

aan Ministerie van Financiën
Via: www.internetconsultatie.nl

uw kenmerk

ons kenmerk SPF20230628B

datum 28 juni 2023

onderwerp Consultatie Wijzigingswet beperking toegang UBO-registers

Geachte heer/mevrouw,

Stichting Privacy First maakt hierbij graag gebruik van de mogelijkheid om haar visie op het consultatievoorstel voor de *Wijzigingswet beperking toegang UBO-registers* (<https://www.internetconsultatie.nl/beperkingtoeganguboregisters/bi>) kenbaar te maken.

Het consultatievoorstel heeft betrekking op wijziging van de Handelsregisterwet 2007 ('Hrw') en de Implementatiewet registratie uiteindelijk belanghebbenden van trusts en soortgelijke juridische constructies ('Trustregisterwet'). Wij geven ook commentaar op enige punten uit de uitwerking van de antiwitwasregelgeving in het Handelsregisterbesluit 2008 ('Hrb'). De Nederlandse regelgeving, onder meer de *Wet ter voorkoming van witwassen en financieren van terrorisme* (Wwft), is gebaseerd op de 4e Europese antiwitwasrichtlijn (Richtlijn (EU) 2015/849), zoals gewijzigd door de 5e Europese antiwitwasrichtlijn (Richtlijn (EU) 2018/843), hierna aan te duiden als 'AMLD4'.

Wij brengen allereerst in herinnering dat het overgrote deel van de mensen die als uiteindelijk belanghebbende (ubo) zijn geregistreerd in het ubo-register nette burgers zijn, die recht hebben op een zorgvuldige omgang met hun persoonsgegevens, in overeenstemming van de principes van de AVG. De Autoriteit Persoonsgegevens heeft in de brief van 28 maart jl.¹ gewaarschuwd voor het via (semi-)openbare registers verspreiden van persoonsgegevens en de daaraan verbonden risico's voor betrokkenen, zoals op fraude, ontvoering, chantage, afpersing, pesterijen, geweld of intimidatie. Wij verzoeken u dat advies te betrekken bij de voorbereiding van het wetsvoorstel en de uitvoeringsregelgeving.

¹ <https://autoriteitpersoonsgegevens.nl/documenten/brief-ap-openbare-registers>

Inleiding

In deze consultatiereactie willen wij de navolgende onderwerpen aan de orde stellen:

- [1] De onwenselijkheid van onbeperkte inzage door alle soorten ondernemingen die onderworpen zijn aan de Wwft, hierna: 'Wwft-plichtigen' (voorstel artikel 22a lid 1 Hrw).
- [2] Het ontbreken van duidelijkheid en waarborgen inzake inzage wegens "legitiem belang" (voorstel artikel 22 lid 5, artikel 22a Hrw).
- [3] Het ontbreken van adequate maatregelen tegen misbruik van ubo-gegevens.
- [4] De wenselijkheid van maatregelen tegen de schadelijke gevolgen voor non-profits van de te ruime ubo-definitie en het ontbreken van vrijstellingen.
- [5] Correctie van de onjuiste implementatie in artikel 51b Hrb van de voorschriften in AMLD4/5 inzake afscherming van de persoonsgegevens van de bedreigde ubo.
- [6] Correctie van artikel 51c Hrb, nu de ubo-gegevens op basis daarvan langer moeten worden bewaard dan door AMLD4 wordt voorgeschreven.

De opmerkingen die wij maken hebben betrekking op wijziging van de bepalingen van de Hrw. In de voorstellen inzake de Trustregisterwet zijn overeenkomstige teksten opgenomen, die wij niet afzonderlijk zullen bespreken en waarop ons commentaar ook van toepassing is.

Daar tekenen wij bij aan dat wij niet zijn overtuigd van het nut van het ubo-register en van het door Wwft-plichtigen op grote schaal verzamelen en up-to-date houden van de persoonsgegevens van de ubo's van hun klanten. Voorts is van belang dat een belangrijk deel van de Wwft-plichtigen niet op integriteit wordt getoetst en er geen enkele zekerheid is dat hun digitale systemen aan de vereisten van de AVG voldoen, aangezien die systemen bij de meeste Wwft-plichtigen evenmin worden getoetst. Het uitwisselen van ubo-gegevens leidt tot zeer grote gegevensbeschermingsrisico's voor ubo's aangezien die uitwisseling meestal zeer onveilig gebeurt, bijvoorbeeld per e-mail.² Voor deze problematiek is tot nu toe onvoldoende aandacht geweest.

Inmiddels is duidelijk geworden dat de concepten van de witwasbestrijding en bestrijding van terrorismefinanciering op zwakke fundamenteen berusten en leiden tot uitsluiting en discriminatie. Voor een toelichting verwijzen wij naar de brief en het memo dat wij op 2

² Voorbeeld is ING Bank, die de ubo-gegevens per e-mail opvraagt en meedeelt dat de gegevens maar beter niet per post verstuurd kunnen worden omdat dat de afhandeling vertraagt.

december 2022 aan de Tweede Kamer hebben gestuurd.³ Dit onderwerp laten wij in deze consultatiereactie verder rusten.

Ons commentaar

Hierna volgt ons commentaar, gerubriceerd per deelonderwerp.

[1] De onwenselijkheid van onbeperkte inzage door alle soorten ondernemingen die onderworpen zijn aan de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft), hierna: 'Wwft-plichtigen' (voorstel artikel 22a lid 1 Hrw)

In veel documenten wordt de indruk gewekt dat de Wwft alleen iets is van banken en andere financiële instellingen ('Fi's'), ondernemingen waarvan de betrouwbaarheid van de beleidsbepalers wordt getoetst en bij wie de IT-systemen worden gescreend. Bij die Fi's gaat ook het een en ander mis op het gebied van gegevensbescherming, maar hopelijk heeft dat voor mensen geen ernstige gevolgen. In ieder geval is er een vorm van toezicht.

Dat is bij de grote groep andere Wwft-plichtigen anders. Wij verwijzen naar onze toelichting gegeven in bijlage 1 bij ons memorandum van 2 december jl., vindplaats via noot 2. Voor zover ons bekend vindt bij geen van deze Wwft-plichtigen (behalve misschien notarissen) enige toetsing van de IT-systemen en de getroffen gegevensbeschermingsmaatregelen plaats. Slechts enkelen van hen kennen betrouwbaarheidstoetsing van beleidsbepalers (trustkantoren).

Wij zijn van mening dat het ongewenst is dat alle Wwft-plichtigen rechtstreekse en ongecontroleerde inzage in het ubo-register verkrijgen.

Daarbij kan worden aangetekend dat uit artikel 30 leden 4, 5 en 6 van de 4e Europese antiwitwasrichtlijn, zoals gewijzigd door de 5e richtlijn⁴, niet volgt dat alle Wwft-plichtigen rechtstreekse toegang dienen te krijgen. Er is slechts voorgeschreven dat zij discrepanties moeten signaleren (lid 4) en dat ze toegang tot informatie over de ubo's dienen te krijgen (lid 5), wat ook via een door de (toekomstige) cliënt verschaft ubo-uittreksel kan plaatsvinden.

Als de toegang door Wwft-plichtigen niet op deze manier zou worden beperkt, is sprake van toegang tot de gegevens voor een zeer grote groep ondernemingen en worden de gegevensbeschermingsrechten van de ubo's ondergraven. Wij menen dat dit in strijd is

³ Te vinden via ons artikel <https://privacyfirst.nl/artikelen/misdaadbestrijding-is-niet-gediend-met-bancair-sleepnet-en-navraagplicht/>.

⁴ <http://data.europa.eu/eli/dir/2015/849/2021-06-30>

met de fundamentele rechtsbeginselen die door het Europese Hof van Justitie in de uitspraak van 22 november 2022 zijn genoemd.

Aanbevelingen:

- De toegang dient te worden beperkt tot die ondernemingen die een toetsing van integriteit en van de IT-systemen kennen. Vermoedelijk zijn dit alleen FI's en notarissen.
- Bij alle overige Wwft-plichtigen kan er mee worden volstaan dat de toekomstige cliënt een uittreksel uit het ubo-register opvraagt en verschaft aan de Wwft-plichtige.

[2] Het ontbreken van duidelijkheid en waarborgen inzake inzage wegens "legitiem belang" (voorstel artikel 22 lid 5, artikel 22a Hrw)

In de huidige digitale samenleving nemen de risico's voor iedere burger dat zijn of haar persoonsgegevens worden gecompromitteerd aanzienlijk toe. Niet voor niets is er een wetsvoorstel ingediend dat doxing strafbaar moet maken.⁵ Dat betekent dat inzage wegens 'legitiem belang' met waarborgen moet worden omgeven en dat moet worden voorkomen dat de persoonsgegevens van ubo's de facto openbaar worden.

Helaas is het concept voor de algemene maatregel van bestuur (amvb) geen onderdeel van de consultatie. Uit de consultatietoelichting maken wij op dat er wordt gedacht aan:

- de pers en maatschappelijke organisaties die zich bezighouden met het voorkomen en bestrijden van witwassen en terrorismefinanciering;
- personen als bedoeld in overweging 30 van de 5e Europese antiwitwasrichtlijn (AMLD5) die een transactie met een entiteit willen aangaan.

Allereerst merken wij op dat het ongewenst is dat de omschrijving wat 'legitiem belang' is in een algemene maatregel van bestuur wordt opgenomen. Dit hoort in de wet thuis, zodat parlementaire controle kan plaats vinden. De praktische uitwerking kan vervolgens in een algemene maatregel van bestuur worden geregeld. (Eigenlijk zou dit onderwerp op Europees niveau dienen te worden geregeld, nu het een beperking is op de gegevensbeschermingsrechten van ubo's.)

Essentieel is dat de toegang tot persoonsgegevens van de ubo op basis van 'legitiem belang' een serieuze bijdrage levert aan de doeleinden van de witwasbestrijdings- en terrorismefinancieringswetgeving, zoals ook door artikel 8 lid 2 van het EU-Handvest wordt

⁵ Wetsvoorstel Strafbbaarstelling gebruik persoonsgegevens voor intimiderende doeleinden, *Kamerstukken* 36171.

geëist (doelbinding). Dit betekent dat een goede onderbouwing van de noodzaak van toegang vereist is.

Daarom achten wij het ongewenst dat alle personen die met een entiteit een transactie willen aangaan de gegevens van de ubo kunnen inzien. In de toelichting wordt verwezen naar de overweging 30 van de 5e antiwitwasrichtlijn, een overweging die betrekking heeft op de algemene openbaarheid van het ubo-register. Uit die passage kan niet worden afgeleid dat degene die een transactie wil aangaan een legitiem belang zou hebben. Bovendien wordt in de consultatietoelichting niet onderbouwd welk misdaadbestedingsbelang gediend wordt door een dergelijke inzage. De facto is het gevolg van het openstellen van het ubo-register voor iedereen die pretendeert een transactie aan te willen gaan, dat het ubo-register alsnog openbaar wordt.

Aanbevelingen:

- De basisregeling inzake legitiem belang dient in de wet te worden opgenomen, waarbij als uitgangspunt geldt dat hergebruik van persoonsgegevens in openbare registers verboden is.⁶
- Het wijzigingsvoorstel voor de amvb waarin de toegang tot het ubo-register nader wordt geregeld dient ter consultatie te worden aangeboden op internetconsultatie.nl.
- Personen die een transactie met een in het Nederlandse ubo-register geregistreerde entiteit willen aangaan, hebben geen legitiem belang bij inzage en dienen geen toegang te verkrijgen tot het ubo-register.

Media en maatschappelijke organisaties

Het is een goede zaak dat mensen van de media en maatschappelijke organisaties zich bezighouden met het onderzoeken van misdaad, wat echter niet betekent dat zij de taken van overheden kunnen overnemen. Het is risicovol voor ubo's als media en maatschappelijke organisaties vrije toegang tot hun persoonsgegevens zouden krijgen zonder te zijn onderworpen aan regels inzake integriteit en zorgvuldigheid.

Overigens veronderstellen wij dat media en maatschappelijke organisaties die onderzoek doen naar misdaad en met het oog daarop persoonsgegevens en andere gegevens verzamelen, zich bezighouden met wat in de *Wet particuliere beveiligingsorganisaties en recherchebureaus* (Wpbr) 'recherchewerkzaamheden' worden genoemd. Zowel bij de media als bij betreffende maatschappelijke organisaties kan worden gezegd dat er recherchewerkzaamheden in opdracht van een derde (de financier van de onderzoeksjournalist / organisatie van onderzoeksjournalisten, respectievelijk de financier

⁶ Zoals aangekondigd in <https://www.digitaleoverheid.nl/nieuws/iedereen-is-en-blijft-baas-over-eigen-persoonsgegevens/>

van de maatschappelijke organisatie) worden verricht, in verband met een eigen (misdaadbestrijdings)belang van die derde, zodat een vergunning op grond van de Wpbr nodig is.

Verzoek:

- Kunt u ons bevestigen dat onderzoeksjournalisten en maatschappelijke organisaties die onderzoek doen naar misdaad en daarbij persoonsgegevens verwerken een vergunning op grond van de Wpbr nodig hebben, en op dit moment – nu zij voor zover wij weten die vergunningen niet hebben – in strijd met de Wpbr handelen? Is dit voor u aanleiding dit te verduidelijken en aan te dringen op naleving van de Wpbr en aanvraag van vergunningen?

Indien de Wpbr niet van toepassing zou zijn

Als de Wpbr niet zou gelden, biedt de uitzondering voor media/maatschappelijke organisaties mogelijkheden voor personen met slechte bedoelingen om zich voor te doen als journalist of relevante maatschappelijke organisatie. Aan inzage dienen eisen te worden verbonden in het belang van de gegevensbescherming van burgers die in overheidsregisters zijn opgenomen. Dit volgt uit de AVG die in dit soort situaties waarborgen eist. Wij zijn van mening dat dit aanleiding is voor integriteits- en zorgvuldigheidseisen.

Aanbeveling / verzoek:

- Toegang tot het ubo-register voor de media en maatschappelijke organisaties dient plaats te vinden op voorwaarde dat betrokkenen voldoen aan integriteits- en zorgvuldigheidseisen en dat wordt getoetst of de gegevensbeschermingsmaatregelen aan de AVG voldoen. Deze vereisten passen goed in de Wpbr.
- Gesteld dat het persoonsgerichte onderzoek door media/maatschappelijke organisaties nu niet onder de Wpbr zou vallen, adviseren wij om de Wpbr aan te passen, zeker nu er plannen voor modernisering zijn⁷ en om te verduidelijken dat deze wet van toepassing is op onderzoeksjournalisten en maatschappelijke organisaties die researchwerkzaamheden ten behoeve van misdaadontdekking respectievelijk – bestrijding verrichten.
- Het is van belang dat de begrippen 'media', 'journalist' en 'maatschappelijke organisaties' zorgvuldig worden gedefinieerd en dat er een procedure tot aanwijzing is met mogelijkheden voor belanghebbenden om bezwaar te maken tegen toegang. Voorts dient te worden onderbouwd dat de keuzes in lijn zijn met EU-regelgeving en

⁷ Zie het jaarverslag JenV van 17 mei 2023, <https://zoek.officielebekendmakingen.nl/kst-36360-VI-1.html>, tussenkopje

'Wet particuliere beveiligingsorganisaties en recherchebureaus (WPBR)'.

rechtspraak.

[3] Het ontbreken van maatregelen tegen misbruik van ubo-gegevens

Anders dan in de toelichting op het consultatievoorstel wordt verondersteld, zijn er onvoldoende maatregelen genomen om de rechten van ubo's op gegevensbescherming te waarborgen. Identificatie en een betaling van een gering bedrag zijn onvoldoende. Voor onze opmerkingen inzake wie inzagerecht heeft wordt verwezen naar wat hiervoor onder [1] en [2] is gezegd. Verder achten wij het van belang dat er extra bestuursrechtelijke en strafrechtelijke waarborgen worden gecreëerd tegen onzorgvuldig gebruik van de ubo-gegevens.

Aanbevelingen:

Wij stellen voor:

- Strafbaarstelling van het verspreiden of anderszins ter beschikking stellen van persoonsgegevens van ubo's, tenzij daarmee een aantoonbaar misdaadbestrijdingsbelang is gediend.
- Verbod op het aanleggen van databases met persoonsgegevens van ubo's en verbod op het aan derden toegang verschaffen tot dergelijke databases.
- Een regeling – in overeenstemming met de AVG (uitspraak EU Hof van Justitie 12 januari 2023, zaak C-154/21, RW/Österreichische Post AG) – dat de ubo het recht heeft om te weten welke personen die niet tot de overheid behoren inzage hebben gehad in zijn/haar persoonsgegevens, zodat de ubo als betrokkene zijn/haar rechten op grond van de AVG kan uitoefenen.

[4] De wenselijkheid van maatregelen tegen de schadelijke gevolgen voor non-profits van de te ruime ubo-definitie en het ontbreken van vrijstellingen

Op dit moment wordt de not-for-profit sector geconfronteerd met het feit dat hun statutair bestuurders in het ubo-register moeten worden ingeschreven als 'uiteindelijk belanghebbende', iets wat bij betrokkenen op veel onbegrip stuit. Een voorbeeld daarvan is de Burgerrechtenvereniging Vrijbit, die op 19 juni jl. schreef over hun bezwaren tegen registratie van hun bestuurders in het ubo-register.⁸ Ook in eerdere artikelen, zoals in *'Stand van zaken actie tegen de verplichte UBO-registratie voor vrijwilligersorganisaties van niet*

⁸ <https://vrijbit.nl/onze-dossiers/dossier-registratie/item/1137-update-drama-ubo-register-sleept-zich-alsnog-voort>

*daadwerkelijk belanghebbenden als fake/pseudo belanghebbenden*⁹ heeft Vrijbit terecht geklaagd over opname in het ubo-register.

Stichtingen en verenigingen met not-for-profit activiteiten moeten hun statutair bestuurders in het ubo-register inschrijven, terwijl die bestuurders geen economisch belang bij de organisatie hebben en die bestuurders al zijn geregistreerd in het handelsregister. Hun registratie als 'uiteindelijk belanghebbende' wekt verwarring bij de buitenwereld (zeker in het buitenland). Privacy First heeft in de totstandkomingsgeschiedenis van de Europese witwasbestrijding geen onderbouwing gevonden van de noodzaak om statutair bestuurders van non-profit organisaties als ubo aan te merken en in het ubo-register op te nemen. Voorts constateert Privacy First dat er landen zijn waarin de ubo-regels niet voor de not-for-profit gelden, een voorbeeld is het Verenigd Koninkrijk waar de regels niet gelden voor *charities*.

Voorts constateren wij dat kleine verenigingen van eigenaars (VvE's), te weten VvE's met vier of minder appartementen, weliswaar niet in het ubo-register hoeven te worden ingeschreven, maar wel geconfronteerd worden met Wwft-plichtigen die hen om de ubo's vragen, terwijl het doel van VvE's niet is om uitkeringen te doen aan de appartementseigenaren, maar om geld bijeen te brengen voor het onderhoud van het gebouw. Gevolg hiervan is dat de persoonsgegevens van appartementseigenaren onnodig worden verspreid, ten eerste doordat de VvE-bestuurder die gegevens moet verwerken (plus bewijsstukken) en ten tweede doordat alle Wwft-plichtigen om die persoonsgegevens vragen. Ons is niet gebleken dat er een misdaadbestedingsbelang is bij de verwerking van persoonsgegevens van appartementseigenaren. Bovendien hebben zij geen recht op uitkering en is hun stemrecht in de vergadering van appartementseigenaren niet relevant.

Aanbevelingen / verzoek:

- Creëer een wettelijke uitzondering voor non-profit stichtingen en verenigingen op de ubo-regels, dus geen opname in het ubo-register en geen verplichting voor Wwft-plichtigen om op zoek te gaan naar de ubo's van deze entiteiten.
- Creëer een wettelijke uitzondering voor VvE's die zich ook uitstrekt tot het cliëntenonderzoek door Wwft-plichtigen.
- Mocht u hier niet voor voelen, dan verzoeken wij u om een gedetailleerde onderbouwing van het belang voor de misdaadbesteding om [a] statutair bestuurders van non-profit stichtingen en verenigingen en [b] appartementseigenaren, als ubo aan te merken. Voorts verzoeken wij u aan te geven hoe wordt voorkomen dat de verkeerde indruk zou

⁹ <https://vrijbit.nl/onze-dossiers/dossier-identificatieplicht/item/1122-stand-van-zaken-actie-tegen-de-verplichte-ubo-registratie-voor-vrijwilligersorganisaties-van-niet-daadwerkelijk-belanghebbenden-als-fake-pseudo-belanghebbenden>

ontstaan dat bestuurders van non-profit stichtingen en verenigingen een economisch belang bij de rechtspersoon hebben.

[5] Correctie is gewenst van de onjuiste implementatie in artikel 51b Hrb van de voorschriften in AMLD4/5 inzake afscherming van de persoonsgegevens van de bedreigde ubo

In artikel 51b lid 2 sub a Hrb heeft alleen de bedreigde ubo die politiebescherming krijgt recht op afscherming van zijn/haar persoonsgegevens. Dat is een te beperkte implementatie van AMLD4, die geen recht doet aan de gegevensbeschermingsbelangen van bedreigde ubo's. In artikel 30 lid 9 en artikel 31 lid 7a AMLD4 is een veel ruimere categorie personen opgenomen. In die bepaling wordt gesproken over het risico dat de ubo door de toegang wordt blootgesteld aan: *"een onevenredig risico, een risico op fraude, ontvoering, chantage, afpersing, pesterijen, geweld of intimidatie"*. Voorts bepaalt AMLD4 dat *"het recht op een bestuurlijke toetsing van het besluit over de uitzondering en op een doeltreffende voorziening in rechte wordt gegarandeerd"* terwijl er geen voorziening is in het Nederlandse recht. Geconcludeerd kan worden dat de huidige wettelijke regeling niet in overeenstemming is met voornoemde bepalingen. Er is geen vrijheid voor Nederland die regeling niet te treffen, aangezien het hier gaat om belangen die door de AVG en het Europese Handvest worden beschermd.

Aanbevelingen:

- Neem op in de wet dat de gegevens van de ubo kunnen worden afgeschermd als sprake is van *"een onevenredig risico, een risico op fraude, ontvoering, chantage, afpersing, pesterijen, geweld of intimidatie"*.
- Regel een heldere en toegankelijke mogelijkheid om beroep te doen op afscherming, inclusief de door AMLD4 vereiste rechtsbescherming.

[6] Correctie is gewenst van artikel 51c Hrb, nu de ubo-gegevens op basis daarvan langer moeten worden bewaard dan door AMLD4 wordt voorgeschreven

In artikel 51c Hrb staat dat de ubo-gegevens moeten kunnen worden ingezien tot tien jaar na uitschrijving van de juridische entiteit uit het handelsregister. Bij entiteiten die lang bestaan heeft dit tot gevolg dat de persoonsgegevens van mensen die bijvoorbeeld twintig jaar geleden ubo waren moeten worden bewaard door het register en kunnen worden ingezien.

Dat volgt niet uit artikelen 30 en 31 AMLD4, waarin is opgenomen dat de ubo-gegevens toegankelijk dienen te zijn gedurende minimaal vijf jaar en maximaal tien jaar nadat de gronden voor registratie van de informatie over de ubo's hebben opgehouden te bestaan.

Een dergelijke regeling is in overeenstemming met de dataminimalisatieprincipes van de AVG en het Europese Handvest.

Aanbeveling:

- Wij adviseren artikel 51c Hrb aan te passen in de zin dat de persoonsgegevens van de ubo beschikbaar blijven tot uiterlijk vijf jaar nadat de grond voor registratie als ubo is opgehouden te bestaan.

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
juridisch adviseur