INTERNETCONSULTATIE

REGELING BETROUWBAARHEIDSNIVEAUS AUTHENTICATIE ELEKTRONISCHE DIENSTVERLENING

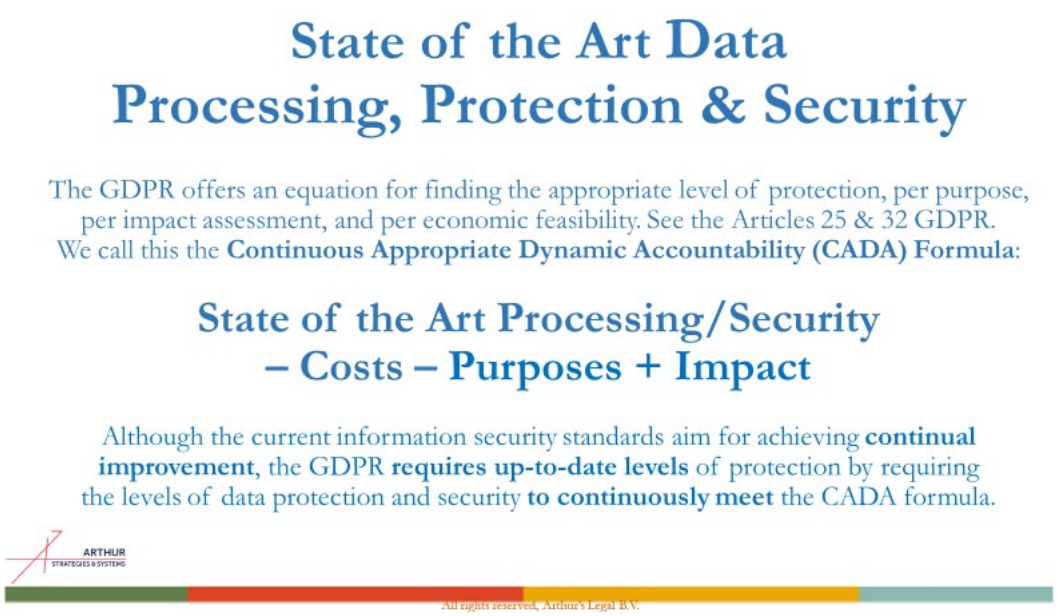
Status per 20200903

1.	**INLEIDING**	De overheid is de publieke dienstverlener. Het betrouwbaar en toegankelijk beschikbaar stellen en verlenen van betrouwbare en toegankelijke publieke diensten aan zowel natuurlijke personen als rechtspersonen is bij uitstek haar primaire taak. Een en ander tegenwoordig zowel fysiek, digitaal of een combinatie daarvan. Zowel betrouwbaarheid als ook toegankelijkheid zijn de twee belangrijkste uitgangspunten. Deze uitgangspunten zijn ook afhankelijkheden van elkaar. De toegankelijkheid moet betrouwbaar zijn. De betrouwbaarheid mag niet voor negatieve impact op toegankelijkheid veroorzaken. Deze uitgangspunten en afhankelijkheden zouden de basis moeten vormen voor het onderhavige voorstel Regeling Betrouwbaarheidsniveaus (‘*Regeling*’). Dwingendrechtelijk is dat immers al het geval, zoals we hieronder zullen toelichten. Een en ander leidt tot de conclusie dat het – anders dan verwoord in het huidige voorstel – niet aan een bestuursorgaan of aangewezen organisatie is om zelf te bepalen welk betrouwbaarheidsniveau een elektronische publieke dienst vereist. We gaan daar hieronder nader op in, inclusief onze aanbevelingen hoe het wel conform de reeds bestaande dwingendrechtelijke bepalingen mogelijk is, met in achtneming van voornoemde uitgangspunten en afhankelijkheden.
2.	**GRONDSLAGEN**	Persoonsgegevens en personen worden beschermd door de Europese Grondwet (die al sinds 2009 directe werking heeft), de Europese verordening 2016/679 (GDPR), de Nederlandse versie daarvan, de Algemene verordening gegevensbescherming (AVG) en nationale keuzes daarbinnen als vastgelegd in de Uitvoering Algemene verordening gegevensbescherming (UAVG). Een verordening gaat voor lokale wet- en regelgeving, maar in onderhavig domein zijn met name de bepalingen relevant waar geen c.q. geen afwijkende nationale keuze is gemaakt. Het is belangrijk vast te stellen dat de Europese eIDAS verordening (EU 2012/0146) en Implementatieverordening daarbij (EU 2015/1502) uit respectievelijk 2014 en 2015 stammen, voordat de GDPR tot stand kwam. De GDPR is als verordening leidend op gebied van persoonsgegevensverwerking, bescherming en management, en enige Regeling dient daar volledig mee in lijn en compliant te zijn. En de GDPR vereist een hogere betrouwbaarheid dan in de Implementatieverordening – als ook in het voorstel van de Regeling – genoemd.

3.	**GDPR/AVG**	Anders dan de Regeling suggereert, zijn in het kader van authenticatie en AVG met name de volgende drie criteria essentieel: A. **Classificering van de persoon**; B. **Classificering van persoonsgegevens**, en; C. **Bescherming**. Zowel van (i) persoon, (ii) persoonsgegevens, (iii) beschikbaarstelling van authenticatiemiddelen, (iv) authenticatie zelf, en (v) en andere persoonsgegevensverwerking. In de Regeling valt op dat met name is gekeken naar Criteria B. Echter, zoals al aangegeven dient bescherming – en dus betrouwbaarheid – onder de AVG een veel groter gebied, en niet alleen de persoonsgegevens. Alleen classificeren op persoonsgegevens zonder rekening te houden met de diverse classificaties van personen – en al hun hoedanigheden, zoals bijvoorbeeld kinderen of andere kwetsbare groepen – is in strijd met de vereisten van de AVG, en betekent inbreuk daarop. De regres-, schade- en boeteregimes van de AVG worden als genoegzaam bekend beschouwd. Zodra de diverse classificaties en afhankelijkheden zijn doorlopen conform de AVG – en dus niet conform hetgeen thans wordt voorgesteld in Bijlagen 1 en 2 van huidige concept van Regeling –, dan kunnen (en moeten) die worden bekeken en getoetst op de bescherming ervan als beschreven in de AVG. Gelezen het huidige concept hebben die beoordeling en validatie niet plaatsgevonden. Voor de elektronische diensten als bedoeld in de Regeling dienen in ieder geval voor elke specifieke context voldoende passende en up-to-date technische en organisatorische maatregelen getroffen te worden als beschreven in de AVG, in het bijzonder de artikelen 25 en 32. Waarbij artikel 25 over de verwerking gaat, en artikel 32 over de bescherming, hebben beide artikelen een gelijke structuur en strekking. Ze beschrijven een dynamische en praktische toets waarmee respectievelijk kan worden getoetst of er voldoende en adequate maatregelen zijn getroffen voor verwerking c.q. bescherming van persoonsgegevens. Deze maatregelen dienen niet periodiek maar continue te worden beoordeeld en geactualiseerd naar de 'state-of-the-art' van dat moment, zowel wat betreft beschikbare maatregelen, als wat betreft veranderende risico's (inclusief gewijzigde hackingmethodieken, cybersecurity kwetsbaarheden, en leergeld uit recente incidenten en meldingen) en gerelateerde impact (die vanwege de digitalisering en afhankelijkheid ervan sowieso steeds groter wordt). Kort samengevat noemen we dit CADA: **Continuous Appropriate Dynamic Accountability**. In het Nederlands per saldo: een dwingendrechtelijke toetsingsmethodiek om op contextuele basis continue en op een transparante en uitlegbare wijze te bepalen en aan te tonen wat het juiste niveau van uitvoering van een rechtsbeginsel, in dit geval betrouwbaarheid, is en wordt nageleefd, en hoe. Het gaat te ver om daar hier dieper op te gaan; wij zijn vanzelfsprekend van harte bereid ben om een en ander nader toe te lichten.

Hieronder delen we een visualisering van de CADA in de artikelen 25 en 32.

Beide artikelen worden ook wel de basisbepalingen van Privacy by Design and by Default (25) respectievelijk Security by Design and by Default (32) genoemd.



Per saldo dient derhalve het betrouwbaarheidsniveau – altijd – hoog te zijn. Immers, de AVG gaat in voornoemde artikelen uit van state-of-the-art en het is nu eenmaal mogelijk om dergelijke maatregelen, zowel technisch als organisatorisch, te nemen.

De reden waarom het kostenaspect van implementatie weinig tot geen effect heeft op een afslag om af te wijken van state-of-the-art verwerkings- en beveiligingsmaatregelen komt omdat zowel de purpose/doel om te communiceren nimmer vrijwillig is. Om contact te maken of anderszins een publieke dienst af te nemen is een persoon immers genoodzaakt om via een elektronische dienst toegang te verkrijgen en te communiceren met de overheid.

Dit argument speelt ook mee bij de impact als opslagfactor. Impact speelt in gevallen waarvoor de Regeling bedoeld is sowieso een grote rol. Immers, voor elk natuurlijk persoon, in welke hoedanigheid dan ook (zoals bijvoorbeeld kind, ouder, toeslagverzoeker, belastingbetaler, zelfstandig ondernemer of bestuurder van een organisatie) geldt dat het aanvragen van een publieke dienst, en dienaangaande communiceren met een bestuursorgaan of andere overheidsorganisatie altijd essentieel en anderszins belangwekkend is. Het rechtvaardigt op generlei wijze een lager niveau van bescherming c.q. betrouwbaarheid dan hoog.

Het is sowieso evident dat uit enige beoordeling en validatie, zeker anno 2020 in deze digitale tijden, dat een betrouwbaarheidsniveau laag nimmer toereikend is. De verwerking- en beveiligingsmaatregelen die gelden voor niveau laag, zoals single-factor authenticatie (SFA)) is eenvoudigweg in strijd met de AVG. De artikelen 25 en 32 stellen immers hoge eisen aan verantwoorde en moderne maatregelen voor adequate verwerking en bescherming van persoonsgegevens.

		Het is een feit van algemene bekendheid dat identiteitsdiefstal een gemakkelijke en veelvoorkomende vorm van misdaad is met een laag risico en hoge beloning voor de dader(s), en een grote bedreiging voor mensen en organisaties (en ons land). Het is de snelst groeiende vorm van criminaliteit. Zwakke of gestolen gebruikersgegevens zijn het favoriete wapen van hackers. Zonder adequate gebruikersauthenticatie staat de voordeur echter wijd open voor indringers. In de Toelichting van de Regeling wordt weliswaar verwezen naar een onderzoek op gebied van betrouwbaarheidsniveaus van patiëntenauthenticatie, maar het kader is veel te beperkt (een persoon in de hoedanigheid van patiënt) èn zodanig gedateerd (mei 2016) dat bovenstaande dwingendrechtelijke bepalingen in de meer recente AVG niet in ogenschouw genomen lijken te zijn. De aanname in de Regeling (en Bijlage 2) dat er wat betreft negatieve impact en andere gevolgen en consequenties alleen naar geldelijke schade kan en mag worden gekeken, is eveneens niet in lijn met voornoemde artikelen 25 en 32 AVG. Geldelijke schade is wel een attribuut om rekening mee te houden, en niet-geldelijke impact en andere gevolgen kunnen weliswaar lastig te kwantificeren zijn, maar die zijn veelal wel vele malen belangrijker, zoals bijvoorbeeld bij identiteitsfraude, integriteit, weerbaarheid en andere kwaliteit van leven. De notie van impact betreft dus zowel kwantitatieve als kwalitatieve impact van enig gebrek aan het juiste niveau van betrouwbaarheid en waarborging daarvan.
4.	**ÉÉN NIVEAU**	Het is niet op basis van de AVG alleen noodzakelijk om altijd niveau hoog te bieden en op dat niveau te opereren. Het is ook prima mogelijk. En, het is veel gebruiksvriendelijker om één niveau hanteren, dan een boeket aan niveaus. Verder hoeft dat bepaald niet duur te zijn om in te voeren, ook omdat het hanteren van één niveau technische, organisatorische en economische schaalvoordelen met zich mee brengt. Dat het prima mogelijk is, komt mede doordat maatregelen om niveau hoog te halen en te houden inmiddels gewoon gemeengoed zijn geworden. Zoals bijvoorbeeld Multifactor authenticatie (MFA): een authenticatiemethode waarbij een gebruiker pas digitale toegang krijgt nadat die met succes twee of meer soorten bewijs (factoren) met behulp van bewijsstukken (attributen) heeft voorgelegd aan een authenticatiemechanisme. Multifactor authenticatie (MFA) helpt bij het adresseren van deze issues, naast het feit dat het gebruikersgemak substantieel kan verhogen. Een ander voordeel om een attributen-gedreven aanpak te hebben is dat attributen veelal dynamisch zijn en dat daarmee het benodigde betrouwbaarheidsniveau kan worden geverifieerd en gehaald zonder dat er statische (en veelal niet te wijzigen, zoals bepaalde gegevens in basisregistraties) persoonsgegevens nodig is waar een hacker bijzonder in geïnteresseerd is. De attributen kunnen uit praktisch elke dataset of databron – zowel uit het publieke als uit het private domein, inclusief dynamische technische en administratieve attributen – komen. Vanzelfsprekend zijn er ook vele andere maatregelen mogelijk, beschikbaar, getest en goedbevonden. Men moet immers niet vergeten dat het hier gaat om de beveiliging van het gehele digitale ecosysteem van de (betreffende) overheid, dus inclusief infrastructuur, communicatie en netwerk, computing, hardware, software, organisatie, et cetera.

		Nederland hoeft hier overigens niet als 'first-mover' te acteren. Andere landen zijn Nederland al voor, zoals met name Spanje (die binnen de Europese Unie echt met vlag en wimpel boven de andere lidstaten uitsteekt) als bijvoorbeeld ook het Verenigd Koninkrijk en Dubai. En met succes, ook voor wat betreft bepaalde internationale interoperabiliteit en de mogelijkheden tot gebruik in niet-overheidsorganisatie communicaties en transacties.
5.	**BIJKOMENDE VOORDELEN**	Er zijn ook bijkomende voordelen bij (A) het hanteren van één niveau, en (B) het hanteren van het betrouwbaarheidsniveau hoog als dat ene niveau, zoals: A. Hoog niveau van vertrouwen voor beide zijden, hetgeen de communicatie- en transactiebereidheid zal doen bevorderen en verbeteren; B. Geen gevoelige en anderszins lastige afwegingskaders te hoeven stellen en actueel te houden door elk bestuursorgaan of aangewezen organisatie wat betreft het te hanteren betrouwbaarheidsniveau; C. Hoog implementatie- en beheergemak en kostenvoordelen voor de overheid, omdat niet elk bestuursorgaan of aangewezen organisatie hoeft te beoordelen en zelfstandig processen hoeft in te richten om het juiste niveau vast te stellen, implementeren en in stand te houden; D. Hoog gebruiksgemak voor de gebruiker, omdat de persoon (burger, bedrijf of andere hoedanigheid) niet verward raakt welk niveau voor welke elektronische dienst geldt, en of die persoon een dergelijke middel wel tot zijn/haar beschikking heeft; E. Lagere kosten (of wellicht zelf geen kosten meer) die eventueel moeten worden doorbelast aan burger of bedrijf, en; F. Met het bovenstaande (A tot en met E) neemt de mate van toegankelijk en laagdrempeligheid juist toe.
6.	**CONCLUSIE**	Het moge duidelijk zijn (A) dat we sterk afraden het huidige voorstel van de Regeling in haar huidige vorm en met haar huidige inhoud ongewijzigd te laten, maar (B) dat we ook meer dan voldoende mogelijkheden – en diverse substantiële voordelen – zien om weldegelijk aan de dwingendrechtelijke vereisten van de artikelen 25 en 32 AVG te kunnen voldoen, en de elektronische diensten voor Nederland hoogst-betrouwbaar en toekomstbestendig te maken. Het is ook de basis voor een modern dynamisch ecosysteem om betrouwbaar kunnen communiceren en betrouwbaar transacties te kunnen doen tussen burgers en bedrijven (ook conform de tevens door Nederland mede-ondertekende Tallinn Verklaring), en opent daarmee ook de weg naar het gebruik van die authenticatiemiddelen tussen Nederland (overheid, burger en bedrijf en publiek-privaat) en andere landen in de wereld.
7.	**NADERE TOELICHTING**	Arthur's Legal is graag bereid de voorgaande opmerkingen en aanbevelingen desgewenst toe te lichten.