Bijdrage Consultatie bij WGK012972[1]

Wetsvoorstel verwerking persoonsgegevens in het kader van coördinatie en analyse terrorismebestrijding en nationale veiligheid

Status per 20210629

a. Arthur's Legal, Strategies & Systems waardeert de werkzaamheden van Rijksoverheid, relevante ministeries en andere overheidsorganisaties, en wat betreft dit voorstel in het bijzonder het ministerie van JeV, om Nederland veilig te houden en terrorisme te bestrijden. De goede en verantwoorde uitvoering van de taken en bevoegdheden maakt een essentieel onderdeel uit van de Nederlandse maatschappij, waaronder mede begrepen onze rechtstaat en de rechtsorde van de Europese Unie, NAVO, onze bondgenoten en andere internationale vrienden.

   We waarderen ook dat het bepaald geen makkelijke taken zijn, en dat er een constante leercurve plaatsvindt en dient plaats te vinden, ook vanwege de dynamiek van de 21ste eeuw. Sinds jaar en dag ondersteunen we daarbij, waarbij we kijken naar alle diverse relevante perspectieven en belangen, met het doel om tot een werkbare, transparante, toetsbare en toekomstbestendige werkmethoden en andere -processen te komen.

b. Mede door de essentiële rol van de overheid als vertrouwde en betrouwbare publieke organisatie om de aan haar door de Nederlandse burgers toevertrouwde taken en bevoegdheden uit te voeren namens en voor Nederland is het zaak om die taken, bevoegdheden en bijbehorende stappen, betrokkenen, informatie en processen zo duidelijk mogelijk te formuleren, ontwerpen, voor te bereiden, uitlegbaar te maken, uit te voeren, te monitoren, en continue tegen het licht te houden, te laten toetsen door onafhankelijke organen, te verbeteren en actueel te houden.

   De huidige structuur, strekking en inhoud van het wetsvoorstel verwerking persoonsgegevens in het kader van coördinatie en analyse terrorismebestrijding en nationale veiligheid ('Wetsvoorstel') voldoet daar nog niet aan.

c. Zonder de diverse life cycles voor, tijdens en na (in onderhavig Wetvoorstel genoemde) analyse- of coördinatietaken (hierna gezamenlijk: 'operatie') – van welk type of met welke impact dan ook – transparant, uitlegbaar en toetsbaar te maken en te houden, zal het moeilijk zijn om het gewenste niveau van vertrouwen en betrouwbaarheid te krijgen – en behouden – van de Nederlandse bevolking en andere essentiële deelgenoten van maatschappij, waaronder ook begrepen de wetgevende macht, beroepsbevolking, economie en NGO's.

d. Als dit echter wèl lukt, dan is dat niet alleen goed voor het vertrouwen binnen Nederland, maar ook voor het vertrouwen in Nederland, en betrouwbaarheid van Nederland. Een duidelijke en betrouwbare rule of law is van grote waarde, en genereert onder meer ook economische en andere relevante aantrekkingskracht en vestigingsklimaatvoordelen boven andere landen.

Wetsvoorstel

e. Het Wetvoorstel strekt er vooral toe om een wettelijke grondslag in de zin van de AVG/UAVG (gezamenlijk: 'AVG') te bewerkstelligen voor het mogen verwerken van (bijzondere en andere) persoonsgegevens.

[1] KetenID WGK012972: Voorstel verwerking persoonsgegevens in het kader van coördinatie en analyse terrorismebestrijding en nationale veiligheid | Overheid.nl | Wetgevingskalender

f. Dat is evident één van de verplichte stappen onder de AVG, maar niet de enige. Andersgezegd, een wettelijke grondslag geeft geen vrijbrief om persoonsgegevens van welke aard dan ook te mogen verzamelen, gebruiken, delen of anderszins te verwerken.

g. Zowel voorafgaande aan het bepalen van een wettelijke grondslag moeten zowel de relevante persoonsgegevens als ook de relevante actoren/belanghebbende worden geïdenficeerd; die focus is essentieel. Nadat die is geduid en vastgelegd, en de wettelijke grondslag (bijvoorbeeld de beoogd-voortvloeiend uit onderhavig Wetsvoorstel) te bepaald dienen de vervolgstappen conform AVG worden bepaald en vastgelegd – per situatie – waaronder mede begrepen:

   A. het speficieke Gerechtvaardigd Doel (generiek zoals in artikel 5 van het huidige Wetsvoorstel bedoeld lijkt te zijn, inclusief de koppelingen, is niet toegestaan),
   B. Data Minimalisatie – zoveel als nodig doch zo weinig als mogelijk, en dat continu heroverwogen en nader beperkt (en voor het overige permanent verwijderd) tijdens enige relevante retentie, waarbij de in het Wetsvoorstel genoemde termijn van 5 jaar praktisch altijd veel te lang is (soms zal het minder dan 24 uur zijn) –,
   C. Data Life Cycles: voor zover toegestaan, per verwerking: verzamelen, afleiden, beschikbaarheid, toegang, gebruiken, delen, dataretentie en verwijderen, èn;
   D. Verantwoorde Verwerking, inclusief doch niet beperkt tot proportionaliteit, subsidiariteit en verantwoorde gegevensbescherming.

   Een en ander moet conform de AVG vooraf duidelijk zijn en worden vastgesteld, en onder meer ook per proces, actualisatie of andere wijziging impact assessments uitgevoerd worden. Een en ander is anders ook niet toetsbaar – ook niet ex tunc -.

h. Het gaat hier te ver om de AVG verder uit te leggen, maar onderhavig Wetsvoorstel schiet te kort in het benoemen van de diverse stappen en overwegingen, hoe men voornemens is die te duiden en wie en hoe daar toezicht op gaat houden.

i. Los van het feit dat de AVG integraal en onvoorwaardelijk ook van toepassing is op het handelen en nalaten van de overheid, kan het verder in het kader van vertrouwen in de overheid immers niet zo zijn dat dergelijke belangrijke taken van ministerie JenV niet helder zijn, of dat de maatschappij moet wachten totdat er iets fout gaat met de verwerking van persoonsgegevens van Nederlandse of andere burgers. Daarbij is opgemerkt dat de Autoriteit Persoonsgegevens direct afhankelijk is van de gelden van dit ministerie, hetgeen kan duiden op een toezichthouder die niet assertief en anderszins strikt AVG toezicht zal willen houden op het handelen van haar broodheer. Onafhankelijke toezicht en toetsing, ex ante en ex tunc, is essentieel voor het opbouwen en houden van vertrouwen door de maatschappij, burgers en andere belanghebbenden.

Inspiratiebronnen

j. Een belangrijke inspiratiebron voor het evidente probleem dat onderhavig Wetsvoorstel tracht te adresseren is de Wet op de Inlichtingen- en Veiligheidsdiensten 2017 ('Wiv 2017') inclusief het toezichtmechanisme, de diverse verslaggevingen van CTIVD, en het Evaluatierapport Wet op de Inlichtingen- en Veiligheidsdiensten 2007 d.d. 20 januari 2021, met aantekening dat de regering heeft bevestigd alle aanbevelingen daarin door gaan te voeren. Zoals terug te lezen in laatstgenoemd rapport hebben wij hier aan bijgedragen, en houden ons graag beschikbaar om in dit en aanverwante domeinen zoals de onderhavige te blijven doen.

k. Een andere belangrijke bron zijn de relevante rapporten van de Inspectie JenV, welke organisatie tegen deels gelijke/gelijksoortige uitdagingen aanloopt zoals bijvoorbeeld onlangs gepubliceerd in haar verslag[2] toezicht wettelijke hackbevoegdheden politie 2019 d.d. 20 augustus 2020, en haar bijlagen.

[2] https://www.rijksoverheid.nl/documenten/rapporten/2020/08/20/tk-bijlage-verslag-toezicht-wettelijke-hackbevoegdheid-politie-2019

l. Verder attenderen we op de publicatie d.d. 12 december 2013 van onafhankelijk comité Clarke dat, Post-Snowden, op verzoek van President Obama heeft onderzocht in hoeverre het post-9/11 staatsveiligheidsbeleid zich verhoudt tot de Amerikaanse en universele grondrechten. De aanbevelingen in het rapport Liberty and Security in a Changing World[3] 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 zijn daarna grotendeels doorgevoerd in wet- en regelgeving. De aanbevelingen zijn voor onderhavig Wetsvoorstel zeer aan te raden de revue te laten passeren en serieus in overweging te nemen, want ze zijn nog steeds zeer actueel en relevant.

m. Voorts attenderen we hierdoor op het alom bekende arrest d.d. 8 april 2014 van het Europese Hof van Justitie[4] waarin de Europese Dataretentierichtlijn ongeldig werd verklaard omdat die onvoldoende waarborgen gaf 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).

In dat arrest geeft het Europese Hof verder een aantal fundamentele handvatten die we als essentiële aanbevelingen willen meegeven aan onderhavige wetgever, zodat gerelateerde intenties, regels, inrichting, uitvoering, toezicht en processen op z'n minst voldoen aan die fundamentele beginselen. Immers, ook de volgende keer zal het Europese Hof in voorkomende geval een wet – inclusief onderhavig Wetsvoorstel – daarop gaan toetsen.

n. Ten slotte attenderen we graag op een recent boek genaamd 'The Dragons and the Snakes' (How the Rest Learned to Fight the West), van David Kilcullen, welke niet alleen een goed beeld geeft over het recente verleden maar ook duidelijke inzichten geeft in waar de diverse relevante – steeds meer convergerende – domeinen zijn c.q. naar toe gaan. De targets worden verder ook al enige tijd verruimd van terrorisme naar andere bijvoorbeeld omvangrijke ondermijning, concentratierisico's, diefstal van bedrijfsgeheimen en intellectuele eigendomsrechten en het delen van desinformatie, welke in vele gevallen en sectoren de nationale veiligheid in gevaar brengen. Hoe dan ook: onderhavig Wetsvoorstel moet immers zo toekomstbestendig als mogelijk zijn.

Balans & Transparantie

o. Het vinden en coördineren van de dynamische balans, per geval, situatie, betrokkenen en beschikbare datasets, en elke zorgvuldig overwogen en gekozen balans transparant en toetsbaar maken, is een complex en dynamisch samenspel van vraagstukken, overlappende spanningsvelden, conflicterende rechten en plichten is, en inzet van technische en organisatorische middelen. Het is niet statisch, en er is geen één oplossing. Het vergt denken en werken als een multi- en interdisciplinair team.

p. Het zou in de lijn der verwachting liggen dat onderhavige wetgever op basis van alle beschikbare OSINT en andere informatie lering trekt en de raamwerken gebruikt om de overlappende en dynamische spanningsvelden beter te kunnen coördineren en zorgen voor een scenario-gebaseerde, risico- en impact-gebaseerde, dynamische doch duidelijke aanpak en verantwoording op gebied van toegang, verzamelen, beheer, getrapte analyse en andere verwerking (als ook de bescherming) van (persoons)gegevens in het kader van de nationale veiligheid.

[3] https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf
[4] http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=nl&mode=lst&dir=&occ=first&part=1&cid=188304

q. In sommige situaties is het heel goed uit te leggen dat – tijdelijke en zo kortstondig mogelijk en ook onder andere voorwaarden – het recht op eerbiediging van de persoonlijke levenssfeer te beperken ter bescherming van de nationale veiligheid. In alle gevallen moet daarbij vanzelfsprekend worden voldaan aan de eisen van legitimiteit, noodzakelijkheid, proportionaliteit en subsidiariteit.

r. Het basisprincipe dat daarbij geldt, is het recht op eerbiediging van de persoonlijke levenssfeer zo snel en zoveel als mogelijk weer integraal moet gelden en kan worden gewaarborgd. Hoe snel en wat wel en niet (en waarom) is per situatie, context en impact te beoordelen, maar kan regulier vooraf al worden voorspeld (en tijdens en achteraf waar nodig worden bijgesteld met behulp van feed-/double-looping). Zo ontstaat een steeds fijnmazige set aan scenario's.

s. Volgens artikel 52 lid 1 van het Europese 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 Europese Hof geeft hiervoor in voornoemd arrest d.d. 8 april 2014 in ieder geval de volgende fundamentele en duidelijke handvatten:

1. Er dient er een verband te bestaan tussen de gegevens die moeten worden bewaard en een bedreiging van de openbare veiligheid. (ro. 59)

2. 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)

3. Het bewaartermijn moet worden verkort en op basis van objectieve criteria worden vastgesteld om proportionaliteit te waarborgen. (ro 64)

4. 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)

5. De toegang tot informatie dient verder (onder meer ook volgens het Europese Hof van Justitie in datzelfde arrest) te worden onderworpen aan een onafhankelijke toets. Een gerechtelijke toetsing dus.

6. 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. Geen enkele wet mag natuurlijk nieuwe dataretentieproblemen veroorzaken. We kunnen wat dat betreft – hoe vreemd dat wellicht ook lijkt – veel leren van het (inmiddels al geruime tijd verbeterde) systeem van gerechtelijk onafhankelijke toetsing en toezicht die in de Verenigde Staten worden toegepast en gehandhaafd.

Dynamische toetsbaarheid

t. Toetsbaarheid vergt overzicht en inzicht. Transparantie dus; vanaf het begin. Als daar voorafgaand aan een operatie geen rekening mee wordt gehouden, is het per saldo onmogelijk later een goed en effectief toezicht te kunnen voeren. Als daar wel vooraf mee rekening is gehouden, is het op termijn mogelijk dat (near)real-time toezicht kan worden gehouden – en waar nodig kan worden bijgestuurd –. Dit vergt vertegenwoordiging van onafhankelijke toezichthouder(s) in de voorfase van (waar mogelijk te categoriseren) operaties zodat – bij ontwerp – rekening kan worden gehouden met randvoorwaarden voor toetsbaarheid, ook tijdens en na een operatie.

u. Dit is geen toekomstmuziek maar reeds nu al mogelijk, wellicht te beginnen bij relatief eenvoudige operaties, en daarna uit te bouwen naar meer complexe operaties. Het is ook noodzakelijk om tot een bruikbare proces trail en daarmee audit trail te komen – en daarmee duurzaam en effectief toezicht als ook double-looping kennis en kunde te bewerkstelligen –. Op deze wijze wordt toetsing op termijn ook minder een eindstation, en minder als een administratieve last gevoeld; het draagt immers bij aan het beter en makkelijker kunnen uitvoeren van de taken van de NCTV en andere relevante diensten.

Continuous Appropriate Dynamic Accountability

v. De artikelen 25 (verwerking) en 32 (bescherming) van de AVG/GDPR zijn niet alleen direct van toepassing op onderhavige Wetvoorstel en taken. Ze beschrijven ook een zeer dynamische en praktische methodiek waaraan respectievelijk kan worden getoetst – hetgeen niet periodiek maar juist permanent dus continue dient te geschieden – of er voldoende en adequate maatregelen zijn getroffen voor dataverwerking c.q. bescherming van de persoonsgegevens. Kort samengevat noemen we dit CADA: Continuous Appropriate Dynamic Accountability.

In het Nederlands, een dwingendrechtelijke methodiek 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 of rechtsregel is en hoe die wordt nageleefd. Het gaat te ver om daar hier dieper op te gaan maar ook hier geldt dat ik natuurlijk van harte bereid ben om een en ander nader toe te lichten.

Tot slot

w. Met de Europese Commissie en stakeholders binnen de Europese Unie uit de private en publieke sectoren als ook universitaire, R&D en andere sectoren organiseert Arthur's Legal, Strategies & Systems al geruime tijd diverse relevante bijeenkomsten. Op een daarvan, op gebied van the 'Nuances of Trust' in cyber-physical en andere IoT ecosystemen en domeinen, waarbij security, privacy, (persoons)gegevensbescherming, digitale sovereiniteit en surveillance maar dus bij uitstek vertrouwen, betrouwbaarheid en balancering van waarden, taken en belangen de hoofdonderwerpen waren, kwamen we op een basisprincipe die door al die partijen is omarmd, en door iedereen – expert of anderszins – direct wordt begrepen:

het principe van geen verrassingen (the Principle of No Surprises).

Niemand houdt van verrassingen, en het is aan ons allen, inclusief Rijksoverheid in het algemeen als ministerie JenV wat betreft onderhavig Wetvoorstel in het bijzonder maar natuurlijk vooral de wetgevende macht, de relevante ministeries en diensten en de toezicht- en toetsingsorganen om te voorkomen dat er verrassingen zijn. Het principe van geen verrassingen is per saldo altijd een beginprincipe en altijd – als toets en validatie – het eindprincipe. Het mag duidelijk zijn dat we daar graag een steentje aan bijdragen. We hopen hiermee van dienst te zijn geweest, en zijn graag tot nadere toelichting en overleg bereid.

Amsterdam, 29 juni 2021 / Arthur's Legal, Strategies & Systems