aan	Ministerie van Financiën via https://www.internetconsultatie.nl/rapportagehypotheekmarkt/b1 en https://www.internetconsultatie.nl/toezichtsondersteunenderapportageafm/b1
uw kenmerk	
ons kenmerk	SPF20240627
datum	27 juni 2024
onderwerp	Consultaties ministerie van Financiën: • Wet rapportage hypotheekmarkt DNB https://www.internetconsultatie.nl/rapportagehypotheekmarkt/b1 • Wet toezichtondersteunende rapportage AFM https://www.internetconsultatie.nl/toezichtsondersteunenderapportageafm/b1

Geachte heer/mevrouw,

Stichting Privacy First maakt hierbij graag gebruik van de mogelijkheid om haar visie te geven op de twee consultatievoorstellen die het mogelijk moeten maken voor De Nederlandsche Bank (DNB) en de Autoriteit Financiële Markten (AFM), hierna ook 'de financiële toezichthouders', om op grote schaal van financiële instellingen afkomstige persoonsgegevens te verwerken.[1] Aan beide consultaties wordt deelgenomen door middel van dit document.

Privacy First neemt deel aan de consultaties vanwege de focus van onze organisatie op financiële privacy. Wij constateren dat de bescherming van de financiële persoonsgegevens van Nederlandse burgers gevaar loopt vanwege allerlei ontwikkelingen die bevorderen dat een grootschalige verspreiding van die gegevens plaatsvindt. Eén van die ontwikkelingen is dat de overheid in toenemende mate - soms zonder wettelijke grondslag - op grote schaal persoonsgegevens van burgers verwerkt en analyseert.

[1] De rapportage die financiële instellingen onder het DNB consultatievoorstel moeten verstrekken, betreft weliswaar een rapportage aan de centrale bank afdeling van DNB. Privacy First wijst er echter op dat deze data op grond van de Bankwet vervolgens gedeeld kunnen worden met de toezichtafdelingen van DNB.

Stichting Privacy First
Nieuwe Herengracht 49
1011 RN Amsterdam
https://privacyfirst.nl
info@privacyfirst.nl
+31 20 810 0297
KvK 34298157
ANBI erkend

De consultatievoorstellen raken alle Nederlanders. Immers, in Nederland beleggen ruim twee miljoen huishoudens, ruim drie miljoen huishoudens hebben een hypotheek en ongeveer acht miljoen Nederlanders hebben een consumptief krediet. Nagenoeg alle Nederlanders hebben een bankrekening, een verzekering of een ander financieel product. In de geconsulteerde voorstellen wordt voorgesteld dat DNB en AFM van banken, verzekeraars en andere financiële instellingen privégegevens van Nederlandse burgers zullen ontvangen. Daarmee zouden deze toezichthouders analyses kunnen maken, inzicht in de markt kunnen krijgen en beter toezicht kunnen houden, zo veronderstelt uw ministerie.

Inhoudsopgave

Inleiding 3

Behoefte aan persoonsgegevens - *machine learning* 3

'Politiek moet in actie komen om burgers te beschermen tegen uitdijende datahonger' 4

Grondrechtentoetsing 7

Carte blanche voor de financiële toezichthouders: uitwerking rapportageplicht in AMvB 8

Koppeling aan andere datasets 9

Gegevensverschaffing aan derden 9

Toezicht op gegevensverwerking door AFM en DNB 10

Tot slot 11

Inleiding

Banken, verzekeraars en andere financiële instellingen vervullen een nutsfunctie in onze maatschappij. Zij bieden essentiële producten aan, waar burgers niet omheen kunnen. Zonder deze producten, bijvoorbeeld een WA-verzekering of een betaalrekening, kunnen burgers niet volwaardig deelnemen aan de maatschappij. Burgers moeten erop kunnen vertrouwen dat hun privacy bij hun bank gewaarborgd is en dat de overheid hun privacy niet stelselmatig schendt door aan de achterdeur bij banken stelselmatig hun data op te vragen en die data vervolgens met elkaar en andere nationale en internationale overheidsinstanties te delen. Dit zou het wettelijke grondrecht op gegevensbescherming tot een dode letter maken.

Op dit moment hebben veel overheidsinstanties al toegang tot bankrekeninggegevens van Nederlanders, bijvoorbeeld via het Verwijzingsportaal Bankgegevens.

DNB en AFM beschikken uit hoofde van hun huidige activiteiten al over veel persoonsgegevens en zouden door middel van de geconsulteerde voorstellen nog meer persoonsgegevens verkrijgen. Dit hoort alleen te gebeuren nadat een behoorlijke grondrechtenafweging heeft plaatsgevonden.

Behoefte aan persoonsgegevens – *machine learning*

Privacy First constateert dat zowel in het financiële toezicht als bij private ondernemingen in de financiële sector een grenzeloze behoefte aan persoonsgegevens is, vanwege het vermeende nut voor hun activiteiten. De persoonsgegevens worden gebruikt om kunstmatige intelligentie (*artificial intelligence*, AI) te trainen (*machine learning*).

In het financiële toezicht wordt door internationale organisaties de grootschalige verwerking van persoonsgegevens bepleit, een voorbeeld daarvan is de *Bank for International Settlements* (BIS), die een paper publiceerde[2] waarin de auteur in de samenvatting constateert dat persoonsgegevens (*'granular data'*, granulaire data) nodig

[2] *Peering through the hype – assessing suptech tools' transition from experimentation to supervision*, FSI Insights on policy implementation No 58, juni 2024.

zouden zijn voor het financiële toezicht:

> *Critical suptech tools leverage granular data. Financial authorities that have collected granular data historically are able to develop tools that make it more efficient to organise, interrogate and analyse these data. This in turn makes it easier to extract useful insights from them. Hence, it is important for financial authorities to enhance their data collection practices first before pursuing the benefits of data analytics tools.*

De auteur concludeert: "*Availability of granular data is key*" , en elders: "*Suptech tools need good-quality granular data*" , en geeft daarmee de heersende gedachte weer.

'Politiek moet in actie komen om burgers te beschermen tegen uitdijende datahonger'

Privacy First is van mening dat uitermate voorzichtig moet worden omgegaan met deze behoefte aan persoonsgegevens en andere granulaire data en brengt het advies van de Raad voor het Openbaar Bestuur (ROB) van mei 2021 in herinnering, bekendgemaakt via het nieuwsbericht '*Politiek moet in actie komen om burgers te beschermen tegen uitdijende datahonger*'.[3] In het advies '*Sturen of gestuurd worden?*'[4] wijst de Raad voor het Openbaar Bestuur volksvertegenwoordigers en bestuurders, maar ook de ambtenaren die hen ondersteunen, op de dringende noodzaak om de legitimiteit van sturen met data te waarborgen.

Een volwassen afweging zoals door de ROB bepleit ontbreekt in beide geconsulteerde voorstellen.

[3] https://www.raadopenbaarbestuur.nl/actueel/nieuws/2021/05/25/politiek-kom-in-actie-om-burgers-te-beschermen-tegen-uitdijende-datahonger

[4] https://www.raadopenbaarbestuur.nl/documenten/publicaties/2021/05/25/advies-sturen-of-gestuurd-worden

Daar komt nog bij dat zowel AFM als DNB al op grote schaal granulaire data verwerken, waarvan sommige worden verkregen op grond van de huidige financiële wetgeving en sommige omdat de toezichthouders dat nuttig lijken te vinden. Een voorbeeld daarvan zijn de persoonsgegevens die AFM verwerkt op grond van Mifid 2: weinig beleggers zijn ervan op de hoogte dat de AFM bij *iedere* aandelenkoop of -verkoop paspoortnummers en/of fiscale nummers en geboortedata van de betrokken belegger ontvangt.[5] Voorts ontvangt AFM bijvoorbeeld op grote schaal data van pensioenfondsen, waarin eveneens persoonsgegevens van burgers zijn opgenomen.[6]

DNB ontvangt zeer veel granulaire gegevens in het kader van het door haar uitgevoerde witwasbestrijdingstoezicht. DNB heeft twee jaar geleden bekendgemaakt dat de Bank op grote schaal deze financiële transactiegegevens analyseert:

> *Bij DNB hebben we een outlier detection tool toegepast in Know Your Customer onderzoeken. We hebben het gebruikt om afwijkende transacties te detecteren in een dataset die miljoenen klanten en bankrekeningen en miljarden transacties bevat.*[7] (machinevertaling)

Privacy First vermoedt dat DNB als grondslag voor deze verwerking 'het toezicht op de witwasbestrijding' door financiële instellingen hanteert. Privacy First heeft echter ernstige bedenkingen bij de vraag of de toezichtbepalingen wel een grondslag in de zin van de AVG bieden voor een dergelijk grootschalige, gedigitaliseerde verwerking van de betaalgegevens van miljoenen Nederlanders. De vraag kan worden gesteld of deze verwerking wel in lijn is met de AVG. Burgers zijn in ieder geval onbekend met dit soort grootschalige verwerking van persoonsgegevens door DNB.

---

[5] https://www.esma.europa.eu/sites/default/files/library/esma-2016-1452_guidelines_mifid_ii_transaction_reporting_nl.pdf

[6] https://www.afm.nl/nl-nl/sector/pensioenuitvoerders/datagedreven-toezicht/toezichtrapportage-tweedepijlerpensioenen

[7] Steven Maijoor schreef op linkedin https://www.linkedin.com/posts/stevenmaijoor_how-can-supervisors-use-the-huge-potential-activity-6930955246798020608-UB6J: "*At DNB we applied an outlier detection tool in Know Your Customer examinations. We used it to detect anomalous transactions in a dataset that contains millions of customers and bank accounts and billions of transactions*."

Een ander doel waarvoor DNB op grote schaal persoonsgegevens ontvangt, is de uitvoering van het depositogarantiestelsel. DNB is op grond van de wet weliswaar bevoegd voor deze taak het BSN van alle Nederlanders bij banken op te vragen, maar DNB lijkt veel verder te gaan dan dat en bijvoorbeeld ook alle adressen en mobiele nummers van burgers op te vragen.[8] Ook hier kan de vraag naar de grondslag worden gesteld.

Voorts nemen zowel DNB als AFM op grote schaal granulaire data (microdata) af van het Centraal Bureau voor de Statistiek (CBS). DNB heeft op dit moment de volgende projecten:

- Financiële buffers en kwetsbaarheden Nederlandse huishoudens en hun implicaties;
- Financiële dynamiek in het bedrijfsleven;
- Analyse producentenprijsontwikkelingen;
- Financiële gevolgen ophoging CO2-heffing.

Ook de AFM heeft diverse projecten gebaseerd op microdata van het CBS:

- Identificatie van kwetsbare huishoudens;
- Krediet en kwetsbaarheid.

In het kader van deze projecten kunnen DNB en AFM beschikken over door het CBS aangelegde verzamelingen gedetailleerde persoonsgegevens van iedereen in Nederland. Zij leggen geen maatschappelijke verantwoording af van deze verwerkingen en het is onduidelijk hoe hun taken zich verhouden tot de voorwaarden waaronder die data beschikbaar worden gesteld door het CBS: het verrichten van statistisch of wetenschappelijk onderzoek.[9]

In geen van beide consultatievoorstellen wordt gerept over de huidige verwerking van granulaire gegevens door de beide financiële toezichthouders. Evenmin wordt gerept over de manier waarop de van financiële instellingen verkregen granulaire gegevens intern bij de toezichthouders kunnen worden gekoppeld of zullen worden verrijkt met granulaire gegevens van derde partijen (zoals die verkregen van CBS). Dat is een groot gemis.

[8] https://www.dnb.nl/media/jagnhi1o/dgs-data-delivery-manual-v3-3-december-2022.pdf, zie pagina 14.

[9] https://www.cbs.nl/nl-nl/onze-diensten/maatwerk-en-microdata/microdata-zelf-onderzoek-doen

Aanbeveling Privacy First: voer eerst een diepgaande toetsing uit van de huidige verwerking van granulaire data door de financiële toezichthouders en de wettelijke grondslag voor die verwerkingen, voordat wordt voorgesteld dat zij meer granulaire gegevens uit andere bronnen mogen ontvangen.

Grondrechtentoetsing

Privacy First brengt u in herinnering dat verwerking van persoonsgegevens door overheidsinstanties zoals DNB en AFM een inmenging is door het openbaar gezag in de persoonlijke levenssfeer van burgers, zoals vastgelegd in artikel 10 van de Grondwet, artikel 8 van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM), artikel 17 van het IVBPR en artikel 7 van het Handvest van de grondrechten van de Europese Unie (Handvest). Artikel 8, eerste lid, EVRM bepaalt dat eenieder recht heeft op respect voor zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie. Het tweede lid van dat artikel staat inmenging in dit recht alleen toe voor zover die inmenging bij wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen. Het noodzaakcriterium wordt in de jurisprudentie van het Europese Hof voor de rechten van de mens (EHRM) nader ingevuld met de vereisten van een dringende maatschappelijke behoefte, proportionaliteit en subsidiariteit.

De consultatievoorstellen dienen aan deze beginselen te worden getoetst. Deze toetsing ontbreekt in de consultatievoorstellen.

Volgens de toelichting op beide voorstellen zouden de financiële toezichthouders de granulaire gegevens nodig hebben voor hun taken. Een onderbouwing van de noodzaak voor de uitvoering van de taken, in het licht van de gegevens waarover zij nu al beschikken, is in geen van beide consultatievoorstellen aan te treffen.

Zoals hiervoor al aangestipt, verwerken zowel DNB als AFM granulaire data afkomstig van CBS en beschikken zij over zeer veel gegevens, ook persoonsgegevens, vanwege hun toezichthoudende taken. Voorts is van belang dat zowel CBS als het Centraal Planbureau

(CPB) onderzoek doen naar en rapporteren over de onderwerpen die in de consultatievoorstellen worden genoemd. Zo brengt het CPB jaarlijks de *Risicorapportage Financiële Markten* uit. De meest recente is deze maand bekendgemaakt: de *Risicorapportage Financiële Markten 2024*.[10]

Op zijn minst mag van uw ministerie worden verwacht dat u aangeeft hoe de onderzoeken door en de rapportages van DNB en AFM zich verhouden tot de vele onderzoeken die andere nationale instellingen, zoals CBS en CPB, verrichten.

Privacy First meent dat niet uit de consultatievoorstellen blijkt dat de verwerking een legitiem doel dient en noodzakelijk is. Van een dringende maatschappelijke behoefte dat DNB en AFM persoonsgegevens van burgers verwerken, is niet gebleken. Ook is niet gebleken dat een en ander proportioneel is.

Aanbeveling Privacy First: leg verantwoording af van de huidige verwerking van granulaire gegevens door DNB en AFM en zorg voor een adequate grondrechtentoetsing.

Carte blanche voor de financiële toezichthouders: uitwerking rapportageplicht in AMvB

Op dit moment is nog niet bekend welke persoonsgegevens de financiële toezichthouders zullen gaan opvragen bij financiële instellingen. Immers, dat wordt uitgewerkt in een nog onbekende algemene maatregel van bestuur (AMvB). Privacy First is van mening dat de hiervoor vermelde afweging op het niveau van de wetgeving hoort plaats te vinden en dat het ongewenst is dat de details van de op te vragen persoonsgegevens bij AMvB worden geregeld.

Aanbeveling Privacy First: (als een en ander de grondrechtentoetsing zou doorstaan) geef exact in het wetsvoorstel aan welke granulaire gegevens de financiële instellingen aan de

[10] https://www.rijksoverheid.nl/documenten/rapporten/2024/06/12/publicatie-risicorapportage-financiele-markten-2024

toezichthouders moeten leveren en om welke reden die gegevens nodig zouden zijn. Zonder dat de lijst granulaire data bekend is, is dit wetsvoorstel niet te beoordelen.

Koppeling aan andere datasets

De consultatievoorstellen geven aan dat de van financiële instellingen verkregen gegevens zullen worden gekoppeld aan andere datasets. Niet wordt toegelicht hoe die koppeling zal plaatsvinden, gelet op de pseudonimisering die zal plaatsvinden. Niet wordt toegelicht of koppeling of verrijking met andere datasets leidt tot een risico op heridentificatie.

Aanbeveling Privacy First: (als een en ander de grondrechtentoetsing zou doorstaan) neem in de consultatietoelichting op aan welke datasets de financiële toezichthouders de van financiële instellingen ontvangen gegevens zullen gaan koppelen. Geef voorts aan op welke manier de gegevensbeschermingsrechten van burgers worden gerespecteerd, nu koppeling betekent dat de persoonsgegevens mogelijk leiden tot heridentificatie en/of dat de pseudonimisering bij alle datasets op dezelfde manier zal plaatsvinden.

Gegevensverschaffing aan derden

In het consultatievoorstel inzake DNB wordt voorgesteld dat DNB persoonsgegevens van Nederlandse burgers mag delen met internationale organisaties zoals IMF, FSB en BIS. Ondanks de verzekering dat niet-geanonimiseerde gegevens uitsluitend ten kantore van DNB en dus binnen de digitale omgeving van DNB op de hardware van DNB (on site) met deze internationale organisaties kunnen worden gedeeld, begrijpt Privacy First niet waarom deze organisaties die persoonsgegevens nodig hebben (al dan niet gepseudonimiseerd).

Een behoorlijke toelichting waarom deze gegevensverschaffing nodig zou zijn, ontbreekt geheel.

Aanbeveling Privacy First: (als een en ander de grondrechtentoetsing zou doorstaan) verbiedt de verschaffing van persoonsgegevens aan buitenlandse organisaties, ongeacht of de gegevens gepseudonimiseerd zijn of niet.

Toezicht op gegevensverwerking door AFM en DNB

Op dit moment ontbreekt transparantie over de grootschalige verwerking van granulaire data door AFM en DNB. Als er na een zorgvuldige grondrechtentoetsing voor gekozen zou worden, hoort daarbij dat waarborgen voor de burger worden gecreëerd. Uit rapporten van de Algemene Rekenkamer blijkt dat uw ministerie het toezicht op DNB en AFM maar in zeer beperkte mate handen en voeten geeft.[11] Voorts strekt de wettelijke vrijwaring van AFM en DNB zich ook uit tot fouten bij de verwerking van persoonsgegevens. Als de door AFM en DNB gewenste grootschalige verwerking van persoonsgegevens van burgers de grondrechtentoetsing zou doorstaan, hoort daarbij dat er volwassen waarborgen worden gecreëerd.

Aanbevelingen Privacy First:

- Zorg voor onafhankelijk gegevensverwerkingstoezicht op AFM en DNB.
- Verplicht AFM en DNB tot het jaarlijks laten uitvoeren van onafhankelijke gegevensbeschermingsaudits.
- Verplicht AFM en DNB om publieke verantwoording af te leggen voor hun gegevensverwerkingsactiviteiten.
- Neem in de regelgeving bepalingen op die *function creep* door de financiële toezichthouders tegengaan.
- Hef de wettelijke vrijwaring van AFM en DNB voor fouten op, tenminste voor zover het de verwerking van granulaire data betreft, zodat benadeelden de financiële toezichthouders kunnen aanspreken als daar aanleiding toe is. Maak het voor burgers makkelijk de toezichthouders aan te spreken door hiervoor bijvoorbeeld een laagdrempelig klachtloket te openen.

---

[11] Zie onder meer het bericht Toezicht op banken in Nederland, 27 september 2017, https://www.rekenkamer.nl/publicaties/rapporten/2017/09/27/toezicht-op-banken-in-nederland: "*Het ministerie van Financiën geeft, waar het gaat om het bankentoezicht, beperkt invulling aan zijn rol als toezichthouder op DNB. De invoering van het gemeenschappelijk toezichtmechanisme voor banken heeft ertoe geleid dat rekenkamers belemmeringen ondervinden bij hun onafhankelijke controle van het bankentoezicht. (…) Aan de minister van Financiën bevelen wij aan (…) om vaker en beter invulling te geven aan zijn rol als toezichthouder op DNB waar het om bankentoezicht gaat. Ook bevelen wij de minister aan in Europa een structurele oplossing te vinden voor de belemmeringen die rekenkamers ondervinden bij het onafhankelijke toezicht op het bankentoezicht.*"

Tot slot

Voor nadere informatie of vragen met betrekking tot bovenstaande is Privacy First te allen tijde bereikbaar op telefoonnummer 020-8100279 of per email: info@privacyfirst.nl.

Hoogachtend,
namens Stichting Privacy First,

Vincent Böhre
directeur