Nota van toelichting

Algemeen

Ingevolge artikel 475, vierde lid, van het Wetboek van Burgerlijke Rechtsvordering worden bij algemene maatregel van bestuur regels gegeven aangaande de registratie van elektronische adressen van derde-beslagenen. Wanneer een derde aan een door de Minister van Justitie aangewezen organisatie een elektronisch adres heeft opgegeven waaraan kan worden betekend, kan aan deze derde het beslagexploot elektronisch worden gelaten. De regels aangaande de registratie kunnen betrekking hebben op de wijze van opgave, wijziging, afmelding en doorhaling van een elektronisch adres en de gevolgen ervan. Naast het elektronisch betekenen aan het elektronisch adres blijft het mogelijk om op conventionele wijze te betekenen aan de woonplaats. Bij algemene maatregel van bestuur dienen tevens regels aangaande de betrouwbaarheid en vertrouwelijkheid van, de voorwaarden waaronder en de wijze waarop een beslagexploot elektronisch kan worden gelaten. Op deze verschillende regels heeft het besluit betrekking.
Het voornemen is de Koninklijke Beroepsorganisatie van Gerechtsdeurwaarders (KBvG) aan te wijzen als organisatie aan wie door een derde een elektronisch adres kan worden opgegeven. Het besluit tot aanwijzing van een organisatie zal worden gepubliceerd in de Staatscourant.
Een ontwerp van het besluit is met de KBvG besproken. Tevens is een ontwerp van het besluit voorgelegd aan het College bescherming persoonsgegevens.

Registratie elektronische adressen

De derde die een mogelijk beslag op een elektronisch adres wenst te ontvangen, dient een elektronisch adres op te geven aan een door de Minister van Justitie aangewezen organisatie (de KBvG). Deze organisatie dient er zorg voor te dragen dat de deurwaarders op de hoogte worden gesteld aan wie zij elektronisch exploot kunnen laten. Het is de bedoeling dat de KBvG een register houdt van derden aan wie elektronisch een derdenbeslagexploot kan worden betekend. Dit register zal te raadplegen zijn op de site van de KBvG (www.kbvg.nl). Met betrekking tot het adres van de derde zal naast de naam van de derde, de datum van opgave door de derde worden vermeld en de datum waarop daadwerkelijk gebruik gemaakt kan worden van het elektronisch adres. Tevens zal de inhoud van de laatste wijziging met betrekking tot het adres, de datum van melding van deze wijziging en de datum waarop daadwerkelijk van het gewijzigde adres gebruik kan worden gemaakt worden opgenomen. Ten slotte zal de afmelding van het elektronisch adres met de bijbehorende datum van melding door de derde en datum van doorhaling van het adres (verwerking) worden aangegeven. Bij het gebruik van de applicatie ziet de deurwaarder het adres zelf niet, het is verwerkt in de toepassing van het systeem (aanklikken van de naam van de derde).
Het betreft hier elektronische adressen die exclusief worden gemaakt voor derdenbeslaglegging. Aan de opgave door een derde zijn geen kosten verbonden.
De opgave van het elektronisch adres door de derde, het doorgeven van wijzigingen met betrekking tot het adres, of het afmelden van het adres is niet aan een bepaalde vorm gebonden.

Naast gerechtsdeurwaarders kan ook door belastingdeurwaarders elektronisch beslag onder derden worden gelaten. Op grond van artikel 4 jo. 13 e.v. van de Invorderingswet 1990 kunnen belastingdeurwaarders overeenkomstig de bepalingen van het Wetboek van Burgerlijke Rechtsvordering dwangbevelen betekenen en tenuitvoerleggen.

Beginselen en mate van betrouwbaarheid en vertrouwelijkheid

Met betrekking tot de eisen die worden gesteld aan de betrouwbaarheid en vertrouwelijkheid van het laten van een elektronisch beslagexploot aan een derde is uitwerking gegeven aan de beginselen van betrouwbaarheid en vertrouwelijkheid die in de memorie van toelichting van de Wet elektronisch bestuurlijk verkeer worden genoemd en is aangesloten bij nationale en internationale normen voor informatiebeveiliging. De deurwaarder is, voorzover deze ambtelijke werkzaamheden verricht, bestuursorgaan. Afdeling 2.3 (verkeer langs elektronische weg) van de Algemene wet bestuursrecht is dan ook van toepassing.
Een belangrijke beginsel van betrouwbaarheid is authenticiteit, dat betrekking heeft op de oorsprong van het document en ziet op de vragen of het document wel echt is en de gegevens wel

afkomstig van de verzender. Ook het beginsel van integriteit, dat ziet op de mogelijkheid dat het document onderweg is gemanipuleerd en betrekking heeft op de vragen of het document volledig is en het niet onbevoegdelijk is gewijzigd, speelt een belangrijke rol.
Het vereiste van vertrouwelijkheid ziet erop dat het document alleen toegankelijk is voor hen voor wie het is bestemd. Op het punt van de beveiliging wordt aangesloten bij nationale en internationale normen voor informatiebeveiliging. Bij nationale normen kan worden gedacht aan normen zoals die voor overheidsorganen zijn opgenomen in het Voorschrift Informatiebeveiliging Rijksoverheid (VIR). Internationale normen zijn op dit moment NEN-ISO/IEC 17799 (Codes voor informatiebeveiliging) en NEN-ISO/IEC 27001 (Managementsystemen voor informatiebeveiliging).
Er kunnen drie niveaus van betrouwbaarheid en vertrouwelijkheid worden onderscheiden: maximale, voldoende en pro forma betrouwbaarheid en vertrouwelijkheid. Maximale betrouwbaarheid en vertrouwelijkheid zien op het toepassen van de beveiliging volgens de hoogste technische standaarden. Van voldoende betrouwbaarheid en vertrouwelijkheid is sprake indien de veiligheid vergelijkbaar is met de situatie dat er uitsluitend gebruik gemaakt wordt van conventioneel verkeer. Pro forma betrouwbaarheid en vertrouwelijkheid omvatten een minimale beveiliging. De aard en de inhoud van het bericht en het doel waarvoor het wordt gebruikt, zijn bepalend voor de mate van betrouwbaarheid en vertrouwelijkheid die is vereist.
Bij het elektronisch laten van een derdenbeslag is het, gelet op de aard en inhoud, noodzakelijk om te kiezen voor beveiliging volgens de hoogste technische standaarden. Gelet op de vertrouwelijkheid en betrouwbaarheid van de te verzenden gegevens ligt het in de rede dat bij het laten van het exploot van derdenbeslag gebruik wordt gemaakt van een (geavanceerde) elektronische handtekening (met gecertificeerde sleutels), derhalve een gekwalificeerde elektronische handtekening in de zin van artikel 3:15a, tweede lid, BW.
Gerechtsdeurwaarders werken al enige tijd met het systeem van elektronische aanlevering van stukken aan het Kadaster. Hierbij wordt door de gerechtsdeurwaarders gebruik gemaakt van een (geavanceerde) elektronische handtekening (met gecertificeerde sleutels). Op deze wijze is ongeveer 75% van alle gerechtsdeurwaarders bekend met het gebruik van een dergelijke elektronische handtekening. Een veelgebruikte techniek voor het aanmaken van een ‘geavanceerde elektronische handtekening’ is een ‘digitale handtekening’. Hierbij wordt gebruik gemaakt van versleuteling van een bericht met behulp van twee codes: een publieke en een private sleutel. Met de private sleutel, die uniek is voor de ondertekenaar en die niet bekend mag raken bij anderen dan de ondertekenaar, versleutelt de ondertekenaar het te verzenden bericht. De ontvanger van dit bericht kan met een bijhorende publieke sleutel het bericht ontcijferen én nagaan of het bericht ongewijzigd is en afkomstig van de bezitter van de bijhorende private sleutel. Welke publieke sleutel bij welke persoon hoort, wordt vastgelegd in een digitaal certificaat door een onafhankelijke derde (certificaatdienstverlener).

Artikelsgewijs

Artikel 1
Zoals hiervoor aangegeven zal de KBvG een register houden met elektronische adressen van derden waaraan elektronisch beslag kan worden gelaten. De registratie van gegevens van natuurlijke personen is een verwerking van persoonsgegevens in de zin van artikel 1 van de Wet bescherming persoonsgegevens (Wbp).Het doeleinde van de registratie is een doelmatige tenuitvoerlegging van vonnissen, beschikkingen en authentieke akten alsmede andere bij de wet als executoriale titel aangewezen stukken (vergelijk artikel 8 en 9 Wbp).
Daar de KBvG als houder van het register en de individuele deurwaarders als gebruikers van het register enige tijd nodig hebben om in te spelen op deze wijze van betekening onder de derde en de latere wijzigingen, zal een bepaalde termijn voor de verwerking van gegevens worden gehanteerd. De KBvG heeft aangegeven een termijn van vijf dagen wenselijk te achten. Deze termijn ziet zowel op de verwerking van de opgave als voor de wijziging van gegevens en de afmelding van het adres waaraan elektronisch kan worden betekend. De opgave van een adres heeft tot gevolg dat na ommekomst van een termijn van vijf dagen na ontvangst hiervan elektronisch kan worden betekend, de wijzigingen hebben tot gevolg dat er na ommekomst van een termijn van vijf dagen volgens de gewijzigde gegevens zal worden betekend en de afmelding heeft tot gevolg dat na ommekomst van een termijn van vijf dagen het elektronisch adres zal worden doorgehaald, waarna niet langer elektronisch zal kunnen worden betekend.

Artikel 2
In artikel 2, onder a, is aangegeven dat aangaande de betrouwbaarheid en vertrouwelijkheid de eis wordt gesteld dat gebruik wordt gemaakt van een systeem van gegevensverwerking dat in staat is om de verzender, de gerechtsdeurwaarder of belastingdeurwaarder, te identificeren en na te gaan of een bericht authentiek is en daadwerkelijk afkomstig is van de verzender. Hiermee wordt recht gedaan aan het beginsel van authenticiteit. Het betekent dat geschikte technieken dienen te worden gekozen om gerechtsdeurwaarders of belastingdeurwaarders te identificeren, vast te stellen of gegevens werkelijk afkomstig zijn van deze personen en de echtheid van een document vast te stellen. Onder een systeem van gegevensverwerking wordt verstaan een systeem voor het genereren, verzenden, ontvangen, opslaan of op andere wijze verwerken van gegevens.
Tevens dient gecontroleerd te worden of het bericht volledig is en niet onbevoegdelijk is gewijzigd. In onderdeel b wordt het beginsel integriteit tot uitdrukking gebracht. Een derde moet er zeker van zijn dat een bericht niet door onbevoegden gewijzigd is. Het moet ervan op aan kunnen dat het elektronisch beslagexploot 'te vertrouwen' is.
In onderdeel c is het vereiste van een goede beveiliging opgenomen. Een bericht dient immers alleen toegankelijk te zijn voor hen voor wie het is bestemd. Hiermee wordt het beginsel van vertrouwelijkheid gewaarborgd. Deze beveiliging dient in elk geval zodanig te zijn, dat deze aansluit bij internationale normen voor informatiebeveiliging. De verdere uitwerking van het systeem voor gegevensverwerking is aan de aan te wijzen organisatie, de KBvG, overgelaten.

Artikel 3
In artikel 3 is opgenomen dat het systeem voor gegevensverwerking erin dient te voorzien dat de deurwaarder langs elektronische weg een ontvangstbevestiging krijgt van de derde. Hiervoor is gekozen omdat het van groot belang kan worden geacht te kunnen constateren of een beslagexploot is ontvangen door de derde. Vanaf het moment van ontvangst is de beslaglegging onder de derde voltooid.
Het betreft hier een automatische ontvangstbevestiging. De ontvangst vindt niet eerst plaats als het bericht daadwerkelijk is geopend. Of en wanneer een bericht wordt geopend behoort tot de verantwoordelijkheid van de derde.

Artikel 4
In artikel 4 is aangegeven dat het besluit gelijktijdig in werking zal treden met de Wet tot wijziging van het Wetboek van Burgerlijke Rechtsvordering en de Gerechtsdeurwaarderswet in verband met de bevoegdheid van deurwaarders om informatie op te vragen en elektronisch te betekenen in geval van derdenbeslag (Stb. 2008, 435). De inwerkingtreding van deze wet is voorzien voor het begin van 2009.

De Staatssecretaris van Justitie,