S.R.P. Bastiaans, M.T. Spuijbroek & C. Michielsen[1]

Elektronische identificatie en ondertekening conform eIDAS

Computerrecht 2019/174

De eIDAS-verordening heeft een juridisch kader geïntroduceerd dat de betrouwbaarheid en acceptatie van elektronische transacties binnen de EU moet vergroten. Hiervoor wordt een gelijk speelveld beoogd waarin burgers en bedrijven binnen de EU met hun eigen nationale elektronische ID zich ook digitaal kunnen identificeren bij openbare instanties uit andere lidstaten. Daartoe worden uniforme eisen gesteld aan de betrouwbaarheidsniveaus van deze elektronische ID's. De eIDAS-verordening bevat daarnaast een kader voor de verschillende types elektronische handtekeningen; de (gewone) elektronische handtekening, de geavanceerde elektronische handtekening en de gekwalificeerde elektronische handtekening. Gebruik van elektronische handtekeningen vereist analyse van het benodigde type handtekening en de bruikbaarheid daarvan voor de beoogde transacties. Deze bijdrage beschrijft verschillende aspecten die voortvloeien uit de hierboven omschreven onderwerpen en is bedoeld als praktische handreiking voor diegenen die gebruikmaken, of willen maken, van elektronische ID's of elektronische handtekeningen.

1. Inleiding

De eIDAS-verordening is grotendeels van toepassing sinds 1 juli 2016.[2] Het doel van de eIDAS-verordening is ambitieus: het vergroten van vertrouwen in elektronische transacties binnen de Europese Unie ("EU"). Daartoe bevat de eIDAS-verordening onder andere regelgeving met betrekking tot elektronische identificatie en authenticatie, en bevat de eIDAS-verordening een regeling voor verplichte intracommunautaire erkenning van bepaalde elektronische identificatie- en authenticatiemiddelen door openbare instanties. Het meest bekende onderdeel van de eIDAS-verordening is wellicht de regeling inzake elektronische handtekeningen. Daarnaast ziet de eIDAS-verordening ook op diverse andere elektronische middelen, zoals elektronische zegels, tijdstempels en documenten.

In dit artikel bespreken wij, na een korte introductie van de eIDAS-verordening, twee specifieke onderwerpen uit de eIDAS-verordening die voor de praktijk relevant zijn. Deze bijdrage strekt ertoe praktische handvatten te bieden voor interpretatie en begrip van deze twee onderwerpen.

Allereerst beschrijven wij de verschillen in betrouwbaarheidsniveaus van elektronische identificatiemiddelen ("eID's") en de verplichting tot erkenning van die middelen binnen de EU. Die erkenning heeft niet alleen directe gevolgen voor onderdelen van de overheid, maar ook voor diverse private partijen die voor een deel van hun werkzaamheden als openbare instantie kwalificeren. Wij werken deze complexe regelgeving beknopt uit, en benoemen enkele aandachtspunten die bij implementatie van elektronische identificatiemiddelen van belang zijn.

Vervolgens gaan wij in op de regelgeving rondom de elektronische handtekening. Deze is voor vrijwel ieder bedrijf van belang. Ook voor de elektronische handtekening illustreren wij welke aspecten bij implementatie hiervan een rol kunnen spelen. Dat doen we aan de hand van enkele praktijkvoorbeelden.

1.1 *De eIDAS-verordening*

De eIDAS-verordening is op 23 juli 2014 aangenomen en vervangt de Richtlijn inzake elektronische handtekeningen.[3] Deze richtlijn heeft een basaal, gemeenschappelijk EU-kader voor elektronische handtekeningen geschapen. De eIDAS-verordening bevat een grondige uitbreiding van dit basale kader: voor elk punt van contact tussen burgers, overheidsinstellingen en – in sommige gevallen – private bedrijven worden mogelijkheden van elektronische identificatie en authenticatie uitgebreider ingevuld. De eIDAS-verordening geeft bovendien meer invulling aan de elektronische handtekening.

Nieuw zijn de regels met betrekking tot eID's.[4] Met een eID kan een burger inloggen bij de online portalen van (semi-) publieke diensten zoals de Belastingdienst of de eigen zorgverzekeraar. Goede voorbeelden van eID's zijn de door de

1 Steven Bastiaans en Marc Spuijbroek zijn advocaat bij Stibbe te Amsterdam. Carolien Michielsen is advocaat bij Stibbe te Brussel.

2 Verordening (EU) Nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG. De afkorting staat voor "electronic IDentification, Authentication and trust Services". De Nederlandse wetgever heeft waar nodig de eIDAS-verordening geïmplementeerd bij Wet van 21 december 2016 tot wijziging van de Telecommunicatiewet, de Boeken 3 en 6 van het Burgerlijk Wetboek, de Algemene wet bestuursrecht alsmede daarmee samenhangende wijzigingen van andere wetten in verband met de uitvoering van EU-verordening elektronische identiteiten en vertrouwensdiensten (uitvoering EU-verordening elektronische identiteiten en vertrouwensdiensten). In België geeft de Wet van 21 juli 2016 verdere uitvoering en aanvulling aan de eIDAS-verordening. Deze wet bracht diverse wijzigingen aan in het Belgisch Wetboek van economisch recht, onder meer met de invoeging van een Titel 2 "Bepaalde regels in verband met het juridisch kader voor vertrouwensdiensten" in Boek XII "Recht van de elektronische economie".

3 Richtlijn 1999/93/EG van het Europees Parlement en de Raad van 13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen.

4 De richtlijn bevatte weliswaar ook enige regels inzake elektronische identificatie, maar uitsluitend als onderdeel van een elektronische handtekening.

Nederlandse overheid uitgegeven DigiD (voor de relatie met burgers) en eHerkenning (voor de relatie met bedrijven en ondernemers) en de door de Belgische overheid uitgegeven elektronische identiteitskaart voor natuurlijke personen.[5] Deze systemen worden veelvuldig gebruikt om natuurlijke personen of rechtspersonen elektronisch te identificeren. Interessant in dit verband is iDIN, een elektronisch identificatiemiddel dat is gecreëerd in een privaat samenwerkingsverband van grote Nederlandse banken, dat inmiddels wordt gebruikt door tal van organisaties.[6] Veelal zijn dit private instellingen zoals banken, zorgverzekeraars, webwinkels en kredietverstrekkers, maar iDIN werd ook gebruikt in een pilot van de Belastingdienst eind 2018.[7] In België zijn elektronische identificatiemiddelen voor rechtspersonen nog niet in gebruik.

De eIDAS-verordening verplicht openbare instanties van lidstaten tot erkenning van bepaalde nationale eID's. Een in Nederland woonachtige Duitser met een vakantiehuis in Spanje kan dan bijvoorbeeld met zijn Duitse eID inloggen bij de Nederlandse Belastingdienst én het portaal van de gemeente waarin zijn Spaanse huis staat. Wederzijdse erkenning vereist onder andere dat aan bepaalde betrouwbaarheidsvereisten wordt voldaan en dat het nationale eID-systeem bij de Europese Commissie wordt aangemeld. Hierna gaan wij nader in op deze vereisten.

1.2 *Aanmelding en erkenning van eID's*

Zoals hiervoor gesteld, verplicht de eIDAS-verordening openbare instanties van lidstaten onder omstandigheden tot erkenning van eID's uit andere lidstaten. Dit heeft tot gevolg dat Nederlandse openbare instanties in bepaalde gevallen verplicht zijn om bij hun online diensten te faciliteren dat burgers en bedrijven daarop kunnen inloggen met hun aangemelde eID uit een andere lidstaat. Omgekeerd moet de eIDAS-verordening het mogelijk maken dat Nederlandse burgers en bedrijven met een inlogmiddel uit Nederland bij instanties van andere lidstaten kunnen inloggen.

Het faciliteren van het gebruik van aangemelde eID's uit andere lidstaten is geen generieke verplichting. Deze verplichting heeft alleen betrekking op eID's die vallen onder het toepassingsbereik van de eIDAS-verordening (artikel 2 lid 1 eIDAS-verordening). Daarnaast geldt deze verplichting uitsluitend voor openbare instanties die vallen binnen de reikwijdte van artikel 6 lid 1 eIDAS-verordening. Hieronder werken wij het toepassingsbereik van beide artikelen nader uit.

1.2.1 *Aangemeld en erkend inlogmiddel*

De eIDAS-verordening is ingevolge artikel 2 lid 1 van toepassing op "stelsels voor elektronische identificatie die zijn aangemeld door een lidstaat (…)".

Artikel 3 lid 4 eIDAS-verordening beschrijft een 'stelsel voor elektronische identificatie' als een stelsel waarbinnen elektronische identificatiemiddelen worden uitgegeven aan natuurlijke personen, rechtspersonen of natuurlijke personen die rechtspersonen vertegenwoordigen. Een 'elektronische identificatie' is conform artikel 3 lid 1 eIDAS-verordening kort gezegd een identificatieproces waarbij persoonsidentificatiegegevens in elektronische vorm worden gebruikt, waarbij die identificatiegegevens op unieke wijze de te identificeren (rechts)persoon aanduiden.[8]

Stelsels voor elektronische identificatie vallen onder het toepassingsbereik van de eIDAS-verordening als zij door een lidstaat zijn aangemeld bij de Europese Commissie. Inmiddels beschikken elf landen, inclusief Nederland, over minstens een Europees erkend middel.[9] Van vijf van deze landen, namelijk België, Duitsland, Estland, Kroatië, Spanje, zijn de inlogmiddelen al aangesloten op het Nederlandse eIDAS-verordening-netwerk.[10] Van zes van deze landen, namelijk Duitsland, Estland, Kroatië, Spanje, Italië en Luxemburg, zijn de inlogmiddelen al aangesloten op het Belgische netwerk. De inlogmiddelen van Italië, Luxemburg, Portugal en Tsjechië zullen naar verwachting ook spoedig worden aangesloten.[11] Ook het Verenigd Koninkrijk beschikt over een aangemeld eID sinds mei 2019. Ons is niet bekend of deze, gelet op de aanstaande Brexit, nog zal worden aangesloten.

DigiD is niet aangemeld onder de eIDAS-verordening. Buitenlandse openbare instanties zijn dus niet verplicht om Nederlandse burgers in te laten loggen met DigiD. Deze plicht geldt sinds kort wel ten aanzien van eHerkenning, het Nederlandse eID voor bedrijven. eHerkenning is in september 2019 als aangemeld eID bekend gemaakt door de EC.[12]

De Belgische eID-regeling is sinds 27 december 2018 aangemeld en erkend bij de Europese Commissie. Bijgevolg moeten de eCard voor Belgische burgers en de eCard voor

5 Wij verwijzen voor de volledigheid in dit kader ook naar de brief van staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties Knops d.d. 5 juli 2019 aan de Voorzitter van de Tweede Kamer der Staten Generaal, kenmerk 2019-0000362393, over zijn voorstel een andere toelatingssystematiek voor inlogmiddelen voor burgers te introduceren (en de mogelijke wijzigingen die dit voorstel meebrengt voor de Wet digitale overheid). Dit voorstel laten wij verder voor nu echter buiten beschouwing.

6 www.idin.nl.

7 www.idin.nl/belasting.

8 Zie in dit kader voor de volledigheid eveneens de definities uit artikel 3 lid 2 en lid 3 eIDAS-verordening.

9 Hier komen per kwartaal ongeveer 3 nieuwe middelen bij, aldus staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties Knops in zijn brief van 5 juli 2019 aan de Voorzitter van de Tweede Kamer der Staten Generaal, kenmerk 2019-0000362393.

10 Telling volgens de laatste informatie in het 'eIDAS-dossier' van de Rijksoverheid: https://www.digitaleoverheid.nl/dossiers/eidas/dossier-berichten/zes-maanden-na-de-ingangsdatum-van-eidas/.

11 https://www.digitaleoverheid.nl/dossiers/eidas/dossier-berichten/zes-maanden-na-de-ingangsdatum-van-eidas/.

12 https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=uriserv:OJ.C_.2019.309.01.0009.01.NLD&toc=OJ:C:2019:309:FULL.

vreemdelingen verplicht erkend worden door buitenlandse openbare instanties.[13]

Valt een eID onder het toepassingsbereik van de eIDAS-verordening, dan dient dat eID onder omstandigheden te worden erkend door openbare instanties van andere lidstaten. Op grond van artikel 3 lid 7 eIDAS-verordening worden als 'openbare instantie' aangemerkt: een staat, regionale of lokale overheden, publiekrechtelijke instellingen en samenwerkingsverbanden tussen één of meer van deze instanties of instellingen. Daarnaast kwalificeert een private entiteit als openbare instantie, als deze is gemachtigd tot het verlenen van openbare diensten door ten minste een van de hiervoor genoemde openbare instanties. Een private entiteit wordt alleen aangemerkt als openbare instantie wanneer hij in die hoedanigheid optreedt.

Het Nederlandse Ministerie van Economische Zaken heeft bij brief van 25 juli 2017 een 'Contactenlijst eIDAS' gepubliceerd, waarin 937 instanties worden opgesomd die volgens het Ministerie kwalificeren als 'openbare instantie' en daarmee onder het toepassingsbereik van de eIDAS-verordening vallen.[14] Een groot deel van deze instanties is hierover rechtstreeks geïnformeerd door het Ministerie.[15] Denk hierbij aan universitaire ziekenhuizen, ministeries, provincies, gemeentes, rechtbanken, omgevingsdiensten, pensioenfondsen en zorgverzekeraars. Deze contactenlijst is niet-limitatief en niet-bindend. Instanties dienen dus onverkort zelf na te gaan of zij onder het toepassingsbereik van de eIDAS-verordening vallen. Private partijen worden uitsluitend verplicht tot erkenning van buitenlandse eID's voor zover het betreft de activiteiten waarvoor zij kwalificeren als openbare instantie.

1.2.2 *Erkenning van eID's*

Als (i) op grond van nationaal recht; of (ii) door gangbare bestuursrechtelijke praktijk een eID is vereist om toegang te krijgen tot een onlinedienst aangeboden door een openbare instantie in een lidstaat, dan moeten ook eID's uit andere lidstaten worden erkend.[16]

Voor een voorbeeld van vereist gebruik van een eID op grond van nationaal recht, denken wij allereerst aan de aankomende Nederlandse Wet Digitale Overheid ("WDO"). Het wetsvoorstel voor de WDO ligt op dit moment ter behandeling bij de Tweede Kamer.[17] Op grond van het wetsvoorstel worden krachtens algemene maatregel van bestuur aangewezen instanties verplicht om bij de inrichting van hun onlinediensten een eID met een bepaald betrouwbaarheidsniveau te gebruiken. Uit de memorie van toelichting op de WDO blijkt dat wordt beoogd om met de werkingssfeer van de WDO aan te sluiten bij de eIDAS-verordening.[18] Hierdoor verwachten wij dat betrouwbaarheidsniveaus als 'laag', 'substantieel' of 'hoog' ook zullen worden voorgeschreven door de Nederlandse wetgever.

Het begrip "gangbare bestuursrechtelijke praktijk" is niet nader gedefinieerd in de eIDAS-verordening. Wij begrijpen dit echter zo dat hiermee wordt gedoeld op het beleid waaraan openbare instellingen zich (dienen te) houden. In alle gevallen waarin een openbare instantie gebruikmaakt van eID, zonder dat zij dat op grond van nationaal recht verplicht is te doen, zal aldus snel sprake zijn van een 'gangbare bestuursrechtelijke praktijk' die tot gebruik van een eID noopt. In elk geval zullen onlinediensten die zijn gericht op min of meer individuele dienstverlening, enige vorm van identificatie vereisen. Zowel vanwege vereisten op grond van privacywetgeving als vanwege gangbare beveiligingsvereisten.

In de context van de 'gangbare bestuursrechtelijke praktijk' die een eID vereist om toegang te krijgen tot een onlinedienst, is ook de Handreiking Betrouwbaarheidsniveaus voor Digitale Dienstverlening, van Forum Standaardisatie relevant.[19] Deze Handreiking hanteert de eIDAS-verordening en de algemene regels uit de Algemene verordening gegevensbescherming ("AVG") als basis voor het voorschrijven van eID's met een bepaald betrouwbaarheidsniveau.[20]

Indien op grond van nationaal recht of door gangbare bestuursrechtelijke praktijk een eID is vereist om toegang te krijgen tot een onlinedienst door een openbare instantie, betekent dit dat toegang tot de betreffende onlinedienst in beginsel ook mogelijk moet zijn met gebruik van een eID uit een andere lidstaat. Zoals gezegd geldt dit uitsluitend voor eID's die zijn aangemeld en door de Europese Commissie zijn bekendgemaakt conform artikel 9 eIDAS-verordening.[21]

Deze verplichting tot erkenning van dergelijke aangemelde eID's uit andere lidstaten geldt alleen als (i) de betreffende openbare instantie het betrouwbaarheidsniveau 'substantieel' of 'hoog' gebruikt voor toegang tot de onlinedienst; en (ii) het betrouwbaarheidsniveau van het te erkennen eID ten minste gelijk is aan het door de openbare instantie gebruikte betrouwbaarheidsniveau. Later in dit artikel meer over deze betrouwbaarheidsniveaus.

13 Europese Commissie, Stelsels voor elektronische identificatie aangemeld overeenkomstig artikel 9 lid 1, van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt, nr. 2018/C 464/08, *Pb.L.* 27 december 2018.

14 Deze brief is gepubliceerd via www.eherkenning.nl, maar blijkt daar niet langer beschikbaar te zijn. De auteurs van deze bijdrage hebben nog een kopie ter beschikking.

15 Daarvoor is de volgende brief gebruikt: https://www.vngrealisatie.nl/sites/default/files/2017-08/2017_07_25_Bestuurlijke_brief_eIDAS__online_versie_.pdf.

16 Artikel 6 lid 1 eIDAS-verordening.

17 *Kamerstukken II* 2017/18, 34972, nr. 2.

18 *Kamerstukken II* 2017/18, 34972, nr. 3.

19 www.forumstandaardisatie.nl/thema/handreiking-betrouwbaarheidsniveaus.

20 Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG.

21 Een actueel overzicht is raadpleegbaar via ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS.

De eIDAS-verordening bevat geen regels over het door openbare instanties minimaal te hanteren betrouwbaarheidsniveau voor toegang tot hun onlinedienst. Als ook niet anderszins een verplichting bestaat tot het hanteren van een bepaald minimum betrouwbaarheidsniveau (denk bijvoorbeeld aan het zojuist aangehaalde wetsvoorstel WDO en de AVG), kan een instantie dus de plicht tot wederzijdse erkenning vermijden door gebruik te maken van een betrouwbaarheidsniveau lager dan 'substantieel'. Dit lijkt ons niet wenselijk: het bewust terugschroeven van het betrouwbaarheidsniveau zal de bescherming van de achterliggende (persoons)gegevens niet ten goede komen. Wij verwachten niet dat, mede in verband met de publieke opinie, overheidsinstanties snel gebruik zullen maken van deze ontsnappingsmogelijkheid.

1.2.3 *Termijn voor wederzijdse erkenning*

Als een eID conform artikel 9 eIDAS-verordening is aangemeld en is bekendgemaakt door de Europese Commissie, dient de wederzijdse erkenning van dit eID door andere lidstaten (en daarmee ook hun openbare instanties) plaats te vinden binnen twaalf maanden na bekendmaking. Dit betekent dat houders van een dergelijk eID binnen twaalf maanden moeten kunnen inloggen bij openbare instanties van andere lidstaten. De aansluiting van een buitenlands inlogmiddel op het Nederlandse eIDAS-netwerk wordt veelal gerealiseerd binnen ongeveer drie maanden na bekendmaking.[22]

1.2.4 *Gebruik van single-sign-on functionaliteit*

In het kader van onlinediensten wordt veel gebruikgemaakt van de single-sign-on ("SSO") functionaliteit.[23] Deze maakt het mogelijk voor de gebruiker om met slechts eenmalig inloggen automatisch toegang te krijgen tot verschillende onlinediensten. SSO op zich is zeer praktisch voor gebruikers die verschillende onlinediensten gebruiken van dezelfde instantie. In het kader van de eIDAS-verordening en het wetsvoorstel WDO moeten echter ook enkele beperkingen in de gaten worden gehouden.

Zo is het onwenselijk om SSO te gebruiken voor verschillende onlinediensten die niet elk hetzelfde betrouwbaarheidsniveau vereisen. Het zou een schending van beveiligingsvereisten opleveren als met een SSO op betrouwbaarheidsniveau 'substantieel' kan worden ingelogd en vervolgens kan worden doorgeklikt naar een onlinedienst waarvoor betrouwbaarheidsniveau 'hoog' is vereist. Andersom is het vanuit beveiligingsoverwegingen wellicht niet problematisch, maar evenwel onpraktisch om voor een onlinedienst waarvoor slechts betrouwbaarheidsniveau 'laag' is vereist, een SSO met betrouwbaarheidsniveau 'substantieel' te hanteren.

In dit verband is ook goed te beseffen dat het op grond van artikel 8 lid 1 wetsvoorstel WDO niet is toegestaan om een publieke eID (zoals DigiD en eHerkenning) te gebruiken voor commerciële dienstverlening. Dit teneinde de markt niet te verstoren. Het is dus niet toegestaan om via een SSO, dat gebruikmaakt van bijvoorbeeld DigiD, in te loggen bij een gemeente, om vervolgens kaartjes te kopen voor een benefietconcert dat in het gemeentehuis wordt georganiseerd. Deze commerciële onlinedienst moet in de SSO gescheiden worden van de aangeboden publieke onlinediensten. Artikel 8 lid 2 wetsvoorstel WDO laat overigens wel ruimte voor uitzondering bij ministeriële regeling. Via die weg kan toestemming worden verkregen om een publieke eID ook te gebruiken voor de toegang tot welbepaalde private onlinediensten. Organisaties die een publieke eID voor hun commerciële diensten willen gebruiken, doen er dan ook goed aan om over deze aanwijzing tijdig in overleg te treden met de Rijksdienst voor Ondernemend Nederland.

2. Betrouwbaarheidsniveaus

Zoals in paragraaf 1.2.3 al is gesteld, is de erkenningsplicht uit artikel 6 lid 1 eIDAS-verordening gekoppeld aan (i) het betrouwbaarheidsniveau dat een openbare instantie die de eID dient te erkennen zelf voor de toegang tot haar onlinedienst gebruikt; en (ii) het betrouwbaarheidsniveau van het buitenlandse eID. In artikel 8 lid 2 eIDAS-verordening worden 3 verschillende betrouwbaarheidsniveaus onderscheiden: betrouwbaarheidsniveaus 'laag', 'substantieel' en 'hoog'.

Het betrouwbaarheidsniveau van een eID wordt bepaald aan de hand van minimumeisen of -criteria. In de Bijlage bij Uitvoeringsverordening (EU) 2015/1502 zijn de minimale technische specificaties, normen en procedures per betrouwbaarheidsniveau uitgewerkt.[24] Zo is de identiteitsverificatie van de aanvrager, de procedure van verlening van het eID, de kwaliteit van de betrokken instanties bij deze verlening, de technische specificaties van het eID en het authenticatiemechanisme van de identificatie van de gebruiker van belang om te bepalen binnen welk betrouwbaarheidsniveau een eID valt.[25] Vervolgens bepaalt de *laagste score* voor bovenstaande factoren het uiteindelijke betrouwbaarheidsniveau. Voor het stelsel van de Nederlandse eHerkenning is vastgesteld dat dit voldoet aan de vereisten voor betrouwbaarheidsniveau's substantieel en hoog.[26] Voor het stelsel van de Belgische eID-regeling werd

22 https://www.digitaleoverheid.nl/dossiers/eidas/dossier-berichten/zes-maanden-na-de-ingangsdatum-van-eidas/.

23 Denk hierbij aan pensioenuitvoeringsorganisaties die tevens een verzekeringstak hebben, of administratie- en accountantskantoren, die voor hun werk gebruikmaken van verschillende online applicaties. Zonder SSO dient voor het gebruikmaken van iedere applicatie opnieuw te worden ingelogd.

24 eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32015R1502&from=NL.

25 Forum Standaardisatie, *"Betrouwbaarheidsniveaus voor digitale dienstverlening"*, www.forumstandaardisatie.nl/thema/handreiking-betrouwbaarheidsniveaus.

26 https://www.eherkenning.nl/nieuws/over-de-grens-online-zaken-doen-met-eherkenning.

reeds vastgesteld dat dit een hoog betrouwbaarheidsniveau betreft.[27]

3. Elektronische handtekeningen

3.1 *Introductie elektronische handtekeningen*

De eIDAS-verordening creëert als gezegd het juridisch kader voor elektronische handtekeningen. Via artikel 3:15a Burgerlijk Wetboek ("BW") is dit kader in de Nederlandse wet verankerd. Het Belgische juridische kader voor elektronische handtekeningen bestaat op heden voornamelijk uit artikel 1322 lid 2 Burgerlijk Wetboek en artikel XII.15 van het Wetboek economisch recht. De volgende drie typen elektronische handtekeningen worden onderscheiden in de eIDAS-Verordening:

(1) de **elektronische handtekening** (verder: de "gewone elektronische handtekening"): deze bestaat uit 'gegevens in elektronische vorm die gehecht zijn aan of logisch verbonden zijn met andere gegevens in elektronische vorm' en die worden gebruikt door de ondertekenaar om te ondertekenen.[28]
Dit is de meest laagdrempelige variant van een elektronische handtekening, en deze kan bestaan uit zoveel (of eigenlijk: zo weinig) als het typen van een naam in een document op de plaats waar moet worden ondertekend. Ook het 'plakken' van een gescand exemplaar van een 'papieren' handtekening valt binnen deze categorie;

(2) de **geavanceerde elektronische handtekening**: dit is een elektronische handtekening die:
   (i) op unieke wijze is verbonden aan de ondertekenaar (de natuurlijke persoon die de ondertekening verricht);
   (ii) het mogelijk maakt de ondertekenaar te identificeren: de ondertekening moet dus te herleiden zijn naar de ondertekenaar;
   (iii) tot stand komt met gegevens die de ondertekenaar, met een hoog vertrouwensniveau, onder zijn uitsluitende controle kan gebruiken: de gegevens waarmee de handtekening kunnen worden gezet, moeten uitsluitend ter beschikking staan aan de ondertekenaar; en
   (iv) op zodanige wijze is verbonden aan de ondertekende gegevens, dat elke wijziging van de gegevens achteraf kan worden opgespoord.[29]
   In de praktijk wordt dit ingevuld met behulp van 'hashing'. Dat is een cryptografische techniek, met behulp waarvan alle data uit het ondertekende document wordt omgerekend naar een unieke hash code. Die code dient louter als controlemiddel, en kan niet worden teruggerekend naar de oorspronkelijke data. Hoewel de code niet kan worden teruggerekend, levert de input van dezelfde data altijd dezelfde unieke hash code op. Zouden gegevens in het oorspronkelijke document worden gewijzigd, dan resulteert toepassing van diezelfde hash-techniek dus in een andere hash code. Daarmee staat direct vast dat wijziging heeft plaatsgevonden en het document geen exacte kopie is van het origineel;

(3) de **gekwalificeerde elektronische handtekening**: dit is een geavanceerde elektronische handtekening die:
   (v) is aangemaakt met een gekwalificeerd middel voor het aanmaken van elektronische handtekeningen; en
   (vi) is gebaseerd op een gekwalificeerd certificaat voor elektronische handtekeningen: dit is een certificaat dat is afgegeven door een gekwalificeerde verlener van vertrouwensdiensten en in overeenstemming is met de vereisten in Bijlage I van de eIDAS-verordening.[30]

De eIDAS-verordening schrijft dwingend voor dat een gekwalificeerde elektronische handtekening hetzelfde rechtsgevolg heeft als een handgeschreven handtekening. Dit geldt binnen de gehele EU.

Voor de twee lichtere varianten van de elektronische handtekening (de geavanceerde elektronische handtekening en de gewone elektronische handtekening) is het aan de nationale wetgever om de rechtsgevolgen daarvan nader te beschrijven. Daarbij geldt wel dat het rechtsgevolg (en de toelaatbaarheid als bewijsmiddel in een gerechtelijke procedure) daarvan niet mag worden ontkend op grond van het enkele feit dat de handtekening slechts een elektronische handtekening is of geen gekwalificeerde elektronische handtekening is.

De Nederlandse wetgever heeft dit zoals gezegd uitgewerkt in artikel 3:15a BW. Daarin wordt bepaald dat als de gebruikte methode voor ondertekening voldoende betrouwbaar is gelet i) op het doel waarvoor de elektronische handtekening is gebruikt; en ii) op alle overige omstandigheden van het geval, ook aan de gewone elektronische handtekening en de geavanceerde elektronische handtekening dezelfde rechtsgevolgen toekomen als aan een handgeschreven handtekening.

Heel behulpzaam is dit niet, nu hiermee een open norm is gecreëerd. Het wordt in wezen aan de betrokken partijen overgelaten om per geval te beoordelen of de gekozen methode voldoende betrouwbaar is. Komt het erop aan, dan zal een rechter dienen te beoordelen of de gebruikte methode voor dat specifieke geval voldoende betrouwbaar is.

Zou een rechter oordelen dat de gebruikte methode in een bepaald geval onvoldoende betrouwbaar is, dan is daarmee de handtekening overigens niet per se ongeldig. Hieraan

27 Europese Commissie, Stelsels voor elektronische identificatie aangemeld overeenkomstig artikel 9 lid 1, van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt, nr. 2018/C 464/08, *Pb.L.* 27 december 2018.

28 Artikel 3 lid 10 eIDAS-verordening.

29 Artikel 26 eIDAS-verordening.

30 Artikel 3 lid 12 en 14 eIDAS-verordening.

komt dan in ieder geval wel verminderde bewijskracht toe. Dat kan bijvoorbeeld betekenen dat aanvullend bewijs zal moeten worden geleverd waaruit blijkt dat de ondertekenaar daadwerkelijk de bedoeling had om het betreffende stuk te ondertekenen. In privaatrechtelijke relaties lijkt dit dus niet onoverkomelijk.

Voor een aantal specifieke toepassingen heeft de Nederlandse wetgever een gekwalificeerde handtekening voorgeschreven, zoals: elektronische opgave door de werkgever aan de werknemer van elementen van de arbeidsovereenkomst (art. 7:655 lid 3 BW), verzekeringspolissen (art. 7:932 BW), arbitrale vonnissen (art. 1072b lid 3 Wetboek van Burgerlijke Rechtsvordering) en bepaalde stukken omschreven in de Kadasterwet (art. 7e Kadasterwet). In de Wet op de omzetbelasting wordt de gekwalificeerde elektronische handtekening genoemd als één van de mogelijke manieren om de authenticiteit van de herkomst en de integriteit van de inhoud van een elektronische factuur te waarborgen (art. 35b lid 4 Wet op de omzetbelasting).

Het Belgische juridische kader voor elektronische handtekeningen bestaat op heden voornamelijk uit artikel 1322 lid 2 Burgerlijk Wetboek en artikel XII.15 van het Wetboek economisch recht.

Artikel XII.15 lid 2 van het Wetboek Economisch Recht stelt dat aan de uitdrukkelijke of stilzwijgende vereiste van een handtekening met het oog op het contracteren langs elektronische weg is voldaan wanneer de handtekening beantwoordt aan de voorwaarden van een (gewone) elektronische handtekening of een gekwalificeerde elektronische handtekening onder de eIDAS-verordening.

Deze bepaling verwees eerder naar de voorwaarden van artikel 1322 lid 2 Burgerlijk Wetboek, dan wel de voorwaarden van een gekwalificeerde elektronische handtekening onder de eIDAS-verordening, maar werd aangepast door de Wet van 20 september 2018 tot harmonisatie van de begrippen elektronische handtekening en duurzame gegevensdrager en tot opheffing van de belemmeringen voor het sluiten van overeenkomsten langs elektronische weg. De memorie van toelichting verduidelijkte hieromtrent:

> "Toch moet worden onderstreept dat artikel 1322 van het Burgerlijk Wetboek geen vorm van elektronische handtekening bepaalt als dusdanig, maar alleen de voorwaarden waaronder een elektronische handtekening kan voldoen aan de vereiste van een handtekening, op het niveau van het recht van bewijsvoering. Deze verwijzing naar het artikel 1322 van het Burgerlijk Wetboek is dus niet adequaat, en daarom beperkt onderhavig wetsontwerp zich tot een verwijzing naar de drie soorten van elektronische handtekening die duidelijk gedefinieerd en geharmoniseerd worden in de eIDAS-verordening, en niet langer naar het artikel 1322 van het Burgerlijk Wetboek."

Volgens artikel 1322 lid 2 Burgerlijk Wetboek kan een geheel van elektronische gegevens dat aan een bepaalde persoon kan worden toegerekend en het behoud van de integriteit van de inhoud van de akte aantoont voldoen aan de vereiste van een handtekening in het kader van een onderhandse akte. Bijgevolg is ook dit een open norm die de uiteindelijke beslissing omtrent de rechtsgevolgen van een gewone en geavanceerde elektronische handtekening overlaat aan de ruime beoordelingsvrijheid van de rechter, hetgeen resulteert in rechtsonzekerheid.

Echter, op 4 april 2019 werd het Boek 8 "Bewijs" van het nieuwe Burgerlijk Wetboek aangenomen.[31] Dit boek omvat nieuwe bewijsregels die in werking zullen treden vanaf 1 november 2020. De open norm van artikel 1322 lid 2 Burgerlijk Wetboek zal daarmee verleden tijd worden. De memorie van toelichting stelt hieromtrent dat:

> "De definitie van artikel 1322 van het Burgerlijk Wetboek wordt geschrapt. Zij was onderhevig aan kritiek van de rechtsleer door het inadequate karakter ervan en de slechte omzetting van de richtlijn betreffende de elektronische handtekening."[32]

In het Boek 8 worden nieuwe definities toegevoegd. Een "handtekening" wordt gedefinieerd als een teken of een opeenvolging van tekens, aangebracht met de hand, elektronisch of via ieder ander procedé, waarmee een persoon zich identificeert en waaruit zijn wilsuiting blijkt. Een "elektronische handtekening" wordt omschreven als een handtekening conform artikelen 3.10 tot 3.12 van de eIDAS-verordening en omvat dus zowel de gewone, geavanceerde als gekwalificeerde elektronische handtekening.

Wat de bewijskracht van een handtekening voor een onderhandse akte betreft (welke in principe vereist is om rechtshandelingen met betrekking tot een som of een waarde die gelijk is aan of hoger is dan 3500 EUR te bewijzen), wordt in het nieuwe Burgerlijk Wetboek niet langer een onderscheid gemaakt tussen een traditionele of een elektronische handtekening. Een onderhandse akte wordt namelijk gedefinieerd als "een geschrift dat rechtsgevolgen beoogt, dat door de partij(en) ondertekend wordt met de bedoeling om met de inhoud ervan in te stemmen, en dat geen authentieke akte is" – zonder daarbij te bepalen op welke manier die ondertekening dient te gebeuren. Voor authentieke akten wordt wel een gekwalificeerde elektronische handtekening vereist.

3.2 *Praktische toepassing*

Wat betekent dit nu in de praktijk voor een bedrijf dat overweegt om bepaalde processen te digitaliseren, of om bepaalde digitale processen uit te breiden met de mogelijkheid van elektronische ondertekening? Kunnen de arbeids-

31 Wetsontwerp tot invoering van een Burgerlijk Wetboek en tot invoeging van boek 8 "Bewijs" in dat Wetboek, Kamer 54 3349/007.

32 Memorie van Toelichting, Kamer 54 3349/001, p. 7.

overeenkomsten voortaan digitaal worden ondertekend? Hoe zit dat met overeenkomsten voor consumentenkrediet? Welke stappen moet een bedrijf in ieder geval doorlopen om te komen tot een antwoord op deze vragen?

3.2.1 *Vormvereiste?*

In beide genoemde voorbeelden gaat het om het tekenen van een overeenkomst door twee partijen. Daarbij is het allereerst van belang om na te gaan of er voor de betreffende overeenkomst een vormvereiste geldt. Een elektronische handtekening kan immers slechts praktische relevantie hebben voor overeenkomsten waarvoor elektronische contractering juridisch mogelijk is. Geldt geen vormvereiste voor de te sluiten overeenkomst, dan is elektronische contractering mogelijk. Geldt wel een vormvereiste, dan moet worden bezien of deze elektronische contractering toelaat.[33]

Een regelmatig voorkomende vormvereiste is het vereiste van schriftelijkheid. Het is goed om voor ogen te houden dat elektronische contractering in de meeste gevallen ook mogelijk is voor overeenkomsten waarvoor de wet voorschrijft dat deze alleen schriftelijk kunnen worden gesloten. Op grond van art. 6:227a BW staat, naar Nederlands recht, contractering langs elektronische weg voor veel van dergelijke overeenkomsten alsnog open. Daarbij gelden wel enkele nadere vereisten aan het proces voor contractering: (i) de overeenkomst dient raadpleegbaar te zijn door partijen; (ii) de authenticiteit van de overeenkomst dient voldoende te zijn gewaarborgd; (iii) het moment van totstandkoming dient met voldoende zekerheid zijn vast te stellen; en (iv) de identiteit van de partijen dient te kunnen worden vastgesteld. Dit levert dus geen hoge drempels op. Zeker niet als wordt bedacht dat aan deze vereisten bij gebruik van een geavanceerde elektronische handtekening in de meeste gevallen wordt voldaan. Overigens blijkt uit de parlementaire geschiedenis dat de rechter in bijzondere gevallen een elektronisch gesloten overeenkomst ook gelijk zou kunnen stellen met een schriftelijk gesloten overeenkomst wanneer niet aan alle vier genoemde voorwaarden is voldaan.[34]

Ook naar Belgisch recht is contractering langs elektronische weg mogelijk op grond van artikel XIII.15 Wetboek Economisch Recht voor zover er sprake is van een functionele equivalentie. Dat artikel bepaalt namelijk dat aan elke wettelijke of reglementaire vormvereiste voor de totstandkoming van contracten langs elektronische weg is voldaan wanneer de functionele kwaliteiten van deze vereiste gevrijwaard zijn. Een tweede lid specificeert daarbij dat: (i) aan de vereiste van een geschrift is voldaan door een geheel van alfabetische tekens of andere verstaanbare tekens aangebracht op een drager die de mogelijkheid biedt toegang ertoe te hebben gedurende een periode die is afgestemd op het doel waarvoor de informatie kan dienen en waarbij de integriteit ervan wordt beschermd; (ii) aan de uitdrukkelijke of stilzwijgende vereiste van een handtekening is voldaan wanneer deze laatste beantwoordt aan de voorwaarden van een (gewone) elektronische handtekening of een gekwalificeerde elektronische handtekening onder de eIDAS-verordening; en (iii) aan de vereiste van een geschreven vermelding van degene die zich verbindt, kan worden voldaan door om het even welk procedé dat waarborgt dat de vermelding effectief uitgaat van deze laatste. Ook hier worden er dus allerminst hoge drempels opgeworpen.

De consumentenkredietovereenkomst uit ons voorbeeld, dient op grond van artikel 7:61 lid 1 BW naar Nederlands recht te worden aangegaan op papier of op een andere duurzame drager. Artikel VII.78 §1 van het Belgisch Wetboek Economisch Recht vereist dat een consumentenkredietovereenkomst wordt gesloten door de handmatige handtekening of de elektronische ondertekening van alle contracterende partijen en wordt opgesteld op een duurzame gegevensdrager. Elektronische contractering is dus mogelijk, mits dat gebeurt op een manier die resulteert in vastlegging op een duurzame drager.[35] Een duurzame drager dient te waarborgen dat de consument de te verstrekken info in bezit heeft, zodat hij in voorkomend geval zijn rechten kan doen gelden. Het HvJ EU oordeelde in de zaak Content Services dat een website niet als duurzame drager kwalificeert.[36] Dit is anders voor E-Banking websites, zo bepaalde het HvJ EU in het BAWAG arrest, nu deze voorzien in de mogelijkheid informatie op te slaan op een manier dat deze ongewijzigd kan worden geproduceerd, zonder dat de bank deze tussentijds eenzijdig kan wijzigen.[37]

Voor de arbeidsovereenkomst geldt naar Nederlands recht geen vormvereiste. Deze kan dus elektronisch worden aangegaan. Belangrijk daarbij is wel om te bedenken dat een concurrentiebeding op grond van artikel 7:653 lid 1 sub b BW schriftelijk moet worden overeengekomen.[38] Betreft het een arbeidsovereenkomst zonder concurrentiebeding, dan is elektronische contractering dus mogelijk. Is de wens om een concurrentiebeding op te nemen in de arbeidsovereenkomst, dan moet een oplossing worden gevonden voor het vereiste van schriftelijkheid. Ook naar Belgisch recht blijft het algemene principe dat arbeidsovereenkomsten door loutere wilsovereenstemming tot stand kunnen komen. Wel legt de Belgische wet voor een heel aantal types arbeidsovereenkomsten (o.m. arbeidsovereenkomsten voor bepaalde duur of voor een duidelijk omschreven werk, deeltijdse arbeidsovereenkomst, arbeidsovereenkomst voor studenten, etc.) op dat deze schriftelijk aangegaan moeten worden. Ook een concurrentiebeding moet op grond van artikel 65, § 2, lid 9 van de Wet van 3 juli 1978 schriftelijk

33 Zie voor een gedetailleerde analyse van de gelijkstelling van elektronische en schriftelijke overeenkomsten: T.J. de Graaf, 'De lappendeken van de gelijkstelling van elektronisch met schriftelijk in het licht van vormvereisten en bewijskracht', *MvV* 2018/7-8, p. 243-248.

34 *Kamerstukken II* 2001/02, 28197.

35 Een 'duurzame drager' is ieder hulpmiddel dat de consument in staat stelt om de overeenkomst op te slaan zodat hij deze in de toekomst kan raadplegen, art. 7:57 lid 1 sub m BW.

36 HvJ EU 5 juli 2012, ECLI:EU:C:2012:419.

37 HvJ EU 25 januari 2017, ECLI:EU:C:2017:38.

38 Hetzelfde geldt bijvoorbeeld ook voor een proeftijdbeding (artikel 7:652 lid 2 BW) en een boetebeding (artikel 7:650 lid 2 BW).

vastgelegd worden. Dergelijke vereisten moeten dus steeds indachtig gehouden worden.

3.2.2 *Welk type handtekening?*

Is eenmaal vastgesteld dat een overeenkomst zich leent voor elektronische ondertekening, dan is de volgende stap om na te gaan welke van de drie typen elektronische handtekening zich hiervoor het beste leent.

Voor elke toepassing geldt dat een gekwalificeerde elektronische handtekening de meeste zekerheid biedt vanwege de gelijkstelling met een schriftelijke handtekening.[39] Beoordeeld vanuit louter het perspectief van (juridische) zekerheid, heeft een gekwalificeerde elektronische handtekening dan ook altijd de voorkeur. Erg praktisch is dit niet. Een vrij evident probleem is dat de gemiddelde consument en de gemiddelde werknemer namelijk niet in staat zijn om een dergelijke handtekening te zetten. De reden hiervoor is dat zij simpelweg niet beschikken over de middelen om een gekwalificeerde elektronische handtekening te plaatsen. De kosten voor het daartoe vereiste certificaat van een aanbieder van vertrouwensdiensten zijn vrij hoog. Nu voor consumenten en werknemers er geen directe noodzaak bestaat om over een gekwalificeerde elektronische handtekening te beschikken, ligt het niet voor de hand dat zij deze kosten zullen maken. Daarnaast is ook vanuit efficiëntieoverwegingen relevant om te bezien in hoeverre een lichtere variant van de elektronische handtekening kan volstaan.

Voor de beoordeling of een gewone elektronische handtekening en/of een geavanceerde elektronische handtekening kan volstaan, zal per geval moeten worden getoetst aan de eerder genoemde open norm van 3:15a BW (Nederlands recht), dan wel art. 1322 lid 2 BW (Belgisch recht). Helaas biedt jurisprudentie hier vooralsnog weinig bruikbare aanknopingspunten, hoewel een recente uitspraak van de Nederlandse Hoge Raad hoop geeft dat dit in de toekomst zal veranderen.[40] Dit betekent dat het aan het bedrijf is om per geval in te schatten wat de meest geschikte handtekening is.

Wij menen dat voor zowel de consumentenkredietovereenkomst als de arbeidsovereenkomst men al snel zal uitkomen bij de geavanceerde elektronische handtekening. Gelet op de aard van de consumentenkredietovereenkomst – en ervan uitgaande dat het om een substantiële lening zal gaan, en niet slechts enkele tientallen euro's – achten wij het niet aannemelijk dat een gewone elektronische handtekening zal volstaan.

Voor een arbeidsovereenkomst met concurrentiebeding lijkt het antwoord relatief eenvoudig. Om de vereisten van artikel 6:227a BW vorm te geven komt men al snel uit bij een proces wat inhoudelijk al zo sterk lijkt op het proces van de geavanceerde elektronische handtekening, dat het voor de hand ligt om dan ook maar voor de geavanceerde elektronische handtekening te kiezen. Let wel, ook hier is ruimte voor interpretatie, omdat de vereisten uit artikel 6:227a BW op het vereiste van raadpleegbaarheid na, ook open normen bevatten.

Bij een arbeidsovereenkomst zonder concurrentiebeding, menen wij dat het vanuit werkgeversperspectief vaak toch de voorkeur zal hebben om toch te kiezen voor een geavanceerde elektronische handtekening in plaats van een gewone elektronische handtekening. De geavanceerde elektronische handtekening biedt nu eenmaal meer zekerheid. Dat neemt niet weg dat er gevallen zijn waarin denkbaar is dat een gewone elektronische handtekening prima kan volstaan. Daarvan zal vooral sprake zijn in gevallen waarin ook denkbaar is dat de afspraken volledig mondeling worden gemaakt. Denk aan de 'arbeidsovereenkomst' zoals je die vroeger sloot voor het bollen pellen als vakantiebaantje. Daar kwamen geen pen en papier aan te pas. Het is goed denkbaar dat die afspraken vandaag de dag per e-mail worden gemaakt met een eenvoudig 'akkoord' in de reply-mail.

Belangrijk is dat de Belgische Arbeidsovereenkomstenwet van 3 juli 1978 bepaalt dat een arbeidsovereenkomst ondertekend met een "*elektronische handtekening die wordt gecreëerd door de elektronische identiteitskaart of door middel van een elektronische handtekening die voldoet aan dezelfde veiligheidswaarborgen als de elektronische handtekening die door de elektronische identiteitskaart wordt gecreëerd*" gelijkgesteld wordt met een papieren arbeidsovereenkomst ondertekend door middel van een handgeschreven handtekening. Een handtekening aan de hand van de Belgische elektronische identiteitskaart is een gekwalificeerde elektronische handtekening onder de eIDAS-verordening. Het zou echter veel duidelijker zijn mocht de wetgeving verwijzen naar de terminologie gehanteerd in de eIDAS-verordening dan naar specifieke toepassingsgevallen. Dit is ook wat de nog niet in werking getreden Wet van 15 januari 2018 houdende diverse bepalingen inzake werk beoogd heeft. In de toekomst zal dit artikel 3bis Arbeidsovereenkomst dan ook bepalen dat een elektronisch ondertekende arbeidsovereenkomst gelijkgesteld wordt met een papieren arbeidsovereenkomst ondertekend met een handgeschreven handtekening, op voorwaarde dat de elektronische ondertekening gebeurt door (i) een gekwalificeerde elektronische handtekening of een gekwalificeerd elektronische zegel zoals bepaald in de eIDAS-verordening; of (ii) een andere elektronische handtekening

39 Artikel 25 lid 2 eIDAS-verordening.

40 Vgl. Hoge Raad 14 juni 2019, ECLI:NL:HR:2019:957. De Hoge Raad heeft in dit arrest gesteld dat voor de toepassing van art. 16 lid 1 Wet bijzondere opnemingen psychiatrische ziekenhuizen ("Wet Bopz") een geavanceerde elektronische handtekening dezelfde rechtsgevolgen heeft als een handgeschreven handtekening (r.o. 3.1.8). Op grond van artikel 16 lid 1 Wet Bopz moet bij een verzoek om een machtiging tot voortgezet verblijf in een psychiatrisch ziekenhuis een verklaring worden overgelegd van de geneesheer-directeur van het desbetreffende psychiatrisch ziekenhuis. De verklaring van de geneesheer-directeur moet door hemzelf worden ondertekend. Op grond van dit arrest volstaat dus ook een geavanceerde elektronische handtekening.

die toelaat de identiteit van de partijen, hun instemming met de inhoud van de overeenkomst en het behoud van de integriteit van die overeenkomst te verzekeren (waarbij het in geval van betwisting aan de werkgever is om aan te tonen dat de elektronische handtekening daadwerkelijk deze functies verzekert). Wat daarvan zij, laten we ervan uitgaan dat in de gegeven voorbeelden wordt gekozen voor een geavanceerde elektronische handtekening, omdat een gekwalificeerde elektronische handtekening geen realistische optie is en een gewone elektronische handtekening te licht wordt bevonden. Daarbij is het belangrijk te beseffen dat de geavanceerde elektronische handtekening dus geen 100% zekerheid biedt. De manier waarop het proces voor ondertekening met de geavanceerde elektronische handtekening wordt ingericht, kan naar onze mening wel bijdragen aan het gewicht dat aan de handtekening wordt toegekend.

3.2.3 *Hoe richt je de geavanceerde elektronische handtekening in?*

Er zijn diverse commerciële aanbieders van elektronische handtekeningdiensten. Over het algemeen bieden deze de klant de mogelijkheid om te kiezen voor een gewone of een geavanceerde elektronische handtekening. Vervolgens kunnen diverse keuzes worden gemaakt bij de uiteindelijke inrichting van het ondertekenproces.

Ook constateerden wij bij enkele aanbieders dat zij wel de middelen aanbieden om ondertekening te faciliteren, maar geen contractuele garantie geven dat hun proces ook daadwerkelijk volstaat om een geavanceerde elektronische handtekening te zetten. Dit betekent dat het aan de klant is om zelf haar behoeften kritisch te analyseren, en bij de uiteindelijke inrichting van de processen de juiste keuzes te maken.

Die keuzes hebben veelal betrekking op de wijze van communicatie met de contractuele wederpartij, en op de manier waarop de informatie die nodig is om te ondertekenen, zoals de inlogcode, wordt verstrekt. Zo kan bijvoorbeeld worden gekozen uit verzending van de overeenkomst via diverse wegen, waaronder per e-mail. Vervolgens kan de contractuele wederpartij inloggen op een onlineportal – via de link in de e-mail – met behulp van een specifieke separaat verkregen code. Die code kan weer fysiek zijn overhandigd, via SMS zijn verzonden, enzovoorts.

Een echte gulden regel voor die keuzes bestaat niet, maar er zijn wel enkele logische aanknopingspunten te bedenken.[41] In alle gevallen heeft een authenticatie via twee verschillende kanalen (bijvoorbeeld e-mail en SMS) de voorkeur boven contact via uitsluitend één kanaal. Als zowel contracten als inloggegevens via hetzelfde e-mailadres worden toegezonden betekent een gecompromitteerd e-mailadres ook direct een gecompromitteerde ondertekening. Dat risico wordt kleiner als de communicatie via meerdere kanalen verloopt.

Een ander punt is dat het verstandig is om kritisch te zijn op de gebruikte gegevens. Uit welke bron zijn de gegevens afkomstig? Is het e-mailadres dat wordt gebruikt ook geverifieerd? Is gecontroleerd dat dit geen tijdelijk wegwerp e-mailadres is? In het geval van de arbeidsovereenkomst lijkt dit punt overkomelijk, aangenomen dat in het sollicitatieproces op enig moment ook face-to-face contact is geweest (hoewel dit in de toekomst wellicht meer zal afnemen).

Ook is het van belang om per situatie nogmaals goed te controleren of de gekozen inrichting de juiste is. Zo lijkt gebruik van een zakelijk e-mailadres niet direct problematisch bij ondertekening van een vernieuwde arbeidsovereenkomst, bijvoorbeeld in het kader van een promotie. Dient tussen werkgever en ex-werknemer echter een vaststellingsovereenkomst te worden getekend, dan lijkt gebruik van dat zakelijke e-mailadres niet aan te raden. Theoretisch heeft de werkgever immers ook toegang daartoe, en zou hij zichzelf zo kunnen 'vrijtekenen'. Ondanks dat dit ver gezocht klinkt, kan door een andere oplossing te kiezen voor de inrichting van die specifieke ondertekenprocessen worden vermeden dat de werkgever deze schijn tegen krijgt.

Er is wat ons betreft veel mogelijk op het gebied van elektronische ondertekening en wij zien in de praktijk ook dat hier steeds meer gebruik van wordt gemaakt. Het is wel zaak dat men kritisch nadenkt over de inrichting van de processen, en hierbij niet te veel leunt op de aanbieders van elektronische ondertekendiensten. Uiteindelijk zijn zij geen partij bij de te ondertekenen stukken, en dragen zij niet het (grootste) risico in het geval dat het toch mis zou gaan. Verder is het belangrijk om eenmaal gemaakte keuzes regelmatig te evalueren. Waar vandaag nog weinig consumenten en werknemers over een gekwalificeerde elektronische handtekening beschikken, kan dat over een jaar heel anders zijn. Dat kan zomaar tot heel andere keuzes en conclusies leiden.

4. Ten slotte

De eIDAS-verordening bevat een complex stelsel van regels. Wij hopen met dit artikel de lezer enige houvast te hebben gegeven bij de duiding van het stelsel voor het gebruik van eID's door openbare instanties en van de verschillende beschikbare (en soms voorgeschreven) betrouwbaarheidsniveaus.

Daarnaast illustreerden wij met behulp van twee praktijkvoorbeelden welke aspecten uit de eIDAS een rol spelen bij implementatie van elektronische handtekeningen. Hoewel de mogelijkheden voor een dergelijke implementatie altijd per geval moeten worden bekeken, hebben wij beoogd te illustreren langs welke lijnen die beoordeling kan worden

41 Vergelijk ook de tien aanknopingspunten geformuleerd door Van Esch, R.E. van Esch, 'Gezichtspunten voor de beoordeling van de betrouwbaarheid van de methode voor elektronische ondertekening', *Tijdschrift voor Financieel Recht* 2018-8/9, p. 397-405.

vormgegeven. Wij willen daarmee het signaal afgeven dat er veel mogelijk is, nu we erg enthousiast zijn over de vlucht die het gebruik van elektronische handtekeningen lijkt te nemen.

Naast het gebruiksgemak van elektronische ondertekening, leveren de geavanceerde en gekwalificeerde elektronische handtekening overigens ook een voor de juridische praktijk zeer relevant neveneffect op. Het ondertekende stuk moet namelijk voor partijen raadpleegbaar zijn. Dit betekent dat bij het inrichten van het proces voor ondertekening ook moet worden voorzien in een deugdelijk archiveringssysteem; iets wat in de papieren wereld toch niet altijd even goed is verlopen.