INTERNETCONSULTATIE
UITVOERINGSWET EU-VERORDENING ELEKTRONISCHE IDENTITEITEN EN VERTROUWENSDIENSTEN

1.	**INLEIDING/ HISTORIE**	Sinds de aanstelling in november van de nieuwe Europese Commissie heeft de digitale agenda prioriteit gekregen, onder de naam de 'Digital Single Market'. Dit houdt in dat er een digitale markt wordt gecreëerd binnen de Europese Unie op het gebied van de digitale economie. Aanleiding hiervoor is het grensoverschrijdend leveren en gebruik van onlinediensten op zorgvuldige wijze aan te moedigen en te laten toenemen met bijzondere aandacht voor vertrouwen, transparantie en verantwoordelijkheid, mede door de facilitering van veilige elektronische identificatie en authenticatie. De digitale economie heeft als gevolg dat er meer beveiligingsincidenten plaatsvinden. In de media wordt regelmatig bericht over dergelijke beveiligingsincidenten en nieuwe voorstellen ter aanscherping van de regelgeving met betrekking tot de bescherming van digitale informatie. Naar aanleiding van de (al weer gedateerde) gebeurtenissen bij DigiNotar, of beter een zeer recent voorbeeld: meer dan 20 miljoen Amerikaanse burgers en meer dan 4 miljoen ambtenaren die getroffen worden door een grote hack bij de overheid (Office of Personnel Management), is het belang van ICT beveiliging bij de overheid en vertrouwensdiensten toegenomen. De voornoemde gebeurtenissen hebben geleid tot de vraag naar de noodzaak voor en de mogelijkheid van effectieve, technisch onafhankelijke reguleringsinstrumenten die de integriteit van elektronische identiteiten en systemen waarborgen. De uitvoeringswet EU-Verordening 910/2014 betreffende elektronische identiteiten en vertrouwensdiensten (*'Uitvoeringswet')* sluit op abstract niveau in bepaalde mate aan bij de actualiteit en de beveiligingseisen die voor de informatiemaatschappij in het leven zijn geroepen. Meer concreet lijkt mede gezien het verleden de praktische uitwerking, deskundigheid, (markt)kennis en de mogelijkheid om binnen bekwame (lees zeer: zeer korte) tijd adequaat te reageren op veiligheidincidenten bij de toezichthouder(s) een punt van grote zorg. De lappendeken van diverse toepasselijke regelgeving en toezichthouders, en dus eenduidige standaarden en normeringen is eveneens een punt van zorg. Verder lijken actuele onderwerpen zoals Internet of Things (IoT), data analytics en constant evoluerende cybersecurity technologieën niet nadrukkelijk in overweging te zijn genomen in de EU-Verordening en de Uitvoeringswet, terwijl ook die de komende decennia de boventoon zullen gaan voeren in de digitale markt.
2.	**DOEL WETSWIJZIGING**	De huidige Richtlijn 1999/93/EG biedt onvoldoende mogelijkheid voor grens- en sector overschrijdend kader voor veilige, betrouwbare en gebruiksvriendelijke elektronische transacties. De nieuwe EU-Verordening 910/2014 biedt dat in een verbeterde mate en heeft tot doel het vertrouwen in elektronische transacties in de interne markt te vergroten door te voorzien in een gemeenschappelijke grondslag voor veilige elektronische interactie tussen burgers, bedrijven en overheden, en bijgevolg

		ook de doeltreffendheid van publieke en private onlinediensten, e-business en elektronische handel in de Europese Unie te verhogen.
3.	**CONCEPT WETSWIJZIGING**	De minister met deze Uitvoeringswet de nieuwe EU-Verordening uit te voeren, nu deze rechtstreekse werking heeft. Dit houdt in dat de elektronische identificatiemiddelen binnen de lidstaten van de Europese Unie **grensoverschrijdende erkenning** krijgen. Een lidstaat is verplicht om de eID's van andere lidstaten te erkennen. Dit geldt alleen voor elektronische identificatiemiddelen die zijn aangemeld bij de Europese Commissie en dus gekwalificeerd zijn. Hierdoor dient aan bepaalde interoperabiliteit en veiligheidseisen te worden voldaan en is beperkt tot middelen met een vrij hoog betrouwbaarheidsniveau. Het streven is naar wederzijdse erkenning van elektronische identificatiemiddelen binnen de Europese Unie. Een grote kans maar ook groot risico hierbij is dat er meerdere partijen betrokken zijn bij de totstandkoming en het gebruik van de elektronische identificatiemiddelen, o.a. de koppeling van de persoonsidentificatiegegevens, de uitgever van het elektronische identificatiemiddel en de verzorger van het authenticatieproces. Om te zorgen dat er niet nogmaals vergelijkbare incidenten als bij DigiNotar en Office of Personnel Management plaatsvinden worden de onderstaande maatregelen genomen: 1. De vertrouwensdiensten dienen **passende technische en organisatorische maatregelen** te treffen. De Europese Commissie zal dergelijke normen nader specificeren, zoals in de nieuwe ISO/IEC 19086 normen, ETSI standaarden en andere standaardisatie normen waar de Europese Commissie aan werkt. 2. De **meldplicht** bij inbreuk op veiligheid of verlies van integriteit is verplicht voor de vertrouwensdiensten en dient binnen 24 uur na ontdekking gemeld te worden bij het toezichthoudende orgaan, en indien er sprake is van aanzienlijke gevolgen onmiddellijk aan de gebruikers. Deze melding dient zowel bij Agentschap Telecom als bij het NCSC te worden gedaan in geval van een veiligheidsinbreuk of integriteitsverlies, als ook een melding bij het Cbp ingeval van inbreuk betreffende persoonsgegevens. Dit laatste is bijna altijd het geval, omdat de elektronische identificatiediensten nu eenmaal zien op persoonsgegevens en dergelijke inbreuken ernstige nadelige gevolgen hebben voor de privacy van gebruikers. Deze meldplicht is concreter en specifieker dan het wetsvoorstel meldplicht datalekken. 3. **Toezicht** op de vertrouwensdiensten komt te liggen bij (i) het Agentschap Telecom, die in het kader van de toegang tot telecommunicatiegegevens eveneens nieuwe toezichts- en handhavingsbevoegdheden heeft gekregen, (ii) het ministerie van Economische Zaken en bij (iii) het NCSC onder verantwoordelijkheid van de minister van Justitie. Bij de gekwalificeerde vertrouwensdiensten vindt toezicht vooraf plaats en structureel is het verplicht om eens in de 24 maanden een audit te laten uitvoeren door een conformiteitsbeoordelingsorgaan. Gevolgen bij het niet naleven van de vereisten is intrekking van de status gekwalificeerd. Inbreuken van persoonsgegevens moeten worden gemeld bij het CBP, grensoverschrijdende gevolgen aan het betreffende land en het Europees Agentschap voor

		Informatieveiligheid (ENISA). Andere sanctie bevoegdheden zijn nog niet vastgelegd, maar dienen doeltreffend, evenredig en stimulerend zijn. 4. Verleners van vertrouwensdiensten bieden diensten aan die het vertrouwen in het elektronisch verkeer waarborgen, daarvoor zijn ze **aansprakelijk** wanneer er een vermoeden bestaat in het geval van opzet of nalatigheid, tenzij de verlener van de vertrouwensdienst bewijst dat schade zonder opzet of nalatigheid van zijn kant is ontstaan. Dit is een gekwalificeerde schuldaansprakelijkheid met omgekeerde **bewijslast** voor de certificaatverleners van gekwalificeerde vertrouwensdiensten. Deze aansprakelijkheid en bewijslast is vooralsnog onvoldoende nauwkeurig beschreven in deze Uitvoeringswet en lastig te toetsten en te handhaven. 5. Net als bij elektronische identiteiten worden bij vertrouwensdiensten persoonsgegevens verwerkt en is op de **verwerking van persoonsgegevens** de Wet bescherming persoonsgegevens van toepassing. Er mogen alleen minimale gegevensset worden verleend aan de vertrouwensdienst, waarbij de aanvullende gegevens enkel op basis van toestemming van de gebruiker verzonden worden. De verzameling van data dient beperkt te worden tot een minimum (data minimization) voor een duidelijk en nauwkeurig omschreven doel, en de verzamelde gegevens dienen zo snel mogelijk vernietigd te worden. Dit is gebaseerd op de waarborgen van de Wbp: proportionaliteit, beschikbaarheid, toegang, dataretentie, gebruik en geheimhouding van gegevens, ook wel aangeduid als de Data Life Cycle. Dit verzamelbegrip is in 2014 mede opgenomen in de, in samenspraak met de Europese Commissie (in het bijzonder DG Connect en DG Justice) en ENISA, door de Drafting Group van de EC Cloud Select Industry Group, opgestelde Cloud Service Level Agreement Standardisation Guidelines (die ook ingaat op cybersecurity, data & incident management, en (persoons)gegevensbescherming), en wordt eveneens verwerkt in de nieuwe ISO/IEC 19086 normen. Arthur's Legal is onder meer een van de experts van voornoemde Drafting Group, en is mede-auteur van voornoemde Guidelines en ISO/IEC normen. Verder is Arthur's Legal actief lid en draagt bij aan voor deze Uitvoeringswet relevante EC werkgroepen over Internet of Things (AIOTI, EC en ETSI).
4.	**RELATIE MET PRIVACY & SECURITY**	Het is algemeen bekend dat gegevensbescherming en informatiebeveiliging met elkaar verbonden en bijna altijd overlappende gebieden zijn. Een van de grootste zorgen is de bescherming van persoonsgegevens en andere gevoelige informatie, en de daarbij behorende beveiliging. Op welke manier wordt dit door de vertrouwensdiensten voldoende gewaarborgd en hoe zorgt men er voor dat het publiek de elektronische identificatie accepteert, vertrouwt en gaat gebruiken? Ondanks dat er enige aandacht wordt geschonken aan de vertrouwelijkheid en de beveiliging in de Uitvoeringswet, kan de vertrouwensdienst deze gevoelige informatie wel degelijk aan derden overdragen in het kader van het bieden van elektronische identificatie diensten, zeker nu het mogelijk is om dit grensoverschrijdend. De Uitvoeringswet zorgt er niet voor dat data inbreuken en andere hacks worden voorkomen en voorkomt ook niet dat data met derden wordt gedeeld. De Minister kan zelfs via dit kanaal ongehinderd cross-over data gebruiken via deze nieuwe bevoegdheden. Dat laatste is

		vanzelfsprekend zeer ongewenst, ook omdat het niet het doel is van de EC-Verordening, Telecommunicatiewet, Wet bescherming persoonsgegevens en andere toepasselijke regelgeving maar nu dus niet goed is ingekaderd en afgedekt. Kort gezegd dient het gebruik van informatie door de bevoegde instanties getoetst en gedefinieerd te worden als onderdeel van de Data Life Cycle. Dit geldt al helemaal voor de gekwalificeerde vertrouwensdiensten. Vooralsnog volgen de beveiligingswaarborgen voor de informatieverzameling en de wijze waarop de vertrouwensdiensten worden gekwalificeerd onvoldoende uit de Uitvoeringswet. Alleen het noemen van de vertrouwelijkheid en verwijzen naar de Wbp en de EU-Verordening is niet voldoende als men wil zorgen voor vertrouwen in het grensoverschrijdend gebruik van elektronische identificatiemiddelen. Het spanningsveld tussen security en privacy wordt door de wetgeving nog altijd niet weggenomen en op een eenduidige wijze opgelost.
5.	**CONCLUSIE**	Privacy en security is een complex samenspel van vraagstukken, overlappende spanningsvelden en conflicterende rechten en plichten. Het gaat hier niet alleen om de techniek, maar ook om menselijk gedrag, om de manier waarop organisaties met hun security omgaan en om de psychische impact van cyberdreiging op maatschappelijk niveau. Deze spanningsvelden bestaan tussen security, privacy, markt- en bedrijfsbelangen, andere (branche of andere) compliance regelgevingen, en natuurlijk scheiding der machten. Kortom, het gaat over een combinatie van mens, organisatie, techniek, proces en besturing. Het delen van best practices en de daarbij behorende ervaringen met inbreuken, alsmede het opstellen van standaarden is van belang om een zo veilig mogelijk digitale maatschappij te kunnen waarborgen. Dit is echter op meerdere manieren in te kleden en hoeft niet altijd te worden opgelost door middel van wetgeving. Los van het feit dat dit niet de meest effectieve manier is, is het ook nog eens de meest ingrijpende manier met het oog op het spanningsveld tussen security en privacy. Grensoverschrijdende elektronische identificatie mag in geen geval een excuus zijn voor de onbeperkte monitoring en analyse van persoonsgegevens zonder enige onafhankelijke toetsing op proportionaliteit, data minimization en geheimhouding daarvan. Het gebruik van elektronische identificatiemiddelen onder het mom van security en veiligheid van de maatschappij is niet gerechtvaardigd als de privacy waarborgen en een afweging van markt- en bedrijfsbelangen achterwege worden gelaten. Zoals al aangegeven is verder de praktische uitwerking, deskundigheid, (markt)kennis en de mogelijkheid om binnen bekwame (lees zeer: zeer korte) tijd adequaat te reageren op veiligheidsincidenten bij de toezichthouder(s) een punt van grote zorg, en is er te weinig oog voor c.q. aandacht gegeven aan actuele onderwerpen zoals Internet of Things (IoT), data analytics en constant evoluerende cybersecurity technologieën.

6.	**BEST PRACTICES**	De Europese Commissie is flink bezig met het standaardiseren van normeringen voor ondersteunende elektronische diensten als cloud computing, IoT en andere platforms, kunnen dus als voorbeeld worden genomen. Voorbeelden als de Cloud Service Level Agreement Standardisation Guidelines van de Europese Commissie, en gerelateerde activiteiten van EC, ENISA, ETSI, NIST en ISO/IEC zijn hiervoor een uitstekend uitgangspunt. Om vertrouwensdiensten te kwalificeren en te toetsen kan men de heldere opzet voor standaardisatie van data management, (persoons)gegevensbescherming en informatiebeveiliging waarborgen voor cloud gebruikers, de Privacy Level Agreement (PLA v2.0) als basis gebruiken, opgesteld samen met de Cloud Security Alliance. Arthur's Legal heeft ook hieraan als co-auteur bijgedragen. Deze PLA is een basisleidraad/raamwerk om te kunnen voldoen aan de EC en nationale regelgeving over de bescherming van persoonsgegevens. Vanwege de elkaar snel opvolgende ontwikkelingen op gebied van technologie en business modellen, dient extra rekening gehouden te worden met standaardisatie die technologisch en business model neutraal is en wereldwijd toepasbaarheid is, en een uniform begripsgebruik kent. Op dit moment en naar verwachting de komende jaren is het codewoord wereldwijde standaardisatie, met daarbij behorende zelfregulering, certificering, best practices en transparantie. Dat dient ook de basis te zijn voor het bewerkstelligen van de digitale economie. Voor uitvoerders, leveranciers, gebruikers en toezichthouders zal de enorme uitdaging zijn en blijven om de ontwikkelingen bij te houden, en veilige vertrouwensdiensten en ander online (data)verkeer te kunnen leveren die bestand zijn tegen de dan bestaande gevaren en risico's in de digitale wereld. Dit laatste gaat alleen lukken als er internationaal wordt samengewerkt door alle belanghebbenden, en dus niet alleen regelgevers en uitvoerders/toezichthouders.
7.	**NADERE TOELICHTING**	Arthur's Legal is graag bereid de voorgaande opmerkingen en aanbevelingen desgewenst toe te lichten.