STAATSCOURANT
Officiële uitgave van het Koninkrijk der Nederlanden sinds 1814.
Nr. 39513
28 juli
2016

Advies Raad van State inzake het ontwerpbesluit digitalisering burgerlijk procesrecht en bestuursprocesrecht

Nader Rapport

12 juli 2016
780592
Directie Wetgeving en Juridische Zaken

Aan de Koning

Nader rapport inzake het ontwerpbesluit digitalisering burgerlijk procesrecht en bestuursprocesrecht

Blijkens de mededeling van de Directeur van Uw kabinet van 8 september 2015, nr. 2015001495, machtigde Uwe Majesteit de Afdeling advisering van de Raad van State haar advies inzake het bovenvermelde ontwerp van een algemene maatregel van bestuur rechtstreeks aan mij te doen toekomen. Dit advies, gedateerd 7 oktober 2015, nr. W03.15.0303/II, bied ik U hierbij aan.
Het ontwerp geeft de Afdeling advisering aanleiding tot het maken van de volgende opmerkingen.

1. Noodkanaal

Zoals de Afdeling terecht opmerkt, is een noodkanaal van essentieel belang voor partijen om met de rechter te communiceren, indien een storing zich voordoet. Het is aan de rechterlijke instanties om een dergelijk noodkanaal in te richten. Dit noodkanaal zal vergelijkbaar werken als de huidige piketregeling, waardoor buiten kantooruren om een partij met spoed kan communiceren met de rechter. In overeenstemming met het advies van de Afdeling is in de nota van toelichting duidelijker verwoord dat bij procesreglement een noodkanaal geregeld zal worden. Het is niet noodzakelijk om in het ontwerpbesluit een bepaling op te nemen die ziet op het instellen van een noodkanaal, aangezien de systematiek van de wetsvoorstellen inzake eenvoudig en digitaal procederen en het ontwerpbesluit uitgaan van het nader uitwerken van de wet- en regelgeving bij procesreglement. Het procesreglement is een landelijk reglement, zodat de zorg van de Afdeling dat niet bij alle gerechten een noodkanaal verzekerd is, niet gerechtvaardigd is. De huidige piketregeling bestaat eveneens al bij alle gerechten. De procesreglementen worden in overleg met ketenpartijen van de rechterlijke instanties opgesteld en kunnen naar aanleiding van ervaringen in de praktijk eenvoudig aangepast worden, indien nodig.

2. Redactionele bijlage

Met de redactionele opmerkingen van de Afdeling is rekening gehouden. Van de gelegenheid is gebruik gemaakt om ook nog enkele andere technische aanpassingen te doen.

Ik moge U hierbij het gewijzigde ontwerpbesluit en de gewijzigde nota van toelichting doen toekomen en U verzoeken overeenkomstig dit ontwerp te besluiten.

De Minister van Veiligheid en Justitie,
G.A. van der Steur.

Advies Raad van State

No. W03.15.0303/II
's-Gravenhage, 7 oktober 2015

Aan de Koning

Bij Kabinetsmissive van 8 september 2015, no. 2015001495, heeft Uwe Majesteit, op voordracht van de Minister van Veiligheid en Justitie, bij de Afdeling advisering van de Raad van State ter overweging aanhangig gemaakt het ontwerpbesluit houdende regels betreffende de digitale rechtsgang in het burgerlijk en bestuursrecht (Besluit digitalisering burgerlijk procesrecht en bestuursprocesrecht), met nota van toelichting.

Verschillende wetswijzigingen maken digitaal procederen in civiel- en bestuursrechtelijke zaken in de toekomst mogelijk.[1] Het onderhavige besluit (hierna: ontwerpbesluit) stelt enerzijds voorwaarden aan het nieuwe digitale systeem van de rechterlijke instanties en anderzijds stelt het voorwaarden aan de rechtzoekende en diens procesvertegenwoordiger als gebruiker van het digitale systeem.

De Afdeling advisering van de Raad van State adviseert het besluit vast te stellen, maar acht aanpassing van het ontwerpbesluit aangewezen, zodat het gebruik van een noodkanaal bij alle gerechten is verzekerd. Dat onder omstandigheden van een dergelijk noodkanaal gebruik gemaakt moet kunnen worden, maakt naar het oordeel van de Afdeling dat daarin voorzien moet worden.

1. Instellen noodkanaal

Artikel 8 van het ontwerpbesluit bepaalt dat een overschrijding van de indieningstermijn van een bericht niet aan de indiener zal worden toegerekend, als deze het gevolg is van een niet aan hem toerekenbare verstoring van de toegang tot het digitale systeem.[2] Een daardoor veroorzaakte overschrijding van de termijn is verschoonbaar als het bericht uiterlijk wordt ingediend op de eerstvolgende dag na de dag waarop de indiener ermee bekend had kunnen zijn dat de verstoring is verholpen. In de consultatie is door diverse instanties de behoefte geuit om voor bepaalde gevallen een noodkanaal beschikbaar te stellen. Hierbij wordt gedacht aan procedures waar binnen een korte periode proceshandelingen moeten worden verricht, met eventueel vergaande en onomkeerbare gevolgen. In de toelichting wordt de wenselijkheid van een dergelijk noodkanaal in uitzonderingssituaties onderschreven.[3] Het noodkanaal kan volgens de toelichting worden geïntegreerd in de huidige piketvoorzieningen. Rechterlijke instanties kunnen hierover bij (proces)reglement nadere regels opstellen.

De Afdeling onderschrijft de noodzaak van een noodkanaal voor situaties waar binnen een korte tijd proceshandelingen moeten worden verricht met eventueel vergaande of onomkeerbare gevolgen. Weliswaar kan via de procesreglementen in een noodkanaal worden voorzien, maar daarmee is het bestaan van een noodkanaal bij alle gerechten niet verzekerd. Dat onder omstandigheden van een dergelijk noodkanaal gebruik gemaakt moet kunnen worden, maakt naar het oordeel van de Afdeling dat daarin voorzien moet worden. De Afdeling adviseert daarom de instelling van een noodkanaal bij alle gerechten te verzekeren en het besluit daarop aan te passen.

Gelet hierop adviseert de Afdeling het ontwerpbesluit op dit punt aan te passen.

---

1 De Wet tot wijziging van het Wetboek van Burgerlijke Rechtsvordering en de Algemene wet bestuursrecht in verband met vereenvoudiging en digitalisering van het procesrecht (EK 2014–15 34 059, A), de Wet tot wijziging van het Wetboek van Burgerlijke Rechtsvordering in verband met vereenvoudiging en digitalisering van het procesrecht in hoger beroep en cassatie (EK 2014–15 34 138, A) en de Wet tot aanpassing van de wetgeving aan en invoering van de Wet vereenvoudiging en digitalisering van het procesrecht en van de Wet vereenvoudiging en digitalisering van het procesrecht in hoger beroep en cassatie (Kamerstukken II 2014–15 34 212, nr. 2) zijn hiertoe momenteel aanhangig bij de Eerste respectievelijk de Tweede Kamer.

2 Artikel 8 van het ontwerpbesluit luidt: Indien op de laatste dag van een voor de indiener geldende termijn voor indiening van een bericht een niet aan hem toerekenbare verstoring plaatsvindt van de toegang tot een digitaal systeem voor gegevensverwerking van de rechterlijke instanties, is een daardoor veroorzaakte overschrijding van die termijn verschoonbaar indien het bericht uiterlijk wordt ingediend op de eerstvolgende dag na de dag waarop de indiener ermee bekend had kunnen zijn dat de verstoring is verholpen. Artikel 1, eerste lid, van de Algemene termijnenwet is van overeenkomstige toepassing op deze eerstvolgende dag.

3 Artikelsgewijze toelichting artikel 8.

2. De Afdeling verwijst naar de bij dit advies behorende redactionele bijlage.

De Afdeling advisering van de Raad van State geeft U in overweging in dezen een besluit te nemen, nadat met het vorenstaande rekening zal zijn gehouden.

De vice-president van de Raad van State,
J.P.H. Donner.

Redactionele bijlage bij het advies van de Afdeling advisering van de Raad van State betreffende no.W03.15.0303/II

– In de toelichting wordt ten onrechte vermeld dat er een Privacy Impact Assessment (PIA) is opgesteld.[4] Het door de Raad voor de Rechtspraak opgestelde Privacykader Digitaal Procederen in het Civiele en Bestuursrecht (KEI), gedateerd 16 april 2015, is een beschrijving van het kader voor mogelijke inbreuken op de privacy en geen PIA.

[4] Algemeen deel van de toelichting, onder 3.

Tekst zoals toegezonden aan de Raad van State: Besluit van ..... houdende regels betreffende de digitale rechtsgang in het burgerlijk en bestuursrecht (Besluit digitalisering burgerlijk procesrecht en bestuursprocesrecht)

Wij Willem-Alexander, bij de gratie Gods, Koning der Nederlanden, Prins van Oranje-Nassau, enz. enz. enz.

Op de voordracht van Onze Minister van Veiligheid en Justitie van 3 september 2015, nr. 680800;

Gelet op de artikelen 30c, derde lid, 30f, 30n, achtste lid, van het Wetboek van Rechtsvordering, artikelen 8:36b, tweede lid, 8:36d, tweede lid en 8:36f van de Algemene wet bestuursrecht en artikel 24, tweede lid, van de Wet bescherming persoonsgegevens;

De Afdeling advisering van de Raad van State gehoord (advies van ..... 201X, nr. .....);

Gezien het nader rapport van Onze Minister van Veiligheid en Justitie van ..... 201X, nr. .....;

Hebben goedgevonden en verstaan:

Artikel 1

In dit besluit worden onder rechterlijke instanties verstaan:
a. de gerechten zoals bedoeld in artikel 2 van de Wet op de Rechterlijke Organisatie;
b. de Afdeling bestuursrechtspraak van de Raad van State;
c. het College van Beroep voor het bedrijfsleven;
d. de Centrale Raad van Beroep.

Artikel 2

1. De rechterlijke instanties stellen een digitaal systeem voor gegevensverwerking ter beschikking. Dit systeem voldoet aan de volgende eisen:
   a. de gebruiker van het systeem wordt geïdentificeerd;
   b. na te gaan is wie wordt beschouwd als verzender van een bericht;
   c. na te gaan is of een bericht is gewijzigd na het moment van verzending;
   d. na te gaan is op welk tijdstip een bericht is ontvangen respectievelijk ter beschikking is gesteld in het systeem;
   e. na te gaan is wanneer zich een storing in het systeem voordoet en heeft voorgedaan; en
   f. de stukken in het digitale dossier zijn in het systeem uitsluitend toegankelijk voor personen die daarvoor zijn geautoriseerd.

2. Het digitale systeem, genoemd in het eerste lid, is ingericht volgens nationale en internationale standaarden voor informatiebeveiliging. Bij ministeriële regeling kan worden bepaald aan welke standaarden dit digitale systeem in ieder geval voldoet.

Artikel 3

Authenticatie om toegang te krijgen tot een digitaal systeem voor gegevensverwerking van de rechterlijke instanties, vindt plaats met een middel dat voldoet aan de volgende eisen:
a. het is uitgegeven door de overheid of een onder toezicht van de overheid staande organisatie;
b. het gaat uit van een tweefactorauthenticatie; en
c. het is aangewezen door de rechterlijke instanties.

Artikel 4

1. Degene die een gerechtelijke procedure start of daarbij is betrokken en gebruik maakt of dient te maken van stukkenwisseling langs elektronische weg als bedoeld in artikel 30c van het Wetboek van Burgerlijke Rechtsvordering en artikel 8:36a van de Algemene wet bestuursrecht, gebruikt voor het elektronisch indienen en ophalen van berichten een door de rechterlijke instanties aangewezen digitaal systeem voor gegevensverwerking.

2. Bij ministeriële regeling kunnen nadere regels worden gesteld aan de wijze waarop berichten worden ingediend langs de weg als bedoeld in het eerste lid. Tevens kunnen nadere regels worden gesteld die betrekking hebben op de eisen waaraan een bericht dient te voldoen dat langs deze weg wordt ingediend.

3. Bij ministeriële regeling kunnen nadere regels worden gesteld die betrekking hebben op de eisen

waaraan het door een gerechtsdeurwaarder te betekenen oproepingsbericht, bedoeld in de artikelen 112 en 113 van het Wetboek van Burgerlijke Rechtsvordering, moet voldoen.

Artikel 5

1. De elektronische handtekening, bedoeld in artikel 30c, derde lid, van het Wetboek van Burgerlijke Rechtsvordering en artikel 8:36d, tweede lid, van de Algemene wet bestuursrecht, voldoet aan de volgende eisen:
   a. de ondertekenaar heeft zich geauthenticeerd met een middel dat voldoet aan de eisen gesteld in artikel 3 van dit besluit; en
   b. zij is op zodanige wijze verbonden aan het elektronische bestand waarop zij betrekking heeft, dat de identiteit van de ondertekenaar, het moment van ondertekening en elke wijziging na ondertekening van het document kunnen worden achterhaald.

2. In afwijking van het eerste lid, onder a, voldoet de handtekening die handmatig op een elektronische gegevensdrager wordt geschreven aan de volgende eisen:
   a. zij heeft plaatsgevonden in het bijzijn van een rechter of griffier of is gezet door een rechter of griffier; en
   b. zij is op zodanige wijze verbonden aan het elektronische bestand waarop zij betrekking heeft, dat de identiteit van de ondertekenaar, het moment van ondertekening en elke wijziging na ondertekening van het document kunnen worden achterhaald.

Artikel 6

1. Indien een natuurlijk persoon over een burgerservicenummer beschikt, is
   a. degene die beroepsmatig rechtsbijstand verleent,
   b. de gerechtsdeurwaarder, of
   c. een andere gemachtigde in zaken waarin partijen in persoon kunnen procederen,
   bevoegd om dit nummer van de persoon die hij vertegenwoordigt of in wiens opdracht hij handelt te verwerken tijdens een procedure.

2. De gerechtsdeurwaarder is tevens bevoegd om bij het indienen van de procesinleiding en het exploot van betekening het burgerservicenummer van de verweerder te verwerken, indien deze een natuurlijke persoon is die hierover beschikt.

Artikel 7

In aanvulling op artikel 30c, vierde lid, van het Wetboek van Burgerlijke Rechtsvordering en artikel 8:36b, tweede lid, van de Algemene wet bestuursrecht geldt de verplichting tot procederen langs elektronische weg niet voor een onderneming of rechtspersoon die niet op grond van artikel 5 of artikel 6 Handelsregisterwet is ingeschreven in het handelsregister, tenzij deze wordt vertegenwoordigd door een derde die in Nederland verplicht is tot digitaal procederen.

Artikel 8

Indien op de laatste dag van een voor de indiener geldende termijn voor indiening van een bericht een niet aan hem toerekenbare verstoring plaatsvindt van de toegang tot een digitaal systeem voor gegevensverwerking van de rechterlijke instanties, is een daardoor veroorzaakte overschrijding van die termijn verschoonbaar indien het bericht uiterlijk wordt ingediend op de eerstvolgende dag na de dag waarop de indiener ermee bekend had kunnen zijn dat de verstoring is verholpen. Artikel 1, eerste lid, van de Algemene termijnenwet is van overeenkomstige toepassing op deze eerstvolgende dag.

Artikel 9

De artikelen van dit besluit treden in werking op een bij koninklijk besluit te bepalen tijdstip, dat voor de verschillende artikelen of onderdelen daarvan verschillend kan worden vastgesteld.

Artikel 10

Dit besluit wordt aangehaald als: Besluit digitalisering burgerlijk procesrecht en bestuursprocesrecht.

Lasten en bevelen dat dit besluit met de daarbij behorende nota van toelichting in het Staatsblad zal worden geplaatst.

De Minister van Veiligheid en Justitie,

NOTA VAN TOELICHTING

Algemeen

1. Inleiding

De samenleving is in de afgelopen jaren in rap tempo gedigitaliseerd. Het is van belang dat de rechtspraak voldoende aansluit bij relevante ontwikkelingen in de maatschappij, om het grote vertrouwen van de maatschappij in de rechtspraak te behouden. De Raad voor de rechtspraak heeft dan ook in 2012 bij mij de wens geuit om de rechtspraak, in het bijzonder de civiel- en bestuursrechtelijke rechtspraak, te moderniseren. De twee hoofdelementen van deze modernisering zijn de digitalisering van de civiel- en bestuursrechtelijke procedure en de vereenvoudiging en versnelling van de civielrechtelijke procedure. Gezien het belang van kwalitatief hoogwaardige rechtspraak voor de rechtstaat, heb ik – tegelijk met de Raad voor de rechtspraak – het programma Kwaliteit en Innovatie rechtspraak gestart. De wetgeving die binnen dit programma is ontwikkeld, faciliteert de modernisering van de rechtspraak.
De Wet tot wijziging van het Wetboek van Burgerlijke Rechtsvordering en de Algemene wet bestuursrecht in verband met vereenvoudiging en digitalisering van het procesrecht, de Wet tot wijziging van het Wetboek van Burgerlijke Rechtsvordering in verband met vereenvoudiging en digitalisering van het procesrecht in hoger beroep en cassatie en de Wet tot aanpassing van de wetgeving aan en invoering van de Wet vereenvoudiging en digitalisering van het procesrecht en van de Wet vereenvoudiging en digitalisering van het procesrecht in hoger beroep en cassatie (hierna ook gezamenlijk: wet vereenvoudiging en digitalisering procesrecht en samenhangende wetten) maken digitaal procederen in civiel- en bestuursrechtelijke zaken mogelijk. De Raad voor de rechtspraak ontwikkelt een digitaal systeem voor gegevensverwerking dat gebruikt zal worden door de rechtbanken, de gerechtshoven, het College van Beroep voor het bedrijfsleven en de Centrale Raad van Beroep. De Hoge Raad en de Afdeling bestuursrechtspraak van de Raad van State zullen beide een eigen, op hoofdlijnen vergelijkbaar, digitaal systeem voor gegevensverwerking ten behoeve van het elektronisch indienen van berichten ter beschikking stellen. Deze drie systemen zullen hierna worden aangeduid als: het digitale systeem van de rechterlijke instanties. Naast deze webportalen wordt onder bepaalde voorwaarden een automatische systeemkoppeling (een aansluitpunt voor geautomatiseerde gegevensverwerking) ter beschikking gesteld. Met deze voorziening kunnen de digitale systemen van ketenpartijen zoals de IND en deurwaarders, geleidelijk worden gekoppeld aan het digitale systeem van de rechterlijke instanties.
Het onderhavige besluit stelt enerzijds voorwaarden aan het nieuwe digitale systeem van de rechterlijke instanties en anderzijds stelt het voorwaarden aan de rechtzoekende en diens procesvertegenwoordiger als gebruiker van het digitale systeem. Twee van de belangrijkste uitgangspunten van dit besluit zijn de bescherming van de persoonsgevoelige gegevens en andere gevoelige gegevens (zoals van bedrijven) die in dossiers voorkomen en de gebruiksvriendelijkheid van het digitale systeem. Hierbij geldt als randvoorwaarde dat voorstellen realiseerbaar moeten zijn, zowel voor de rechterlijke instanties als voor de rechtzoekende en diens vertegenwoordiger. Waar deze toelichting ingaat op een beschrijving van het digitale systeem wordt hiermee niet een wijziging van het huidige procesrecht beoogd, voor zover dat ziet op welke partijen proceshandelingen mogen verrichten en de bevoegdheid tot het verrichten van een proceshandeling namens een partij. Zo verandert de huidige praktijk niet dat alleen een advocaat die zich gesteld heeft processtukken mag indienen. Evenmin wordt een wijziging beoogd van de regel dat alleen een medewerker van een rechtspersoon of bestuursorgaan die over een mandaat of volmacht beschikt, in opdracht van de desbetreffende organisatie proceshandelingen (zoals het indienen van stukken) mag verrichten. De technische mogelijkheden doorkruisen daarmee niet het huidige procesrecht. Om de digitalisering van het strafprocesrecht nader te regelen wordt een vergelijkbaar besluit opgesteld.
Het besluit is zo veel mogelijk techniekneutraal geformuleerd, om te voorkomen dat het vanwege nieuwe technische ontwikkelingen op korte termijn zou moeten worden aangepast. De beschrijving van het digitale systeem gaat uit van de huidige stand van de techniek. Bij nieuwe ontwikkelingen kunnen bepaalde beschreven situaties (zoals het inloggen via eHerkenning) wijzigen. De rechterlijke instanties kunnen op grond van dit besluit bepaalde aspecten van het digitaal procederen – zoals de technische voorwaarden – nader regelen bij (proces)reglementen. Gezien de positie van de rechterlijke instanties in het Nederlandse rechtsbestel mag erop worden vertrouwd dat zij zorgvuldig omgaan met de belangen van partijen. Dit houdt onder meer in dat zij ketenpartijen en andere rechtzoekenden betrekken bij het opstellen en wijzigen van de benodigde procesreglementen. Vanzelfsprekend moet aan ketenpartijen en andere rechtzoekenden voldoende tijd worden geboden om zich deugdelijk op dergelijke wijzigingen voor te bereiden.
Overigens wordt in dit besluit met het digitale systeem van de rechterlijke instanties niet uitsluitend verwezen naar het portaal ‘Mijn Zaak’, waarmee partijen toegang kunnen krijgen tot hun digitale dossier, maar ook naar de automatische systeemkoppeling tussen het digitale systeem van de rechterlijke instanties en ketenpartijen. Het digitale systeem dat door de Raad voor de rechtspraak wordt ontwikkeld stelt onder voorwaarden een automatische systeemkoppeling ter beschikking. Voor

de andere rechterlijke instanties geldt dat een goede afweging gemaakt moet worden omtrent de kosten van de ontwikkeling en het beheer van een dergelijke systeemkoppeling, afgezet tegen het aantal zaken dat zij op jaarlijkse basis behandelen en het aantal ketenpartijen dat procedures bij hen voert. De eisen die het besluit stelt aan het digitale systeem gelden voor beide wijzen van het elektronisch indienen en ophalen van berichten.

2. Digitale procesvoering

Een rechtzoekende of, namens hem, een (al dan niet professioneel) gemachtigde moet onderscheidenlijk kan een civiel- of bestuursrechtelijke procedure digitaal voeren. Dat wil zeggen dat digitaal zullen plaatsvinden: het starten van een procedure, het indienen en ontvangen van berichten (onder berichten wordt in het besluit en in deze toelichting onder meer verstaan: (proces)stukken, mededelingen, bestanden en formulieren), het volgen van de voortgang van de procedure, de toegang tot het digitale dossier, de communicatie met de rechter en het ontvangen van de uitspraak van de rechter. De mondelinge behandeling blijft in persoon plaatsvinden. Ook worden de regels voor verplichte procesvertegenwoordiging niet gewijzigd. Waar deze toelichting ingaat op communicatie door of met de rechter, kan hiervoor mede gelezen worden een rechtspraakmedewerker die in zijn opdracht handelt, zoals de griffier, of de desbetreffende rechterlijke instantie.
De digitale mogelijkheden bieden partijen en de rechtspraak veel voordelen. Het digitale systeem van de rechterlijke instanties maakt de rechtspraak toegankelijker. Het is voor een rechtzoekende of zijn gemachtigde eenvoudiger en laagdrempeliger om (vanuit huis of kantoor) digitaal een procedure te starten of verweer te voeren en direct alle relevante berichten in te dienen. Tegenwoordig hebben partijen het merendeel van de stukken digitaal voorhanden. Dankzij de digitalisering hoeven zij deze stukken niet eerst uit te printen, eventueel te kopiëren en per post naar de rechter te sturen en, afhankelijk van de procedure, naar de wederpartij. Verder kan een partij eenvoudig zelf, zonder tussenkomst van haar advocaat, het digitale dossier inzien en zo bijvoorbeeld alle berichten bekijken en de voortgang van haar procedure volgen. De rechter kan voorts laagdrempelig en snel een bericht aan partijen sturen. Zo kan hij bijvoorbeeld voorafgaand aan de mondelinge behandeling vragen aan partijen stellen die hij tijdens de mondelinge behandeling wil bespreken. Onder meer advocaten hebben aangegeven hier behoefte aan te hebben, omdat het hen helpt bij de voorbereiding van de zitting. Verder kunnen partijen voortaan documenten uit het digitale dossier in hun eigen systeem opslaan, bijvoorbeeld uit het oogpunt van archivering (waarvoor zij net als nu zelf verantwoordelijk blijven).
Professionele partijen zijn verplicht om digitaal te procederen. Natuurlijke personen die onder de uitzondering van artikel 30c, vierde lid, van het Wetboek van Burgerlijke Rechtsvordering (hierna: Rv) en artikel 8:36b, tweede lid, van de Algemene wet bestuursrecht (hierna: Awb) vallen, kunnen desgewenst kiezen voor digitaal procederen. Partijen moeten hierbij gebruikmaken van het digitale systeem van de rechterlijke instanties. Voor alle gebruikers van het digitale systeem geldt dat zij vertrouwen moeten kunnen hebben in de stabiliteit en beveiliging van dat systeem. Zij moeten er zeker van kunnen zijn dat zorgvuldig en vertrouwelijk wordt omgegaan met de persoonsgegevens of bedrijfsgevoelige gegevens die zij tijdens de procedure aan de rechter verstrekken. Daarom worden voorwaarden gesteld aan het digitale systeem om de bescherming van deze gegevens te waarborgen. In de toelichting bij artikel 2 wordt hier nader op ingegaan.

3. Persoonsgegevens

De onderscheiden rechterlijke instanties verwerken de gegevens naar de normen in de Wet bescherming persoonsgegevens (hierna: de Wbp). De Wbp vereist dat een organisatie of instelling waar persoonsgegevens worden verwerkt, als verantwoordelijke wordt aangewezen. De verantwoordelijke bepaalt welke gegevens worden verwerkt, ten behoeve van welk doel en op welke wijze deze verwerking plaatsvindt. Deze gegevensverwerking moet op behoorlijke en zorgvuldige wijze plaatsvinden. De verantwoordelijke is voorts verplicht om de verwerking van de persoonsgegevens voldoende te beveiligen (bij de relevante bepalingen in het besluit wordt nader toegelicht hoe dit plaatsvindt). Het doel van de verwerking van persoonsgegevens door de rechterlijke instanties is: een goede en zorgvuldige rechtspleging en procesvoering.
Dit doel is niet anders dan in de oude situatie waarbij persoonsgegevens in papieren dossiers voorkwamen en door de betrokken rechterlijke instanties vervolgens digitaal in het eigen systeem werden verwerkt. De wijze van verwerking van de persoonsgegevens door de rechterlijke instanties wijzigt daarom niet. Wel de wijze waarop de persoonsgegevens bij de rechterlijke instanties terecht komen. Naast de papieren route (die voor bepaalde personen of organisaties openstaat, zie de toelichting bij artikel 7), worden persoonsgegevens langs elektronische weg gezonden aan de rechterlijke instanties. De persoonsgegevens die partijen aan de rechterlijke instanties verstrekken zijn, met uitzondering van het burgerservicenummer (hierna: BSN; zie de toelichting bij artikel 6), dezelfde als in de oude situatie. De gegevens die voorkomen in een dossier, zoals normaliter het adres van een partij, zijn uitsluitend toegankelijk voor de bij het geding betrokken partijen. Het BSN is alleen vereist voor een goede werking van het digitale systeem en is niet zichtbaar voor de bij het geding betrokken

partijen. Het digitale systeem heeft het BSN van een natuurlijke persoon nodig om hem aan het juiste dossier te koppelen. Op kleinere schaal was het langs elektronische weg aanleveren van gegevens (inclusief het BSN) al het geval in procedures op grond van artikel 8:40a Awb en bij de e-kantonprocedure.
Op grond van de Wbp dient de verantwoordelijke partij (in de zin van de Wpb) informatie te verschaffen over onder meer het doel waarvoor gegevens worden verwerkt. Zo kan deze informatie worden verstrekt op de website van de rechterlijke instanties of bij invulling van het digitale formulier. Een partij die wil weten welke persoonsgegevens van haar worden verwerkt, kan deze vraag stellen aan de rechterlijke instantie waar haar zaak in behandeling is. Een partij kan ook een verzoek doen tot een correctie van haar gegevens, bijvoorbeeld als zij feitelijk onjuist zijn. Op de website van de verschillende rechterlijke instanties wordt hierover meer informatie gegeven.
Voor wat betreft het digitale systeem van de rechtbanken, gerechtshoven, het College van beroep voor het bedrijfsleven en de Centrale Raad van Beroep is er een gedeelde verantwoordelijk voor de verwerking van persoonsgegevens als bedoeld in de Wbp. In dit kader is ook relevant om te vermelden dat de Raad voor de rechtspraak opdrachtgever is van Spir-IT, het ICT-bedrijf van de Raad dat het digitale systeem van de gerechten ontwikkelt. De Raad draagt zorg voor een zorgvuldige gegevensverwerking door onder meer de ontwikkeling van privacykaders. Daarnaast voldoet de Raad aan de informatieplicht jegens de betrokkene in de zin van de Wbp en geeft hij informatie over de wijze waarop deze betrokkene haar rechten kan uitoefenen, onder meer door informatieverschaffing via de website van de rechtspraak. De ontwikkeling van het digitale systeem vindt plaats in samenspraak met de gerechtsbesturen. De gerechtsbesturen zijn verantwoordelijk voor de juistheid van de gegevens in een specifiek zaakdossier wanneer een procedure bij dat gerecht aanhangig is. De Hoge Raad onderscheidenlijk de Afdeling bestuursrechtspraak ontwikkelt zijn, respectievelijk haar, eigen digitale systeem. De Hoge Raad is verantwoordelijk voor de verwerking van persoonsgegevens in het digitale systeem dat hij ter beschikking stelt. Hetzelfde geldt voor de Afdeling bestuursrechtspraak ten aanzien van het digitale systeem dat zij ter beschikking stelt.
Een Privacy Impact Assessment (PIA) is opgesteld. Een PIA is een hulpmiddel voor het meewegen van privacybelangen in de besluitvorming over de ontwikkeling van producten, diensten of wetgeving. Ten behoeve van het wetsvoorstel digitalisering en vereenvoudiging procesrecht is eveneens een PIA opgesteld. De PIA ten behoeve van dit besluit gaat in op de verschillende aspecten van privacy in het kader van de digitalisering van de civiele en bestuursrechtelijke procedure.

4. Toegang tot het digitale dossier

Een dossier in een rechtszaak is vanzelfsprekend niet voor eenieder toegankelijk. Van openbaarheid van het dossier is geen sprake. Dat was al zo en dat blijft zo. Nieuw is wel dat berichten digitaal worden opgeslagen en dat partijen toegang hebben tot hun digitale dossier via het portaal ‘Mijn Zaak’ (waar zij voorheen kopieën van het papieren dossier hadden). Daarom is opnieuw bezien hoe kan worden voorkomen dat gegevens verder worden verspreid dan noodzakelijk is voor de behandeling van de zaak. Het digitale systeem van de rechterlijke instanties moet de vertrouwelijkheid van gegevens waarborgen. In beginsel hebben bij de rechterlijke instanties alleen de daartoe bevoegde medewerkers toegang tot een specifiek dossier. Verder hebben de partijen bij het geding toegang. Hierbij kan gedacht worden aan de eiser of de verzoeker (waaronder begrepen de indiener van een beroepschrift), de verweerder, (derde) belanghebbenden, degene die zich voegt of tussenkomt en de (eventuele) gemachtigden van al deze partijen. Doordat al deze partijen en betrokkenen toegang hebben tot hetzelfde digitale dossier is de informatievoorziening van partijen toegankelijker en overzichtelijker dan in de oude situatie. Werkaantekeningen vallen vanzelfsprekend niet onder het inzagerecht van partijen, zoals ook voortvloeit uit artikel 35 van de Wbp. Ook dit is niet anders dan in de oude situatie met papieren dossiers.
De burger met een gemachtigde heeft in beginsel het recht om zelf zijn digitale dossier in te zien. Het is een van de voordelen van de digitalisering van de civiel- en bestuursrechtelijke rechtsgang dat een burger zelf de voortgang van de procedure kan inzien. Waar het procedures betreft waarin een gemachtigde namens vele, soms tientallen, rechtzoekenden optreedt (bijvoorbeeld bestemmingsplanzaken of massaschadezaken) kunnen de rechterlijke instanties bij (proces)reglement het aantal rechtzoekenden dat zelf toegang heeft tot het digitale dossier beperken. Dit houdt verband met de omstandigheid dat anders per persoon zou moeten worden nagegaan wat de identiteit van de desbetreffende persoon is en of hij recht heeft op toegang tot het digitale systeem. Deze afweging kan niet volledig geautomatiseerd plaatsvinden en zou een te grote belasting op de organisatie van de rechterlijke instanties leggen. De rechtzoekenden zullen in zo’n geval toegang tot het dossier kunnen verkrijgen via de gemachtigde, vergelijkbaar met de oude situatie.
Ook anderen die betrokken worden bij de procedure hebben toegang tot hun digitale dossier. Zo is het voor een belanghebbende bij een verzoek in een civiele procedure van belang dat hij toegang kan krijgen tot het digitale dossier, nadat het gerecht hem als belanghebbende heeft opgeroepen. Op basis van het verzoek en de onderliggende stukken kan hij vervolgens beoordelen of hij in de procedure wil verschijnen en verweer wil voeren. Hieraan kunnen namelijk bepaalde kosten verbonden zijn, bijvoorbeeld voor het inschakelen van een rechtsbijstandverlener of voor griffierechten. Een derdebe-

langhebbende in het bestuursrecht krijgt toegang tot het digitale dossier, nadat hij als zodanig is aangemerkt door de bestuursrechter. Hij moet toegang kunnen krijgen tot het digitale dossier om zijn standpunten naar voren te brengen bij de rechter. Bepaalde besluiten, zoals een bestemmingsplan, kennen veel belanghebbenden. Gelet op de bescherming van onder meer de persoonsgegevens in een dossier, is van belang dat alleen een derdebelanghebbende die als partij is aangemerkt, toegang krijgt tot het digitale dossier. Overigens kan pas tijdens de procedure blijken of een partij die beroep heeft ingesteld wel 'belanghebbende' is in de zin van de Awb. Als deze partij is opgekomen tegen bijvoorbeeld een omgevingsvergunning van een derde, dan is de houder van die omgevingsvergunning de derdebelanghebbende. Beide moeten toegang kunnen krijgen tot het digitale dossier, in het kader van de gerechtelijke procedure.
In dit besluit is gekozen voor de term 'betrokkenen', als het een persoon of organisatie betreft, die geen partij is maar wel betrokken is bij de procedure. Deze term volgt uit artikel 30c, eerste lid, Rv en artikel 8:36a, tweede lid, Awb, waarin wordt gesproken van 'anderen dan partijen, die bij de procedure worden betrokken'. Dat kunnen derdebelanghebbenden in het bestuursrecht zijn voordat zij als partij deelnemen aan de procedure, maar ook bijvoorbeeld deskundigen, tolken, getuigen, werkgevers of bestuursorganen die geen partij zijn, de Europese Commissie of de Autoriteit Consument & Markt (artikel 8:45a Awb). Het uitgangspunt voor deskundigen en andere betrokkenen, voor zover zij geen natuurlijke personen zijn, is dat zij stukken digitaal indienen. De rechter kan indiening op papier echter toestaan op grond van de voormelde artikelen.
Het kan voorkomen dat partijen of anderen die bij een procedure worden betrokken alleen toegang krijgen tot een bepaald deel van het dossier of alleen gedurende een bepaalde periode. Indien zij op papier procederen, krijgen zij alleen het voor hen relevante deel van het dossier toegezonden. Hierbij kan gedacht worden aan een deskundige die een deskundigenrapport moet opmaken en indienen. In bepaalde zaken kan het onwenselijk zijn als een dergelijke deskundige toegang zou krijgen tot het hele dossier en bovendien gedurende de hele procedure. Verder kan gedacht worden aan zaken waarin de rechter besluit over de uithuisplaatsing van een kind. Het kind is een belanghebbende bij het verzoek dat in beginsel door de Raad voor de kinderbescherming is ingediend en mag bepaalde onderdelen van zijn dossier inzien. Het kan echter onwenselijk zijn dat hij het hele dossier zou kunnen inzien, waaronder een rapport van een deskundige over het kind of diens gezinssituatie. Voorts kan worden gedacht aan loonvorderingszaken, waarbij de werkgever de medische stukken van de werknemer niet mag inzien. Partijen kunnen hierbij een beroep doen op artikelen 22 en 22a Rv en artikelen 8:29 en 8:32 Awb. Het is aan de rechter om te bepalen tot welk deel van het dossier een dergelijke persoon of partij toegang krijgt en gedurende welke periode. Het ligt in de rede dat de rechterlijke instanties hiervoor bij (proces)reglement uitgangspunten zullen formuleren, die de rechter in het individuele geval houvast geven. Overigens vond deze toets ook in de oude situatie plaats, waarbij de rechter kon besluiten dat bepaalde partijen of betrokkenen uitsluitend bepaalde delen van het dossier konden inzien. Naar aanleiding van de reactie op de consultatie van de Nederlandse Orde van Belastingadviseurs merk ik dan ook op dat het besluit aansluit bij de bestaande wetgeving en jurisprudentie ten aanzien van het omgaan met persoonsgevoelige gegevens en bedrijfsgevoelige gegevens. Het instellen van een beroepsmogelijkheid omtrent een beslissing van de rechter over de vraag welke partijen tot welk onderdeel van het dossier toegang hebben, acht ik niet nodig.
De rechter, griffier, partijen en anderen die bij de procedure worden betrokken, moeten op zorgvuldige wijze omgaan met de persoonsgegevens in het dossier. Deze plicht is mede verankerd in de Wbp. Er kunnen ook andere gevoelige gegevens in een dossier staan, zoals bedrijfsgeheimen. Het delen van een dossier waarin gevoelige gegevens voorkomen kan tot schade leiden en daarmee een onrechtmatige daad zijn. De verplichting om op zorgvuldige wijze om te gaan met gevoelige gegevens in een dossier geldt ongeacht of het een papieren dossier of een digitaal dossier is. Een separate regeling over de bescherming van persoonsgegevens en andere gevoelige gegevens die beveiligd moeten worden (zoals bedrijfsgeheimen) is in dit besluit dan ook niet nodig.

5. Authenticatie en autorisatie

Om te waarborgen dat alleen bevoegden toegang kunnen krijgen tot een individueel dossier moeten in het portaal 'Mijn Zaak' drie stappen worden doorlopen om toegang te krijgen tot een zaakdossier: identificatie, authenticatie en autorisatie. Allereerst is het van belang dat degene die toegang wenst te krijgen tot het digitale systeem, om een procedure te starten, om verweer te voeren of om anderszins inzage te krijgen in het dossier, zich op betrouwbare wijze identificeert. Authenticatie dient ertoe om met voldoende betrouwbaarheid vast te stellen dat degene die deze toegang wenst te krijgen, ook degene is die hij zegt te zijn. Zijn identiteit wordt hiermee vastgesteld.
De gebruiker van het digitale systeem van de rechterlijke instanties authenticeert zich met een middel dat voldoet aan de voorschriften die zijn opgenomen in dit besluit (zie de toelichting bij artikel 3). De rechterlijke instanties kunnen op grond van dat artikel bij (proces)reglement voorschrijven met welke middelen een partij of een andere betrokkene bij de procedure, zich kan authenticeren om toegang te krijgen tot het digitale systeem. Bij het bepalen van de toegelaten middelen, wordt zo veel mogelijk aangesloten bij geldende overheidsstandaarden. Wanneer een gebruiker op deze wijze heeft ingelogd, ziet hij uitsluitend het desbetreffende dossier waaraan hij (bij de start van de procedure of bij het

voeren van verweer) is gekoppeld. Dat dossier is voor hem toegankelijk. Betreft het een natuurlijke persoon, dan zal hij in beginsel inloggen met zijn DigiD. Een gemachtigde zal er zorg voor moeten dragen dat de desbetreffende rechterlijke instantie ervan op de hoogte is namens wie hij als gemachtigde optreedt. De niet-professionele gemachtigde zal zich – als natuurlijke persoon – moeten authenticeren, in beginsel met zijn eigen DigiD. De professionele gemachtigde authenticeert zich bijvoorbeeld met eHerkenning of een Advocatenpas. De gemachtigde legt (net als in de oude situatie op papier) een machtiging van de natuurlijke persoon of rechtspersoon over. Een cliënt kan eenvoudig in het dossier controleren wie namens hem optreedt. Voor advocaten geldt overigens niet dat zij een machtiging moeten overleggen. Als een advocaat zich namens een partij meldt, dan wordt hij geacht daartoe te zijn gemachtigd, zo merk ik op naar aanleiding van het advies van de Nederlandse Vereniging voor Rechtspraak.
Bij rechtspersonen en bestuursorganen is de gang van zaken tot op grote hoogte vergelijkbaar. Rechtspersonen en bestuursorganen die als partij optreden, maken in beginsel gebruik van eHerkenning. In de toekomst kan dit vanzelfsprekend wijzigen. Zo gaat eHerkenning op in het eID-stelsel. De huidige werkwijze bij het gebruik van eHerkenning is als volgt. De rechtspersoon of het bestuursorgaan meldt bij zijn middelenuitgever medewerkers aan voor specifieke diensten (bijvoorbeeld de dienst van de rechtspraak). Het middel wordt vervolgens op persoonsniveau, dus per aangemelde medewerker, aangeschaft. Niet iedere medewerker van een rechtspersoon of een bestuursorgaan zal over een eHerkenningsmiddel beschikken. Dat hangt samen met de kosten daarvan. De medewerkers die over een eHerkenningsmiddel beschikken, zullen voorts niet voor alle diensten waarvan de rechtspersoon gebruikmaakt aangemeld zijn. Dit hangt samen met de bedrijfsvoering van de rechtspersoon of het bestuursorgaan, maar bijvoorbeeld ook met de omstandigheid dat de rechtspersoon en het bestuursorgaan ervoor verantwoordelijk zijn dat gegevens uit het dossier niet verder worden verspreid dan nodig of toegestaan is. De medewerker die namens de rechtspersoon of het bestuursorgaan inlogt krijgt alleen toegang tot het digitale systeem als hij door de rechtspersoon of het bestuursorgaan aangemeld is voor de dienst van de rechtspraak. Het digitale systeem controleert of de medewerker aangemeld is aan de hand van het eHerkenningsmiddel dat de desbetreffende medewerker heeft verkregen van de rechtspersoon of het bestuursorgaan.
Er zijn ook rechtspersonen of bestuursorganen die gebruik maken van PKI-certificaten (Public Key Infrastructure). Een persoonsgebonden PKI-overheidscertificaat dat in het eHerkenning-stelsel is geregistreerd, is met voldoende waarborgen omkleed om toegang te kunnen verkrijgen tot het digitale systeem van de rechterlijke instanties. Waar dat PKI-service certificaten betreft die op organisatieniveau zijn uitgegeven, ligt dat evenwel anders. Een dergelijk certificaat wordt op de computer van een of meerdere medewerkers van bijvoorbeeld een rechtspersoon geïnstalleerd. Medewerkers kunnen niet voor specifieke diensten worden aangemeld. Iedere medewerker die over het certificaat beschikt, zou dan in beginsel toegang kunnen hebben tot alle lopende procedures van de rechtspersoon voor wie hij werkt. Dergelijke certificaten zijn niet uitgegeven als authenticatiemiddel voor een dienst als ‘Mijn Zaak’ die door de rechterlijke instanties wordt aangeboden. Naar verwachting zal dit middel dan ook niet worden aangewezen door de rechterlijke instanties. Waar een organisatie gebruik maakt van de automatische systeemkoppeling is het gebruik van PKI-overheidscertificaten overigens wel standaard binnen de overheid. Hiermee herkent het ene systeem het andere systeem en weten beide systemen dat zij elkaar kunnen vertrouwen. Aangezien de systeemkoppeling een andere systematiek kent dan het gebruik van het portaal ‘Mijn Zaak’ en over het gebruik van de systeemkoppeling afspraken worden gemaakt (onder meer over het beperken houden van inzage in toegezonden of ontvangen stukken door medewerkers van een organisatie), is het gebruik van PKI-overheidscertificaten hier wel mogelijk.
De rechterlijke instanties zijn voornemens om het gebruik van andere authenticatiemiddelen, zoals de deurwaarderspas, mogelijk te maken. Met de desbetreffende ketenpartijen zijn de rechterlijke instanties hierover in gesprek.

6. Administratieve lasten en andere effecten

De lasten die gepaard gaan met de informatie-uitwisseling met de rechter of de wederpartij hangen samen met de waarborgen die het civiele en bestuursprocesrecht bieden voor een eerlijke en efficiënte procesvoering. Strikt genomen vallen de lasten die met deze informatieverplichtingen gepaard gaan onder het begrip administratieve lasten, maar vanwege het bijzondere karakter worden ze niet onverkort als administratieve lasten aangemerkt. Het civiele en bestuursprocesrecht vallen met het oog daarop buiten de kwantitatieve reductiedoelstellingen voor administratieve lasten (zie hierover Actal, brochure «Meten is weten II», p. 33). Evenmin als met het wetsvoorstel vereenvoudiging en digitalisering procesrecht, worden met dit besluit nieuwe informatieverplichtingen in het leven worden geroepen.
Een natuurlijke persoon wordt niet verplicht tot procederen via elektronische weg. Hij heeft echter wel de mogelijkheid om digitaal te procederen. In dat geval moet hij beschikken over DigiD. Aan de aanvraag van DigiD zijn voor burgers geen kosten verbonden. Veel burgers beschikken reeds over dat middel in verband met hun jaarlijkse belastingaangifte. Advocaten kunnen inloggen met een Advocatenpas, waarover zij ook al beschikken. Medewerkers van rechtspersonen en bestuursorganen

moeten voor het inloggen beschikken over een eHerkenningsmiddel of een ander middel dat door de rechterlijke instanties wordt aangewezen. Vanzelfsprekend hoeft dat middel uitsluitend beschikbaar te zijn voor de medewerkers die toegang tot het digitale dossier in 'Mijn Zaak' moeten kunnen krijgen. Een eHerkenningsmiddel dat voldoet aan het in dit besluit vereiste betrouwbaarheidsniveau kan voor ongeveer 40 euro per jaar worden aangeschaft en is ook te gebruiken bij andere overheidsdiensten die dit middel toestaan. Wie toegang wil krijgen tot de eigen zaken, moet beschikken over een computer of laptop met internetverbinding. Indien naast de procesinleiding of het beroepschrift nadere stukken moeten worden geüpload, zal men in veel gevallen tevens over een scanvoorziening moeten beschikken. Tegenwoordig hebben vrijwel alle printers een ingebouwde scanfunctionaliteit. In de praktijk beschikken de meeste professionele partijen over deze apparatuur, zodat daaruit geen extra kosten voortvloeien. Ketenpartijen kunnen ook kiezen voor een automatische systeemkoppeling met het digitale systeem van de rechterlijke instanties. Zij kiezen daar zelf voor, alsook voor de eventuele technische complexiteit van deze koppeling. Welke kosten daaraan verbonden zijn, hebben partijen daarmee zelf in de hand.
De digitalisering van de communicatie van partijen met de rechter kan voor partijen tot besparingen leiden. Zo hebben zij onder meer geen kopieer- of frankeerkosten meer en kunnen zij op ieder moment de voortgang van hun procedure in het portaal 'Mijn Zaak' inzien. Een aantal ketenpartijen dat op jaarlijkse basis veel procedeert kan dankzij deze maatregelen zelfs aanzienlijke besparingen realiseren. Dit geldt des te meer voor de ketenpartijen die kiezen voor een automatische systeemkoppeling.

7. Ontvangen adviezen

Een ontwerp van dit besluit is eind 2014 in consultatie gebracht. De internetconsultatie heeft tot reacties geleid van de Koninklijke Beroepsorganisatie van Gerechtsdeurwaarders en de Nederlandse Orde van Belastingadviseurs. Deze ontvangen consultaties zijn voor een ieder raadpleegbaar via: www.internetconsultatie/amvbkei. Daarnaast zijn adviezen ontvangen van de Adviescommissie voor burgerlijk procesrecht, de Afdeling bestuursrechtspraak van de Raad van State, de president en de procureur-generaal van de Hoge Raad, de Nederlandse Vereniging voor Rechtspraak en de Raad voor de rechtspraak. Naar aanleiding van de reacties is het ontwerpbesluit dat is voorgelegd aan de Afdeling advisering van de Raad van State op een aantal punten aangepast en is de nota van toelichting waar nodig nader aangevuld of aangepast. Voorafgaand aan de advisering door de Afdeling advisering van de Raad van State is het College Bescherming Persoonsgegevens om advies gevraagd.
Hieronder bespreek ik de adviezen in alfabetische volgorde. Waar relevant ga ik in het algemene deel en de artikelsgewijze toelichting nader in op een specifiek onderdeel uit een of meerdere van de adviezen. Voor zover de adviezen ingaan op de wet vereenvoudiging en digitalisering procesrecht en samenhangende wetten of specifieke technische onderdelen van het digitale systeem van de rechterlijke instanties, leent deze toelichting zich niet voor een bespreking daarvan.
De Adviescommissie voor burgerlijk procesrecht vraagt er aandacht voor dat moet zijn uitgesloten dat partijen wijzigingen kunnen aanbrengen in elkaars berichten die in 'Mijn Zaak' staan. Verder acht de Adviescommissie het van belang dat een procedure gestart kan worden of verweer gevoerd kan worden, ook als de gemachtigde nog niet beschikt over het BSN van zijn cliënt, als deze een natuurlijke persoon is. De toegang tot de rechter voor partijen moet gewaarborgd blijven. De Adviescommissie onderschrijft het nut van de in het besluit voorgestelde regeling ten aanzien van de verschoonbaarheid van de termijnoverschrijding met één werkdag in geval van een storing van de toegang tot of storing in het digitale systeem van de rechterlijke instanties. De Adviescommissie doet de suggestie om te regelen dat ook buiten deze werkdag processtukken kunnen worden ingediend. Het is aan de rechter om over de eventuele verschoonbaarheid hiervan te oordelen, aldus de Adviescommissie. In de artikelsgewijze toelichting ga ik op de verschillende onderdelen van het advies in.
De Afdeling bestuursrechtspraak van de Raad van State onderschrijft de noodzaak van de digitalisering van bestuursrechtelijke procedures. Zij vraagt om een verheldering van de term betrokkene, zoals die volgt uit artikel 8:36a van de Awb en artikel 30c Rv. De Afdeling vraagt in dit kader op basis waarvan de rechter kan afdwingen dat een betrokkene documenten digitaal aanlevert. De Afdeling wijst erop dat kan voorkomen dat een entiteit naar buitenlands recht een dochteronderneming heeft die in Nederland is gevestigd. Een dergelijk geval zou niet uitgezonderd moeten worden op grond van artikel 7. Verder wijst de Afdeling op het belang dat de rechter te allen tijde voor partijen bereikbaar is, desnoods via een noodkanaal. Ten behoeve van het rekening houden met storingen van het digitale systeem wijst de Afdeling erop dat een goede registratie van dergelijke storingen essentieel is en dat deze registratie toegankelijk moet zijn voor partijen of andere betrokkenen bij een procedure. De Afdeling onderschrijft het in dit besluit voorgeschreven betrouwbaarheidsniveau ten behoeve van de authenticatie voor het verkrijgen van toegang tot een zaakdossier. In de artikelsgewijze toelichting ga ik op de verschillende onderdelen van het advies in.
Het College Bescherming Persoonsgegevens (CBP) vraagt aandacht voor het gebruik van beeld- en geluidsopnamen tijdens de zitting en verzoekt om een nadere motivering van de keuze om het nader regelen van deze opnamen te laten plaatsvinden in procesreglementen in plaats van dit te regelen bij algemene maatregel van bestuur. In reactie hierop wil ik graag wijzen op de passage in de memorie

van toelichting van het voormelde wetsvoorstel, zoals dat is ingediend bij de Tweede Kamer (Kamerstukken II 2014–2015, 34 059, nr. 3, p. 34), waarin staat dat bij (proces)reglement nadere regels kunnen worden gesteld over het maken van beeld- en geluidsopnamen. Ik verwacht dat de rechterlijke instanties hierbij het advies van het CBP naar aanleiding van het voorontwerp van het wetsvoorstel zullen opvolgen, om zich te houden aan de informatieplicht richting de procesdeelnemers indien tijdens een zitting beeld- of geluidsopnamen worden gemaakt. Het CBP adviseert verder om een aparte privacyparagraaf in de toelichting op te nemen. In reactie hierop wil ik het volgende opmerken. In deze toelichting wordt uitvoerig ingegaan op de verscheidene aspecten van veiligheid en de bescherming van persoonsgegevens en andere gevoelige gegevens. Er is niet voor gekozen om dit in één paragraaf te bespreken, juist omdat er verschillende aspecten relevant zijn. Hiermee kunnen de aparte aspecten de vereiste aandacht krijgen. Voorts vraagt het CBP om nader toe te lichten of is voldaan aan de subsidiariteitstoets voor het gebruik van het BSN van een natuurlijke persoon om een koppeling te leggen met diens zaakdossier in het digitale systeem van de rechterlijke instanties. Het CBP vraag op dit punt nader te motiveren waarom er geen minder ingrijpende alternatieven zijn. Ten slotte vraagt het CBP om een nadere toelichting op de vraag op welke momenten tijdens de procedure het BSN gebruikt wordt. In de toelichting bij artikel 6 wordt nader op deze vragen ingegaan.
De Koninklijke Beroepsorganisatie van Gerechtsdeurwaarders (KBvG) benadrukt in haar reactie op de consultatie het belang van de gerechtsdeurwaarders om via een automatische systeemkoppeling berichten uit te kunnen wisselen met de gerechten. Zij vraagt om een waarborg in dit besluit dat deze systeemkoppeling in het civiele recht beschikbaar is bij de tweede fase van de inwerkingtreding van de wet vereenvoudiging en digitalisering van procesrecht en samenhangende wetten. De KBvG kan zich vinden in de eisen die gesteld worden aan de authenticatie bij het inloggen. Eveneens kan zij zich vinden in de eisen die het besluit stelt aan een elektronische handtekening. De KBvG vraagt om op termijn een digitale grosse mogelijk te maken. Tot slot vraagt de KBvG er aandacht voor dat deurwaarders voldoende tijd krijgen om zich voor te bereiden op de nieuwe digitale procedure. In de artikelsgewijze toelichting ga ik in op de verschillende onderdelen van de reactie van de KBvG.
De Nederlandse Orde van Belastingadviseurs (NOB) is een groot voorstander van een snellere en doelmatige rechtsgang. Zij vraagt in haar reactie op de consultatie om meer uitleg in de nota van toelichting over de mogelijkheden tot aansluiting op een systeemkoppeling. De NOB acht het onwenselijk als alle partijen en andere betrokkenen bij een procedure inzage krijgen in alle stukken in het dossier. Zo kunnen stukken met bedrijfsgevoelige gegevens onderdeel zijn van de dossiers. In de artikelsgewijze toelichting ga ik in op de verschillende onderdelen van de reactie van de NOB. Verder uit de NOB de behoefte dat verschillende medewerkers van een organisatie gekoppeld kunnen worden aan een specifiek dossier en dat zij ook allen op de hoogte worden gehouden door middel van notificatieberichten. De rechterlijke instanties zijn op de hoogte van deze behoefte en zullen waar mogelijk daarmee rekening houden bij de bouw van het digitale systeem.
De Nederlandse Vereniging voor Rechtspraak (NVvR) vraagt in haar advies aandacht voor voldoende waarborgen bij de ontwikkeling van het digitale systeem. Zo acht zij het van belang dat een partij altijd toegang heeft tot de rechter, ongeacht of zij of haar gemachtigde het BSN van de natuurlijke persoon in kwestie op dat moment aan de desbetreffende rechterlijke instantie kan verstrekken. De NVvR ziet geen noodzaak tot het verstrekken van het BSN door een natuurlijke persoon die kiest voor procederen op papier. Verder benadrukt de NVvR dat het BSN van een bij een procedure betrokken natuurlijke persoon niet zichtbaar dient te zijn in het dossier. Zij vraagt partijen en andere betrokkenen goed te informeren als een storing verholpen is, zodat partijen weten wanneer een proceshandeling kan worden verricht. In de artikelsgewijze toelichting ga ik in op de verschillende onderdelen van het advies van de NVvR.
De president en de procureur-generaal van de Hoge Raad doen in hun advies de suggestie om artikel 8 ook te laten zien op anderen die bij een procedure worden betrokken en langs elektronische weg berichten indienen. Deze suggestie is verwerkt in artikel 8.

Artikelsgewijze toelichting

Artikel I

Het besluit spreekt over het digitale systeem van de rechterlijke instanties. Het eerste artikel geeft een definitie van de term ‘rechterlijke instanties’. Hieronder vallen:

a. de gerechten in de zin van artikel 2 van de Wet op de Rechterlijke Organisatie, dat wil zeggen de rechtbanken, de gerechtshoven en de Hoge Raad;
b. de Afdeling bestuursrechtspraak van de Raad van State;
c. het College van Beroep voor het bedrijfsleven (hierna: het CBb);
d. en de Centrale Raad van Beroep (hierna: de CRvB).

Hierbij is niet expliciet de procedure opgenomen voor het beroep tegen een beslissing van de officier van justitie op grond van artikel 9 van de Wet administratiefrechtelijk handhaving verkeersvoorschriften (hierna: Wahv). Dit beroep bij de kantonrechter tegen een beslissing van de officier van justitie naar aanleiding van een verkeersovertreding, wordt ingediend bij de officier van justitie die heeft beslist op het administratieve beroep. Op grond van artikel 10 van de Wahv brengt de officier van

justitie het beroepschrift en de op de zaak betrekking hebbende stukken ter kennis van de bevoegde rechtbank. De Centrale Verwerking Openbaar Ministerie (hierna: CVOM) stuurt het beroep dat door degene tot wie de Wahv-beschikking is gericht bij de kantonrechter wordt ingediend, door naar de bevoegde rechtbank. De CVOM handelt hiermee feitelijk als een doorgeefluik voor de rechterlijke instantie. Het zou onwenselijk zijn als het voor een rechtzoekende uitmaakt of hij beroep instelt direct bij de kantonrechter, dus via het portaal van de gedefinieerde rechterlijke instanties, of indirect via het portaal van de CVOM. Om deze reden zal het openbaar ministerie zijn reeds operationele portaal in de komende periode waar nodig aanpassen aan de bepalingen uit dit besluit.

Artikel 2

Eerste lid

Het eerste lid van artikel 2 bepaalt dat de rechterlijke instanties een digitaal systeem voor gegevensverwerking ter beschikking stellen. Dit systeem moet aan een aantal specifieke eisen voldoen. Deze eisen betreffen doelbepalingen. Het artikel schrijft geen specifieke methoden of techniek voor, maar is erop gericht om de gebruikers van het digitale systeem waarborgen te bieden bij gebruik van dit systeem. De eisen van dit artikellid zien erop dat het systeem het mogelijk maakt om bepaalde dingen na te gaan. Dit kan relevant zijn in een specifieke procedure voor de gebruiker van dit systeem, zijnde de rechter en griffier, partijen en hun gemachtigden of anderen die betrokken worden bij een procedure. De eisen van dit artikellid geven de gebruiker evenwel niet het recht, noch de mogelijkheid, om zelf in het digitale systeem van de rechterlijke instanties onderzoek te doen. Het zijn de rechterlijke instanties die alle relevante gegevens zullen loggen. Waar nodig kan een gebruiker deze gegevens opvragen. De rechterlijke instanties zullen voorschrijven op welke wijze dat kan.
De Raad voor de rechtspraak is (gelet op artikel 91, tweede lid, onder a en b, van de Wet op de rechterlijke organisatie) ten aanzien van het digitale systeem van de rechtbanken, de gerechtshoven, het Cbb en de CRvB, medeverantwoordelijk voor naleving van de eisen als genoemd in dit besluit en in het bijzonder dit artikel.
De Afdeling bestuursrechtspraak vraagt in haar advies aandacht voor de omstandigheid dat er drie digitale systemen voor gegevensverwerking komen en doet de suggestie om in het besluit te spreken over het digitale systeem voor gegevensverwerking van de desbetreffende rechterlijke instantie. De KBvG vraagt in haar reactie op de consultatie of er op termijn één digitaal systeem komt voor alle rechterlijke instanties. Het is aan de rechterlijke instanties om te onderzoeken hoe en wanneer er één digitaal systeem gevormd kan worden. Op grond van artikel 4, eerste lid, van dit besluit kunnen de rechterlijke instanties aanwijzen welk specifieke digitale systeem toegang verleent tot welke instantie. Dat kan in een (proces)reglement worden neergelegd.

Eerste lid, onder a

Dit artikel is erop gericht dat het digitale systeem zodanig wordt gebouwd dat het waarborgen biedt voor de betrouwbaarheid en vertrouwelijkheid van de verwerking van de gegevens van partijen en anderen die bij een procedure worden betrokken. Het gaat hier in het bijzonder om persoonsgegevens in de zin van de Wbp en bedrijfsgevoelige gegevens. Alleen degene die daartoe gerechtigd is, mag toegang krijgen tot een individueel zaakdossier in het digitale systeem van de rechterlijke instanties. Het is dan ook essentieel dat het systeem de rechterlijke instanties in staat stelt de desbetreffende gebruiker te identificeren, doordat hij zich moet authenticeren (eerste lid, onder a). De gebruikers van het digitale systeem zijn de rechter, de griffier en andere rechtspraakmedewerkers, partijen en hun gemachtigden en anderen die in de procedure worden betrokken (waaronder deskundigen). Aan welke eisen de authenticatie door de gebruiker moet voldoen, wordt geregeld in artikel 3.

Eerste lid, onder b

Het digitale systeem van de rechterlijke instanties moet het mogelijk maken om na te gaan wie de verzender is van een bericht dat langs elektronische weg is ingediend. De rechter of griffier, een partij en haar gemachtigde of een andere betrokkene moet na kunnen gaan van wie een bericht afkomstig is. Zo moet de rechter bijvoorbeeld weten wie van partijen een bepaald bericht heeft ingediend. Dit artikel is er daarom op gericht dat in het digitale dossier vermeld staat welke partij een bericht heeft ingediend of dat het een bericht van een rechter of griffie is. Dit artikel verplicht evenwel niet dat bij ieder bericht de naam staat vermeld van de persoon die het bericht heeft ingediend. De term verzender moet dan ook breed worden opgevat en omvat in ieder geval de volgende categorieën: de persoon die het bericht digitaal heeft ingediend en het stuk heeft opgesteld, of de functionaris die uit hoofde van zijn functie het bericht heeft opgesteld of ingediend.
Partijen, bijvoorbeeld natuurlijke personen zonder gemachtigde, stellen zelf een bericht op en indienen dit in. Als een partij met een advocaat procedeert, zal deze laatste in de regel berichten en stukken indienen. Bovendien kan alleen een advocaat berichten indienen in procedures met verplichte procesvertegenwoordiging. Zijn cliënt heeft inzage in het digitale dossier, maar kan zelf geen berichten

indienen. De eisen van onder meer authenticatie waarborgen dat verifieerbaar is wie de indiener is. Alleen degene die gerechtigd is om toegang te krijgen tot het digitale dossier kan via het digitale systeem berichten indienen. Partijen die betrokken zijn bij een procedure kunnen berichten indienen. Het digitale systeem registreert wie ingelogd heeft in een dossier en welke partij of gemachtigde berichten heeft ingediend.
Het is ook mogelijk dat een bericht wordt ingediend door een functionaris, die dit uit hoofde van zijn functie doet. Hierbij moet in de eerste plaats gedacht worden aan rechters en griffiers. Het is voor partijen niet relevant welke specifieke rechter een bericht heeft geplaatst of heeft laten plaatsen door de griffier, maar wel dat het een rechter was. Dit geldt des te meer in de eerste fase van de procedure waar een regierechter beslissingen neemt. Ook voor partijen kan deze categorie gelden. In vreemdelingenzaken is het bijvoorbeeld de Staatsecretaris van Veiligheid en Justitie die als verweerder (of als appellant in hoger beroep) optreedt. Namens hem heeft een procesvertegenwoordiger van de IND een stuk opgesteld en ingediend. Deze procesvertegenwoordiger zal (net als in de oude situatie) over het juiste mandaat moeten beschikken, anders is het stuk onbevoegdelijk ingediend. De huidige regels van het procesrecht over wie welke stukken in een procedure mag indienen worden niet gewijzigd, door de nieuwe technische mogelijkheden. Zo kan de rechter gevolgen verbinden aan de situatie dat een medewerker technisch in staat blijkt om een stuk te kunnen indienen, maar daartoe procesrechtelijk gezien niet bevoegd is. Het is de verantwoordelijkheid van iedere partij om, net als in de oude situatie, ervoor zorg te dragen dat alleen medewerkers van een rechtspersoon, bestuursorgaan of alleen advocaten die over een mandaat, machtiging of volmacht beschikken, (proces)stukken indienen of proceshandelingen verrichten.
De Adviescommissie voor burgerlijk procesrecht stelt in haar advies de vraag of dit artikel er ook toe strekt dat partijen moeten kunnen nagaan welke specifieke rechter of griffiemedewerker een bericht heeft geplaatst. Gelet op het voorgaande merk ik op dat dit artikel er niet toe strekt dat bij ieder bericht vermeld staat welke specifieke medewerker (van bijvoorbeeld een rechtspersoon) of rechter een bericht heeft geplaatst, maar wel dat zichtbaar is van of namens welke partij een bericht is, of dat het een bericht van een rechter of griffier is. Als voor behandeling van de zaak relevant is om te weten welke specifieke persoon een bericht heeft ingediend of geplaatst, dan moet dit na te gaan zijn. Voor zover dit niet zichtbaar is in het digitale dossier, kan de rechter – al dan niet op verzoek van partijen – deze gegevens opvragen. Als het een rechtspersoon betreft wiens medewerker met eHerkenning heeft ingelogd, zal de rechtspersoon bij de eHerkenningsmakelaar (de 'tussenpersoon' die de verbinding legt tussen de medewerker die wil inloggen en het systeem van de rechterlijke instanties) moeten nagaan welke medewerker het betrof. Die gegevens zijn zichtbaar noch na te gaan in het digitale systeem van de rechterlijke instanties.
De KBvG merkt in haar advies op dat gerechtsdeurwaarders berichten indienen en ontvangen via een bewerker, zijnde de Stichting Netwerk Gerechtsdeurwaarders. De deurwaarder is en blijft verantwoordelijk voor de inhoud van het ingediende bericht. De rol van de bewerker is om het door de deurwaarder aangeleverde bericht te versturen naar het digitale systeem van de rechterlijke instanties. Voor de rechterlijke instanties moet controleerbaar zijn van welke deurwaarder het bericht afkomstig is, dat door tussenkomst van de SNG naar het digitale systeem is verstuurd. Hetzelfde geldt voor andere partijen die berichten indienen via een tussenpersoon. De desbetreffende rechterlijke instanties kunnen met partijen als de SNG afspraken maken over hoe deze controle ingericht wordt.

Eerste lid, onder c

Tevens moet het digitale systeem van de rechterlijke instanties het mogelijk maken om te kunnen controleren of het desbetreffende bericht is gewijzigd. Voorkomen moet worden dat partijen of anderen die bij de procedure worden betrokken elkaars berichten kunnen wijzigen. De Adviescommissie voor het burgerlijk procesrecht heeft hier in het bijzonder aandacht voor gevraagd. Evenmin mag mogelijk zijn dat na indiening een bericht wordt gewijzigd.
De KBvG heeft in haar reactie op de consultatie aandacht gevraagd voor het uitwisselen van berichten binnen een beveiligde omgeving. Hier zouden andere eisen van integriteit van berichten aan moeten worden gesteld. Overeenkomstig hetgeen in de memorie van toelichting bij het wetsvoorstel Wet digitale processtukken Strafvordering[1] staat, is het van belang dat berichten worden versleuteld zodra zij in het digitale systeem van de rechterlijke instanties worden ingediend. Een van de technische mogelijkheden om dit te regelen is door een hashwaarde[2] toe te voegen. De integriteit van een bericht, zijnde de zekerheid dat een bericht volledig is en niet onbevoegdelijk is gewijzigd, wordt daarmee gewaarborgd door de rechterlijke instanties. In beginsel worden alleen bestanden ingediend van een bepaald formaat waarin het niet mogelijk is om nadien nog wijzigingen aan te brengen (hierbij kan bijvoorbeeld gedacht worden aan (een versie van) PDF-bestanden). Net als in de oude

[1] Kamerstukken II, 2014–2015, 34 090, nr. 3, p. 9 e.v.
[2] Een hashwaarde is een unieke waarde, met vaste lengte, van een tekenreeks (document) die berekend wordt met een (hash)algoritme, op een wijze die resulteert in een geheel andere unieke waarde als de tekenreeks wijzigt. Dit kan al voorkomen bij het wijzigen van een komma.

situatie, kan een partij binnen de daartoe bestaande mogelijkheden nog een of meer aanvullende berichten toevoegen aan het digitale dossier. Mocht blijken dat indiening heeft plaatsgevonden nadat een indieningstermijn is verstreken, dan kan de rechter oordelen dat het bericht niet wordt meegenomen in de behandeling van de zaak. Nadat een partij die op papier mag procederen een bericht op papier indient, wordt het onder verantwoordelijkheid van de bevoegde rechterlijke instantie gedigitaliseerd en in het digitale dossier geplaatst. Het digitale bericht geldt voortaan als het origineel, waarna het papieren bericht kan worden vernietigd (artikel 7 van de Archiefwet).

Eerste lid, onder d

Verder bepaalt het besluit dat in het systeem van de rechterlijke instanties is na te gaan op welk tijdstip berichten hierin zijn ontvangen respectievelijk hieruit zijn verzonden. Dit geldt zowel voor de rechter als voor partijen en andere betrokkenen bij een procedure. Een partij die gebruikmaakt van het portaal dient berichten in via 'Mijn Zaak'. Als de rechter of griffier, een partij, of een andere betrokkene in de procedure een bericht langs elektronische weg indient, ontvangen partijen (anders dan de partij die het bericht heeft ingediend) hiervan desgewenst een notificatie (zie artikel 30d Rv en artikel 8:36c Awb). In vergelijking met de oude situatie waarbij berichten per post tussen partijen en de rechter werden uitgewisseld, worden dankzij deze ontvangstbevestiging en andere functionaliteiten in het digitale systeem, aanzienlijk meer waarborgen aan partijen en de rechter geboden. In 'Mijn Zaak' krijgt een partij bovendien een overzicht van haar zaken te zien, waarin naast de berichten ook de openstaande acties zichtbaar zijn. Hierbij kan gedacht worden aan het verrichten van een proceshandeling, zoals het indienen van een verweerschrift. In het bijzondere geval dat een partij geen notificatie heeft ontvangen (bijvoorbeeld vanwege een storing bij haar
e-mailprovider of omdat haar e-mailbox vol is), kan zij dankzij het overzicht dat 'Mijn Zaak' biedt eenvoudig terugzien welke openstaande acties er zijn. Bijvoorbeeld wat de eindtermijn is voor het indienen van een bepaald bericht, zoals een deskundigenbericht.
Het overzicht in het portaal 'Mijn Zaak' geeft een partij de mogelijkheid om na te gaan op welk tijdstip haar bericht door het digitale systeem is ontvangen, of op welk tijdstip een bericht van de rechter of een andere partij hierin ter beschikking is gesteld. Van partijen in een lopende procedure wordt verwacht dat zij met enige regelmaat in 'Mijn Zaak' inloggen. Als een partij via 'Mijn Zaak' een bericht indient en er geen ontvangstbevestiging in 'Mijn Zaak' verschijnt, moet zij ervan uitgaan dat het bericht niet is ontvangen door het digitale systeem. Dit kan het gevolg zijn van een tijdelijke storing in dit systeem. Als dat het geval is en daardoor een indieningstermijn niet is gehaald, kan er sprake zijn van een verschoonbaarheid van de termijnoverschrijding. Zie in dit kader de toelichting bij artikel 8.
Naast het portaal stellen de rechterlijke instanties onder voorwaarden een aansluitpunt voor geautomatiseerde gegevensverwerking ter beschikking. Dit betreft een geautomatiseerde koppeling tussen het digitale systeem van de rechterlijke instanties en dat van een partij of professioneel rechtsbijstandsverlener. Hierbij valt te denken aan gerechtsdeurwaarders, rechtsbijstandsverzekeraars en grote bestuursorganen, zoals de IND en het UWV. Bij de uitwisseling van berichten via de systeemkoppeling met een partij, diens gemachtigde, of met een ander die bij de procedure is betrokken, worden eveneens diverse waarborgen geboden opdat berichten goed aankomen. Aan beide kanten van de koppeling moeten deze waarborgen worden ingericht in het eigen digitale systeem. De verwerking van ontvangen berichten dient vervolgens door iedere gebruiker goed te worden ingericht binnen de eigen organisatie. Het eerste lid, onder d, dient ertoe om te waarborgen dat de berichtenuitwisseling zorgvuldig en betrouwbaar verloopt. Voor de systeemkoppeling betekent dit dat de rechterlijke instanties de eigen verwerking van het berichtenverkeer monitoren en indien zij een foutmelding krijgen op een verzonden bericht contact opnemen met de partij in kwestie. Omgekeerd geldt ook dat een partij haar eigen verwerking van de berichten monitort en contact opneemt met de desbetreffende rechterlijke instanties, als er van hen een foutief verwerkingsresultaat afkomstig is. Van beide zijden wordt dus actieve bewaking van het succesvol uitwisselen van berichten verwacht.
De Raad voor de rechtspraak stelt een generiek aansluitpunt voor een systeemkoppeling ter beschikking. Hiertoe stelt de Raad een (proces)reglement op, waarin de eisen voor de aansluiting staan opgenomen. Ketenpartijen zoals de advocatuur, rechtsbijstandsverzekeraars en bestuursorganen kunnen op termijn voor een systeemkoppeling kiezen als zij hieraan kunnen voldoen. Voor zowel de rechterlijke instanties als de ketenpartijen geldt dat zij hierbij een eigen afweging zullen maken tussen de kosten van investering in een systeemkoppeling en de te realiseren besparingen op de werklast. Het volume van het aantal jaarlijkse zaken zal hierop van invloed zijn. De Raad beziet per fase van de inwerkingtreding van de Wet vereenvoudiging en digitalisering procesrecht, de daarmee samenhangende wetten en dit besluit voor de relevante ketenpartijen of, en zo ja, wanneer het mogelijk is om de aansluiting te bewerkstelligen. Onder meer kan dat afhangen van de omstandigheid of een ketenpartij wel aan alle aansluitvoorwaarden voldoet. Die voorwaarden behelzen onder meer eisen ten aanzien van het waarborgen van de veiligheid van de gegevensverwerking. Met de IND al ten behoeve van de twee pre-releases een systeemkoppeling gelegd. Op deze wijze wordt hiermee ervaring opgedaan en kan direct bij de start van de eerste release in het bestuursrecht, betreffende asiel- en bewaringszaken, gecommuniceerd worden via de systeemkoppeling. De KBvG benadrukt in haar consultatiereactie dat de inwerkintreding van de systeemkoppeling essentieel is in de tweede civielrechtelijke fase,

betreffende de huidige dagvaardingszaken zonder verplichte procesvertegenwoordiging. Ik ben mij terdege bewust van het belang dat de KBvG heeft bij een automatische uitwisseling van berichten bij grote zaakaantallen, zoals de incassozaken. KEI Rechtspraak ziet dit belang ook en streeft er dan ook naar om samen met de KBvG deze systeemkoppeling tijdig voor de tweede fase gereed te maken. Het is vervolgens aan de individuele gerechtsdeurwaarderskantoren om te bezien of zij aansluiten bij deze systeemkoppeling of dat zij gebruikmaken van het portaal 'Mijn Zaak'.
De waarborgen die het digitale systeem van de rechterlijke instanties biedt, resulteren in een goed werkend berichtenverkeer via 'Mijn Zaak' en de systeemkoppeling, voor zover dat in de beïnvloedingssfeer van dit systeem ligt. Partijen zijn zelf verantwoordelijk om hetzij via 'Mijn Zaak', hetzij via de systeemkoppeling de berichtenuitwisseling goed te monitoren en binnen de eigen organisatie op juiste wijze te verwerken.
Artikel 30d, vierde lid, Rv en artikel 8:36c, vierde lid, Awb geven partijen en andere betrokkenen de mogelijkheid om af te zien van het ontvangen van notificaties. Ook zij kunnen ingevolge dit artikellid nagaan op welk tijdstip berichten zijn ontvangen in dan wel verzonden uit het digitale systeem via het overzicht dat in 'Mijn Zaak' wordt geboden. Waar het de automatische systeemkoppeling betreft kunnen partijen niet afzien van het ontvangen van systeemmeldingen. Dit is namelijk een technisch vereiste om ervoor zorg te dragen dat een partij berichten kan ophalen. Dit wordt nader voorgeschreven in de (proces)reglementen van de rechterlijke instanties.

Eerste lid, onder e

Nu een partij of andere betrokkene langs elektronische weg berichten kan of moet indienen in het digitale systeem van de rechterlijke instanties, is het van belang dat zij de mogelijkheid heeft om na te gaan of er een storing is in dat systeem en dat dit aantoonbaar is als zij een beroep doet op de verschoonbaarheid van de termijnoverschrijding (zie ook de toelichting bij artikel 8). Het betreft hier uitsluitend een storing in het digitale systeem: het is niet aan de rechterlijke instanties om storingen buiten dat systeem te monitoren, zoals bij de provider van een partij.
Voor een partij die haar termijn voor het indienen van een bericht (zoals een verweerschrift) niet haalt vanwege een storing in het digitale systeem, is het mogelijk om na te gaan op welk moment een storing heeft plaatsgevonden. Als een wezenlijke storing in dat systeem plaatsvindt, communiceren de rechterlijke instanties dit via hun websites. Het kan ook voorkomen dat een storing heeft plaatsgevonden waarover de website geen informatie biedt. Een partij kan in deze gevallen gegevens hierover opvragen bij de desbetreffende rechtelijke instantie. De rechterlijke instanties stellen informatie beschikbaar over de wijze waarop dat kan. Als een partij tijdens de procedure bij de rechter aanvoert dat zij de indieningstermijn heeft overschreden vanwege een storing in het digitale systeem van de rechterlijke instanties, legt zij deze gegevens over.
Een bericht, in de zin van artikel 30d, eerste lid Rv en artikel 8:36c, eerste lid Awb, is door de rechter ontvangen op het moment dat het digitale systeem van de rechterlijke instanties het bericht ontvangt. Dit is nadrukkelijk niet het moment waarop de partij het bericht heeft verzonden. Het is de verantwoordelijkheid van de indienende partij om er rekening mee te houden dat het indienen ('uploaden') van een bericht enige tijd kan duren. Als zij tot op het laatste moment van de indieningstermijn wacht, neemt zij daarmee het risico dat zij deze termijn overschrijdt. Het ligt niet in de rede dat de rechter onder zulke omstandigheden een beroep op de verschoonbaarheid van de termijnoverschrijding honoreert.

Eerste lid, onder f

Alleen degene die daartoe gerechtigd is, mag toegang krijgen tot het digitale dossier dat door het digitale systeem van de rechterlijke instanties ter beschikking wordt gesteld. Een dossier van een gerechtelijke procedure is niet openbaar. In een dossier kunnen namelijk persoonsgevoelige en bedrijfsgevoelige gegevens voorkomen. Tijdens expertmeetings met rechters en bij de rechtspraak betrokken ketenpartijen (zoals advocaten, deurwaarders en bestuursorganen) is besproken op welke wijze het vraagstuk van autorisatie (wie toegang heeft tot een specifiek dossier) geregeld kan en moet worden. In ieder geval zullen partijen aan de hierboven in paragraaf 5 vermelde verplichtingen op basis van onder meer de Wbp moeten voldoen. Daarover bestaat consensus en overigens moest dat ook al in de oude situatie. Ik onderschrijf hetgeen de Raad voor de rechtspraak in dit kader benadrukt in zijn advies. Het privacybeginsel '*need to know*' is hier leidend, zowel voor partijen en hun gemachtigden als voor rechters en medewerkers van de rechterlijke instanties. Het is aan een partij om te beslissen of, en zo ja, welke van haar medewerkers geautoriseerd zijn om inzage te krijgen in een specifiek dossier. De rechterlijke instanties ontwikkelen een autorisatiemodel, waarbij medewerkers van een partij op grond van hun werkzaamheden in een specifieke zaak de benodigde toegang tot het dossier kunnen krijgen. Een bevoegde medewerker kan collega's autorisatie verlenen tot een zaakdossier. Zo kunnen de medewerkers elkaar waar nodig vervangen en samen aan een (omvangrijke) zaak werken. Uitsluitend degene die voor een zaak geautoriseerd is, kan toegang krijgen tot het desbetreffende digitale dossier. Aldus doorloopt een medewerker van een rechtspersoon of een bestuursorgaan twee stappen: eerst authenticeert hij zich met eHerkenning of een ander toegelaten

middel, waarbij het digitale systeem controleert of hij aangemeld is tot de dienst van de rechtspraak, en vervolgens controleert het digitale systeem of, en zo ja, tot welke dossiers hij toegang mag krijgen. Alleen die dossiers zijn voor een medewerker toegankelijk. Bij de ontwikkeling van het autorisatiemodel houden de rechterlijke instanties rekening met de eventuele beheerlast van rechtspersonen en bestuursorganen om hiervan gebruik te maken. Een balans wordt hierin gevonden tussen het waarborgen van de bescherming van persoonsgevoelige en bedrijfsgevoelige gegevens in dossiers en de gebruiksvriendelijkheid van het autorisatiemodel voor rechtspersonen. De KBvG doet in haar reactie op de consultatie een voorstel voor een authenticatiemethode voor rechtspersonen. De KBvG doet het voorstel dat grote organisaties door middel van PKI-certificaten toegang moeten kunnen krijgen tot 'Mijn Zaak' en zelf kunnen bepalen welke medewerkers van die partij over dit middel kunnen beschikken. Naar aanleiding hiervan merk ik op dat de rechterlijke instanties voornemens zijn om voor het digitale systeem van de gerechten authenticatie door middel van een persoonsgebonden PKI-overheidscertificaat dat is geregistreerd in het eHerkenning-stelsel toe te laten. Ongeacht met welk middel een rechtspersoon zich authenticeert, is het van belang dat de toegang tot zaakdossiers van diens medewerkers beperkt kan worden. Ik onderschrijf de opmerking van de KBvG dat het de verantwoordelijkheid van de rechtspersoon is om hier prudent mee om te gaan.
Een advocaat kan met zijn Advocatenpas inloggen in het digitale systeem. Een advocaat geeft bij de rechterlijke instanties aan namens welke partij hij optreedt. Mocht een partij zelf een nieuwe procedure starten of verweer voeren, maar wel een advocaat hebben, dan geeft zij diens naam door. Als de advocaat toegang wenst te krijgen tot het digitale dossier, legt hij de gegevens over die de rechterlijke instanties daartoe nodig hebben. Het digitale systeem kan de advocaat in beide gevallen dankzij deze gegevens aan het juiste dossier koppelen.
Voor een professionele partij (bijvoorbeeld een advocaat, rechtsbijstandsverzekeraar of een bestuursorgaan) betekent de verantwoordelijkheid om zorgvuldig om te gaan met persoonsgegevens en andere gevoelige gegevens evenwel niet dat uitsluitend één persoon of medewerker toegang zou mogen hebben tot het digitale dossier. Indien die medewerker bijvoorbeeld uitvalt wegens ziekte, moet een andere bevoegde collega de partij kunnen vertegenwoordigen. De partij (bijvoorbeeld een bestuursorgaan) stelt hier zelf de benodigde mandaatregelingen voor op. Een advocaat kan onder bepaalde omstandigheden een advocaat vervangen van een eigen of een ander kantoor (bijvoorbeeld als deze alleen kantoor voert) om te werken in diens dossiers, indien hij niet beschikbaar is. Het regelen van vervanging vond ook al plaats in de oude situatie. De daarvoor geldende procesrechtelijke bepalingen worden hierbij in acht genomen. Tot slot kan er in een beperkt aantal gevallen reden zijn om een persoon of partij geen toegang te geven tot het gehele dossier, maar uitsluitend tot een bepaald deel daarvan. Het digitale systeem zal voorzien in deze mogelijkheid (zie hierboven paragraaf 4).

Tweede lid

Voorts moet het systeem van de rechterlijke instanties voldoen aan relevante internationale en nationale standaarden voor informatiebeveiliging. Bij ministeriële regeling kan worden aangewezen aan welke standaarden de informatiebeveiliging ten minste moet voldoen. Nationale en internationale standaarden worden nu al toegepast door de rechterlijke instanties. Zo kent de Raad voor de rechtspraak al een eigen normenkader voor de beveiliging van het digitale systeem. Deze kaders zijn mede gebaseerd op nationale standaarden voor informatiebeveiliging, zoals het Voorschrift Informatiebeveiliging Rijksdienst (VIR) 2007, het Voorschrift Informatiebeveiliging Rijksdienst Gerubriceerde Informatie (VIR-GI), de Baseline Informatiebeveiliging Rijksdienst (BIR), de Code voor informatiebeveiliging (NEN-ISO/IEC 27001:2013 en 27002:2013) en de 'Richtsnoeren beveiliging van persoonsgegevens' van het CBP. Als de standaarden bij ministeriële regeling worden bepaald, dan zal worden aangesloten bij de huidige standaarden en geschiedt dit in overleg met de rechterlijke instanties. Waar het internationale standaarden betreft, moet worden voldaan aan standaarden die bijvoorbeeld binnen Europees niveau als leidend zijn afgesproken.

Artikel 3

Het besluit schrijft in artikel 3 voor aan welke eisen een middel moet voldoen als een gebruiker zich wil authenticeren om toegang te krijgen tot het digitale systeem van de rechterlijke instanties. De eisen waaraan een authenticatiemiddel moet voldoen, hangen samen met het gekozen betrouwbaarheidsniveau. Met betrekking tot het betrouwbaarheidsniveau wordt binnen Europees verband gesproken van het STORK-niveau[3]. Er zijn vier STORK-niveaus. Des te hoger het niveau, des te zwaarder zijn de eisen die worden gesteld aan de middelenuitgever en de gebruiker van het middel (in dit kader partijen of andere betrokkenen bij een procedure).
Een betrouwbaarheidsniveau dat voldoet aan de eisen van STORK-niveau 3 of 4 stelt verdergaande

[3] STORK staat voor Secure idenTity acrOss boRders linKed. Het betreft een door de EU opgesteld raamwerk voor grensoverschrijdende online dienstverlening en het wederzijds erkennen van nationale elektronische identiteiten, vgl. https://www.eid-stork.eu/.

eisen aan het authenticatieproces, dan de niveaus 1 en 2. Dit kan leiden tot meer lasten voor de gebruiker. Zo moet de gebruiker bijvoorbeeld meer kosten maken om een middel aan te schaffen dat voldoet aan STORK-niveau 4 en kunnen ook anderszins zijn administratieve lasten hoger liggen, dan bij bijvoorbeeld het STORK-niveau 2. Verder is van belang welke betrouwbaarheidsniveaus de middelen bieden die nu aan de gebruiker ter beschikking staan. De stand van de techniek is dan ook leidend bij het bepalen van het betrouwbaarheidsniveau. Authenticatie dient ertoe om de toegang tot zaakdossiers te kunnen beperken tot de betrokken partijen. Dit is onder meer van belang omdat persoonsgegevens kunnen voorkomen in dossiers. In dit kader is de Wbp dan ook van belang. Artikel 13 van de Wbp schrijft voor:
'De verantwoordelijke legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen.'
In expertmeetings met rechters en bij de rechtspraak betrokken ketenpartijen is ter voorbereiding van dit besluit onder meer gesproken over het vereiste betrouwbaarheidsniveau. Concreet zijn de STORK-niveaus 3 en 4 aan de orde gekomen. Het meeste draagvlak onder de rechterlijke instanties en de ketenpartijen bestaat voor het STORK-niveau 3. Dit niveau voldoet aan beveiligingseisen die mogen worden gevraagd van de dienst die door de rechterlijke instanties wordt geboden en legt tezelfdertijd niet onredelijk hoge lasten op de gebruiker van die dienst. Zo eist STORK-niveau 3 een tweefactorauthenticatie van het middel.
De keuze voor het STORK-niveau 4 zou tot gevolg hebben dat alle partijen en andere betrokkenen middelen zouden moeten aanschaffen en gebruiken die substantieel hoger zijn dan middelen met STORK-niveau 3. Verder moeten bij het STORK-niveau 4 de medewerkers van een rechtspersoon die van het middel gebruik moeten kunnen maken, in persoon verschijnen om hun ID-document te laten controleren door de middelenuitgever. Voor wat betreft natuurlijke personen is dit geen mogelijkheid, aangezien DigiD 'Midden' het hoogst beschikbare betrouwbaarheidsniveau voor DigiD is. Het eisen van een uitgifte in persoon zou ertoe leiden dat natuurlijke personen niet digitaal toegang kunnen krijgen tot de rechter. Ook waar het een rechtspersoon betreft met veel medewerkers die toegang moeten kunnen krijgen tot het digitale systeem van de rechterlijke instanties, zou dit betrouwbaarheidsniveau tot aanzienlijke administratieve lasten leiden. Het aanschaffen van een middel (bijvoorbeeld eHerkenning) op STORK-niveau 4 zou gezien de hoge lasten voor de gebruiker tot een beperking en voor natuurlijke personen tot een belemmering van de toegang tot de rechter kunnen leiden, hetgeen onwenselijk is. Uit ervaringen in het buitenland (bijvoorbeeld in Duitsland) blijkt dat indien wordt voorgeschreven dat uitsluitend middelen mogen worden gebruikt die voldoen aan het STORK-niveau 4, het gebruik daarvan in de praktijk beperkt blijft, omdat deze middelen kennelijk tot (te) hoge administratieve lasten voor partijen leiden.
Artikel 3 schrijft voor dat het authenticatiemiddel, waarmee een partij of een andere betrokkene bij een procedure zich toegang wil verschaffen tot het digitale systeem, aan drie voorwaarden moet voldoen. Ten eerste moet het middel worden uitgegeven door de overheid of door een organisatie die onder overheidstoezicht staat (onder a). Dat betekent dat de overheid of de onder toezicht van de overheid staande organisatie bepaalde verantwoordelijkheden, rechten en plichten heeft ten aanzien van de middelenverstrekking die waarborgen dat dit proces op betrouwbare, veilige en zorgvuldige wijze verloopt.
Ten tweede moet er sprake zijn van een tweefactorauthenticatie (onder b). Een tweefactorauthenticatie vereist twee of meer authenticatiemethoden van verschillende typen, zoals: iets wat de gebruiker weet en iets wat de gebruiker heeft. Het is gangbaar bij inloggen (bijvoorbeeld bij het doen van internetaankopen) dat een gebruiker alleen gebruikmaakt van een gebruikersnaam en een wachtwoord om in te loggen. Dit is iets wat alleen de gebruiker weet en betreft een eenfactorauthenticatie. Als een dienst (een applicatie) ook gebruik maakt van iets wat in het bezit is van de gebruiker, zoals een token of een mobiele telefoon waarnaar een SMS-bericht met een code wordt gestuurd, is sprake van een tweefactorauthenticatie. Hiermee vindt een extra controle plaats om te waarborgen dat degene die gebruikmaakt van het middel ook degene is aan wie het middel is uitgegeven en wordt de gebruiker beschermd tegen misbruik van zijn gegevens.
De derde voorwaarde die wordt gesteld is dat een partij of een andere betrokkene, zich alleen kan authenticeren met een middel dat door de rechterlijke instanties is voorgeschreven (onder c). Het kan voorkomen dat voor partijen een middel beschikbaar is dat wel aan het vereiste betrouwbaarheidsniveau voldoet, maar waarvan het technisch gezien zo ingewikkeld zou zijn voor het digitale systeem om aansluiting mogelijk te maken, dat dit een te grote belasting op dat systeem zou leggen. Dit zou ook de stabiliteit van dat systeem niet ten goede komen. Ook vanuit het oogpunt van het kunnen beperken van de toegang van medewerkers van bepaalde partijen, zoals bestuursorganen en rechtspersonen, tot de dossiers van die partij, kan het onwenselijk zijn dat zij van een specifiek middel gebruikmaken, zoals PKI-certificaten die niet persoonsgebonden zijn en niet geregistreerd staan bij eHerkenning. De rechterlijke instanties wijzen daarom bij (proces)reglement aan met welke middelen partijen en anderen die bij de procedure worden betrokken zich kunnen authenticeren in het digitale systeem. Het uitgangspunt hierbij is de herbruikbaarheid van dat middel. Daarom worden in ieder geval middelen

voorgeschreven die overheidsbreed gebruikt kunnen worden, zoals DigiD voor burgers, eHerkenning voor rechtspersonen en de Advocatenpas voor advocaten. Veel burgers beschikken al over DigiD. Rechtspersonen kunnen nu al toegang krijgen tot overheidsdiensten door zich te authenticeren door middel van eHerkenning. De Advocatenpas is sinds 2012 landelijk ingevoerd, waardoor alle advocaten inmiddels over een dergelijke pas beschikken.
Als een partij berichten met het digitale systeem van de rechterlijke instanties uitwisselt via een automatische systeemkoppeling, vindt geen authenticatie op persoonsniveau, maar op organisatieniveau plaats. De eisen in dit artikel zien daarmee tevens op de authenticatie in het kader van de systeemkoppeling. Een middel dat in dit kader standaard gebruikt wordt, is een PKI-overheidscertificaat. Organisaties kunnen met bijvoorbeeld de Belastingdienst en het Kadaster digitaal berichten uitwisselen door zich met een PKI-overheidscertificaat te authenticeren. Deze certificaten voldoen overigens aan de eisen van STORK-niveau 4.
In de verschillende reacties op de consultatie wordt de hiervoor beschreven keuze onderschreven. De KBvG merkt evenwel in haar reactie bij dit artikel onder c op, dat het een vergaande delegatie van bevoegdheden betreft. De KBvG pleit voor een regeling in dit besluit. Het is echter aan de rechterlijke instanties om een digitaal systeem te bouwen, waartoe rechtzoekenden en hun gemachtigden toegang kunnen krijgen. Het in dit besluit opnemen van de specifieke authenticatiemiddelen acht ik onwenselijk, gezien de technische ontwikkelingen op dit gebied. Zo zullen DigiD en eHerkenning binnen een aantal jaren opgaan in het eID-stelsel. Voorts is voorstelbaar dat na verloop van tijd de rechterlijke instanties het inloggen met aanvullende of andere authenticatiemiddelen mogelijk maken. De rechterlijke instanties zullen bij landelijk (proces)reglement bepalen met welke authenticatiemiddelen partijen of andere betrokkenen, kunnen inloggen via het portaal in het digitale systeem van de rechterlijke instanties. Zij zullen hierbij aansluiten bij hetgeen gebruikelijk is binnen de overheid en waar nodig in overleg treden met de relevante ketenpartijen die op jaarbasis veel procederen. Voor het gebruikmaken van de automatische systeemkoppeling stellen de desbetreffende rechterlijke instanties aansluitvoorwaarden op.

Artikel 4

Eerste lid

Dit artikel schrijft voor dat de rechterlijke instanties aanwijzen via welk digitaal systeem voor gegevensverwerking partijen berichten elektronisch moeten respectievelijk kunnen indienen. Het ligt in de rede dat zij dit bij eigen (proces)reglement zullen voorschrijven. De KBvG suggereert in haar advies om in het besluit het digitale systeem aan te wijzen. Ik zie hiertoe geen noodzaak. Zoals ik al in het algemene deel heb beschreven, beperkt dit besluit zich waar mogelijk tot het regelen van techniekneutrale ontwikkelingen. Het digitale systeem dat in specifieke procedures gebruikt moet worden is een gedetailleerde door technische ontwikkelingen te bepalen regeling, die zich beter leent voor een (proces)reglement. Mochten zich ontwikkelingen voordoen waardoor het (proces)reglement ter zake wijzigt, dan krijgen partijen en andere betrokkenen voldoende tijd om zich hierop voor te bereiden. Uitsluitend het aangewezen digitale systeem kan worden gebruikt voor het digitale verkeer met de rechter, omdat alleen daarmee zorg kan worden gedragen voor een voldoende beveiligd berichtenverkeer. De indiening van berichten via e-mail wordt dan ook niet geaccepteerd, aangezien e-mail niet voldoende kan worden beveiligd. Hetzelfde geldt voor de indiening van berichten door verzending van bijvoorbeeld een USB-stick per post naar het gerecht. Alleen als bij procesreglement hiervoor een uitzondering is gemaakt, kan een partij via andere weg dan het aangewezen digitale systeem een bericht indienen. Dit kan bijvoorbeeld gelden voor het indienen van fysieke bewijsstukken in octrooizaken.
Mocht een partij een procedure digitaal zijn gestart bij een onbevoegde rechter, dan kan de rechter de zaak naar de juiste rechter verwijzen als hiervoor een wettelijke grondslag is (specifiek in het civiele recht kan dat aan de orde zijn). Het digitale dossier wordt vervolgens door deze rechter doorgestuurd (op grond van de artikelen 34 en 74 Rv en artikel 6:15 Awb) naar de bevoegde rechter.

Tweede lid

Berichten kunnen langs twee verschillende kanalen worden uitgewisseld met de rechterlijke instanties. Via het portaal ‘Mijn Zaak’ of via de automatische systeemkoppeling. Voordat een partij kan aansluiten op het koppelvlak van de rechterlijke instanties die dit ter beschikking stellen, moet zij aan bepaalde eisen voldoen. Deze eisen worden in beginsel door de rechterlijke instanties bij (proces)reglement voorgeschreven. Onder meer worden hierin eisen gesteld aan de beveiliging van het digitale systeem van de partij in kwestie, aan de wijze waarop zij interne regels stelt over de bewaking van persoonsgevoelige en andere gevoelige informatie, aan de aanvraagprocedure, en aan andere technische aspecten in het digitale systeem van de partij. Uitsluitend als een partij aan de voorgeschreven eisen voldoet, kan een koppeling via de automatische systeemkoppeling worden gelegd. Indien de noodzaak daartoe blijkt, kunnen deze eisen of bepaalde (minimum)waarborgen bij ministeriële regeling worden voorgeschreven.

Als een partij een bericht indient, moet dit voldoen aan specifieke eisen. Dit geldt onder meer voor een procesinleiding, een beroepschrift, een verweerschrift of een ander bericht, de eventuele bijlagen hierbij, een geluidbestand of een beeldbestand. De Adviescommissie voor burgerlijk procesrecht en de Afdeling bestuursrechtspraak vragen in hun adviezen om duiding van de in het artikel genoemde term 'kenmerken'. Naar aanleiding hiervan merk ik op dat kenmerken verschillende soorten eisen zijn die aan een bericht gesteld kunnen worden. Zo valt hierbij te denken aan het bestandsformaat, de omvang of de leesbaarheid van een bericht. Om de terminologie in dit artikel toegankelijker te maken, spreekt het besluit inmiddels van 'eisen'. De KBvG vraagt in haar reactie om een definitie van de term 'bericht' in het besluit op te nemen. Ik acht dat niet nodig. Zoals hierboven (in paragraaf 2) al is beschreven kan onder een bericht onder meer worden verstaan een (proces)stuk, een mededeling, een bestand of een formulier. Hiervoor geldt dat het opnemen van een definitie in het besluit niet opportuun is gezien mogelijke technologische ontwikkelingen.
De rechterlijke instanties stellen een digitaal formulier ter beschikking dat partijen moeten invullen, bijvoorbeeld bij het starten van een civiel- of bestuursrechtelijke procedure of bij voeren van verweer. Als een partij het formulier (volledig) heeft ingevuld, krijgt zij de procesinleiding of het beroepschrift te zien dat het systeem voor haar heeft gegenereerd. De verwachting is dat bepaalde partijen, met name advocaten, een eigen stuk met daarin de gronden of middelen (in geval van cassatie) willen indienen. De NOB suggereert in haar reactie op de consultatie dat het mogelijk moet zijn om in het tekstveld in het digitale formulier te verwijzen naar de bijlage, waarin de gronden van de vordering, het verzoek, het beroep of het verweer zijn opgenomen. Naar aanleiding hiervan merk ik op dat mijn verwachting is dat bij de bouw van de formulieren rekening wordt gehouden met deze wens. Zo is voorstelbaar dat partijen in het formulier kunnen aangeven dat zij hun gronden of middelen in een apart stuk willen uploaden. De in een apart stuk ingediende gronden of middelen worden vervolgens (al dan niet als bijlage) opgenomen in of gehecht aan de procesinleiding of het beroepschrift.
Het invullen van een formulier zorgt ervoor dat de door de desbetreffende rechterlijke instantie benodigde gegevens gestructureerd verwerkt kunnen worden door het digitale systeem. De rechterlijke instanties kunnen hierbij een onderscheid maken naar formulieren per doelgroep (zoals natuurlijke personen en advocaten). Tijdens het ontwikkelen van deze formulieren toetsen de rechterlijke instanties het gebruiksgemak van de formulieren bij de toekomstige gebruikers.
Een partij of een ander die in een procedure wordt betrokken, kan berichten indienen in het digitale systeem. Hierbij kan gedacht worden aan documentbestanden (zoals (een versie van) PDF-documenten) en aan geluid- of beeldbestanden. Gezien de veelheid aan soorten bestandstypen dat beschikbaar is, zou het een aanzienlijk beslag leggen op het digitale systeem als al deze bestandstypen zouden moeten worden toegelaten. Bovendien zou dan bij archivering het risico ontstaan dat een relatief onbekend bestandstype in de toekomst niet meer toegankelijk is, omdat dat bestandstype dan niet meer op de markt is. De bestandstypen die ten minste worden toegelaten, zullen dezelfde zijn voor alle rechterlijke instanties. Hierbij wordt aangesloten bij standaarden die gebruikelijk zijn binnen de overheid. Berichten van een ander bestandstype dan is voorgeschreven, hoeven door het digitale systeem niet toegelaten te worden. Mocht de uitzonderlijke situatie zich voordoen dat de omzetting van een bepaald bewijsstuk in een toegelaten bestand onmogelijk is voor een partij of in redelijkheid niet van haar verwacht kan worden, dan kan de rechter op grond van artikel 30c, zevende lid, Rv en artikel 8:36a, zesde lid, Awb bepalen dat het bericht op andere wijze wordt ingediend.
De Afdeling bestuursrechtspraak uit in haar advies de behoefte aan een grondslag om bij procesreglement kenmerken van berichten, zoals bestandsformaten en maximale omvang van bestanden vast te kunnen stellen. De KBvG vraagt in haar reactie om dergelijke technische eisen in dit besluit voor te schrijven. Het besluit biedt een grondslag om bij ministeriële regeling eisen te stellen aan de formulieren, bestandsformaten en andere technische aspecten van het berichtenverkeer met de rechterlijke instanties. Zolang deze ministeriële regeling niet is opgesteld, kunnen de rechterlijke instanties bij (proces)reglement voorschrijven aan welke eisen (waaronder bestandsformaten en – gelet op de technische limieten – de maximale omvang) elektronische berichten moeten voldoen. Hetzelfde geldt voor de formulieren waarmee een procesinleiding, een beroepschrift of een verweerschrift kan worden opgesteld en ingediend. De KBvG suggereert om modellen hiervoor bij wet of in dit besluit vast te stellen. Ik wil echter voldoende ruimte bieden aan toekomstige technische ontwikkelingen. Daarom geniet het de voorkeur als de specifieke technische aspecten van het digitaal communiceren met de rechter nader worden geregeld bij (proces)reglement. Partijen mogen erop vertrouwen dat de rechterlijke instanties hiervoor aansluiten bij geldende overheidsstandaarden en dat de rechterlijke instanties ketenpartijen betrekken bij het opstellen en eventueel nadien aanpassen van de (proces)reglementen. Voor het geval dat de noodzaak zou ontstaan om bij ministeriële regeling eisen te stellen aan de berichten (waaronder formulieren en bestandsformaten), dan kan dat op grond van dit artikel. Desgewenst kan een ministeriële regeling ook minimumeisen stellen aan zowel het digitale systeem van de rechterlijke instanties als aan de elektronische berichten die daarin worden ingediend of via het systeem ter beschikking worden gesteld.

Derde lid

Dit artikellid biedt de gerechten een grondslag om voor te schrijven aan welke eisen het door de

gerechtsdeurwaarder op te stellen oproepingsbericht moet voldoen. Artikel 111, eerste lid, Rv schrijft voor dat de griffier aan de eiser een oproepingsbericht stuurt nadat de procesinleiding is ontvangen. Het tweede lid van dat artikel schrijft voor aan welke eisen het oproepingsbericht ten minste moet voldoen. Artikel 113 Rv geeft de gerechtsdeurwaarder de mogelijkheid om een oproepingsbericht (met daarin de procesinleiding opgenomen) te betekenen bij verweerder, alvorens de procesinleiding wordt ingediend in het digitale systeem van de rechterlijke instanties. Het tweede lid van artikel 113 Rv geeft de gerechtsdeurwaarder de bevoegdheid om daartoe zelf het oproepingsbericht op te stellen. Het is onwenselijk als het oproepingsbericht dat een deurwaarder opstelt, verschilt van het oproepingsbericht dat de griffier opstelt. Het enige relevante verschil tussen beide oproepingsberichten is de mededeling of de procedure is gestart voorafgaand aan de betekening of dat deze onverwijld na de betekening wordt gestart (zie artikel 113, derde lid, Rv). Het is voorts onwenselijk als verschillende deurwaarders verschillende soorten oproepingsberichten zouden opstellen. De geautomatiseerde verwerking van de informatie in het oproepingsbericht is gediend met een vaststaande indeling (*lay-out*) van het oproepingsbericht. Net zoals het eerste lid van dit artikel, kunnen eisen aan het oproepingsbericht bij ministeriële regeling worden voorgeschreven. Het is in beginsel aan de gerechten om voor te schrijven aan welke eisen het oproepingsbericht voldoet. Mocht de noodzaak ontstaan om deze eisen bij ministeriële regeling voor te schrijven, dan zal daartoe een regeling worden opgesteld. De eisen vormen een aanvulling op de eisen die artikel 111 Rv stelt aan het oproepingsbericht. Onder de eisen kan onder meer worden verstaan het voorschrift welke onderdelen het oproepingsbericht kent en wat de opmaak daarvan is.

Artikel 5

Artikel 30c, derde lid, Rv en artikel 8:36d, eerste lid, Awb geven de definitie van een elektronische handtekening, zijnde een handtekening die bestaat uit elektronische gegevens die gehecht zijn aan of logisch verbonden zijn met andere elektronische gegevens en die worden gebruikt door de ondertekenaar om te ondertekenen. Uit artikel 30c, derde lid, Rv en artikel 8:36d, derde lid, Awb vloeit voort dat een elektronische handtekening uitsluitend vereist is voor processtukken die derdenwerking kunnen hebben. Het betreft vonnissen, beschikkingen, uitspraken, arresten, processen-verbaal en schikkingen. Omdat dit stukken betreft met derdenwerking, is het van belang dat een derde ook kan nagaan door wie en wanneer het stuk is ondertekend. Hiertoe dient het zetten van een elektronische handtekening. Artikel 5 van het besluit is een nadere uitwerking van artikel 30c, derde lid, Rv en artikel 8:36d, tweede lid, Awb en regelt waaraan de elektronische handtekening moet voldoen.
De voormelde artikelen uit Rv en de Awb maken het mogelijk dat als een partij een bericht indient waarvoor de verplichting tot ondertekening geldt (bijvoorbeeld een procesinleiding of een beroepschrift), dat bericht wordt geacht te zijn ondertekend als het langs elektronische weg is ingediend. Voordat een partij een bericht langs elektronische weg kan indienen, heeft zij zich namelijk al moeten authenticeren. Voorts legt het digitale systeem van de rechterlijke instanties vast door wie een bericht is ingediend. Hiermee is in het digitale systeem zichtbaar wie de indiener van het bericht is. Het is voor partijen daarom niet nodig om nog apart een elektronische handtekening te zetten. Deze berichten hebben ook geen derdenwerking en zijn alleen voor de rechter, partijen of anderen dan partijen die bij de procedure worden betrokken relevant. De rechter en deze partijen en anderen kunnen in het digitale dossier nagaan welke partij welke stukken heeft ingediend. Het hiermee vergelijkbare geldt voor berichten die via de automatische systeemkoppeling worden uitgewisseld. Op basis van de gegevens die worden meegeleverd met een bericht of uit het bericht zelf, blijkt van wie (de rechter, een der partijen of een andere betrokkene) het bericht afkomstig is.
Totdat de rechterlijke instanties gereed zullen zijn om gebruik te maken van de mogelijkheden die de elektronische handtekening of een variant daarvan, de tablethandtekening, biedt, wordt een bericht van een rechter of griffier met derdenwerking nog op papier ondertekend, waarna dat bericht gedigitaliseerd wordt. Dat is dan echter geen elektronische handtekening, maar een digitale kopie van het ondertekende document. De rechterlijke instanties ontwikkelen momenteel de benodigde voorzieningen waarmee rechters, griffiers en partijen een elektronische handtekening (waaronder tablethandtekening) zullen kunnen zetten.

Eerste lid

Alvorens een ondertekenaar een elektronische handtekening kan zetten, moet hij zich geauthenticeerd hebben. Artikel 3 stelt eisen aan de authenticatie van de gebruiker van het digitale systeem van de rechterlijke instanties. Vooralsnog wordt gebruik van de elektronische handtekening voorzien door rechters en griffiers. Voorstelbaar is evenwel dat ook partijen, advocaten of deurwaarders, een voorziening ontwikkelen of kopen om desgewenst zelf een elektronische handtekening te zetten. Door in het eerste lid te spreken van ‘ondertekenaar’ laat dit artikel deze ontwikkeling vrij. Authenticatie van de ondertekenaar is noodzakelijk, omdat diens identiteit alleen aan het document verbonden kan worden als hij zich heeft geauthenticeerd.
Door het zetten van een handtekening geeft de ondertekenaar de wilsuiting dat hij de te tekenen inhoud en de consequenties van ondertekening begrijpt en de inhoud van het document bevestigt.

Voorts levert de ondertekening bewijs op. Deze drie elementen moeten verifieerbaar zijn voor derden. Om na te kunnen gaan wie de ondertekenaar is, moet zijn identiteit verifieerbaar zijn in of in relatie tot het document. Dit is te vergelijken met het zetten van een 'natte' handtekening op een papieren document. De combinatie van naam en handtekening van de ondertekenaar geven zijn identiteit en wilsuiting weer in een papieren document. Voor de elektronische versie geldt in beginsel hetzelfde. Doordat de ondertekenaar (specifiek de rechter of griffier die het vonnis, de uitspraak enz. ondertekent), is ingelogd in het digitale systeem van de rechterlijke instanties, is zijn identiteit bekend. De identiteit van de ondertekenaar en het moment van ondertekening zijn zichtbaar in respectievelijk af te leiden uit het digitale document. Dat vergt dat het niet voldoende is dat een handtekening als een afbeelding in een digitaal document wordt geplaatst (bijvoorbeeld door een scan te maken van de 'natte' handtekening), maar dat de gegevens van de ondertekening achteraf verifieerbaar zijn in of in relatie tot het document. Dankzij de gegevens die verstrekt worden tijdens het ondertekenen (gegevens over de ondertekenaar, zoals zijn identiteit en het moment van ondertekenen) wordt de elektronische handtekening op unieke wijze aan de ondertekenaar verbonden. Het staat de rechterlijke instanties vrij om de elektronische handtekening zodanig in te richten dat bijvoorbeeld ook te zien is wat de functie van de ondertekenaar is. Zo is voorstelbaar dat als een rechter een vonnis of uitspraak ondertekent, naast zijn naam en het moment van ondertekening, zichtbaar is dat hij rechter is. Als iemand de elektronische handtekening wil controleren, kan hij dat via een verificatiedienst doen, met de gegevens die in het ondertekende document staan. De rechterlijke instanties kunnen hiertoe een verificatiedienst ter beschikking stellen.
Nadat een document elektronisch is ondertekend, moet het document ongewijzigd blijven. Als, op wat voor manier dan ook, wel wijzigingen worden aangebracht, moet zichtbaar zijn dat dat is gebeurd. Dat kan op verschillende manieren mogelijk worden gemaakt. Een mogelijkheid is door op het document, plus de ondertekening ervan, een wiskundige berekening toe te passen, waardoor een uniek nummer ontstaat, de zogeheten *hashwaarde*. Indien dit nummer later verandert, is duidelijk dat het document gewijzigd is.
Verordening 910/2014 van het Europees Parlement en de Raad betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van richtlijn 1999/93/EG (PbEU 2014, L 257) schrijft voor aan welke eisen een geavanceerde en een gekwalificeerde elektronische handtekening moeten voldoen, in geval van grensoverschrijdend dienstenverkeer. Een elektronische handtekening verbonden aan een (proces)stuk afkomstig uit een EU-lidstaat zal aan de minimumeisen gesteld in artikel 5 moeten voldoen. Een elektronische handtekening die aan hogere eisen voldoet (bijvoorbeeld een gekwalificeerde handtekening), zal eveneens toegelaten moeten worden door de Nederlandse rechter. Het stellen van voldoende hoge eisen aan een elektronische handtekening is daarmee ook relevant voor (proces)stukken met een elektronische handtekening die vanuit EU-lidstaten afkomstig zijn.

Tweede lid

De techniek biedt steeds meer mogelijkheden. Zo is er de mogelijkheid om een elektronische handtekening op een draagbare elektronische gegevensdrager te schrijven, zoals een tablet. Deze zogeheten tablethandtekening is een vorm van een elektronische handtekening. De eis die het tweede lid, onder a, stelt is een andere dan het eerste lid onder a stelt. De ondertekenaar authenticeert zich namelijk niet bij het zetten van een tablethandtekening. Waarborgen omtrent de identiteit van de ondertekenaar moeten dan ook op een andere manier geboden worden. Daarom is bepaald dat alleen een handtekening die op een elektronische gegevensdrager wordt gezet, in het bijzijn van een rechter of een griffier, of door een rechter of een griffier zelf wordt gezet, voldoet. De aanwezigheid van de rechter of de griffier geeft de benodigde waarborgen omtrent de verifieerbaarheid van de identiteit van de ondertekenaar. Het betreft hier een handgeschreven 'droge' handtekening, in tegenstelling tot een 'natte' handtekening zoals die op papier wordt gezet. Door middel van een 'pennetje' kan de ondertekenaar een handgeschreven handtekening op bijvoorbeeld een tablet zetten. Een elektronische gegevensdrager is meer dan alleen een tablet, ook een USB-stick kan een gegevensdrager zijn. Maar via een USB-stick kan geen handtekening op een document worden geschreven, die daaraan bovendien op unieke wijze is verbonden.
De eis onder b, in het tweede lid is hetzelfde als in het eerste lid, onder b. De identiteit van de ondertekenaar en het moment van ondertekening moeten zichtbaar zijn in respectievelijk af te leiden zijn uit het document. Eveneens geldt voor deze handtekening dat zij op zodanige wijze wordt verbonden aan het document, dat elke wijziging na ondertekening kan worden achterhaald. In de rechtspraktijk zijn toepassingen te voorzien voor een dergelijke handtekening. Bijvoorbeeld voor het ondertekenen van een schikking tussen partijen tijdens de mondelinge behandeling. De rechterlijke instanties zijn op dit moment nog niet gereed om een tablethandtekening toe te passen. Zodra zij zo ver zijn, kan op basis van dit besluit in civiel- en bestuursrechtelijke procedures gewerkt worden met de tablethandtekening.

Artikel 6

Eerste lid

Om een goed gebruik van het digitale systeem te bewerkstelligen is het noodzakelijk dat de rechterlijke instanties beschikken over het BSN van een betrokken natuurlijke persoon. De rechterlijke instanties digitaliseren ieder dossier, ongeacht of een partij op papier of digitaal procedeert. De Wet algemene bepalingen burgerservicenummer (Wabb) geeft op grond van de artikelen 10 en 13 een bevoegdheid aan de rechterlijke instanties om het BSN van een burger te vragen. De rechterlijke instanties hebben het BSN nodig voor de vervulling van hun publieke taak – rechtspleging – om de identiteit van de betrokken burger te kunnen vaststellen en deze te kunnen koppelen aan het zaakdossier waarbij zij als partij of anderszins is betrokken. Natuurlijke personen kunnen zich toegang verschaffen tot het digitale systeem van de rechterlijke instanties via DigiD. Het is van belang dat de juiste persoon aan het juiste dossier wordt gekoppeld. Als een natuurlijke persoon inlogt door middel van DigiD ziet de dienstverlener (in dit geval het digitale systeem) het BSN van die natuurlijke persoon. Het systeem ziet echter niet de naam van degene die inlogt. Het is dan ook noodzakelijk dat het BSN van deze persoon bekend is in het digitale systeem, om bij het inloggen de koppeling naar het juiste dossier te kunnen maken. Ook de natuurlijke persoon die ervoor kiest om op papier te procederen, heeft het recht om zijn dossier digitaal in te zien. Dat kan alleen als het digitale systeem hem aan een digitaal dossier heeft gekoppeld. Het gebruik van het BSN door de rechterlijke instanties voorkomt bovendien een vervuiling van gegevens in het digitale systeem. Het kan voorkomen dat een partij of haar gemachtigde haar eigen naam verkeerd invult (Janssen in plaats van Jansen), waardoor er verkeerde gegevens in het dossier zouden komen. Het gebruik van het BSN voorkomt dat op basis van dergelijke verkeerde persoonsgegevens een partij geen toegang zou kunnen krijgen tot het dossier of dat de rechterlijke instanties werken met verkeerde gegevens. Het CBP vraagt in zijn advies of een subsidariteitstoets is gedaan en vraagt om een nadere toelichting van de noodzaak van het gebruik van het BSN. De rechterlijke instanties hebben onderzocht op welke wijze een natuurlijke persoon op een beveiligde manier toegang kan krijgen tot zijn of haar digitale dossier. Hieruit is naar voren gekomen dat de rechterlijke instanties aansluiten bij de overheidsstandaarden op dit gebied. De overheidsstandaard voor het authenticeren met een elektronische identiteit voor een natuurlijke persoon is DigiD. Dit authenticatiemiddel maakt identificatie uitsluitend mogelijk door het gebruik van het BSN. Daarmee is het BSN de enige unieke sleutel om een natuurlijke persoon die een partij of een andere bij de procedure betrokkene is, te koppelen aan diens zaakdossier. Minder ingrijpende alternatieven zijn naar de huidige stand van overheidsstandaarden voor elektronische identiteit nog niet voorhanden. Een natuurlijke persoon die digitaal wil procederen, moet zich langs elektronische weg authenticeren en dat kan alleen met DigiD, waardoor de rechterlijke instanties moeten kunnen beschikken over diens BSN.
Als een verkeerd BSN wordt verstrekt, betekent dat overigens niet dat dan een ander toegang zou kunnen verkrijgen. Als eiser zijn eigen BSN verkeerd heeft doorgegeven (al dan niet via zijn vertegenwoordiger), dan kan hij geen toegang krijgen tot een digitaal dossier. Hij zal zich niet succesvol kunnen authenticeren, omdat zijn echte BSN en het eerder verstrekte BSN niet overeenkomen. Hij zal dan eerst zijn juiste BSN moeten doorgeven aan de rechterlijke instantie. Dat voorkomt dat onbevoegden toegang zouden kunnen krijgen tot het digitale dossier. Hiermee voldoen de rechterlijke instanties ook aan hun plicht op grond van artikel 11 van de Wbp om maatregelen te treffen om de kwaliteit van gegevens te waarborgen.
Als een natuurlijke persoon een procedure start, geeft hij zijn naam, adresgegevens en BSN op. Een natuurlijke persoon heeft vanzelfsprekend de bevoegdheid om zijn eigen persoonsgegevens te verstrekken. Er is dan ook geen noodzaak om dat in dit besluit te regelen. Indien een natuurlijke persoon met een gemachtigde procedeert en hij de procedure niet zelf start, verstrekt zijn gemachtigde het BSN van die natuurlijke persoon. Zo heeft de natuurlijke persoon met een gemachtigde ook zelf inzage in zijn digitale dossier. De natuurlijke persoon of namens hem zijn gemachtigde kan ook in een later stadium het BSN doorgeven, waarna hij toegang krijgt tot zijn digitale dossier.
Aangezien de gemachtigde geen overheidsorgaan is, kan hij geen grondslag voor de verwerking van het BSN aan de Wabb ontlenen. Artikel 24, tweede lid, van de Wbp stelt dat bij algemene maatregel van bestuur nadere regels kunnen worden gesteld over het gebruik van een wettelijk geregeld persoonsnummer (zoals het BSN). Bij dit besluit wordt de grondslag gegeven aan gemachtigden om het BSN van hun cliënt die een natuurlijke persoon is en over een BSN beschikt, door te geven aan het digitale systeem van de rechterlijke instanties. Deze bevoegdheid geldt voor beroepsmatig rechtsbijstandverleners en gemachtigden en niet-professionele gemachtigden. De niet-professionele gemachtigde die op papier wil procederen kan langs die weg het BSN verstrekken van de natuurlijke persoon die hij vertegenwoordigt, mits die persoon over een BSN beschikt.
Het CBP verzoekt in zijn advies om nader in te gaan op de momenten waarop het BSN verwerkt kan worden tijdens de procedure. Bestuursorganen vermelden op grond van de Wbp in hun correspondentie het BSN van de betrokken natuurlijke persoon. Zij doen dat dan ook in de communicatie met de rechterlijke instanties. Voor een goede werking van de automatische systeemkoppeling is van belang dat zo veel mogelijk met unieke nummers wordt gewerkt. Naast het zaaknummer is dat het BSN van

de betrokken natuurlijke persoon of personen. Het gebruik hiervan vindt zogeheten 'onder water' plaats. Dat betekent dat betrokken medewerkers het BSN niet zonder meer kunnen zien, maar dat het nummer wordt gebruikt in de communicatie tussen het systeem van de rechterlijke instanties en dat van de desbetreffende partij. Dit geldt ook voor partijen als rechtsbijstandsverzekeraars, advocaten en deurwaarders. Op grond van artikel 6 mogen zij het BSN van de betrokken natuurlijke persoon verwerken, wat onder meer inhoudt dat dit nummer als verificatie kan worden gebruikt tijdens het uitwisselen van berichten via de automatische systeemkoppeling. Omdat natuurlijke personen betrokken zijn bij de bulk van de zaken, draagt dit bij aan een zorgvuldige en efficiënte manier van berichten uitwisselen. Voor zover een professionele vertegenwoordiger gebruik maakt van het portaal 'Mijn Zaak' zal hij slechts één maal het BSN van zijn cliënt behoeven door te geven aan de rechterlijke instanties. Waar het de rechterlijke instanties betreft, zal op ieder moment dat een natuurlijke persoon toegang wenst te krijgen tot het digitale dossier, een verwerking plaatsvinden van diens BSN. Alleen op die wijze kan een koppeling worden gelegd tussen het authenticeren via DigiD door deze natuurlijke persoon en hem toegang geven tot zijn digitale dossier(s). De rechterlijke instanties verwerken het BSN van een natuurlijke persoon als deze inlogt in zijn of haar digitale dossier. Iedere keer als een natuurlijke persoon die partij is of een andere betrokkene bij de procedure is, inlogt, moet hij zich authenticeren door middel van DigiD. Om hem toegang te geven tot het juiste dossier, zal het systeem van de rechterlijke instanties zijn BSN verwerken.
Het kan ook voorkomen dat een natuurlijke persoon geen BSN heeft, bijvoorbeeld als hij een asielzoeker is. In dat geval kan hij ook niet over DigiD beschikken en heeft hij zelf geen inzage in het digitale dossier. Het blijft in dat geval aan zijn gemachtigde om hem te informeren over de stukken in het dossier of het dossier desgewenst aan hem te verstrekken. Dat is hetzelfde als in de oude situatie. Bij (proces)reglement kunnen de rechterlijke instanties nadere regels stellen over het gebruik van andere unieke cijfers, zoals het V-nummer dat wordt toegepast in vreemdelingenzaken, op basis waarvan partijen met de rechter kunnen communiceren over een individuele zaak. Voor bepaalde ketens, zoals de vreemdelingenketen is van belang dat bij de communicatie gebruik gemaakt wordt van unieke gegevens. Juist in vreemdelingenzaken is niet altijd een BSN voorhanden en is uitsluitend het gebruiken van een naam foutgevoelig. Dankzij het gebruik van een uniek nummer, zoals het V-nummer, kan de benodigde informatie (bijvoorbeeld of een beroep wel of niet gegrond is en een asielzoeker wel of niet mag worden uitgezet) vrijwel onmiddellijk binnen de keten worden gedeeld. Dit vergt evenwel ook van advocaten dat zij in dergelijke gevallen het unieke cijfer doorgeven aan de rechter bij het starten van de zaak. Zo nodig kunnen de rechterlijke instanties bij (proces)reglement nadere eisen stellen aan de aansluitvoorwaarden voor de systeemkoppeling en aan het formulier van 'Mijn Zaak' (zie artikel 4 en de bijbehorende toelichting).
Voorstelbaar is ook dat een natuurlijke persoon zijn BSN niet wenst te overleggen. In dat geval kiest hij er bewust voor om zelf geen toegang te hebben tot zijn digitale dossier. Zo veel mogelijk moet echter worden voorkomen dat betrokken natuurlijke personen hun BSN niet afgeven. Zo kunnen de rechterlijke instanties informatie bieden over de noodzaak van het verstrekken van dit persoonsgegeven en de waarborgen waarmee zij hiermee omgaan. Met name een gemachtigde (of in geval van het tweede lid een deurwaarder tijdens de oproeping van de verweerder) zal degene die hij vertegenwoordigt, moeten wijzen op het belang van het verstrekken van diens BSN. De gemachtigde zal zijn cliënt wijzen op de mogelijkheid dat de cliënt zelf inzage kan hebben in het digitale dossier.
Er is niet voor een verplichting gekozen in artikel 6, omdat het de toegang tot de rechter zou kunnen belemmeren indien een natuurlijke persoon of zijn gemachtigde in iedere procedure verplicht zou zijn om het BSN van deze persoon te verstrekken aan de rechterlijke instanties. Ik onderschrijf hetgeen de Adviescommissie voor burgerlijk procesrecht en de NVvR in dit kader in hun adviezen opmerken. Degene die het BSN mag verstrekken, kan niet belet worden om een proceshandeling te verrichten, als hij op het moment van het verrichten van de proceshandeling niet over het BSN beschikt. Zo kan het zijn dat hij bijvoorbeeld een beroepstermijn moet halen. Het is evenwel noodzakelijk om in de gevallen waarin men wel over het BSN beschikt, dat aan de rechterlijke instanties te verstrekken. Zoals hierboven al is toegelicht, is het voor een goede werking van het digitale systeem noodzakelijk dat het BSN van bij procedures betrokken natuurlijke personen bekend is bij de rechterlijke instanties. Ook als de desbetreffende natuurlijke persoon geen toegang wenst te krijgen tot het digitale dossier, is het verstrekken van het BSN nog steeds noodzakelijk voor de goede werking van het digitale systeem.
Zo mogelijk bij het verrichten van de eerste proceshandeling in het digitale dossier verstrekt de desbetreffende partij het BSN van de betrokken natuurlijke persoon. Dit kan de natuurlijke persoon zelf zijn of diens gemachtigde. De eerste proceshandeling kan het starten van de procedure zijn, het verschijnen in de procedure of het indienen van verweer. Als het een derde belanghebbende betreft, is dat als die zich in de procedure meldt. Als de natuurlijke persoon of diens gemachtigde pas na het verrichten van de eerste proceshandeling over het BSN beschikt, verstrekt hij dat alsnog zo spoedig mogelijk via 'Mijn Zaak' of via de systeemkoppeling aan de rechterlijke instantie.
Het BSN wordt op zodanige wijze in het digitale systeem verwerkt dat het niet zichtbaar wordt voor procesdeelnemers. De NVvR vraagt hier terecht nadrukkelijk aandacht voor in haar advies. Het BSN is een persoonsgevoelig gegeven dat niet zomaar zichtbaar mag zijn of worden voor anderen. De Raad voor de rechtspraak onderschrijft dit ook in zijn advies. Er dient evenwel onderscheid te worden gemaakt tussen het gebruik van het BSN dat nodig is voor de goede werking van het digitale systeem

en het gebruik van het BSN op processtukken in zaken waarvoor dit relevant is. In bepaalde (met name bestuursrechtelijke) zaken zal het BSN op processtukken staan. Gedacht kan worden aan fiscale besluiten of besluiten op het terrein van de sociale zekerheid. Het voorgaande betekent niet dat het BSN op deze processtukken onleesbaar gemaakt zou moeten worden. Zij zijn immers relevant voor de procedure. De indiening langs elektronische weg verandert hier niets aan. Uiteraard blijft het van belang dat alle bij de procedure betrokkenen zorgvuldig dienen om te gaan met de gegevens die voorkomen in een dossier.

Tweede lid

In kantonzaken treedt de gerechtsdeurwaarder in het merendeel van de gevallen als gemachtigde op. In dat geval verstrekt hij het BSN namens zijn cliënt op grond van het eerste lid. Het kan ook voorkomen dat de deurwaarder niet als gemachtigde optreedt (bijvoorbeeld in vorderingszaken waar een verplichting tot procesvertegenwoordiging geldt), maar uitsluitend het oproepingsbericht betekent. De deurwaarder die in opdracht van zijn cliënt of diens gemachtigde een oproepingsbericht betekent voordat de procedure is gestart, kan eenvoudig en snel die procedure starten na betekening en de benodigde berichten indienen. Hij doet dat dan namens zijn opdrachtgever, maar treedt dus niet op als gemachtigde in de procedure (waardoor het eerste lid niet in deze situatie van toepassing is). In de oude situatie stuurde een deurwaarder in het algemeen de uitgebrachte dagvaarding naar de gemachtigde van zijn opdrachtgever, die de dagvaarding vervolgens zelf naar het gerecht stuurde. In sommige gevallen deed de deurwaarder dat namens zijn cliënt. Het is voorstelbaar dat de deurwaarder dit vaker zal doen nu dit digitaal kan. De deurwaarder betekent dan het oproepingsbericht en vervolgens dient hij de scan van het betekende oproepingsbericht (waarin de procesinleiding is opgenomen) in en start hij daarmee de procedure. De deurwaarder moet bij deze indiening ook invullen wie zijn opdrachtgever is en indien dat een burger is diens BSN doorgeven. Het tweede lid biedt hiervoor de grondslag.
Hetzelfde geldt voor het BSN van de verweerder in vorderingszaken (tweede lid). Bij een aanzienlijk deel van de vorderingsprocedures is een gerechtsdeurwaarder betrokken. Een deurwaarder mag op grond van de huidige wet- en regelgeving voor het betekenen van een oproepingsbericht de persoonsgegevens van de verweerder controleren en diens BSN verwerken. Op grond van dit artikel is hij bevoegd om dit BSN te verwerken en aan de gerechten doorgeven, opdat het digitale systeem de verweerder aan het juiste digitale dossier kan koppelen. De gerechten hebben erop gewezen dat het voor hen tot een aanzienlijk grotere werklast leidt, indien in vorderingsprocedures de deurwaarder het BSN van de verweerder niet zou kunnen verschaffen. Dit heeft te maken met het grote aantal jaarlijkse vorderingsprocedures waarbij een deurwaarder betrokken is (de incassozaken bij rechtbanken betreffen jaarlijks ongeveer 450.000 zaken). De vorderingsprocedures waarbij geen deurwaarder is betrokken, de verzoekprocedures en de bestuursrechtelijke procedures vergen een andere methode om een verweerder aan het juiste digitale dossier te koppelen. Omdat dit minder zaken betreft, kunnen de rechterlijke instanties deze werkzaamheden zelf verrichten.

Artikel 7

Artikel 30c, vierde lid, Rv en artikel 8:36b, tweede lid, Awb geven een uitzondering op de verplichting van het digitaal procederen voor natuurlijke personen en verenigingen waarvan de statuten niet zijn opgenomen in een notariële akte, tenzij zij worden vertegenwoordigd door een derde die beroepsmatig rechtsbijstand verleent. In aanvulling daarop maakt dit besluit een uitzondering voor een rechtspersoon of onderneming die niet is ingeschreven in het handelsregister in Nederland (op grond van de artikelen 5 en 6 van de Handelsregisterwet) en die evenmin wordt vertegenwoordigd door een derde die in Nederland verplicht stukken moet indienen langs elektronische weg. Als een onderneming naar buitenlands recht een Nederlandse procesvertegenwoordiger heeft, dan geldt de uitzondering van dit artikel niet, aangezien deze vertegenwoordiger onder de verplichting valt. Naar aanleiding van het advies van de Afdeling bestuursrechtspraak merk ik op dat dit artikel verder ziet op alle buitenlandse rechtspersonen die geen hoofdvestiging of nevenvestiging in Nederland hebben. Rechtspersonen of ondernemingen die uitsluitend zijn gevestigd in het Caraïbisch deel van het Koninkrijk vallen eveneens onder de uitzondering van dit artikel. Dergelijke partijen kunnen niet over een authenticatiemiddel beschikken waarmee in Nederland gevestigde partijen toegang kunnen krijgen tot het digitale systeem van de rechterlijke instanties. Om een eHerkenningsmiddel aan te schaffen, moet een rechtspersoon of onderneming namelijk ingeschreven staan in het Handelsregister bij de Nederlandse Kamer van Koophandel. Dat is het geval wanneer een hoofdvestiging of nevenvestiging in Nederland in stand wordt gehouden. Een verplichting tot digitaal procederen zou voor de niet in Nederland gevestigde partijen tot een onmogelijke situatie leiden.
Om diezelfde reden kunnen deze partijen evenmin vrijwillig gebruikmaken van het digitale systeem. Hetzelfde geldt overigens voor natuurlijke personen die woonachtig zijn in het Caraïbisch deel van het Koninkrijk of die niet over de Nederlandse nationaliteit beschikken of anderszins niet de beschikking hebben over een BSN. Alleen met een BSN kan een natuurlijke persoon namelijk over DigiD beschikken en inloggen in ‘Mijn Zaak’.

Op grond van de Verordening 910/2014 (zie hierboven in de toelichting bij artikel 5, eerste lid) geldt een verplichting voor online dienstaanbieders om elektronische identificatiemiddelen uit andere lidstaten te erkennen, indien deze middelen met dit doel zijn aangemeld bij de Europese Commissie. Gerechtelijke procedures zijn echter van de Dienstenrichtlijn uitgesloten (zie artikel 2 van de Dienstenwet). In reactie op het advies van de NVvR merk ik daarom op dat het Europese recht geen verplichting inhoudt om het digitaal procederen open te stellen voor natuurlijke personen uit andere EU-lidstaten. De rechterlijke instanties kunnen er evenwel op termijn voor kiezen om het digitaal procederen ook aan partijen uit andere EU-lidstaten aan te bieden en hierbij aan te sluiten bij de eisen uit de Verordening.

Artikel 8

De Wet vereenvoudiging en digitalisering procesrecht stelt digitaal procederen voor professionele partijen verplicht. Voor natuurlijke personen geldt deze verplichting niet, maar zij mogen wel gebruikmaken van het digitale systeem van de rechterlijke instanties. De rechterlijke instanties bouwen waarborgen en controles in hun digitale systeem in, om ervoor te zorgen dat het digitale systeem in beginsel altijd toegankelijk is voor de rechter, partijen en anderen die in een procedure worden betrokken. In beginsel mag een partij er op vertrouwen dat als zij digitaal kan respectievelijk moet procederen, zij op ieder moment gebruik kan maken van het digitale systeem van de rechterlijke instanties.[4] Het blijft echter de verantwoordelijkheid van partijen om berichten tijdig in te dienen. Dat is niet anders dan bij het verzenden van berichten per fax of per post in de oude situatie. Het digitaal versturen van verschillende omvangrijke documenten zal bijvoorbeeld meer tijd in beslag nemen, dan alleen het 'ja' aanvinken in het digitale systeem als antwoord op de vraag of een verweerder wel of niet verschijnt.
Artikel 30c, achtste lid, Rv, 6:11 en artikel 8:36a, zevende lid, Awb bepalen dat de rechter een bericht dat te laat is ingediend niet buiten beschouwing laat, indien redelijkerwijs niet kan worden geoordeeld dat de indiener in verzuim is geweest. Artikel 30f Rv en artikel 8:36f Awb bieden de grondslag om bij of krachtens algemene maatregel van bestuur nadere regels te stellen ten aanzien van de verschoonbaarheid van de termijnoverschrijding als gevolg van verstoring van het digitale systeem voor gegevensverwerking van de gerechten en de bestuursrechter of de toegang daartoe. Naar aanleiding van het advies over een voorontwerp van dit besluit van de Raad voor de rechtspraak is het wetsvoorstel vereenvoudiging en digitalisering procesrecht hiertoe aangepast. In de reacties op het voorontwerp van de Wet vereenvoudiging en digitalisering procesrecht hebben ketenpartijen, zoals advocaten en rechtsbijstandsverzekeraars, naar voren gebracht dat met de introductie van digitaal procederen een concrete invulling van de verschoonbaarheid van de termijnoverschrijding wenselijk is voor die gevallen waarin een verstoring van de toegang tot of een verstoring in het digitale systeem van de rechterlijke instanties ontstaat, waardoor een partij haar indieningstermijn niet kan halen. Een bepaling die regelt waar een partij beroep op kan doen indien een verstoring van de toegang tot of een verstoring in het digitale systeem van de rechterlijke instanties optreedt en welke termijn zij vervolgens heeft, geeft rechtszekerheid aan partijen. Deze bepaling kan voorts de rechtseenheid bevorderen. De Adviescommissie burgerlijk procesrecht en de KBvG onderkennen eveneens het nut ervan. De NVvR betwijfelt de noodzaak van dit artikel, gezien artikel 6:11 Awb. Dat artikel geldt echter niet voor civielrechtelijke procedures, al is daar wel vergelijkbare jurisprudentie op dit gebied ontwikkeld. Gelet ook op het hiervoor beschrevene, acht ik een specifieke regeling ten aanzien van de verschoonbaarheid van de termijnoverschrijding wenselijk. De president en de procureur-generaal van de Hoge Raad hebben in hun advies de suggestie gedaan om deze bepaling eveneens van toepassing te laten zijn op anderen dan partijen die bij de procedure worden betrokken. Dit voorstel is overgenomen, doordat het artikel spreekt over 'indiener' in plaats van 'partij'. Zo kan een getuige of een deskundige een termijn hebben gekregen om bijvoorbeeld een rapport in te dienen. Als hij deze termijn niet haalt vanwege een verstoring van de toegang tot of verstoring in het digitale systeem, kan hij een beroep doen op de verschoonbaarheid van de termijnoverschrijding op grond van artikel 8. Het artikel bepaalt dat in geval van een verstoring van de toegang tot of een verstoring in het digitale systeem op de laatste dag van de voor een partij geldende termijn en zij langs elektronische weg procedeert, deze partij alsnog een bericht (bijvoorbeeld een beroepschrift of een verweerschrift) langs elektronische weg kan indienen op de eerstvolgende dag na de dag waarop zij ermee bekend had kunnen zijn dat de verstoring is verholpen. Als op enig moment tijdens de termijn, niet zijnde de laatste dag, een partij haar proceshandeling niet kan verrichten vanwege een verstoring, dan kan geen beroep worden gedaan op dit artikel. Per slot van rekening kan gedurende de rest van de termijn de proceshandeling alsnog verricht worden, zonder dat daarmee een termijnoverschrijding aan de orde zou zijn. Dit vereiste is geregeld overeenkomstig de verschoonbaarheid van de termijnoverschrijding van artikel 6:11 Awb, omdat voor een rechter niet kenbaar hoeft te zijn wat de reden van de termijnoverschrijding is. De rechter zal dat dan ook niet ambtshalve hoeven te toetsen, aangezien een partij wel een beroep moet doen op de verschoonbaarheid van haar termijnoverschrijding. De dag tot en

[4] Dit sluit aan bij een uitspraak van de Hoge Raad van 21 februari 2014, ECLI:NL:HR:2014:340.

met de dag waarop de termijnoverschrijding verschoonbaar is, is altijd een werkdag. Naar aanleiding van de adviezen van de Afdeling bestuursrechtspraak en de NVvR is in artikel 8 opgenomen dat artikel 1 van de Algemene termijnenwet van overeenkomstige toepassing is.
Dit artikel heeft uitsluitend betrekking op een verstoring van de toegang tot of een verstoring in het digitale systeem die zich voordoet op de laatste dag van een termijn, waardoor een partij een bericht niet tijdig kan indienen. Van partijen mag verwacht worden dat zij het nogmaals proberen als zij bemerken dat de eerste poging om toegang te krijgen tot het digitale systeem of om hierin een bericht in te dienen mislukt. Een storing van bijvoorbeeld een minuut zal zo in beginsel geen gevolgen hebben voor de termijn van indiening. Van partijen kan evenwel niet verwacht worden dat zij meerdere malen op een dag proberen om een bericht in te dienen in het digitale systeem. Een storing van langer dan enkele minuten mag dan ook niet voor rekening van een partij komen, als deze storing niet aan haar toerekenbaar is. Storingen zullen in de regel niet langer dan enkele uren aanhouden. Het aantal zaken waarin een termijn voor indiening verstrijkt op de dag waarop de storing plaatsvindt, zal daarom naar verwachting beperkt zijn. De verwachting is dat ook een partij met veel lopende procedures (bijvoorbeeld een bestuursorgaan of een rechtsbijstandsverzekeraar) in staat is om op de eerstvolgende werkdag nadat de verstoring is verholpen, berichten in te dienen in die zaken waarin een indieningstermijn verstreek op de dag waarop de storing plaatsvond. Het is dan ook niet noodzakelijk om een overschrijding van de termijn van langer dan één werkdag in dit besluit toe te laten. Een partij of andere betrokkene heeft overigens ook nog een andere mogelijkheid om te voldoen aan haar termijn. Op grond van artikel 30c, zesde lid, Rv, 6:11 en artikel 8:36a, vijfde lid, Awb, geeft de rechter een termijn om het verzuim te herstellen als een partij of andere betrokkene het (proces)stuk ten onrechte op papier indient. Een partij die niet zeker weet of zij wel een beroep kan doen op de verschoonbaarheid van de termijnoverschrijding, op grond van artikel 8 van dit besluit, kan ervoor kiezen om het stuk op papier in te dienen. In dat geval voldoet zij niet aan de eis van artikel 30c Rv of artikel 8:36a Awb, maar heeft zij wel haar termijn kunnen halen (mits zij de stukken nog tijdig op papier indient bij de rechterlijke instantie). De rechter geeft haar vervolgens een termijn om de stukken alsnog langs elektronische weg in te dienen. Ten overvloede geldt wel dat het stuk dat nadien langs elektronische weg wordt ingediend, identiek moet zijn aan het eerder op papier ingediende stuk. Anders is niet voldaan aan de voorwaarde tot herstel van het verzuim en kan de rechter een stuk buiten beschouwing laten of zelfs een partij (bijvoorbeeld als het een beroepschrift betreft) niet-ontvankelijk verklaren in haar beroep of het verzoek niet-ontvankelijk verklaren.
In de uitzonderlijke situatie waarin er een grootschalige storing plaatsvindt die meerdere dagen aanhoudt, in het digitale systeem van de rechterlijke instanties of een storing daarbuiten volstaat de regel uit dit besluit niet. Zo kan er bijvoorbeeld een langdurige storing zijn bij DigiD of eHerkenning, waardoor natuurlijke personen respectievelijk rechtspersonen en bestuursorganen geen toegang kunnen krijgen tot het digitale systeem. Een zo uitzonderlijke situatie zal door de rechter opgevangen kunnen worden, doordat partijen of andere betrokkenen een beroep kunnen doen op de algemene leer van de verschoonbaarheid van de termijnoverschrijding. Waar het een partij betreft, bijvoorbeeld een bestuursorgaan, met veel procedures waarin proceshandelingen verricht moesten worden in de tijd waarin de storing plaatsvond, kan van hen niet verwacht worden dat zij de eerstvolgende werkdag na het verhelpen van een dergelijke storing de vereiste proceshandelingen verrichten in al die procedures. Afhankelijk van de omstandigheden van het geval kan de rechter dan een overschrijding van de termijn met meerdere dagen, of zelfs weken toestaan. Tijdens een dergelijke storing kunnen de rechterlijke instanties hier ook informatie over bieden, bijvoorbeeld via de website van de rechtspraak.
Een partij kan alleen een beroep doen op artikel 8 in gevallen waarin een verstoring niet aan haar is toe te rekenen. Dat is in beginsel het geval wanneer de verstoring plaatsvindt door een oorzaak in of buiten het digitale systeem van de rechterlijke instanties, waarop de partij geen invloed heeft. De eerste situatie waarin een partij haar indieningstermijn niet kan halen, betreft een verstoring in of verstoring van het digitale systeem van de rechterlijke instanties. Zo kan het portaal ‘Mijn Zaak’ of de automatische systeemkoppeling vanwege onderhoud niet beschikbaar zijn of kan er een verstoring van andere aard optreden. Onder de term verstoring wordt dus ook (regulier) onderhoud verstaan. In deze situaties kan er sprake van zijn dat een partij geen toegang heeft tot het digitale systeem, maar ook dat er een verstoring is in het digitale systeem (bijvoorbeeld dat in een bepaald dossier geen stukken geüpload kunnen worden). In dit kader is van belang dat van een partij die gebruik maakt van de automatische systeemkoppeling niet verwacht kan worden dat zij bij een verstoring daarvan alsnog gebruik maakt van ‘Mijn Zaak’. Het gebruik van ‘Mijn Zaak’ is een andere dan het gebruik van de systeemkoppeling. Zo heeft een rechtspersoon die partij is een middel als eHerkenning nodig en moet haar medewerker geautoriseerd zijn om toegang te krijgen tot een of meerdere van haar dossiers. Van een partij kan niet verwacht worden dat zij dit regelt op het moment dat zich een verstoring van de systeemkoppeling voordoet en haar indieningstermijn dreigt te verstrijken. Evenwel kunnen in de aansluitvoorwaarden afspraken gemaakt worden over hoe stukken kunnen worden ontvangen en verzonden, indien de systeemkoppeling voor langere tijd niet beschikbaar zou zijn. Op grond van artikel 30d, eerste lid, Rv en artikel 8:36c, eerste lid, Awb ontvangt de indiener van een bericht in het digitale systeem van de rechterlijke instanties een ontvangstbevestiging. Als een partij geen ontvangstbevestiging ontvangt, moet zij ervan uitgaan dat het bericht niet is ontvangen. Dit kan het gevolg zijn van een storing in het digitale systeem, maar ook bij de partij zelf. De rechterlijke instanties

zullen bijhouden ('loggen') of er storingen in of storingen van het digitale systeem zijn en hoelang die hebben geduurd. Dergelijke storingen zijn redelijkerwijs niet aan een partij toe te rekenen. Zij kan daarom op grond van dit artikel een beroep doen op de verschoonbaarheid van de termijnoverschrijding en één werkdag nadat zij op de hoogte kon zijn van het feit dat de verstoring is verholpen, alsnog het bericht indienen. De Afdeling bestuursrechtspraak benadrukt in haar advies het belang van een nauwkeurige registratie van storingen. Zij vraagt hoe partijen kunnen bewijzen dat sprake is van een storing in het digitale systeem of een storing van de toegang daartoe. KEI Rechtspraak heeft mij verzekerd dat alle storingen aan haar kant, zowel kleine als grote, gelogd worden. De Afdeling bestuursrechtspraak en de Hoge Raad zullen eveneens storingen in hun eigen digitale systemen loggen. Een partij of andere betrokkene die vanwege een storing haar indieningstermijn niet heeft kunnen halen, kan om een bevestiging van een specifieke storing vragen. Deze bevestiging kan zij vervolgens als bewijs overleggen aan de rechter. Voorstelbaar is dat bij (proces)reglement nader geregeld wordt hoe partijen of andere betrokkenen dergelijke informatie kunnen opvragen.
De tweede situatie die zich kan voordoen, is dat het digitale systeem wel toegankelijk is en er daarin geen storingen zijn, maar dat er een verstoring is buiten het digitale systeem. Daardoor kan een partij geen gebruikmaken van het internet, heeft zij geen toegang tot het digitale systeem en kan zij geen bericht indienen in het digitale systeem, waardoor zij haar indieningstermijn niet haalt. Hierbij kan gedacht worden aan landelijke of regionale stroomstoringen, of storingen bij een provider van een partij, dan wel lokale werkzaamheden als gevolg waarvan een partij geen gebruik kan maken van het internet. Zo'n verstoring is voor een partij niet te voorzien, noch aan haar toe te rekenen. Zij is voorts niet bij machte om deze storing te verhelpen. In dergelijke gevallen kan zij eveneens op grond van dit artikel een beroep doen op de verschoonbaarheid van de termijnoverschrijding met één werkdag, nadat de verstoring is verholpen en zij hiermee bekend is of had kunnen zijn. De Afdeling bestuursrechtspraak wijst er in haar advies op dat zich ook storingen bij bijvoorbeeld DigiD kunnen voordoen of in andere systemen die niet van de rechterlijke instanties zijn, maar waar een partij wel gebruik van moet maken om toegang te krijgen tot het digitale systeem van de rechterlijke instanties. De Afdeling bestuursrechtspraak en de NOB stellen in hun commentaren de vraag hoe partijen hier weet van kunnen krijgen en dit kunnen bewijzen. Er is een landelijke website waarop storingen bij bijvoorbeeld DigiD en energieleveranciers staan vermeld: https://allestoringen.nl. Een partij kan de melding op deze site gebruiken ter onderbouwing van het beroep dat zij doet op de verschoonbaarheid van haar termijnoverschrijding als bedoeld in dit artikel. Niet alle (plaatselijke) storingen zullen vermeld worden op die site. Het is dan aan een partij om bij de veroorzaker van de storing (bijvoorbeeld de energieleverancier) of anderszins een bewijs te krijgen van de storing in kwestie. De rechterlijke instanties onderzoeken daarom welke mogelijkheden een partij heeft om een dergelijke storing te melden, opdat zij nadien bij de rechter een beroep kan doen op de verschoonbaarheid van de termijnoverschrijding.
Een andere situatie bestaat wanneer de computer van een partij gebreken vertoont en uitvalt, of dat een partij vanwege het niet (tijdig) betalen van de rekening van de internetprovider geen internet meer heeft. In deze gevallen kan die partij geen beroep doen op de verschoonbaarheid van de termijnoverschrijding die is bedoeld in dit artikel. Het is haar verantwoordelijkheid dat zij over deugdelijke middelen beschikt waarmee zij digitaal procedeert. De strikte eisen die in de jurisprudentie op dit punt zijn ontwikkeld, blijven gelden.
Indien andere hoogstpersoonlijke omstandigheden tot termijnoverschrijding aanleiding hebben gegeven, bijvoorbeeld omdat de partij op een cruciaal moment een ongeluk heeft gehad, kan dit anders liggen, mits de partij aannemelijk maakt dat het bericht zo spoedig als dit redelijkerwijs kon worden verlangd, is ingediend. Het kan ook voorkomen dat een partij de indieningstermijn niet haalt, vanwege een storing die niet aan haar kan worden toegerekend, maar dat zij niet in staat is om de eerstvolgende werkdag dit verzuim alsnog te herstellen. Zo kan het voorkomen dat een partij de eerstvolgende werkdag een operatie ondergaat. In deze gevallen kan zij een beroep doen op het algemene leerstuk verschoonbaarheid van de termijnoverschrijding (artikel 30c, achtste lid, Rv en artikel 6:11 Awb). Ik onderschrijf het advies van de Adviescommissie voor burgerlijk procesrecht dat het aan de rechter is om te bepalen of hij een dergelijk beroep op de verschoonbaarheid van de termijnoverschrijding honoreert of niet. In deze gevallen kan een langere termijn voor de overschrijding worden gehonoreerd dan die gegeven in artikel 9.
Voorts bepaalt het artikel dat beslissend is of een partij op de hoogte is of had kunnen zijn van het einde van de verstoring. Op de website van de desbetreffende rechterlijke instantie wordt een wezenlijke storing vermeld, hoe lang die naar verwachting zal duren en wanneer deze verholpen is. De NVvR stelt in haar advies voor om een meldingsplicht voor de rechterlijke instanties op te nemen. Ik acht een dergelijke verplichting niet nodig. Er mag op worden vertrouwd dat de rechterlijke instanties het voorkomen en vervolgens verhelpen van een storing via onder meer de eigen website deugdelijk vermelden. Een individuele rechter beoordeelt bovendien de omstandigheden van het geval waarin sprake was van een storing en de wijze waarop de partij of andere betrokkene ervan op de hoogte had kunnen zijn dat de storing is verholpen. Vanwege het belang van de voortgang van de procedure en het daarom tijdig indienen van stukken, wordt van partijen verwacht dat zij regelmatig (in ieder geval één keer per dag) op de website van de rechterlijke instanties kijken, indien zij bemerken dat zich een storing voordoet op de laatste dag van een termijn voor indiening. Gedurende één werkdag nadat op de website is gemeld dat de storing is verholpen, weet een partij die dan het bericht indient (zoals het

indienen van een procesinleiding in hoger beroep) zich verzekerd van de verschoonbaarheid van haar termijnoverschrijding, indien zij daar een beroep op doet. Waar het een beperkte storing in het digitale dossier betreft, zal hier naar verwachting geen melding van worden gemaakt op de website van de rechterlijke instanties. Een partij zal in zulke gevallen nogmaals moeten nagaan of de storing inmiddels is verholpen. Hiervoor geldt eveneens dat van partijen wordt verwacht dat zij ten minste éénmaal per dag proberen om hun bericht nogmaals in te dienen. De NOB stelt in haar consultatiereactie voor dat alle partijen een melding krijgen vanuit 'Mijn Zaak' dat de storing is verholpen. Dat zou echter betekenen dat partijen en andere betrokkenen bij alle op dat moment lopende procedures (wat er op jaarlijkse basis ongeveer 1,8 miljoen zijn), dan een melding moeten krijgen. Het overgrote deel van die partijen heeft geen behoefte aan een dergelijke melding, omdat haar indieningstermijn niet eindigde op de dag van de storing. Ook vanuit logistiek opzicht lijkt het onwenselijk als de rechterlijke instanties bij iedere kort of langdurende storing in hun digitale systeem een melding moeten versturen naar alle partijen bij alle lopende procedures op het moment dat die storing is verholpen. Naast de mogelijkheden die het besluit biedt in geval van een verstoring van het digitale systeem, heeft met name de NOvA de behoefte geuit om voor bepaalde gevallen een noodkanaal beschikbaar te stellen. De Afdeling bestuursrechtspraak onderschrijft de noodzaak van een noodkanaal in haar advies. Een noodkanaal biedt bescherming aan partijen, naast een mogelijk beroep op de verschoonbaarheid van de termijnoverschrijding. Het betreft hier procedures waar binnen een korte periode proceshandelingen moeten worden verricht, met eventueel vergaande en onomkeerbare gevolgen. Indien bijvoorbeeld een besluit is genomen om een asielzoeker uit te zetten en diens advocaat geen toegang kan krijgen tot het digitale systeem om hiertegen beroep in te stellen, kan de asielzoeker al zijn uitgezet tegen de tijd dat de storing verholpen is. Dat risico kan de advocaat niet nemen. Voor die gevallen is een noodkanaal vereist. Hetzelfde kan gelden voor verzoeken om voorlopige voorzieningen of voor kort gedingen, om te voorkomen dat onomkeerbare stappen worden gezet tijdens of vlak na de verstoring van de toegang tot of verstoring in het digitale systeem. Een dergelijk noodkanaal is vergelijkbaar met de huidige piketregeling. Met name voor spoedeisende maatregelen buiten kantoortijden is een piketregeling nog steeds nodig. Het noodkanaal kan geïntegreerd worden in de huidige piketvoorzieningen. Bij (proces)reglement kunnen de rechterlijke instanties hier nadere regels over opstellen. Bij het ter beschikking stellen van een dergelijk noodkanaal, is het wel zaak dat dit alleen voor uitzonderingen gebruikt wordt. De rechterlijke instanties zijn in gesprek met de NOvA om hierover zo nodig tuchtrechtelijke regels op te stellen.

Artikel 9

Dit artikel regelt de inwerkingtreding van het besluit. Voorzien is dat de verschillende onderdelen van het besluit bij Koninklijk Besluit op een verschillend tijdstip in werking kunnen treden. Dit hangt samen met de gefaseerde inwerkingtreding van Wet vereenvoudiging en digitalisering procesrecht, de Wet vereenvoudiging en digitalisering procesrecht in hoger beroep en cassatie en de Wet tot aanpassing van de wetgeving aan en invoering van de Wet vereenvoudiging en digitalisering van het procesrecht en van de Wet vereenvoudiging en digitalisering van het procesrecht in hoger beroep en cassatie. Deze bepaling is dan ook gelijkluidend aan de desbetreffende bepalingen in voormelde wetsvoorstellen.

Artikel 10

Dit artikel bevat de citeertitel van het besluit.

De Minister van Veiligheid en Justitie,