INTERNETCONSULTATIE
DATARETENTIE

Status per 20141230

1.	**INLEIDING / HISTORIE**	Dataretentie gaat over een belangrijk onderdeel van de data life cycle. Uit de voorgeschiedenis van de Europese dataretentie blijkt dat een maand na de terroristische aanslagen van 11 september 2001 ('9/11') de behoefte naar het uitbreiden van opsporingsbevoegdheden binnen Europa is versterkt. De brief van toenmalig President George W. Bush aan de Europese Commissie droeg uiteindelijk bij aan de expliciete grondslag voor dataretentie en de totstandkoming van Europese richtlijn 2006/24/EG ('*Dataretentierichtlijn*'). '9/11' heeft ook invloed gehad 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. Ondanks dat deze maatregelen van tijdelijke aard diende te zijn, is de richtlijn laat geïmplementeerd en na verloop van tijd nooit meer geëvalueerd en ingeperkt, met als resultaat; klokkenluider Snowden. De praktijk van het over en weer uitwisselen van data met buitenlandse opsporingsinstanties via de afspraken onder Mutual Legal Assistance Treaty ('MLAT') versterken de gerezen inbreuken op privacy, en de daardoor ontstane, grote maatschappelijke zorgen. In de Verenigde Staten heeft Obama in de zomer van 2014, naar aanleiding van Snowden een onafhankelijk comité ingeschakeld, dat heeft onderzocht in hoeverre het post-9/11 staatsveiligheidbeleid zich verhoudt tot de Amerikaanse en universele grondrechten. Een groot deel van de aanbevelingen in het rapport over verbetering in de drempel van het verzamelen van data, verbetering van de gerechtelijke toetsing van verzoeken, minimalisatie van data, duur van dataretentie en transparantie is begin 2014 al doorgevoerd en wet- en regelgeving. In Europa is de Dataretentierichtlijn en daarop gebaseerde c.q. daaraan gerelateerde nationale wet- en regelgeving, ondanks de Snowden onthullingen echter (nog) niet aangepast. 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 gewaarborgde grondrechten, 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).
2.	**TOETSING HOF VAN JUSTITIE**	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)
3.	**DOEL WETSWIJZIGING**	De door het Hof van Justitie nietig verklaarde bepalingen van de voormalige richtlijn dataretentie, zijn destijds omgezet in Nederlandse wetgeving. De toetsing van deze wettelijke bepalingen aan het Handvest leidt tot de conclusie dat deze nationale wetgeving moet worden aangepast.
4.	**CONCEPT WETSWIJZIGING**	Naar aanleiding van de uitspraak van het Hof van Justitie, stelt de minister voor om (i) de toets voorafgaand aan de toegang tot gegevens iets te verzwaren en (ii) de bewaartermijnen te verkorten: (i) **Toegang** tot de telecommunicatiegegevens in het kader van strafrechtelijk onderzoek krijgt de officier van justitie pas na toestemming van de Rechter Commissaris. Daarnaast krijgt het Agentschap Telecom nieuwe toezichts- en handhavingsbevoegdheden. Voor toegang tot telecommunicatiegegevens in het kader van de 'nationale veiligheid', blijft de minister als enige bevoegd. (ii) Telefoniegegevens kunnen alleen de volle **bewaartermijn** van twaalf maanden worden geraadpleegd, in geval van een ernstig misdrijf. Bij lagere straffen geldt een termijn van 6 maanden. De regels voor toegang tot internetgegevens blijven hetzelfde, namelijk 6 maanden. Hiermee houdt het wetsvoorstel massaal vast aan het kunnen verzamelen van alle soorten gegevens van alle burgers. Kort gezegd komt het gebruik van telecommunicatiegegevens door opsporingsinstanties neer op **vier stadia: (a) beschikbaarheid, (b) toegang, (c) dataretentie en (d) het gebruik**. Deze stadia worden ook wel 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, 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. Ons kantoor, Arthur's Legal is een van de experts van voornoemde Drafting Group, en is mede-auteur van voornoemde Guidelines en ISO/IEC normen. Wat betreft die Data Life Cycle: (a) Aan de verplichte **beschikbaarheid** van het telecommunicatieverkeer met betrekking tot alle gebruikers wordt bijna niks veranderd. Hiermee blijven Telecomproviders verplicht tot het verzamelen van gegevens van alle burgers. Het hof van Justitie heeft hierover geen bezwaren aangegeven met het oog op de veiligheid en het belang van terrorisme bestrijding. Wel geeft het Hof aan dat de categorieën van de data nauwkeurig moeten worden omschreven. (b) De **toegang** tot informatie dient volgens het Hof te worden onderworpen aan een onafhankelijke toets. De wetgever heeft met betrekking tot het strafrechtelijk onderzoek het Agentschap Telecom hiervoor aangewezen, echter deze toezichthouder is niet onafhankelijk en geldt niet voor dreiging in het kader van de 'nationale veiligheid.' (c) Wat betreft **dataretentie** worden met de wetswijziging de termijnen iets aangepast. Echter dit is niet voldoende. Er dient een onderscheid te worden gemaakt tussen noodzakelijke/relevante informatie, oftewel en minimum vereiste. Dit minimumvereiste dient wederom te worden getoetst door een onafhankelijke gerechtelijke instantie. (d) **Het gebruik** van de data wordt verder niet aangepast. Dit is momenteel geregeld in de Politiewet. Daarbij blijkt uit onderzoek dat daar 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. Dit doet af aan het belang van transparantie.
5.	**CONCLUSIE**	De doelstelling van de wetswijziging zou een balans moeten zijn tussen (i) de dataretentie voor aanbieders, (ii) de toegangsbevoegdheden van opsporingsdiensten en (iii) het recht op privacy en openbaarheid. Deze doelstelling wordt echter niet gehaald. De thans voorliggende wetswijziging toetsend aan de vastgestelde normen van het Europese Hof leidt tot de conclusie dat de artikelen in de wetswijziging (i) de lading van de uitspraak van het Hof niet dekken, (ii) niet objectief genoeg zijn, en (iii) onvoldoende het primaire doel – privacy van de personen – dienen. Zo blijft voor toegang tot telecommunicatiegegevens 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. Het voorstel om het Agentschap Telecom toezichtsbevoegdheden te

		geven, kan niet worden gezien als een zodanige onafhankelijke instantie, maar eerder als een slager die zijn eigen vlees keurt. De toegang tot informatie dient van geval tot geval bekeken te worden en alleen strikt noodzakelijk na een onafhankelijke rechterlijke toets verleend te worden. Daarnaast dient de verzameling van data beperkt te worden tot een minimum voor een duidelijk en nauwkeurig omschreven doel, en de verzamelde gegevens dienen zo snel mogelijk vernietigd te worden.
6.	**BEST PRACTICE**	Kijkend naar een oplossing zijn er in omringende landen al verschillende best practices onderzocht, ontwikkeld en getest om dergelijke objectieve criteria op te stellen. Zo zijn bijna alle 64 aanbevelingen uit het eerder vermelde rapport van de Review Group on Intelligence and Communications Technologies inmiddels door president Obama overgenomen en doorgevoerd. Hierdoor zijn onder meer de betreffende rechters beter uitgerust om de verzoeken deskundig toetsen, inclusief kennisneming van de contra-argumenten waarom bepaalde verzoeken zouden moeten worden geweigerd c.q. beperkt of geconditioneerd. Daarnaast is de Europese Commissie flink bezig met het standaardiseren van Data Life Cycles, zoals hierboven al kort aangestipt. Voorbeelden als NIST, ISO/IEC, en de Cloud Service Level Agreement Standardisation Guidelines van de Europese Commissie zijn hiervoor een mooi uitgangspunt.