende wachtwoorden, maar waar

[9] Deze zorgplicht is uitgewerkt in art. 14 Wbp.
[10] Art. 12 lid 1 Wbp.
[11] Art. 12 lid 2 Wbp.
[12] Zie in deze zin R. van der Hoeven, *Poging tot omzeiling van het verschoningsrecht?* JBN 2013/13.
[13] Art. 27 Wbp.
[14] Bij 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) zijn blijkens art. 15 van dit besluit juridische en financiële dienstverleners, waaronder notarissen en advocaten , voor hun dienstverlening en advisering aan cliënten van de meldplicht vrijgesteld.
[15] Wet van 4 juni 2015 tot wijziging van de Wet bescherming persoonsgegevens en enige andere wetten in verband met de invoering van een meldplicht bij de doorbreking van maatregelen voor de beveiliging van persoonsgegevens alsmede uitbreiding van de bevoegdheid van het College bescherming persoonsgegevens om bij overtreding van het bepaalde bij of krachtens de Wet bescherming persoonsgegevens een bestuurlijke boete op te leggen (meldplicht datalekken en uitbreiding bestuurlijke boetebevoegdheid Cbp); Stb. 2015 nr. 230. Ten tijde van het schrijven van dit artikel was de invoeringsdatum nog niet bekend.

medewerkers hun wachtwoord met een sticker op hun computer plakken, aan een organisatie waar USB-sticks met persoonsgegevens kwijtraken of waar papieren dossiers worden aangeboden bij het oud papier.

Stel dat een insluiper het notariskantoor is binnengedrongen en een server heeft meegenomen waarop persoonsgegevens zijn opgeslagen. Wat er al zij van het beveiligingsniveau van dat kantoor, er is dan sprake van wat in het nieuwe artikel 34a Wbp wordt genoemd 'een inbreuk op de beveiliging (…), die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens'. De inbreuk kan immers leiden tot diefstal, verlies of misbruik van deze gegevens. Een datalek is een reële mogelijkheid.
De notaris als de verantwoordelijke voor de Wbp, moet in zo'n geval het College bescherming persoonsgegevens onverwijld van het voorval in kennis stellen. Hetzelfde moet hij doen in de richting van iedere de cliënt van wie het de persoonsgegevens betreft, 'indien de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer'[16]. Wanneer de gegevens waarop is ingebroken voor derden onbegrijpelijk of ontoegankelijk zijn – zij zijn bijvoorbeeld goed versleuteld –, dan geldt de verplichting de cliënten op de hoogte te stellen niet[17].
Het ligt in de rede dat een software leverancier die als bewerker optreedt evenzeer verplicht is om de notaris(sen) als zijnde verantwoordelijke(n) onverwijld te informeren, wanneer de inbreuk bij hem is opgetreden. Een notaris die het betreft moet vervolgens de melding doen bij het College.

Artikel 34a beschrijft ook wat precies moet worden gemeld in geval van een mogelijke datalek. De melding betreft de aard van de inbreuk, de instanties waar meer informatie over de inbreuk kan worden verkregen en de aanbevolen maatregelen om de negatieve gevolgen van de inbreuk te beperken[18]. Tevens beschrijft de verantwoordelijke in zijn melding aan het College de geconstateerde en de vermoedelijke gevolgen van de inbreuk voor de verwerking van de persoonsgegevens en de maatregelen die de organisatie heeft genomen of voorstelt te nemen om deze gevolgen te verhelpen[19].
Een verantwoordelijke die een lek heeft gemeld, krijgt in veel gevallen van het College eerst een bindende aanwijzing om de bescherming van gegevens in orde te maken. Wanneer zo'n

[16] Art. 34a lid 2 Wbp, het artikel spreekt van 'de betrokkene'.
[17] Art. 34a lid 6 Wbp.
[18] Art. 34a lid 3 Wbp.
[19] Art. 34a lid 4 Wbp.

aanwijzing niet wordt nagevolgd of indien sprake is van opzet of grove nalatigheid riskeert de verantwoordelijke een boete die kan oplopen tot € 810.000[20].

De aanpassing van de Wbp met een meldplicht voor datalekken en mogelijk een zware boete moet een aansporing zijn voor organisaties om hun gegevens beter te beveiligen. Het betreft hier wetgeving met tanden. De sanctie op niet naleving van de meldplicht moet een krachtige stimulans zijn iedere inbreuk op de beveiliging tijdig te melden. Personen van wie gegevens zijn uitgelekt, zullen er sneller van op de hoogte zijn wanneer hun gegevens in verkeerde handen zijn gekomen. Maar bovenal, een inbreuk op de beveiliging met mogelijk een datalek gaat leiden tot een serieus imagoprobleem, zeker voor een professioneel geheimhouder als de notaris.

1.3 Het wettelijk kader: de Algemene verordening gegevensbescherming

Het belang van een stevig kader voor de beveiliging van persoonsgegevens speelt ook op Europees niveau. Er moet meer vertrouwen komen in de digitale gegevensuitwisseling. Dit bracht de Europese Commissie tot haar voorstel voor een Algemene verordening gegevensbescherming (Avg)[21], voor het eerst gepresenteerd op 25 januari 2012. Doel van deze ontwerp verordening is een coherente, eigentijdse invulling te geven aan de gegevensbescherming op Europees niveau en in het bijzonder om het vertrouwen van de burger in *online* omgevingen te vergroten. De Avg komt in de plaats van de hiervoor al genoemde Europese privacyrichtlijn 95/46/EG van 1995, die de grondslag was voor de Wbp. Het gebruik van het instrument ‘verordening’ impliceert dat de Avg, na goedkeuring door het Europees Parlement, rechtstreeks van kracht zal zijn in alle lidstaten. Aanvankelijk leek het erop dat de verordening reeds in 2014 zou worden aangenomen, maar ook hier blijkt *the devil in the detail* en vragen de onderhandelingen meer tijd [22]. Maar de uitgangspunten voor zover van belang voor deze bijdrage staan niet ter discussie en nog steeds is niet uitgesloten dat de Avg nog dit jaar in werking treedt. Daarna geldt nog overgangstermijn van twee jaar voordat

[20] Art. 66 lid 2 Wbp geeft het College het recht een bestuurlijke boete op te leggen tot ten hoogste de zesde categorie van art. 23 lid 4 van het Wetboek van Strafrecht.
[21] Voorstel voor een Verordening van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (algemene verordening gegevensbescherming).
[22] Van de onderhandelingen in Brussel worden beide Kamers ieder kwartaal bij brief door de Staatssecretaris van Veiligheid en Justitie op de hoogte gehouden. De laatste kwartaalrapportage dateert van 2 februari 2015 (kst-33169-W).

de verordening in al haar onderdelen in alle lidstaten van de Europese Unie van toepassing is[23].

De Avg haakt in op de snelle opkomst van de internet gerelateerde diensten en –applicaties sinds de privacyrichtlijn van 1995. De positie van de consument, ook hier betrokkene genoemd, moet worden versterkt. Zo wordt het recht op bescherming tegen profilering wat scherper aangezet[24]. Persoonsgegevens mogen niet voor commerciële doeleinden worden verwerkt dan met uitdrukkelijke toestemming van de betrokkene[25]. De verantwoordelijke moet kunnen aantonen dat de betrokkene die toestemming heeft gegeven[26] en de betrokkene heeft hij het recht die toestemming te allen tijde in te trekken[27].

Daarnaast krijgt de consument twee nieuwe rechten, die hem verdergaand controle kunnen geven over zijn eigen gegevens. Hij krijgt het recht om volledige verwijdering te eisen van zijn persoonsgegevens uit een bestand, indien hij zijn toestemming voor opslag intrekt en er geen andere legitieme redenen zijn om de data te bewaren[28]. De verantwoordelijke moet er voor zorgen dat dit 'recht om vergeten te worden' ook werkelijk kan worden geëffectueerd. Hij zal dus moeten beschikken over een protocol met procedures en maatregelen die dit 'recht om vergeten te worden' kunnen bewerkstelligen.

Het tweede nieuwe recht betreft de overdracht van gegevens. De consument krijgt het recht om een kopie te krijgen van zijn persoonsgegevens die worden verwerkt en om te verlangen dat zijn gegevens en alle andere informatie die hij heeft verstrekt en die is bewaard, op zijn verzoek in een algemeen gebruikt elektronisch format worden overgedragen aan een ander geautomatiseerd verwerkingssysteem. Men spreekt van het recht van gegevensoverdraagbaarheid of dataportabiliteit[29].

---

[23] Deze overgangstermijn blijkt uit art. 91 lid 2 Avg.

[24] Richtlijn 95/46/EG kent in art 15 lid 1 'een ieder het recht toe niet te worden onderworpen aan een besluit waaraan voor hem rechtsgevolgen zijn verbonden of dat hem in aanmerkelijke mate treft en dat louter wordt genomen op grond van een geautomatiseerde gegevensverwerking die bestemd is om bepaalde aspecten van zijn persoonlijkheid, zoals beroepsprestatie, kredietwaardigheid, betrouwbaarheid, gedrag, enz. te evalueren.'
De Avg formuleert de bescherming tegen profilering wat scherper als 'het recht om niet te worden onderworpen aan een geautomatiseerde verwerking van zijn persoonsgegevens, die bestemd is om bepaalde aspecten van zijn persoonlijkheid te evalueren of om bijvoorbeeld zijn beroepsprestaties, economische situatie, verblijfplaats gezondheid, persoonlijke voorkeuren, betrouwbaarheid of gedrag te analyseren of te voorspellen'; zie art. 20 Avg. Voor veel situaties van *profiling* zal de verordening een privacy effectbeoordeling verplicht stellen (Privacy Impact Assessment, PIA); zie art 33 Avg.

[25] Zie art. 6 Avg; de toestemming moet voor een of meer specifieke doeleinden gegeven zijn. Dit artikel geeft een aantal voor de hand liggende uitzonderingen op het toestemmingsvereiste, bijvoorbeeld dat de verwerking noodzakelijk is om te voldoen aan een wettelijke verplichting van de voor de verwerking verantwoordelijke.

[26] Art. 7 lid 1 Avg.

[27] Art. 7 lid 3 Avg.

[28] Zie art. 17 Avg. Belangrijke uitzonderingen op dit recht zijn dat sprake is van een botsing met het recht op vrijheid van meningsuiting of van een bewaarplicht op grond van de wet.

[29] Art. 18 Avg.

Deze nieuwe rechten van de consument/betrokkene zullen de notaris in zijn klassieke rol niet snel deren. De tot zijn protocol behorende gegevensbestanden beheert hij met een specifiek doel en uit hoofde van een wettelijke taak. Wanneer wij hierna de notaris in de digitale wereld beschrijven vanuit onze tweede invalshoek – een nieuw 'product' waaraan de notaris deel heeft -, moet met de hier beschreven rechten wel terdege worden gerekend.

De ontwerp verordening zet sterk in op technische en organisatorische maatregelen om aan de gegevensbescherming gestalte te geven. Ook in de Nederlandse tekst gebruikt men de termen *privacy by design* en *privacy by default*. Hiermee wordt bedoeld, dat technische en organisatorische maatregelen die privacy verhogend zijn al vanaf de ontwerpfase van de te gebruiken systemen moeten worden meegenomen en dat de systeeminstellingen op een maximale privacybescherming moeten worden gericht [30].
Ook de verordening kent een meldplicht voor datalekken. Hier wordt voorgeschreven dat de inbreuk zo mogelijk binnen 24 uur wordt gemeld[31]. De plicht om gegevensverwerkingen te melden bij het Cbp zal vervallen. Daarvoor in de plaats komt een algemene documentatieverplichting. De verantwoordelijken en bewerkers (nu verwerkers genoemd) krijgen een documentatieplicht inzake alle verwerkingen die onder hun verantwoordelijkheid hebben plaatsgevonden. Deze documentatieplicht ziet onder meer op de gegevensbeveiliging[32].

Een belangrijke wijziging die de verordening brengt, is de verplichting onder omstandigheden een functionaris voor de gegevensbescherming aan te wijzen, hierna te noemen FG. Deze verplichting geldt wanneer de verantwoordelijke een overheidsinstantie of een overheidsorgaan, wanneer de verwerking wordt uitgevoerd door een onderneming met ten minste 250 werknemers of sprake is van een organisatie die hoofdzakelijk belast is met verwerkingen die regelmatige en stelselmatige observatie van betrokkenen vereisen[33]. Ook de Wet bescherming persoonsgegevens voorziet reeds in de mogelijkheid van zo'n functionaris,

[30] Zie art. 23 lid 1 Avg: 'Met inachtneming van de stand van de techniek en de uitvoeringskosten legt de voor de verwerking verantwoordelijke, zowel bij de vaststelling van de middelen voor de verwerking als bij de verwerking zelf, zodanig passende technische en organisatorische maatregelen en procedures ten uitvoer dat de verwerking aan de voorwaarden van deze verordening voldoet en de bescherming van de rechten van de betrokkene gewaarborgd is.'
Het tweede lid van art. 23 Avg benadrukt in dit kader de eis van dataminimalisatie, uitgangspunt ook van de Wbp: niet meer gegevens verwerken dan strikt noodzakelijk in relatie tot het tevoren omschreven doel, niet langer bewaren dan nodig.
[31] Art. 31 Avg.
[32] Zie hierover art. 28 Avg.
[33] Art. 35 lid 1 Avg.

maar onderlijnt het vrijblijvend karakter[34].
Er ligt een voorstel vanuit het Europees Parlement de verplichting tot aanstelling van een FG sterk uit te breiden. Ook voor een organisatie die gegevens verwerkt van meer dan 5000 betrokkenen in een aaneengesloten periode van twaalf maanden of die gevoelige persoonsgegevens verwerkt, gegevens over de verblijfplaats van personen of gegevens over kinderen of werknemers in grote bestanden, zou de FG verplicht moeten worden aangesteld[35]. Het komt ons voor dat, indien dit amendement alsnog wordt aangenomen, ieder geval de KNB verplicht zal worden een functionaris voor de gegevensbescherming aan te stellen, gezien het grote bestand aan gegevens dat zij onder zich heeft[36].

Opvallend, ook bij de verordening, zijn de stevige sancties. Het Cbp krijgt nu de bevoegdheid draconisch aandoende boetes op te leggen, wanneer niet aan de eisen van de verordening zijn voldaan. Enige voorbeelden die de notaris kunnen raken: een mogelijk datalek moet tijdig wordt gemeld, de geheimhouding moet voldoende zijn gewaarborgd en, *last but not least*, er moet een passend beveiligingsniveau in acht zijn genomen; boete bij overtreding tot € 1.000.000 of 2% van de jaaromzet[37]. Een zelfde boete kan de KNB verbeuren wanneer zij verplicht zou worden een FG aan te stellen en zij dit nalaat[38].

1.4 Geen paniek, wel beleidsmatige aandacht

Wij menen niet, dat het nodig is van deze wetgeving of van die boetedreiging nu in paniek te raken. De Avg zal op zijn vroegst in de tweede helft van dit jaar worden aangenomen en daarna geldt – het is al opgemerkt – een overgangstermijn van twee jaar. De aanpassingen van de Wbp zullen er eerder zijn. Aandacht van de beleidsmakers van de KNB moet wat hier gaande is nu wel gaan krijgen. De richting is duidelijk. Een ‘passend beveiligingsniveau’ is niet een statisch gegeven, de eisen worden strenger. Datalekken zullen moeten worden gemeld en de digitale systemen die persoonsgegevens bevatten die aan notarissen zijn toevertrouwd, zullen steeds dat ‘passend beveiligingsniveau’ moeten hebben, met toenemend aandacht voor privacy *by design and by default*. De systemen zullen gedocumenteerd en

[34] Art. 62 e.v. Wbp.
[35] Zie www.europarl.europa.eu. Verslag 22 november 2013 over het voorstel voor een Verordening van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (algemene verordening gegevensbescherming), amendement 132
[36] Wij denken hier aan het beheer van het CDR ten behoeve van de Belastingdienst en aan het CTR.
[37] Art. 79 lid 6 sub h), o), en e) Avg.
[38] Art. 79 lid 6 sub j) Avg.

daarmee transparant moeten zijn. Het ligt in de rede dat hun toetsing onderdeel moet worden van het toezicht door het Bft en van de *peer reviews*.

1.5 Voorschriften of richtsnoeren voor de beveiliging van persoonsgegevens; een voorschot

De toegenomen aandacht voor de beveiliging van persoonsgegevens in digitale systemen is het gevolg van bezorgdheid over wat met digitale technieken mogelijk is. De nieuwe regelgeving kenmerkt zich door een aanscherping van de algemene zorgvuldigheidsnormen, door een verzwaring van eisen en sancties. Voor wie een rol heeft als verantwoordelijke in dit zich verder verbredende regelgebied, zoals in ons geval de notaris, begint het met bewustwording; bewustwording van het feit dat voor hem de risico's toenemen. Bewustzijn van die risico's kan nieuwe beroepsvoorschriften acceptabel maken[39].

Het ligt in de rede dat de beroepsorganisatie nu een start gaat maken met het ontwikkelen van een reeks aanbevelingen voor 'passende technische en organisatorische maatregelen en procedures' in het kader van de digitale gegevensverwerking[40]. Uiteindelijk doel lijkt ons de ontwikkeling van een set van standaarden, die periodiek getoetst moeten worden. De aanbevelingen dan wel standaarden moeten voor alle partners in dit veld zien op de technische beveiliging en organisatorische maatregelen[41]. Voor de softwareleveranciers en hostingpartijen zou tevens de continuïteit van de dienstverlening onderwerp moeten zijn[42].

[39] Om notarissen en hun personeel bewust te maken van het belang van een voldoende beveiliging van de hen toevertrouwde gegevens is de Vragenlijst beveiliging persoonsgegevens opgesteld. De Vragenlijst kan worden benaderd via Notarisnet, het digitale netwerk van de KNB. Door antwoord te geven op de vragen en stellingen van de Vragenlijst, wordt het inzicht vergroot in de mate van betrouwbaarheid en beveiliging van de eigen systemen en worden knelpunten zichtbaar (zelf evaluatie). De antwoorden worden geanonimiseerd vergeleken met die van andere deelnemende kantoren (benchmark).

[40] Deze aanbevelingen zouden betrekking moeten hebben op de notariskantoren, de software leveranciers en de hostingproviders, waarbij zij aangetekend dat een software leverancier tevens hosting provider kan zijn en het notariskantoor soms ook alle rollen zelf vervult.

[41] De Richtsnoeren 'Beveiliging van persoonsgegevens' van februari 2013 van het Cbp lijken hier een goede invalshoek. Deze Richtsnoeren leggen een expliciete koppeling naar de norm NEN-ISO/IEC 27002: 2007, Informatiebeveiliging . Dit geeft een basis voor een normenkader dat extern kan worden getoetst. De Richtsnoeren benoemen een aantal maatregelen die in veel situaties in een of andere vorm noodzakelijk zijn. Genoemd worden onder meer: aandacht voor beveiligingsbewustzijn, een beleidsdocument voor informatiebeveiliging, toegangsbeveiliging, beveiliging van apparatuur, aandacht voor correcte verwerking in toepassingssystemen, voor logging en controle, incidentenbeheer en afhandeling van beveiligingsincidenten, voor continuïteitsbeheer, voor geheimhouding en geheimhoudingsovereenkomsten.
Speciaal voor opslag in de cloud bestaat er sinds kort een nieuwe standaard, de ISO 27018, waarin eisen voor een verantwoorde opslag zijn verwerkt op het gebied van beveiliging en privacy.

[42] Te denken valt aan een regeling voor de beschikbaarheid van programmatuur en data, ook ingeval van een calamiteit, een regeling die voorkomt dat in het geval van een conflict tussen het notariskantoor en de bewerker de ambtsuitoefening in gevaar komt, een regeling voor het geval dat een bewerker failleert (escrow, stichting continuïteit, licentie vennootschap).

Naast en in het verlengde van dit alles staat het belang van een voldoende veilige communicatie met de cliënt in een digitale omgeving. Ook hiervoor zullen ons inziens eisen moeten worden geformuleerd[43].

2. De tweede invalshoek: een rol voor de notaris als hoeder van de integriteit van data

De gemiddelde burger lijkt zich er vaak nog weinig van bewust, dat al zijn handelen op internet in beginsel door derden kan worden nagezien en opgeslagen. Tenzij hij zijn berichtenverkeer deugdelijk heeft beveiligd, betreft het in wezen openbare informatie. De wetgever probeert burgers en markten nu bewust te maken van de gevaren van een ongelimiteerde proliferatie van privacygevoelige informatie. We zagen al, dat de op handen zijnde Algemene verordening gegevensbescherming (Avg) het perspectief hanteert dat de burger in de informatiesamenleving zelf baas moet zijn over zijn eigen persoonsgegevens. Bedrijven zullen van de burger steeds gegevens nodig hebben, maar dit mag niet méér zijn, dan dat nodig is volgens het *need to know* principe. De markten zullen hun digitale systemen moeten gaan aanpassen aan de eisen van de komende wetgeving. Die systemen zijn sowieso al kwetsbaar[44] en de risico's nemen toe[45]. Bedrijven krijgen er belang bij die risico's waar mogelijk te minimaliseren.
Het beheersbaar maken van risico's, de zorg voor rechtszekerheid, het past van oudsher bij het speelveld van de notaris, zoals dat ook opgaat voor het bieden van vertrouwen en van vertrouwensdiensten. Het is te begrijpen, dat dat er naarstig naar wordt gezocht hoe deze 'toegevoegde waarden' van het notariaat kunnen worden overgebracht naar de digitale wereld. Hoe mooi zou het zijn, dat door de inzet van het notariaat enige lastige puzzels in de digitale wereld zouden kunnen worden opgelost.

In dit tweede onderdeel beschrijven wij een project waaraan ten tijde van het schrijven van dit artikel enthousiast wordt gewerkt. Men bouwt aan een systeem dat een landelijk identificatiemiddel introduceert, waarbij het notariaat de basis levert voor het vertrouwen dat de burger daarin kan hebben. Men denke aan een sterk verbeterd en op nieuwe leest geschoeid

[43] Beveiligd e-mail verkeer en een beveiligde verzending van stukken lijkt steeds beter mogelijk nu hiervoor betaalbare programma's op de markt komen. Deze zouden op hun bruikbaarheid moeten worden getest.
[44] Een aardig recent boek in de grote stroom van analyses en beschouwingen over de kwetsbaarheid van onze informatiesamenleving is Brenno de Winter, Victor Broers, *De rode hack*, maart 2015, http://www.derodehack.nl, een informatieve thriller over risico's rond informatiebeveiliging, in het bijzonder in het bancaire systeem.
[45] Zie het steeds terugkerende nieuws over grote hacks in binnen- en buitenland, gericht op spionage, identiteitsroof en roof van privacygevoelige gegevens die voor chantage en afpersing kunnen worden gebruikt.

DigiD[46].

In de volgende paragrafen beschrijven we het systeem dat voor ogen staat en wat dit systeem, zoals wij er naar willen kijken, nog aan extra zou kunnen gaan bieden.We onderscheiden daarbij drie mogelijkheden - we spreken daarbij van 'modellen'-, het basismodel en twee modellen die verder gaan. Het gaat dus om drie modellen, die wij in opeenvolgende paragrafen nader onder de loep zullen nemen.

Het basismodel biedt het de burger een stuk privacybescherming en het gemak dat hij niet steeds opnieuw zijn gegevens hoeft af te geven bij zijn rondgang door de digitale wereld. In het tweede model kan het systeem daarnaast bedrijven en instellingen die zijn toegetreden een stuk ontzorging bieden. De risico's die kleven aan het beheer van privacygevoelige gegevens van klanten worden voor hen beter beheersbaar. In zijn laatste, derde variant wordt het systeem tot zijn laatste consequenties toegepast. In dit derde model wordt het risico van succesvol hacken, waar dan ook in de keten, zeer sterk gereduceerd en krijgt de burger het beheer terug over zijn eigen persoonsgegevens.

2.1 Het idee achter het systeem

De notaris is er bij uitstek voor toegerust de identiteit vast te stellen van degenen die van zijn dienst gebruik willen maken. Zijn authentieke akte levert van die identiteit dwingend bewijs[47]. Het te ontwerpen systeem haakt aan op deze kwaliteit. Basis van het concept is dat aan de burger een middel wordt uitgereikt waarmee hij zich digitaal kan legitimeren, waarbij de in dat middel op te nemen gegevens door de notaris zijn gevalideerd. Zo'n middel waarmee de burger zich digitaal kan legitimeren wordt in de regel 'verpakt' in een chip-kaartje, maar kan bijvoorbeeld ook als een app op een smartphone, tablet of computer zijn geplaatst. In 'ons' systeem heeft de gebruiker een smartphone nodig en tevens een inlognaam en een pincode [48]. Voor de 'technische' kwaliteit van het uit te geven identificatiemiddel en voor de feitelijke uitgifte zijn marktpartijen verantwoordelijk[49]. Het identificatiemiddel noemen we hierna het certificaat[50].

---

[46] Het project is een samenwerkingsverband tussen de KNB en enige private partijen. Het 'product' zal waarschijnlijk NotarisID gaan heten.

[47] Art 157 lid 1.

[48] De gebruiker moet dus één ding hebben en twee dingen weten. Denkbaar is dat een komende generatie smartphones met biometrische beveiliging zal zijn toegerust, waarmee het risico van onrechtmatig gebruik van het middel door diefstal van de smartphone in combinatie met inlognaam en pincode, zal zijn geweken.

[49] De kwaliteit van het uit te geven identificatiemiddel moet op basis van overeenkomsten en door periodieke audits worden verzekerd.

[50] Het certificaat is een computerbestand dat fungeert als een digitaal 'paspoort'. De term is in zwang binnen de Public key infrastructure (PKI). Hoewel het door ons beschreven systeem niet binnen de PKI valt, willen we toch de term 'certificaat' gebruiken. Dit bevordert in ieder geval de leesbaarheid.

De basis van het systeem is de notaris en het vertrouwen dat wordt ontleend aan diens vaststelling van de identiteit van een persoon. Daarnaast ontleent het systeem zijn waarde aan een centrale databank waarin de gegevens worden opgeslagen[51]. Wij beschrijven hier nu kort hoe de burger aan zijn certificaat kan komen en wat het is, dat derden het vertrouwen geeft.

De burger krijgt zijn certificaat op basis van een verklaring van een notaris. De notaris bewaart zijn verklaring die gaat behoren tot zijn protocol, hij maakt contact met een in de uitgifte van certificaten gespecialiseerd bedrijf dat tot de uitgifte van certificaten is toegelaten en plaatst de gevalideerde persoonsgegevens tevens in de databank, waarin alle bij het systeem aangesloten notarissen deze gegevens opslaan.
Deze databank heeft een spilfunctie. Hij moet gaan dienen als kenbron, zowel voor de marktpartijen die zorgen voor het certificaat, als voor die partijen die op een certificaat willen vertrouwen. Wij zullen deze databank hierna aanduiden met de naam die ten tijde van het schrijven van dit artikel binnen de projectorganisatie gangbaar is: het DNA, hetgeen staat voor Depot Notariële Attributen. Partijen die certificaten (mogen) uitgeven, ontlenen aan het DNA de gegevens voor het certificaat, partijen die op deze certificaten willen vertrouwen, kunnen via het DNA nagaan of de gebruiker van een certificaat is wie hij zegt te zijn en mag doen wat hij doen wil. Het DNA geeft echter aan zo'n vertrouwende partij niet meer gegevens dan voor de transactie noodzakelijk zijn; het *need-to-know* beginsel.

2.2 Het basismodel: vereenvoudiging en rechtszekerheid

Het notariële certificaat kan het rechtsverkeer op internet efficiënter maken. Wij willen dit demonstreren aan de hand van een voorbeeld. Ook wanneer we de twee opvolgende modellen bespreken komt dit voorbeeld opnieuw terug.
De heer Jansen meldt zich op internet aan bij een drankenhandel. Hij wil een partij alcoholische drank bestellen. Tevens bezoekt hij een site waar hij een vliegticket bestelt. Hij gebruikt voor beide transacties zijn certificaat, beide wederpartijen (h)erkennen dit middel. Zij zijn als vertrouwende partijen aangesloten bij het DNA.
Jansen heeft zijn certificaat in werking gezet door zijn inlogcode in te geven. Daarmee treedt automatisch een proces in werking, waarbij het DNA nagaat of Jansen daar geregistreerd is als houder van een geldig certificaat. Tevens komt automatisch de verbinding tot stand tussen het DNA en de vertrouwende partijen, de drankenhandelaar en de site voor vliegtickets. Jansen ontvangt van het DNA in zijn app het bericht dat deze partijen naar hem hebben

[51] Wij gebruiken hier het begrip 'databank' zoals omschreven in de Databankenwet (art. 1 lid 1 sub a).

geïnformeerd, met de vraag of dat voor hem akkoord is.
Nu volgt het moment dat de voor de rechtshandeling benodigde persoonsgegevens door het DNA moeten worden vrijgegeven. Het DNA bevestigt dat het certificaat dat voor de beoogde transactie is ingezet, wordt gebruikt door de rechtmatige houder. Met iedere vertrouwende partij is vastgelegd dat het DNA nooit meer gegevens zal verstrekken dan dat nodig is voor de beoogde transactie; opnieuw het *need-to-know* beginsel.
Voor de drankenhandel is uitsluitend van belang of Jansen meerderjarig is. Zelfs zijn naam doet er niet toe en hij kan de drank op iedere plaats laten afleveren. Voor het vliegticket gaan de eisen verder. Voor deze transactie zullen naam, voornaam, geboorteplaats, geboortedatum en mogelijk de nationaliteit en een e-mail adres of postadres moeten worden opgegeven. In veel gevallen zal met zogenaamde *presets* kunnen worden gewerkt[52].

Het komt er dus kort op neer, dat het basismodel bedrijven en instellingen zekerheid biedt bij de beantwoording van de vraag met wie zij handelen. Die zekerheid wordt geboden doordat een notaris de identiteitskenmerken heeft vastgesteld, in combinatie met de mogelijkheid tot verificatie bij het DNA.

2.3 Het tweede model: ontzorging voor de houders van databestanden

Volgens het basismodel blijven alle gegevens die door de notaris zijn ingevoerd, opgeslagen in het DNA en zijn daar, met inachtneming van het *need-to-know* principe, beschikbaar voor vertrouwende partijen. Die vertrouwende partijen beheren vaak tevens hun eigen bestanden van persoonsgegeven, of wel, zij hebben een eigen databank. Maar zoals uit het voorgaande bleek, het ligt in de rede dat de kosten voor onderhoud en beveiliging van bestanden met persoonsgegevens de komende jaren sterk zullen stijgen. Het aanhouden van die bestanden brengt voor bedrijven en instellingen toenemende risico's met zich mee – door strengere wetgeving, cyberaanvallen – en daarmee steeds hogere kosten. Het ligt in de lijn der verwachtingen dat men die risico's wil indammen en wellicht ook die kosten terug wil dringen. In deze paragraaf schetsen we een verdergaand model voor de toepassing van het notariële certificaat. In dit tweede model kunnen bedrijven en instellingen hun eigen databanken met persoonsgegevens outsourcen bij het DNA.

[52] Hiermee wordt bedoeld een met een bedrijf, instelling of groep van bedrijven tevoren overeengekomen set van data die voor het uitvoeren van de transactie nodig zijn. Een overeenkomst als die voor de levering van drank heeft een andere *preset* dan die voor het afsluiten van een verzekering.

Dit vraagt om de invoering van een nieuw element: het pseudoniem[53]. Uitgangspunt is dat een bedrijf zijn databank nodig heeft om te weten wie zijn klanten zijn. Die databank zal in de regel gevuld zijn met 'echte', herkenbare persoonsgegevens . De naam die iemand bij zijn geboorte meekreeg identificeert hem als persoon. Dit doel kan echter ook worden bereikt door niet de 'echte' persoonsnaam op te slaan, maar (slechts) een pseudoniem, mits dat pseudoniem gekoppeld kan worden aan de 'echte' persoonsnaam.
In ons tweede model is het niet langer noodzakelijk, dat een bedrijf of instelling volledige bestanden met persoonsgegevens onder zich heeft. Men kan volstaan met bestanden van pseudoniemen, die via het DNA gekoppeld kunnen worden aan 'echte' persoonsgegevens[54]. Op het moment dat een bedrijf een klant uit zijn bestand wil bereiken, geeft het bedrijf het pseudoniem van de betreffende klant door aan het DNA. Daar wordt bezien of de koppeling van het pseudoniem met een 'echt' persoonsgegeven mogelijk is, waarna afhankelijk van onderliggende afspraken kan worden gehandeld.
Het betreft hier dus een andere dimensie van het *need-to-know* beginsel. De volledige set van gegevens van hun klanten hebben de bij het systeem aangesloten bedrijven en instellingen niet langer zelf in beheer. De klant wordt nog slechts gekend aan zijn pseudoniem, dat uitsluitend identificeert voor wie over de juiste sleutel beschikt. De aangesloten bedrijven en instellingen hoeven slechts dit pseudoniem in hun databestanden op te slaan. Dat is voldoende, zolang maar vaststaat dat het pseudoniem is terug te voeren naar een persoon die houder is van een certificaat[55].

Wij voeren bij wijze van voorbeeld opnieuw onze modelburger op, de heer Jansen. Jansen wil een verzekering afsluiten. Hij logt in met zijn certificaat bij een verzekeringsmaatschappij die is aangesloten bij het DNA. De maatschappij registreert op het moment van inloggen het pseudoniem dat Jansen voor de beoogde transactie vanuit het DNA is toegekend. Op basis van het *need-to-know* principe geeft het DNA daarnaast aan de verzekeringsmaatschappij de persoonsgegevens van Jansen vrij, die nodig zijn voor de overeenkomst. Het is nu voor de maatschappij niet nodig om deze gegevens in een eigen databestand op te nemen. De

[53] Met een pseudoniem, ook wel alias genoemd, wordt hier bedoeld een al dan niet willekeurige reeks die via een mechanisme identificeert. Pseudoniemen zijn metagegevens, omdat zij het mogelijk maken een persoon virtueel te 'kennen' zonder op de hoogte te zijn van zijn werkelijke naam. Een voorbeeld van een pseudoniem in deze zin is het BSN.
[54] In het basismodel wordt reeds op deze ontwikkeling vooruit gelopen. Ook binnen dit model is reeds voorzien in de mogelijkheid een pseudoniem te kiezen.
[55] Dit herleiden van het pseudoniem tot een voor ieder kenbaar persoonsgegeven vindt plaats binnen een gesloten systeem van machines die elkaar 'kennen'. De eisen die dit stelt aan inrichting en beveiliging van het DNA laten wij hier onbesproken.

registratie van het pseudoniem van de heer Jansen is voldoende. Dit pseudoniem wordt aan de overeenkomst gekoppeld en wij voorzagen al dat de maatschappij zich waar nodig met dit pseudoniem kan melden bij het DNA.

2.4 Het derde model: werkelijke privacybescherming

Het derde en laatste model is een logische vervolgstap. Wanneer bedrijven en instellingen hun databestanden kunnen reduceren tot opgeslagen metagegevens, dan is dit ook mogelijk voor het DNA. In dit derde model worden de gegevens van de aanvrager zoals de notaris die bij de aanvraag van een certificaat vastlegt, niet langer bewaard in het DNA. Uitsluitend het pseudoniem van de aanvrager wordt daar nog opgeslagen. Ook het DNA 'kent' de achterliggende persoonsgegevens niet. De registratie van de persoonsgegevens geschiedt alleen nog bij de notaris, die ook het pseudoniem vastlegt en bewaart.
In dit model kan de koppeling tussen de persoon en zijn pseudoniem gevonden worden bij het notariskantoor. Daarnaast zal ook de gebruiker zelf zijn pseudoniem kennen, verbonden aan zijn certificaat, dus naar de stand van zaken bij het schrijven van dit artikel, op de app van zijn smartphone.

Hoe vergaat het onze modelburger Jansen wanneer hij op basis van dit model een verzekering aanvraagt? Niet zo heel anders dan in het vorige model. Met zijn certificaat logt hij in bij de verzekeringsmaatschappij. Het inloggegeven is nu niet gekoppeld aan zijn naam, maar aan zijn pseudoniem. De maatschappij checkt het pseudoniem bij het DNA en het DNA vraagt aan Jansen of hij de gegevens wil vrij geven die voor de transactie nodig zijn. Wanneer dit akkoord is, stuurt Jansen vanuit de app van zijn smartphone de benodigde (persoons)gegevens naar de maatschappij. Hij doet dit rechtstreeks of via een beveiligde verbinding met het DNA.

Dit derde model heeft als voordeel dat er niet langer sprake is van enige centrale opslag van persoonsgegevens. Er is opslag bij de notarissen, maar die is sterk verspreid, en daarnaast heeft de burger met zijn notariële certificaat zijn eigen persoonsgegevens in beheer gekregen. Dat maakt dit model weinig kwetsbaar voor grootschalig misbruik en sluit aan bij wat de wetgever voor ogen staat: de burger als baas over zijn eigen gegevens[56].

Tot slot: zes punten van overweging

[56] Zie in het bijzonder onder 1.3, de Algemene verordening gegevensbescherming. Wel zien wij een risico op het vlak van de beveiligingsmogelijkheden voor smartphones op dit moment.

Wij hebben in het tweede onderdeel van dit artikel een poging gedaan vanuit het wettelijke kader buiten de box te denken en het is algemeen bekend dat buiten de box denken, hoezeer ook gewaardeerd en vaak geëist, op het moment van toepassing allerlei aarzelingen oproept. Met een paar overwegingen hierover willen wij deze bijdrage beëindigen.

Om te beginnen de techniek. Dit punt stelt gerust. Wij hebben de indruk - en dit op gezag van de kenners van deze materie -, dat de techniek op dit moment niet langer een belemmering is voor de bouw van een systeem als hier beschreven. Het kan gewoon. De techniek zal in de toekomst nog beter en veiliger worden, maar hetzelfde geldt voor de technieken om in te breken en het systeem te verstoren. Daarom zijn we vooral gecharmeerd van het derde model, dat we onder 2.4 beschreven. De verspreiding van persoonsgegevens, dus opslag van delen over verschillende locaties, maakt het systeem minder kwetsbaar en past ook bij wat de wetgever voor ogen staat.

Een tweede overweging hebben wij bij de medewerking van het bedrijfsleven. Daarvoor zijn sterke prikkels nodig. Dat geldt zeker voor outsourcing van eigen databestanden. De strenger wordende wetgeving en de hoge boetes zullen daarvoor nauwelijks helpen, want dat zijn calculeerbare risico's. De decisieve prikkel is er wanneer het besef doorbreekt dat bij aansluiting bij het door ons beschreven systeem de torenhoge kosten van het onderhouden en beveiligen van een eigen databank vervallen.

Ons derde punt van aandacht ligt bij de burger. De burger wil een notarieel certificaat wanneer bedrijven en instellingen dit van hem vragen en dit certificaat met name daarom zijn leven gemakkelijker maakt. Zo ver zijn we nog niet.

De vierde overweging betreft de rol van de overheid. Het verschaffen van ook een digitale identiteit lijkt in beginsel een overheidstaak. Een hybride systeem zoals hier beschreven heeft goede papieren, omdat het in zijn opzet lenigheid kan bieden en door het vertrouwen dat het notariaat geniet. Daarmee lijkt het beter te kunnen inspelen op de wensen van de markt, terwijl ook op de wensen van de wetgever wordt ingegaan. Maar dit zal thans niet de opvatting zijn die alom wordt gedeeld.

Een vijfde punt betreft de acceptatie van juist deze oplossing. Willen bedrijven en instellingen erop vertrouwen, en als commerciële partijen er ook in berusten, dat het systeem in voldoende mate kan voorzien in hun wensen op het vlak van gegevensinformatie? Wil de burger

aannemen dat het notariële certificaat er is ter bescherming van zijn recht op privacy en wil hij daar het belang van inzien?

Het vernieuwende van het systeem dat wij in deze bijdrage beschreven, ligt niet in de techniek maar in de aanwending van de ‘toegevoegde waarden’ die in het notariaat besloten liggen, en dat laatste in een nieuwe context. De pretentie van het systeem en met name ook zijn potentie, kunnen gaan vragen om een organisatiemodel dat groter is, dan dat de KNB en de andere aan het project deelnemende partijen alleen kunnen bieden. Dit zien wij als een laatste punt van aandacht.