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. (Dit zal hierna worden aangeduid als: het digitale systeem van de rechterlijke instanties.) Naast deze webportalen stelt de Raad voor de rechtspraak onder bepaalde voorwaarden een automatische systeemkoppeling ter beschikking. Dit wordt ook wel aangeduid als een “system-to-system” voorziening, waarmee de digitale systemen van grote ketenpartners zoals de IND en deurwaarders, geleidelijk kunnen worden gekoppeld aan het digitale systeem van de gerechten.

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. Dit besluit is zo veel mogelijk techniekneutraal geformuleerd, om te voorkomen dat het vanwege technische ontwikkelingen regelmatig zou moeten worden aangepast. Waar technische aspecten van het digitale systeem worden beschreven, gaat dit uit van de huidige stand van de technologische ontwikkelingen. Het besluit geeft de benodigde ruimte aan nieuwe technologische ontwikkelingen die in de komende jaren benut kunnen worden om het digitale systeem te verbeteren en te optimaliseren. De rechterlijke instanties regelen bepaalde aspecten van het digitaal procederen - zoals de technische voorwaarden - nader bij procesreglementen.
2. Digitale procesvoering
Een rechtzoekende of, namens hem, een (al dan niet professioneel) procesvertegenwoordiger moet of 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.

De digitale mogelijkheden bieden partijen en de rechtspraak veel voordelen. 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 op te sturen naar de rechter en afhankelijk van de procedure naar de wederpartij. Verder kan een partij eenvoudig zelf het digitale dossier inzien en zo bijvoorbeeld alle berichten bekijken en de voortgang van zijn 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 helpt bij hun voorbereiding van de zitting. Het digitale systeem van de rechterlijke instanties waarvan rechtzoekenden, hun gemachtigden, (derde) belanghebbenden, rechters en griffiers gebruikmaken, biedt deze en meer mogelijkheden en maakt de rechtspraak daarmee toegankelijker. 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 worden verplicht gesteld om digitaal te procederen. Natuurlijke personen die onder de uitzondering van artikel 30c, vierde lid, van het Wetboek van Burgerlijke Rechtsvordering (hierna ook: Rv) en artikel 8:36b, tweede lid, van de Algemene wet bestuursrecht (hierna ook: Awb) vallen, kunnen desgewenst kiezen voor digitaal procederen. Partijen moeten hierbij gebruik maken 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 ook: de Wbp). De Wbp vereist dat een organisatie of instelling waar persoonsgegevens worden verwerkt, als verantwoordelijke wordt aangewezen. Deze 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 daarmee 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 8), kunnen de rechterlijke instanties nu langs elektronische weg over persoonsgegevens beschikken. De persoonsgegevens waarover zij beschikken zijn, met uitzondering van het burgerservicenummer (zie de toelichting bij artikel 7), dezelfde als in de oude situatie. De gegevens die voorkomen in een dossier, zoals persoonsgegevens (bijvoorbeeld het adres van partijen), zijn uitsluitend toegankelijk voor de bij het geding betrokken partijen. Specifieke persoonsgegevens zijn alleen vereist voor een goede werking van het digitale systeem en zijn niet inzichtelijk voor de bij het geding betrokken partijen. Zo heeft het digitale systeem het burgerservicenummer van een natuurlijke persoon nodig om hem aan het juiste dossier te koppelen. In het dossier staat dit persoonsgegeven niet vermeld.

Voorstelbaar is dat informatie over de verantwoordelijke partij in de zin van de Wpb en het doel waarvoor gegevens worden verwerkt, wordt verstrekt 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 onderscheiden rechterlijke instanties wordt hierover meer informatie gegeven.

Binnen de gerechten, het CBb en de CRvB vindt momenteel besluitvorming plaats over wie verantwoordelijk is voor de verwerking van persoonsgegevens in het digitale systeem, als bedoeld in

de Wbp. 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 hij ter beschikking stelt.

Een Privacy Impact Assessment (PIA) wordt 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 in de oude situatie niet anders. Nieuw is wel dat berichten digitaal worden opgeslagen en dat alle partijen toegang hebben tot hetzelfde 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 alleen de daartoe bevoegde medewerkers van de rechterlijke instanties 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 en degene die zich voegt of tussenkomt en de (eventuele) procesvertegenwoordigers of gemachtigden van al deze partijen. Doordat partijen toegang hebben tot hetzelfde digitale dossier is de informatievoorziening van partijen toegankelijker en overzichtelijker dan in de oude situatie.

De burger met een vertegenwoordiger of 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 vertegenwoordiger of een gemachtigde namens vele, soms tientallen rechtzoekenden optreedt (bijvoorbeeld bestemmingsplanzaken of massaschadezaken) kunnen de rechterlijke instanties bij procesreglement 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 dan partijen die betrokken zijn 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. Hieraan kunnen namelijk bepaalde kosten verbonden zijn, bijvoorbeeld voor het inschakelen van een rechtsbijstandverlener of voor griffierechten. Een derdebelanghebbende 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.

Het kan voorkomen dat partijen of anderen die bij een procedure zijn betrokken alleen toegang krijgen tot een bepaald deel van het dossier of alleen gedurende een bepaalde periode. 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 is echter onwenselijk als hij het hele dossier zou kunnen inzien, waaronder een rapport van een deskundige over het kind of diens gezinssituatie. Gedacht kan

voorts worden aan loonvorderingszaken, waarbij de werkgever de medische stukken van de werknemer niet mag inzien. 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 procesreglement uitgangspunten zullen formuleren, die de rechter in het individuele geval houvast geven.

Het bovenstaande geldt overigens eveneens als een natuurlijke persoon die op papier mag procederen van die mogelijkheid gebruik maakt. Deze natuurlijke persoon kan een partij zijn of een ander die bij de procedure is betrokken. Hij krijgt net als in de oude situatie op papier (een deel van) het dossier toegezonden door de betrokken rechterlijke instantie.

De rechter, griffier, partijen en anderen die bij de procedure zijn betrokken, moeten op zorgvuldige wijze omgaan met de persoonsgegevens in het dossier. Deze plicht volgt uit 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 digitale portaal “Mijn Zaak” twee stappen worden doorlopen om toegang te krijgen tot een zaaksdossier: 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 schrijven bij procesreglement voor 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 waar mogelijk aangesloten bij geldende overheidsstandaarden. De middelen die in ieder geval ter beschikking staan aan de gebruiker zijn DigiD voor burgers, eHerkenning voor rechtspersonen en de Advocatenpas voor advocaten.

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 inloggen met zijn DigiD. Indien de natuurlijke persoon wil dat iemand anders voor hem in het dossier kan kijken en handelingen kan verrichten, dan zal hij deze gemachtigde moeten aanmelden via het digitale systeem van de rechterlijke instanties. Uit die aanmelding blijkt dan dat de natuurlijke persoon iemand anders heeft gemachtigd om voor hem te handelen. De niet-professionele gemachtigde zal zich – als natuurlijke persoon – moeten authenticeren met zijn eigen DigiD. De professionele gemachtigde authenticeert zich met eHerkenning of een Advocatenpas (zie hieronder). Het digitale systeem controleert vervolgens of hij als gemachtigde is aangemerkt.

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. De rechtspersoon of het bestuursorgaan meldt bij zijn middelenuitgever welke medewerkers hij voor welke diensten (bijvoorbeeld de dienst van de rechtspraak; e-herkenning kan ook voor andere diensten worden gebruikt, zoals het aanvragen van subsidies) heeft gemachtigd. Het middel wordt vervolgens op persoonsniveau, dus per gemachtigde 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 gebruik maakt gemachtigd 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. Wanneer ten behoeve van een rechtspersoon of bestuursorgaan wordt

ingelogd, controleert het digitale systeem dus eerst of deze rechtspersoon als partij bekend is. De rechtspersoon krijgt immers alleen toegang tot het dossier van de eigen zaken. De medewerker die namens de rechtspersoon of het bestuursorgaan inlogt krijgt vervolgens alleen toegang tot het digitale systeem als hij door de rechtspersoon of het bestuursorgaan gemachtigd is voor de dienst van de rechtspraak. Het digitale systeem controleert of de medewerker gemachtigd is aan de hand van het eHerkenningsmiddel dat de desbetreffende medewerker heeft verkregen van de rechtspersoon of het bestuursorgaan.

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 voormelde verplichtingen op basis van onder meer de Wbp moeten voldoen. Daarover bestaat consensus en overigens moest dat ook al in de oude situatie. Het is aan een partij om te beslissen of, en zo ja, welke medewerkers geautoriseerd zijn om inzage te krijgen in een specifiek dossier. De rechterlijke instanties zijn voornemens een autorisatiemodel te ontwikkelen, waarbij een of enkele medewerkers aan een specifieke zaak gekoppeld kunnen worden. 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, waarbij het digitale systeem controleert of hij gemachtigd is tot de dienst van de rechtspraak, en vervolgens controleert het digitale systeem of hij gekoppeld is aan een specifiek dossier. Alleen dat dossier is voor de medewerker toegankelijk.

Een advocaat kan met zijn Advocatenpas inloggen in het digitale systeem. Een partij die zelf een nieuwe procedure start of verweer voert, maar wel een procesvertegenwoordiger heeft, moet doorgeven wie zijn gemachtigde is. Als de advocaat namens zijn cliënt een proceshandeling verricht, vult hij in namens wie hij optreedt. 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 als procesvertegenwoordiger toegang zou mogen hebben tot het digitale dossier. Indien die medewerker bijvoorbeeld uitvalt wegens ziekte, moet iemand anders de partij kunnen vertegenwoordigen. Ook advocaten die alleen kantoor voeren, zullen een advocaat van een ander kantoor moeten kunnen machtigen om te werken in hun dossiers, indien zij niet beschikbaar zijn. De overdracht van een zaak en vervanging binnen een kantoor is mogelijk in het digitale systeem van de rechterlijke instanties. Het regelen van vervanging en het in verband daarmee verschaffen van toegang tot het zaaksdossier in het digitale systeem betreft een standaard bedrijfsvoering en dient plaats te vinden ongeacht de vorm van het dossier (papier of digitaal). 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 tot een bepaald deel daarvan. Het digitale systeem zal voorzien in deze mogelijkheid (zie paragraaf 4).

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, gerechtshoven en de Hoge Raad;

b. de Afdeling bestuursrechtspraak van de Raad van State;

c. het College van Beroep voor het bedrijfsleven (hierna ook: het CBb);

d. en de Centrale Raad van Beroep (hierna ook: de CRvB).

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 voorwaarden voldoen.

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 zijn 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 zaaksdossier 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 anderen die in de procedure zijn betrokken (waaronder deskundigen) en hun vertegenwoordigers. Aan welke eisen de authenticatie door deze gebruiker moet voldoen, wordt geregeld in artikel 2.

Eerste lid, onder b
Het digitale systeem van de rechterlijke instanties moet voorts de gebruiker in staat stellen om na te gaan wie de verzender is van een bericht dat langs elektronische weg is ingediend. De eisen van onder meer authenticatie waarborgen dat verifieerbaar is wie een specifiek bericht heeft ingediend. Alleen degene die gerechtigd is om toegang te krijgen tot het digitale dossier kan via het digitaal systeem berichten indienen. Partijen die betrokken zijn bij een procedure kunnen berichten indienen. De rechter, of namens hem de griffier, kan eveneens berichten via het digitale dossier ter beschikking stellen aan partijen. Voor de rechter, partijen of andere betrokkenen bij een procedure moet kenbaar zijn wie de indiener van een bericht is. Het digitale systeem registreert wie ingelogd heeft in een dossier en wie welke berichten heeft ingediend. Voor zover deze gegevens niet zichtbaar zijn in het digitale dossier, kan de rechter indien nodig deze gegevens achterhalen (bijvoorbeeld op verzoek van een partij). Overigens 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.

Eerste lid, onder c
Tevens moet het digitale systeem van de rechterlijke instanties de gebruiker in staat stellen om te kunnen controleren of het desbetreffende bericht is gewijzigd. Zo zou het onwenselijk zijn als een eiser een bericht indient en vervolgens de verweerder hierin wijzigingen zou kunnen aanbrengen. Evenmin is wenselijk dat de indiener na indiening van een bericht, dat bericht wijzigt of verwijdert. 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 pdf-bestanden). Net als in de oude 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 rechter 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 de gebruiker van het systeem van de rechterlijke instanties kan nagaan 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. Als een partij een bericht indient, ontvangt zij een ontvangstbevestiging in het digitale systeem (zie de artikelen 30c, eerste lid, Rv en 8:36c, eerste lid, Awb). In vergelijking met de oude situatie waarbij berichten per post tussen partijen en de rechter werden uitgewisseld, worden dankzij deze ontvangstbevestiging en andere waarborgen die in het digitale systeem worden ingebed, aanzienlijk meer waarborgen aan partijen en de rechter geboden. Een partij (of diens gemachtigde) wisselt via het portaal “Mijn Zaak” berichten uit met de rechter. Daarnaast stellen de rechterlijke instanties onder voorwaarden een systeemkoppeling (system-to-system) voor het berichtenverkeer ter beschikking (in beginsel alleen met het digitale systeem dat door de Raad voor de rechtspraak wordt ontwikkeld). Dit betreft een geautomatiseerde koppeling tussen het digitale systeem van de rechterlijke instanties en dat van een

partij of diens gemachtigde die op jaarbasis op grote schaal procedeert. Hierbij valt te denken aan partijen als gerechtsdeurwaarders, rechtsbijstandsverzekeraars en grote bestuursorganen, als de IND en het UWV. De rechterlijke instanties zullen de system-to-system koppeling fasegewijs beschikbaar stellen na de inwerkingtreding van de Wet vereenvoudiging en digitalisering procesrecht, de daarmee samenhangende wetten en dit besluit.

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 de artikelen 30d Rv en 8:36c Awb). 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 verweerschrift.

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. Indien 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 9.

Bij de uitwisseling van berichten via system-to-system met een partij, diens procesvertegenwoordiger of 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 desbetreffende rechterlijke instanties maken hier met de aangesloten partijen afspraken over. De verwerking van ontvangen berichten dient vervolgens door iedere gebruiker zelf goed te worden ingericht binnen de eigen organisatie. De waarborg die het eerste lid, onder d, biedt, dient ertoe om te waarborgen dat de berichtenuitwisseling zorgvuldig en betrouwbaar verloopt. Voor system-to-system betekent dit dat als het systeem van de rechterlijke instanties ziet dat een bericht niet is opgehaald, de desbetreffende partij hiervan een melding krijgt. De desbetreffende rechterlijke instanties maken afspraken met partijen over de vormgeving van deze melding.

De waarborgen die het digitale systeem van de rechterlijke instanties biedt, resulteren in een goed werkend berichtenverkeer via “Mijn Zaak” en - indien van toepassing - via system-to-system, voor zover dat in de beïnvloedingssfeer van dit systeem ligt. Partijen zijn zelf verantwoordelijk om hetzij via “Mijn Zaak”, hetzij via system-to-system 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 geeft partijen en anderen 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.

Eerste lid, onder e

Nu een partij langs elektronische weg berichten kan of moet indienen in het digitale systeem van de rechterlijke instanties, is het van belang dat hij kan nagaan of er een storing is in dat systeem en dat hij dit nadien kan bewijzen als hij een beroep doet op de verschoonbaarheid van de termijnoverschrijding (zie ook de toelichting bij artikel 9). 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 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 kleinschalige of kortdurende storing

heeft plaatsgevonden, waarover de website geen informatie biedt. Wanneer 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, vraagt de rechter vervolgens gegevens over storingen op binnen de eigen organisatie.

Het moment waarop een bericht, in de zin van artikel 30d, eerste lid Rv en artikel 8:36e, eerste lid Awb, is ontvangen, is het moment waarop het digitale systeem van de rechterlijke instanties het bericht heeft ontvangen. 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.

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 voldoet. 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. Waar het internationale standaarden betreft, wordt voldaan aan die 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, komen terug in het zogeheten betrouwbaarheidsniveau. Met betrekking tot het betrouwbaarheidsniveau wordt binnen Europees verband gesproken van het STORK-niveau. 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 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 3. 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 zaaksdossiers 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. Het STORK-niveau 3 vereist verdergaande methoden voor de verificatie van de identiteit van de gebruiker, dan de niveaus 1 en 2. Zo eist het STORK-niveau 3 dat middelenuitgevers onder overheidstoezicht staan. Voorts wordt van het middel

een tweefactorauthenticatie vereist.

De keuze voor het STORK-niveau 4 zou tot gevolg hebben dat alle partijen en andere betrokkenen PKI-certificaten (Public Key Infrastructure) moeten aanschaffen en gebruiken. De kosten voor een PKI-certificaat zijn substantieel hoger dan voor middelen met STORK-niveau 3. Verder moeten de medewerkers van de rechtspersoon die van het middel gebruik moeten kunnen maken, in persoon verschijnen om hun ID-document te laten controleren door de middelenuitgever. Zeker waar het een rechtspersoon betreft met veel medewerkers die toegang moeten kunnen krijgen tot het digitale systeem van de rechterlijke instanties, zou dit 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 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.

Het artikel 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 wachtwoord of een code 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 ander die bij de procedure is betrokken, 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. De rechterlijke instanties wijzen daarom bij procesreglement aan met welke middelen partijen en anderen die bij de procedure zijn 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 digitaal systeem van de rechterlijke instanties uitwisselt via een automatische systeemkoppeling (system-to-system), vindt geen authenticatie op persoonsniveau, maar op organisatieniveau plaats. De eisen in dit artikel zien daarmee tevens op de authenticatie in het kader van system-to-system. Een middel dat in dit kader standaard gebruikt wordt, is een PKI-certificaat. Organisaties kunnen met bijvoorbeeld de Belastingdienst en het Kadaster digitaal berichten uitwisselen door zich met een PKI-certificaat te authenticeren. Deze certificaten voldoen overigens aan de eisen van STORK-niveau 4.

Artikel 4

De artikelen 30c, derde lid, Rv en 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. Dit artikel regelt de voorwaarden waaraan een elektronische handtekening moet voldoen. Uit artikel 30c, vierde lid, Rv en 8:36d, derde lid, van de 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. Waar het berichten betreft met derdenwerking, is van belang dat die derde ook kan nagaan door wie en wanneer het bericht is ondertekend. Hiertoe dient het zetten van een elektronische handtekening. Indien een partij een bericht indient waarvoor de verplichting tot ondertekening geldt (bijvoorbeeld een procesinleiding of een beroepschrift), dan wordt dat bericht 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 denkbaar dat, totdat de rechterlijke instanties zover zijn om gebruik te maken van de mogelijkheden die de elektronische handtekening of de tablethandtekening biedt, een bericht met derdenwerking nog op papier wordt 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 de benodigde voorzieningen waarmee rechters, griffiers en partijen een elektronische of tablethandtekening kunnen zetten.

Eerste lid
Onder a

De eisen die aan het authenticatiemiddel worden gesteld, zijn onder artikel 3 reeds toegelicht. Het authenticeren gaat vooraf aan het zetten van de elektronische handtekening. De identiteit van de ondertekenaar kan alleen aan het document verbonden worden als hij zich heeft geauthenticeerd. Authenticatie is daarmee de eerste voorwaarde waaraan een elektronische handtekening moet voldoen.
Onder b

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 digitale versie geldt in beginsel hetzelfde. De identiteit van de ondertekenaar en het moment van ondertekening zijn zichtbaar in respectievelijk af te leiden uit het digitale document. Het artikel eist verder dat het document duurzaam en onlosmakelijk verbonden is met de identiteit van de ondertekenaar en het moment van ondertekening. Dit 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. De elektronische handtekening kan verder zodanig ingericht worden 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.

Uit het voorgaande volgt bovendien dat elke wijziging in het document moet kunnen worden vastgesteld. Als iemand zijn handtekening op een document plaatst, moet het document daarna ongewijzigd blijven. Als, op wat voor manier ook, wel wijzigingen worden aangebracht, moet zichtbaar zijn dat dat is gebeurd. Dit gebeurt bijvoorbeeld 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.

Tweede lid

De techniek biedt steeds meer mogelijkheden. Zo is er de mogelijkheid om een elektronische handtekening op een elektronische gegevensdrager te zetten, zoals een tablet. De bepaling biedt een grondslag om bij ministeriële regeling nadere eisen te stellen aan een dergelijke handtekening. Deze zogeheten tablethandtekening voldoet niet aan precies dezelfde eisen als die gelden voor de elektronische handtekening in het eerste lid. Zo is er geen sprake van authenticatie door de ondertekenaar. Voorstelbaar is dat als eis gesteld wordt dat de tablethandtekening daarom alleen door een rechter of griffier, of door een partij alleen in aanwezigheid van een rechter of griffier gezet kan worden.

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 evenwel nog niet gereed om een tablethandtekening toe te passen. Zodra zij zo ver zijn, kan de tablethandtekening bij ministeriële regeling worden voorgeschreven.

Artikel 5

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 procesreglement zullen voorschrijven. 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 een usb-stick per post naar het gerecht. Alleen daar waar bij procesreglement hiervoor een uitzondering is gemaakt, kan een partij via andere weg dan het aangewezen digitale systeem een bericht indienen. Hetzelfde is ook denkbaar voor berichten die een zeer omvangrijk bestand vormen, waardoor het digitale systeem van de rechterlijke instanties overbelast zou kunnen raken.

Mocht een partij een procedure digitaal zijn gestart bij een onbevoegde rechter, dan verwijst de rechter de zaak naar de juiste rechter. Het digitale dossier wordt dan door deze rechter doorgestuurd (op grond van artikelen 34 en 74 Rv en artikel 6:15 Awb) naar de bevoegde rechter.

Als een partij een bericht indient, moet dit voldoen aan de door de rechterlijke instanties voorgeschreven kenmerken. 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 rechterlijke instanties stellen een digitaal formulier ter beschikking dat partijen moeten invullen, bijvoorbeeld bij het starten van een civiel- of bestuursrechtelijke procedure. Als een partij het formulier (volledig) heeft ingevuld, krijgt zij de procesinleiding of het beroepschrift te zien dat het systeem voor haar heeft gegenereerd. 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 tussen 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, zoals burgers, advocaten en deurwaarders.

Een partij of anderen die in een procedure zijn betrokken, kunnen elektronische berichten indienen in het digitale systeem. Dit kunnen bestanden zijn als pdf/a-documenten, maar ook geluid- of beeldbestanden. Gezien de veelheid aan soorten bestandtypen dat beschikbaar is, zou het een aanzienlijk beslag leggen op het digitale systeem als al deze bestandtypen zouden moeten worden toegelaten. Bovendien zou dan het risico bij archivering ontstaan dat een relatief onbekend bestandtype in de toekomst niet meer toegankelijk is, omdat dat bestandtype dan niet meer op de markt is. Bij procesreglement wordt voorgeschreven welke bestandtypen toelaatbaar zijn. De bestandtypen die ten minste worden toegelaten, zullen dezelfde zijn voor alle rechterlijke instanties. Berichten van een ander bestandtype dan is voorgeschreven, hoeven door het digitale systeem niet toegelaten te worden. Mocht de uitzonderlijke situatie zich voordoen dat het een bepaald bewijsstuk betreft waarvan omzetting in een toegelaten bestand onmogelijk is voor een partij of niet in redelijkheid van hem 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.

Artikel 6

Dit artikel biedt de gerechten onderscheiden de Hoge Raad een grondslag om bij procesreglement voor te schrijven aan welke kenmerken 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 wordt gestart na de betekening (zie artikel 113, derde lid, Rv). Het is voorts onwenselijk als verschillende deurwaarders verschillende soorten oproepingsberichten kunnen opstellen. De gerechten schrijven daarom voor aan welke kenmerken het oproepingsbericht moet voldoen. Deze kenmerken vormen een aanvulling op de eisen die artikel 111 Rv stelt aan het oproepingsbericht.

Artikel 7

Eerste lid

De Wet algemene bepalingen burgerservicenummer (Wabb) geeft op grond van artikelen 10 en 13 de bevoegdheid aan de rechterlijke instanties om het burgerservicenummer (hierna ook: het BSN) van een burger te vragen. De rechterlijke instanties hebben het BSN nodig voor de vervulling van hun publieke taak, zijnde rechtspleging, om de identiteit van de betrokken burger te kunnen vaststellen en deze te kunnen koppelen aan het zaaksdossier 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 in geval een natuurlijke persoon op papier procedeert, moeten de rechterlijke instanties over zijn BSN beschikken om het juiste dossier aan de juiste persoon te koppelen. De rechterlijke instanties digitaliseren ieder dossier, ongeacht of een partij op papier of digitaal procedeert.

Als een natuurlijke persoon een procedure start, geeft hij zijn naam, woonplaats en BSN op. Indien het een natuurlijke persoon betreft met procesvertegenwoordiging of een gemachtigde en hij de procedure niet zelf start, moet zijn vertegenwoordiger of gemachtigde het BSN van die natuurlijke persoon invullen in het digitale systeem. Dit kan alleen als de natuurlijke persoon over een burgerservicenummer beschikt. Het kan voorkomen dat een natuurlijke persoon hierover niet beschikt, 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.

Niet-professionele gemachtigden zijn op grond van artikelen 30c Rv en 8:36a Awb niet verplicht om een procedure langs elektronische weg te starten. Ook als een dergelijke gemachtigde en zijn cliënt er niet voor kiezen om langs elektronische weg te procederen, is er een noodzaak voor het vermelden van het BSN van de natuurlijke persoon die wordt vertegenwoordigd. De natuurlijke persoon die ervoor kiest om op papier te procederen heeft het recht om digitaal zijn dossier in te zien. Dat kan alleen als het digitale systeem hem aan een dossier heeft gekoppeld. Tevens hebben de rechterlijke instanties het BSN van deze partij nodig om haar in het digitale systeem aan het interne digitale dossier te kunnen koppelen.

Een burger kan alleen via DigiD toegang krijgen tot zijn digitale dossier, als zijn BSN bekend is bij het systeem van de rechterlijke instanties. Aangezien de vertegenwoordiger of 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 procesvertegenwoordigers en 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 professionele vertegenwoordigers en gemachtigden en niet-professionele gemachtigden. De niet-professionele gemachtigde die op papier wil procederen geeft op papier het BSN door van de natuurlijke persoon die hij vertegenwoordigt, mits die persoon over een BSN beschikt.

Tweede lid

In kantonzaken treedt de gerechtsdeurwaarder in het merendeel van de gevallen als gemachtigde op. In dat geval kan hij het BSN namens zijn cliënt verstrekken 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 cliënt, 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 over het algemeen genomen de uitgebrachte dagvaarding naar de gemachtigde van zijn cliënt, 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 in en start hij daarmee de procedure. De deurwaarder moet bij deze indiening ook invullen wie zijn cliënt is en indien dat een burger is diens BSN kunnen doorgeven. Het tweede lid biedt hiervoor de grondslag.

Hetzelfde geldt voor het BSN van de verweerder in vorderingszaken. Bij een aanzienlijk deel van de vorderingsprocedures is een deurwaarder betrokken. Een deurwaarder mag voor het betekenen van een oproepingsbericht de persoonsgegevens van de verweerder controleren en diens BSN verwerken. Op grond van dit artikel mag hij dit BSN vervolgens 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 kan verschaffen. Dit heeft te maken met het grote aantal jaarlijkse vorderingsprocedures waarbij een deurwaarder betrokken is (de incassozaken betreffen jaarlijks ongeveer 450.000 zaken). Het aantal 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 wel verrichten.

Artikel 8

De artikelen 30c, vierde lid, Rv en 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 het besluit een uitzondering voor een rechtspersoon, vennootschap of andere entiteit naar buitenlands recht die niet vertegenwoordigd wordt door een derde die in Nederland beroepsmatig rechtsbijstand verleent. Een dergelijke partij zal niet over een authenticatiemiddel kunnen beschikken waarmee Nederlandse partijen toegang kunnen krijgen tot het digitale systeem van de rechterlijke instanties. Een verplichting tot digitaal procederen zou voor dergelijke partijen tot een onmogelijke situatie leiden.

Het is voor deze partijen evenmin mogelijk om vrijwillig gebruik te maken van het digitale systeem, aangezien zij zich niet met de toegelaten middelen kunnen authenticeren.

Vanaf 2018 zal dit overigens anders zijn. Nederland en ook de Nederlandse rechtspraak is op grond van de Verordening 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 (Verordening 2012/146) vanaf dan verplicht om elektronische identificatiemiddelen uit andere lidstaten te erkennen, indien deze middelen met dit doel zijn aangemeld bij de Europese Commissie. De rechterlijke instanties sluiten voor de implementatie van deze verordening aan bij de rijksbrede ontwikkelingen. Ter gelegenheid van de implementatie van de verordening zal worden bezien of dit artikel aanpassing behoeft.

Artikel 9

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. Om ervoor te zorgen dat het digitale systeem in beginsel altijd toegankelijk is voor de rechter, partijen en anderen die in een procedure zijn betrokken, bouwen de rechterlijke instanties waarborgen en controles in hun digitale systeem in. In beginsel mag een partij er op vertrouwen dat als zij digitaal kan of moet procederen, zij op ieder moment gebruik kan maken van het digitale systeem van de rechterlijke instanties. Het blijft echter de verantwoordelijkheid van partijen om berichten tijdig in te dienen. Indien een partij een bericht op het allerlaatste moment indient, neemt zij daarmee het risico dat er bij die indiening iets misgaat en een termijn verstrijkt. 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 'ja' aanvinken in het digitale systeem als antwoord op de vraag of een verweerder wel of niet verschijnt.

De artikelen 30c, achtste lid, Rv, 6:11 en 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. In het bestuursrecht bestaat al uitvoerige jurisprudentie over de verschoonbaarheid van de termijnoverschrijding. 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 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 in het digitale systeem van de rechterlijke instanties optreedt, geeft rechtszekerheid aan partijen. Deze bepaling kan voorts de rechtseenheid bevorderen.

Het artikel bepaalt dat in geval van een verstoring van de toegang tot of in het digitale systeem, een partij die langs elektronische weg procedeert, 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 kan zijn dat de verstoring is verholpen. Daarmee is de overschrijding van de termijn van indiening die verliep op de dag van de verstoring verschoonbaar, indien een partij zich hierop beroept (overeenkomstig de overige gevallen waarin een partij een beroep doet op de verschoonbaarheid van de termijnoverschrijding op grond van artikel 6:11 Awb). Artikel 1 van de Algemene termijnenwet brengt mee dat indien de eerstvolgende dag na die waarop de verstoring is verholpen op een zaterdag, een zondag of op een feestdag valt, deze termijn wordt verlengd tot en met de eerstvolgende dag die niet een zaterdag, zondag of een feestdag is. Daarmee is de dag tot en met de dag waarop de termijnoverschrijding verschoonbaar is altijd een werkdag.

Artikel 9 heeft uitsluitend betrekking op een verstoring van de toegang tot of 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 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. 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 kan indienen 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 kan alleen beroep doen op artikel 9 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 oorzaak kan zijn gelegen in een storing in het digitale systeem van de rechterlijke instanties zelf of in een technische storing buiten dat systeem.

De eerste situatie waarin een partij haar indieningstermijn niet kan halen, betreft een verstoring in of van het digitale systeem van de rechterlijke instanties. Zo kan het portaal "Mijn Zaak"

vanwege onderhoud niet beschikbaar zijn of kan er een verstoring van andere aard optreden. Op grond van artikelen 30d, eerste lid, Rv en 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. De rechterlijke instanties zullen bijhouden ("loggen") of er storingen zijn in of van het digitale systeem 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 tweede situatie die zich kan voordoen, is dat het digitale systeem wel toegankelijk is en daarin geen storingen zijn, maar dat er een verstoring is buiten het digitale systeem. Daardoor kan een partij geen gebruik maken 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.

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 bedoeld in artikel 9. 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 is aan de rechter om te bepalen of hij een dergelijk beroep op de verschoonbaarheid van de termijnoverschrijding honoreert of niet.

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. Van partijen wordt 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.

Hetzelfde geldt als er een storing is buiten het digitale systeem van de rechterlijke instanties. Een partij zal nogmaals dan wel dagelijks moeten nagaan of zij inmiddels wel toegang kan krijgen tot het digitale systeem van de rechterlijke instanties. Het digitale systeem van de rechterlijke instanties kan niet monitoren of er storingen zijn bij elektriciteitsleveranciers of internetproviders. 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.

Naast de mogelijkheden die het besluit biedt in geval van een verstoring van het digitale systeem, onderzoekt de Rechtspraak of voor bepaalde gevallen een noodkanaal beschikbaar gesteld kan worden. Zo zijn er gevallen voorstelbaar waarin een partij een zeer korte termijn heeft om een bericht in te dienen (bijvoorbeeld in het vreemdelingenrecht). Aangezien het niet halen van de termijn vanwege een storing (van de toegang tot of in het digitale systeem) vergaande gevolgen kan hebben

voor partijen, is een alternatief in noodgevallen wenselijk. Indien de rechterlijke instanties een dergelijk noodkanaal ter beschikking stellen, is het wel zaak dat dit alleen voor uitzonderingen gebruikt wordt. De rechterlijke instanties zijn in gesprek met de Nederlandse Orde van Advocaten om hierover zo nodig tuchtrechtelijke regels op te stellen.

Artikel 10

Het Besluit elektronisch verkeer met de bestuursrechter voorziet in de mogelijkheid om een beroepschrift langs elektronische weg bij de bestuursrechter in te dienen. Het Besluit elektronische indiening dagvaarding biedt gerechtsdeurwaarders de mogelijkheid om een dagvaarding langs elektronische weg in te dienen. Aangezien de Wet vereenvoudiging en digitalisering procesrecht het mogelijk maakt om na inwerkingtreding een beroepschrift, een procesinleiding en andere (proces)stukken langs elektronische weg in te dienen en het onderhavige besluit dat nader uitwerkt, vervallen de in dit artikel vermelde besluiten.

Artikel 11

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.

Artikel 12

Dit artikel bevat de citeertitel van het besluit.

De Minister van Veiligheid en Justitie,

I.W. Opstelten