INTERNETCONSULTATIE
WET OP DE INLICHTINGEN- EN VEILIGHEIDSDIENSTEN

Status per 20150901

1.	**INLEIDING/ HISTORIE**	Uit de voorgeschiedenis van de Wet op de inlichtingen en veiligheidsdiensten (hierna te noemen: 'WIV') blijkt dat na de terroristische aanslagen van 11 september 2001 ('9/11') de behoefte naar terrorismebestrijding binnen Europa is versterkt. De brief van toenmalig President George W. Bush aan de Europese Commissie droeg uiteindelijk bij aan de expliciete grondslag voor onder meer dataretentie en samenwerkingen tussen de inlichtingen- en veiligheidsdiensten en politiediensten. '9/11' heeft niet alleen invloed gehad op de inlichtingen en veiligheidsdiensten, maar ook op de reikwijdte van dataretentie, met als gevolg dat die niet alleen tot terrorismebestrijding diende maar ook bevoegdheden met betrekking tot de vervolging van (andere) strafbare feiten omvat. 9/11 heeft geleid tot de vraag naar de noodzaak voor en de mogelijkheid van effectieve, technisch onafhankelijke reguleringsinstrumenten die voor het uitbreiden van opsporingsbevoegdheden om terrorismebestrijding te waarborgen. In de Verenigde Staten heeft Obama in de zomer van 2014, naar aanleiding van Snowden een onafhankelijk comité Clarke ingeschakeld, dat heeft onderzocht in hoeverre het post-9/11 staatsveiligheidsbeleid zich verhoudt tot de Amerikaanse en universele grondrechten. Een groot deel van de aanbevelingen in het rapport 'Liberty and Security in a Changing World' over verbetering in de drempel van het verzamelen van data, verbetering van de gerechtelijke toetsing van verzoeken, minimalisatie van data, relevantie van de data, duur van dataretentie en transparantie is begin 2014 al doorgevoerd in wet- en regelgeving en recent is de Amerikaanse Freedom Act in werking getreden, waarin deze verbeterpunten verzameld en gestructureerd zijn. In Europa was na de Snowden-onthullingen de Dataretentierichtlijn en daarop gebaseerde c.q. daaraan gerelateerde nationale wet- en regelgeving niet aangepast of onder het vergrootglas gelegd. Hoewel het in de rede had gelegen dat zowel Europese als nationale wet- en regelgevers zelf een herijking van dataretentie hadden toegepast, moest het Europees Hof van Justitie er aan te pas komen om de Dataretentierichtlijn ongeldig te verklaren. Het Europese Hof stelt terecht vast dat de Dataretentierichtlijn onvoldoende waarborgen geeft voor de grondrechten zoals in het bijzonder het recht op bescherming van het privéleven (artikel 7 van het Handvest) en het recht op bescherming van persoonsgegevens (artikel 8 van het Handvest). Verder geeft het Europese Hof een aantal fundamentele handvatten, die hieronder eveneens als essentiële aanbevelingen worden gesteld voor de wetgever om onderhavige WIV wetswijziging onder de loupe te nemen en structureel aan te passen zodat het op z'n minst voldoen aan die fundamentele beginselen. Immers, ook de volgende keer zal het Europese Hof een wet – inclusief enige wijziging van de WIV – daarop gaan toetsen.

2.	**DOEL WETSWIJZIGING**	In Nederland heeft de overheid de afgelopen jaren al diverse wetsvoorstellen omtrent privacy, cybersecurity, meldplichten, data-lekken en dataretentie gedaan, waarbij iedere keer blijkt dat dit een complex samenspel van vraagstukken, overlappende spanningsvelden en conflicterende rechten en plichten is. Het zou in de lijn der verwachting liggen dat de wetgever op basis van alle bovenstaande informatie lering trekt en de evidente raamwerken gebruikt om de overlappende spanningsvelden beter te kunnen coördineren en zorgen voor een duidelijke lijn op gebied van toegang, bescherming van persoonsgegevens en de nationale veiligheid. De WIV is sinds de inwerkingtreding in 2002 al verschillende malen geëvalueerd en ingeperkt. Volgens de minister Binnenlandse zaken en koninkrijksrelaties (BZK) biedt de huidige WIV onvoldoende mogelijkheden voor het gebruik van nieuwe technologische ontwikkelingen in de informatie en communicatietechnologie, en blijkt de huidige WIV in de praktijk onvoldoende technologisch neutraal te zijn, reden waarom de WIV aangepast te worden.
3.	**CONCEPT WETSWIJZIGING**	De taken en bevoegdheid van de Algemene Inlichtingen- en Veiligheidsdiensten en de Militaire Inlichtingen en Veiligheidsdiensten (hierna gezamenlijk: '*Veiligheidsdiensten*') wil de minister BZK meer laten aansluiten op de huidige en nieuwe technologische ontwikkelen zoals het verzamelen en verwerken van (persoons)gegevens door de Veiligheidsdiensten voor onderzoek en data-analyse in het kader van de nationale veiligheid. De minister BZK geeft aan zich ervan bewust te zijn dat deze taken een beperking vormen op het recht op eerbiediging van de persoonlijke levenssfeer en legt in de memorie van toelichting op het wetsvoorstel WIV uit dat de persoonlijke levenssfeer onder voorwaarden kan worden beperkt ter bescherming van de nationale veiligheid. In alle gevallen moet daarbij worden voldaan aan de eisen van legitimiteit, noodzakelijkheid, proportionaliteit en subsidiariteit, aldus de minister. Deze waarborgen zouden er voor moeten zorgen dat de inbreuk op de persoonlijke levenssfeer die de inzet van bijzondere bevoegdheden in het belang van de nationale veiligheid tot gevolg kan hebben, in balans is met het recht op bescherming van de persoonlijke levenssfeer van de burger waarmee het wetsvoorstel WIV volgens de minister aan de wettelijke vereisten voldoet. Helaas is dat nog niet correct en accuraat. De minister gaat er gemakshalve aan voorbij dat niet alleen de bovengenoemde waarborgen voor het verwerken van persoonsgegevens door de Veiligheidsdiensten in acht genomen moeten worden, maar het massaal verzamelen van persoonsgevoelige informatie dient van geval tot geval bekeken te worden, dient alleen strikt noodzakelijk te zijn, en zal feitelijk in geen enkele geval gerechtvaardigd zijn. Daarnaast dient de verzameling van gegevens op z'n minst (a) beperkt te worden tot het absolute minimum (data-minimalisatie), (b) alleen gebruikt voor een duidelijk en nauwkeurig omschreven doel waarbij er sprake is een daadwerkelijke bedreiging van de openbare veiligheid (doel en proportionaliteit van gebruik), en (c) de verzamelde

		gegevens slechts beperkt bewaard te worden èn vervolgens direct en permanent vernietigd te worden (dataretentie en data-vernietiging). Kort gezegd zou het gebruik van persoonsgegevens verzameld door communicatie- en telecommunicatiediensten door Veiligheidsdiensten neer komen op de volgende vier stadia: (a) beschikbaarheid, (b) toegang, (c) dataretentie en (d) het gebruik. Deze stadia worden ook aangeduid als 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, en wordt eveneens verwerkt in de nieuwe ISO/IEC 19086 normen. In het bijzonder wordt hier verwezen naar de Hoofdstukken 2, 5.3, 6.3 en 6.4 en 6.5 van die Guidelines. Arthur's Legal is een van de experts van voornoemde Drafting Group, en is mede-auteur van voornoemde Guidelines en ISO/IEC normen.
4.	**DATA LIFE CYCLE**	In het kader van de nationale veiligheid mogen de Veiligheidsdiensten binnen geldende wet- en regelgeving (persoons)gegevens verzamelen en verwerken over het communicatie- en telecommunicatieverkeer van gebruikers. Hierdoor blijven ook alle communicatie- en telecomproviders verplicht tot het verzamelen en **beschikbaar** houden van gegevens van alle burgers. Aanbieders van clouddiensten zijn met de huidige wet niet verplicht om gegevens te bewaren, maar door de medewerkingsverplichting voor de aanbieders van clouddiensten zouden zij nu toch verplicht worden gegevens beschikbaar te houden zoals de inhoud van een mailbox van een gebruiker, voicemail of andere gegevens die in data-opslagdiensten zijn opgeslagen. Het Europese Hof van Justitie heeft in haar arrest over de Dataretentierichtlijn hierover geen bezwaren aangegeven met het oog op de veiligheid en het belang van terrorisme bestrijding. Wel geeft het Europese Hof van Justitie aan dat de categorieën van de data nauwkeurig moeten worden omschreven. Volgens artikel 52 lid 1 van het Handvest moeten beperkingen op het in dit Handvest erkende rechten en vrijheden, als artikel 7 en 8, bij wet worden gesteld en de wezenlijke inhoud van die rechten en vrijheden eerbiedigen, en kunnen, met inachtneming van het **evenredigheidsbeginsel**, alleen beperkingen worden gesteld indien zij **noodzakelijk** zijn en daadwerkelijk aan door de EU erkende doelstellingen van het algemeen belang of aan de eisen van de bescherming van rechten en vrijheden van anderen, beantwoorden. Het Hof geeft hiervoor in ieder geval de volgende fundamentele handvatten: (i) Er dient er een **verband** te bestaan tussen de gegevens die moeten worden bewaard en een bedreiging van de openbare veiligheid. (ro. 59) (ii) De toegang van de bevoegde nationale autoriteiten tot de bewaarde gegevens moet **onderworpen zijn aan enige voorafgaande controle door een rechterlijke instantie** of een onafhankelijk administratieve instantie die hierover uitspraak doet en waarvan de beslissing beoogt om de toegang tot de gegevens en het gebruik ervan te beperken tot wat strikt noodzakelijk is ter verwezenlijking van het nagestreefde doel. (ro 60)

		(iii) Het **bewaartermijn** moet worden verkort en op basis van objectieve criteria worden vastgesteld om proportionaliteit te waarborgen. (ro 64) (iv) Er moeten duidelijke en precieze regels betreffende de reikwijdte en de toepassing van de maatregelen opgesteld worden die minimale vereisten opleggen ten aanzien van de toegang tot en exploitatie van de gegevens, zodat personen van wie gegevens zijn bewaard over voldoende garanties beschikken dat hun persoonsgegevens **doeltreffend worden beschermd tegen het risico van misbruik, elke onrechtmatige raadpleging en onrechtmatig gebruik**. (ro 66) De **toegang** tot informatie dient onder meer volgens het Europese Hof van Justitie in datzelfde arrest te worden onderworpen aan een **onafhankelijke toets**. De wetgever heeft in dit wetvoorstel WIV, de minister als enige deze bevoegdheid gegeven, waarbij er geen sprake is van een gerechtelijke toetsing van de gegevens en data door een onafhankelijk orgaan. Daarnaast hoeft niet altijd de minister toestemming te geven voor het intern of extern verstrekken van gegevens, de verantwoordelijke van de dienst mag dat ook, zowel nationaal als internationaal. Dit is onwenselijk. Juist omdat de grootste zorgen omtrent bescherming van persoonsgegevens is dat de overheid ongehinderd kan mee-/afluisteren en het cross-over data gebruik van de overheid (nationaal en internationaal). Geen enkele wet mag natuurlijk nieuwe (Nederlandse) Prism/Patriot- of Freedom Act en dataretentie issues veroorzaken. Wat betreft **dataretentie** wordt daar in de WIV praktisch geen aandacht aangegeven. In het kader van de nationale veiligheid mogen gegevens minimaal drie maanden en maximaal twaalf maanden bewaard worden, en worden verlengd met drie jaar. Echter, er dient een onderscheid te worden gemaakt tussen noodzakelijke/relevante informatie, oftewel een minimum vereiste. Dit minimum vereiste dient wederom te worden getoetst door een onafhankelijke gerechtelijke instantie. Uit de aanbevelingen van het comité Clarke volgt dat verzamelen en bewaren van data relevant dient te zijn voor het doel waarvoor de data zijn verzameld. Dat houdt in dat bij een opsporingsonderzoek de eerste toestemming door een gerechtelijk orgaan breed kan zijn voor een bepaalde tijd, na afloop van de bepaalde tijd zou de Veiligheidsdienst weer terug naar het gerechtelijk orgaan moeten gaan voor toestemming voor de relevante data. De verlening van de bewaartermijn dient eveneens getoetst te worden door een onafhankelijk orgaan. Het **gebruik** van de data wordt zowel intern als extern mogelijk gemaakt door de Veiligheidsdiensten over en weer. Uit onderzoek dat bijvoorbeeld bij de Politiewet massaal fouten in worden gemaakt, wegens de onduidelijke scheidslijn tussen het Wetboek van Strafvordering en de Politiewet. Dit heeft ertoe geleid dat een politieambtenaar in feite toegang heeft tot alle gegevens van alle burgers. Daarnaast blijkt de notificatieplicht van art. 126bb Wetboek van Strafvordering in de praktijk massaal te worden genegeerd, omdat dit geen prioriteit kent binnen het Openbaar Ministerie, en dit op geen enkel moment wordt getoetst. En dit is nog maar een onderdeel waarop de bijzondere bevoegdheden van de Veiligheidsdiensten op zien.

		De Veiligheidsdiensten kunnen de persoonsgevoelige informatie ook aan derden overdragen in het kader van het bieden van hulp en overleg voeren met soortgelijke diensten. Het bevorderen van de nationale en internationale samenwerking voor opsporingen heeft er mede voor gezorgd dat in de praktijk het principe 'voor wat hoort wat' tussen de diensten is ontstaan. De praktijk van het over en weer uitwisselen van data met buitenlandse opsporingsinstanties onder andere via de afspraken onder Mutual Legal Assistance Treaty ('MLAT') waarbij Nederland partij is versterken de gerezen inbreuken op privacy, en de daardoor ontstane, grote maatschappelijke zorgen bij burgers betreffende overheidsinterventie. Doordat de Veiligheidsdiensten steeds meer elektronische communicatiemiddelen onderzoeken en ook gebruik van maken voor het verzamelen van (persoons)gegevens wordt in het wetsvoorstel WIV de middelen (o.a. hacken) die openstaan voor data-analyse door Veiligheidsdiensten technologisch neutraal gemaakt. Het is bij de minister BZK bekend dat met deze manier er onvermijdelijk gegevens van personen die niet de aandacht van de diensten hebben ook worden verwerkt, omdat deze nu eenmaal een logisch en onlosmakelijk onderdeel uitmaken van een gegevensbestand, die noodzakelijk is om de data-analyse mogelijk te maken, aldus de minister BZK. Met name deze **'bijvangst'** van de data-analyse kunnen de Veiligheidsdiensten delen met een beperkte kring van derden, zoals (internationale) Veiligheidsdiensten. Bovendien is dergelijke bijvangst niet nodig en noodzakelijk in het kader van de nationale veiligheid en niet noodzakelijk om met derden te delen. De Minister kan via dit kanaal ongehinderd meeluisteren en cross-over data gebruiken via deze nieuwe bevoegdheden. Hiermee bevestigt het wetsvoorstel WIV dat de wetgever blijkbaar graag wil dat de Veiligheidsdiensten massaal alle soorten gegevens van alle burgers kunnen verzamelen onder het mom van nationale veiligheid. Dusdanige overheidsinterventie onder het mom van nationale veiligheid is niet rechtvaardig als de privacy waarborgen achterwege worden gelaten. Het is ook in strijd met nationale en Europese wet- en regelgeving.
5.	**CONCLUSIE**	De doelstelling van de wetswijziging zou een balans moeten zijn tussen (i) de toegangsbevoegdheden van Veiligheidsdiensten in belang van de nationale veiligheid en (ii) het recht op bescherming van de persoonlijke levenssfeer van de burger en bescherming van persoonsgegevens. Deze doelstelling wordt echter niet gehaald met het onderhavige wetsvoorstel, met name omdat de wetswijziging (i) onvoldoende de waarborgen van legitimiteit, noodzakelijkheid, proportionaliteit en subsidiariteit met massaal verzamelen van data niet naleeft, (ii) de data en toegang niet objectief en gerechtelijk wordt getoetst, en (iii) onvoldoende het primaire doel – bescherming van persoonsgegevens en de persoonlijke levenssfeer van de burgers – dient. De bescherming van de nationale veiligheid en democratie mag in geen geval een direct of indirect excuus zijn voor de onbeperkte monitoring en analyse van persoonsgegevens zonder enige onafhankelijke toetsing op proportionaliteit, data minimalisatie, dataretentie, en geheimhouding daarvan.

		Zo blijft voor toegang tot (persoons)gegevens in het kader van de nationale veiligheid, de minister als enige bevoegd. Dit is geen gerechtelijk onafhankelijk toezicht, een systeem dat zelfs in de Verenigde Staten wordt gehandhaafd, welke inmiddels dus zelfs is verbeterd. Kort gezegd dient het gebruik van informatie door de Veiligheidsdiensten getoetst en gedefinieerd te worden als onderdeel van de Data Life Cycle.
6.	**EXTRA AANBEVELING**	Om het gebruik van gegevens en data door de Veiligheidsdiensten 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 in opdracht van de Cloud Security Alliance en gesteund door gerenommeerde Europese instanties en organisaties. Arthur's Legal heeft 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 gerelateerde zaken dient extra rekening gehouden te worden met standaardisatie die op z'n minst technologisch model neutraal is en wereldwijd toepasbaarheid is, en een uniform begripsgebruik kent, zonder daarbij inbreuk te maken op de huidige wet- en regelgeving. Dat is eigenlijk makkelijker dan men denkt. Het is te betreuren dat die gedachte, basis en structuur in het huidige wetsvoorstel niet is terug te vinden.
7.	**NADERE TOELICHTING**	Arthur's Legal is graag bereid de voorgaande opmerkingen en aanbevelingen desgewenst toe te lichten.

Arthur's Legal, Amsterdam v20150901 / WIV