Reactie Wet plan van aanpak witwassen

Graag reageer ik op het wetsvoorstel met betrekking tot de subsidiariteit van informatie-uitwisseling in het perspectief van de AVG.

Onder "§3. Gegevensbescherming" in de Memorie van Toelichting wordt gesteld dat, ik citeer,

> *"Deze vereisen dat elke inbreuk op de privacy getoetst moet worden op proportionaliteit en subsidiariteit. Daarbij moet de afweging worden gemaakt of de inbreuk zich verhoudt tot het te bereiken doel en of er geen minder ingrijpende manier mogelijk is om hetzelfde doel te bereiken."*

Vervolgens wordt gesteld dat:

> *"Deze meerwaarde* [verkregen door delen van transactiedata, ten behoeve van de effectiviteit van de poortwachtersrol] *is niet op andere, minder ingrijpende manier te bereiken."*

Ik zou u erop willen attenderen dat deze laatste stelling mijns inziens onjuist is, daar ik ervan overtuigd ben dat deze meerwaarde in veel gevallen bereikt kan worden door toepassing van privacy-beschermende technologiëen uit de moderne cryptologie, de zogenaamde *privacy-enhancing technologies* (PETs), en in het bijzonder *secure multiparty computation* (MPC).

Kort gezegd stelt MPC meerdere partijen in staat om berekeningen uit te voeren op hun gezamenlijke dataset, zonder deze data als klare tekst met elkaar te delen. Als voorbeeld kan deze berekening een fraude-detectie "rule" zijn, die betrekking heeft op rekeningen van een klant bij verschillende banken.

Het doemscenario bij het "initiatief Transactie Monitoring Nederland" is een datalek waarbij transacties van alle banken in één keer vrijkomen ("op straat komen te liggen"). Inzet van MPC (of een andere PET) zou dit risico kunnen mitigeren.

De Britse financiële toezichthouder, de FCA, heeft in 2019 een succesvolle *TechSprint* georganiseerd over het toepassen van PETs inzake de Anti-Money Laundering problematiek. U vindt een link naar deze *TechSprint* onderaan deze memo.
Tevens verwijs ik u graag naar een recent rapport van de Verenigde Naties, waarin het toepassen van PETs wordt aanbevolen, en verschillende privacy-beschermende technologieën in detail worden besproken.

Ik vraag u derhalve om te overwegen om, waar mogelijk (technisch en organisatorisch), het gebruik van privacy-beschermende technologie verplicht te stellen. U zou bijvoorbeeld in Artikel 34b uit het wetsvoorstel een bepaling in de geest van onderstaande formulering op kunnen nemen:

> *Het delen van transacties in klare tekst (onversleuteld of zonder toepassing van secret-sharing) is louter toegestaan wanneer het beoogde doel niet kan worden bereikt door middel van het toepassen van privacy enhancing technologies (PETs) en/of secure computation-technieken, waarmee o.a. secure multiparty computation en homomorfische encryptie worden bedoeld.*

Link: FCA 2019 Global AML and Financial Crime TechSprint
https://www.fca.org.uk/events/techsprints/2019-global-aml-and-financial-crime-techsprint

Link: Verenigde Naties, BigDataUN Global Working Group, *UN Privacy Preserving Techniques Handbook*
https://marketplace.officialstatistics.org/privacy-preserving-techniques-handbook