

Gegevensbeschermingseffectbeoordeling (GEB) met betrekking tot de Wijziging van de Handelsregisterwet 2007 en de Implementatiewet registratie uiteindelijk belanghebbenden van trusts en soortgelijke juridische constructies ter beperking van de toegang tot informatie over uiteindelijk belanghebbenden van vennootschappen en andere juridische entiteiten alsmede van de toegang tot informatie over uiteindelijk belanghebbenden van trusts en soortgelijke juridische constructies (Wijzigingswet beperking toegang UBO-registers)

A. Beschrijving algemene kenmerken gegevensverwerkingen

1. Voorstel

De Wijzigingswet beperking toegang UBO-registers strekt ertoe de regels rondom de toegang tot geregistreerde informatie over de uiteindelijk belanghebbende (in het Engels: ultimate beneficial owner, afgekort UBO) van zowel vennootschappen en andere juridische entiteiten als trusts en soortgelijke juridische constructies aan te passen.

Op 22 november 2022 heeft het Hof van Justitie van de Europese Unie (hierna: het HvJ EU) uitspraak gedaan in een prejudiciële zaak over het Luxemburgse UBO-register.¹ In deze uitspraak wordt een specifiek onderdeel van de gewijzigde Europese anti-witwasrichtlijn² over de openbare toegankelijkheid van het UBO-register ongeldig verklaard. Dit wetsvoorstel zal voorzien in een wijziging van het wettelijk kader voor de verwerking van persoonsgegevens door de Kamer van Koophandel, in het kader van de registratie van de gegevens van uiteindelijk belanghebbenden .

UBO's zijn natuurlijke personen die de uiteindelijke eigenaar zijn van of zeggenschap hebben over een vennootschap of een andere juridische entiteit. Een percentage van eigendom of zeggenschap van 25% geldt daarbij als indicatie. De UBO-informatie zal worden opgenomen in het handelsregister en het UBO-register trusts. Beide registers worden beheerd door de Kamer van Koophandel. De registers waarin UBO-gegevens zijn opgenomen, kenden een openbaar deel – voor een ieder toegankelijk – en een besloten deel, dat slechts voor bevoegde autoriteiten en de Financiële inlichtingen eenheid toegankelijk is. Dit wetsvoorstel ziet op een wijziging van deze toegang. De toegang wordt beperkt tot vier categorieën:

1. Partijen die in het kader van anti-witwasbeleid toegang dienen te hebben op grond van de richtlijn (bevoegde autoriteiten en de FIU, Wwft-instellingen, personen of organisaties die een legitiem belang kunnen aantonen en natuurlijke personen en rechtspersonen voor zover het juridische constructies betreft met een meerderheidsbelang in een buiten de EU opgerichte juridische entiteit.³
2. Partijen die in het kader van de naleving van sancties en het toezicht daarop toegang moeten krijgen (instellingen met een wettelijke verplichting en autoriteiten met een wettelijke taak).
3. Bestuursorganen waarvoor het in verband met een wettelijke of Europeesrechtelijke taak noodzakelijk is dat UBO's worden achterhaald.
4. De entiteiten of trustees voor hun eigen gegevens.

2. Persoonsgegevens

Dit wetsvoorstel brengt geen wijziging in de gegevens die geregistreerd worden in de registers. Op grond van de richtlijn moeten de navolgende gegevens van een UBO worden verwerkt:

- a. achternaam en voornamen;
- b. geboortemaand en -jaar;

¹ HvJ EU 22 november 2022, ECLI:EU:C:2022:912.

² Richtlijn (EU) 2018/843 van het Europees parlement en de Raad van 30 mei 2018 tot wijziging van Richtlijn (EU) 2015/849 inzake de voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld of terrorismefinanciering, en tot wijziging van de Richtlijnen 2009/138/EG en 2013/36/EU (*PbEU* 2018, L 156/43).

³ Deze categorie heeft alleen betrekking op het register met informatie over de uiteindelijk belanghebbenden van trusts en soortgelijke juridische constructies.

- c. nationaliteit;
- d. woonstaat en
- e. aard en omvang van het door de UBO gehouden economisch belang. Dit gegeven betreft het belang (binnen bepaalde bandbreedtes) dat de UBO in een bepaalde onderneming of rechtspersoon heeft.

Naast deze gegevens zal er in het handelsregister aanvullende informatie betreffende de UBO worden opgenomen. De gewijzigde vierde anti-witwasrichtlijn geeft EU-lidstaten, naast bovenstaande UBO-gegevens, de mogelijkheid om aanvullende gegevens betreffende een UBO te registreren. In een eerder stadium heeft Nederland van deze lidstaatoptie gebruik gemaakt. In het onderhavige wetsvoorstel verandert hier niets aan.

De volgende gegevens zijn alleen toegankelijk voor autoriteiten:

- f. geboortedag, -plaats en -land;
- g. adres;
- h. burgerservicenummer (BSN), indien dat is toegekend en, eveneens indien dat is toegekend, het fiscaal identificatienummer (TIN);
- i. informatie betreffende de aard, het nummer alsmede datum en plaats van uitgifte van het document met behulp waarvan de identiteit van de UBO is geverifieerd of een kopie van dat document;
- j. documentatie waarmee wordt onderbouwd waarom een persoon de status van UBO heeft en waarmee de aard en omvang van het door de UBO gehouden economisch belang wordt aangetoond.

Nationaliteit kan, in combinatie met de naam en/of de geboorteplaats, een gegeven zijn waaruit de etnische afkomst van iemand kan blijken. Deze combinatie van persoonsgegevens kan dan ook worden aangemerkt als een bijzonder persoonsgegeven. De (kopie van de) pasfoto op het document als bedoeld onder categorie i. is eveneens aan te merken als een bijzonder persoonsgegeven.

Alle andere genoemde persoonsgegevens vallen in de categorie 'gewoon'. Daarbij dient het navolgende te worden opgemerkt.

De gegevens onder categorie h. zijn persoonsidentificerende nummers, nu het hier wettelijke identificatienummers betreft.

De gegevens onder e en j. kunnen nader worden aangemerkt als 'gevoelige persoonsgegevens', nu dit gegevens zijn betreffende de financiële of economische situatie van betrokkenen. Het gaat hier om informatie over de reden waarom deze persoon kwalificeert als UBO. De gegevens onder e. worden verplicht openbaar, maar zullen alleen worden uitgedrukt in bandbreedtes (in percentages) en niet in bedragen. De gegevens onder j. zijn alleen toegankelijk voor autoriteiten. Deze gegevens bevatten de onderbouwing van de gegevens onder e.

De hierboven genoemde persoonsgegevens hebben alle betrekking op de uiteindelijk belanghebbende en diens gehouden belang.

Een uiteindelijk belanghebbende kan minderjarig of handelingsonbekwaam zijn. Gegevens van minderjarige of handelingsonbekwame UBO's (met uitzondering van de aard en omvang van het door de UBO gehouden economisch belang) kunnen worden afgeschermd indien daartoe een verzoek wordt gedaan. Een dergelijk verzoek kan ook worden ingediend indien een UBO door het beschikbaar maken van diens gegevens blootgesteld wordt aan een onevenredig risico, een risico op fraude, ontvoering, chantage, geweld, pesten of intimidatie.

Er worden geen strafrechtelijke gegevens verwerkt.

3. Gegevensverwerkingen

Vennootschappen en andere juridische entiteiten en trusts en soortgelijke juridische constructies dienen informatie betreffende hun uiteindelijk belanghebbende(n) in te winnen en te registreren in de betreffende UBO-registers.

Vennootschappen en andere juridische entiteiten en trusts en soortgelijke juridische constructies moeten deze UBO-informatie doorgeven aan de Kamer van Koophandel, de beheerder van de UBO-registers. Bepaalde informatie (hierboven categorie a. tot en met e.) is opvraagbaar voor Wwft-instellingen, personen en organisaties die een legitiem belang kunnen aantonen en instellingen in het kader van de naleving van de Sanctiewet 1977, na betaling van een vergoeding. De (aanvullende) UBO-informatie is uitsluitend toegankelijk voor en opvraagbaar door bevoegde autoriteiten en de FIU-Nederland, de aangewezen autoriteiten op grond van de Sanctiewet 1977 en de autoriteiten die op grond van een wet een noodzaak hebben om over UBO-informatie te beschikken en zijn aangewezen.

4. Verwerkingsdoeleinden

Het doel van de gewijzigde vierde anti-witwasrichtlijn is het voorkomen van het gebruik van het financiële stelsel voor het witwassen van geld en het financieren van terrorisme. Dit is eveneens het doel van de registratie van UBO-informatie. Dit doel kwalificeert als een zwaarwegend algemeen belang in de zin van artikel 8, tweede lid, van het EVRM, op grond waarvan een inbreuk op het recht op privacy mogelijk is. Voor het bereiken van dit doel zijn de eerdergenoemde typen persoonsgegevens direct van belang en onontbeerlijk. Accurate en actuele informatie over uiteindelijk belanghebbenden is een belangrijke factor bij het opsporen van criminelen, die hun identiteit achter vennootschappen en andere juridische entiteiten kunnen verbergen. Door deze informatie meer transparant te maken kan misbruik van vennootschappen en andere juridische entiteiten beter worden tegen gegaan. Zodoende wordt het gebruik (misbruik) van het financiële stelsel voor het witwassen van geld of terrorismefinanciering bestreden.

Het Hof van Justitie van de Europese Unie heeft geoordeeld dat toegang tot informatie uit het UBO-register voor een ieder lid van de bevolking niet goed onderbouwd is en dat dit daarom een te grote inbreuk maakt op het recht van privacy. In lijn met deze uitspraak beperkt dit wetsvoorstel toegang tot UBO-informatie. Informatie uit de UBO-registers is derhalve niet meer openbaar toegankelijk voor eenieder.

Allereerst regelt dit wetsvoorstel dat partijen genoemd in de vierde anti-witwasrichtlijn toegang krijgen. Dit zijn bevoegde autoriteiten en de FIU-Nederland, Wwft-instellingen en personen die een legitiem belang kunnen aantonen.

In het kader van hun publieke taakuitoefening hebben de FIU-Nederland en bevoegde autoriteiten die een rol hebben in het kader van het tegengaan van witwassen, onderliggende gronddelicten en het financieren van terrorisme, baat om te weten wie de UBO van een vennootschap, juridische entiteit of trust is. Het is voor hen van belang om ook toegang te hebben tot aanvullende gegevens (hierboven onder f. tot en met j.). De keuze voor deze aanvullende gegevens hangt samen met de inschatting welke informatie de bevoegde autoriteiten en de FIU-Nederland nodig hebben voor de uitvoering van de op hen rustende taken onderscheidenlijk verplichtingen op grond van de richtlijn. De richtlijn biedt de mogelijkheid om deze aanvullende gegevens te registreren.

Bepaalde – bij algemene maatregel van bestuur – aangewezen autoriteiten en de FIU-Nederland krijgen toegang tot aanvullende gegevens die relevant zijn in het kader van hun publieke taakuitoefening. De bevoegde autoriteiten en de FIU-Nederland kennen in dit verband een geheimhoudingsplicht.

In het onderhavige wetsvoorstel wordt tevens toegang geregeld voor Wwft-instellingen. Toegang wordt in dit kader beperkt voor zover de instelling taken verricht uit hoofde van de Wet ter voorkoming van witwassen en het financieren van terrorisme (Wwft). Omdat UBO-informatie niet meer volledig openbaar is, zullen voor raadplegers van de registers strengere toegangseisen

gelden. Identificatie en autorisatie van raadgevers zullen op niveau substantieel vormgegeven worden (e-Herkenning 3 en DigiD Substantieel).

Voor de derde categorie, personen en organisaties die een legitiem belang kunnen aantonen, is in dit wetsvoorstel aangegeven dat dit bij lagere regelgeving vorm zal krijgen. In het kader van die regelgeving zal ook gekeken worden naar consequenties ten aanzien van de verwerking van persoonsgegevens.

De tweede groep partijen die toegang krijgt, zijn partijen die de wettelijke verplichting hebben op grond van de Sanctiewet 1977 om de UBO's van hun cliënten te kennen ten behoeve van de naleving van sancties en het bevriezen van tegoeden, en autoriteiten die op grond van de Sanctiewet 1977 een taak hebben in het kader van de naleving van sancties. Een deel van deze instellingen en autoriteiten valt samen met de bevoegde autoriteiten hierboven genoemd en de Wwft-instellingen.

Voor deze instellingen en autoriteiten geldt dat het van groot belang is voor een goede toepassing van sancties dat zij weten wie achter juridische entiteiten en juridische constructies zitten voor een goede toepassing van sancties en het internationaal recht. Het gaat hierbij om financiële instellingen die verplicht zijn om te waarborgen dat zij op het gebied van de administratieve organisatie en interne controle maatregelen hebben getroffen ter naleving van de sanctieregelgevingen autoriteiten die op grond van de Sanctiewet 1977 belast zijn met het toezicht op de naleving van deze regelgeving. Partijen krijgen slechts voor die specifieke taken toegang tot de informatie in de registers. Net als ten behoeve van de taken in het kader van het voorkomen van witwassen en financieren van terrorisme geldt dan instellingen toegang hebben tot de beperkte set aan gegevens en autoriteiten tot de aanvullende gegevens.

De derde groep betreft bestuursorganen waarvoor het in verband met een wettelijke taak of op basis van Europese regelgeving noodzakelijk is om UBO's te achterhalen. Een voorbeeld van deze regelgeving is de Europese verordening die het herstel en veerkrachtplan regelt. In die verordening is aan lidstaten als voorwaarde voor verstrekking van de middelen opgelegd dat zij informatie over de begunstigen van de middelen en de uiteindelijk belanghebbenden daarvan verzamelen en delen met de Europese Commissie. Alle taken en autoriteiten die hieronder vallen worden specifiek aangewezen bij algemene maatregel van bestuur en daarbij gemotiveerd. Deze autoriteiten krijgen toegang tot alle gegevens in de registers.

Tot slot krijgen ook de entiteiten en constructies zelf toegang tot hun eigen gegevens. Dit enerzijds om te kunnen voldoen aan de plicht om de gegevens van hun UBO's actueel en accuraat te houden en anderzijds om zelf te kunnen verstrekken indien zij dat nodig achten. Een voorbeeld van die laatste situatie is het geval dat de entiteit een zakelijke relatie wil aan gaan en de wederpartij graag inzicht wil in de gegevens van de UBO's. Deze situatie wordt ook genoemd in het arrest van het Hof van Justitie. Besloten is om niet in algemene zin wederpartijen toegang te geven, maar het oordeel over verstrekking aan de betrokken entiteit of constructie te laten of inzage in die gegevens gewenst of noodzakelijk is.

5. Betrokken partijen

De Kamer van Koophandel is op grond van artikel 3, tweede lid, van de Handelsregisterwet 2007 verwerkingsverantwoordelijke voor gegevensverwerking ten behoeve van het handelsregister aangemerkt. De Kamer van Koophandel is dus ook verwerkingsverantwoordelijke voor de in het handelsregister opgenomen UBO-informatie. Ten aanzien van het UBO-register trusts is de minister van Financiën verwerkingsverantwoordelijke ten aanzien van de registratie van gegevens en zijn de minister van Financiën, de minister van Justitie en Veiligheid en de Kamer van Koophandel gezamenlijk verwerkingsverantwoordelijk ten aanzien van het beheer.

In het kader van het opstellen van de UBO-wetgeving zijn de ministeries van Financiën, Justitie en Veiligheid en Economische Zaken en Klimaat gezamenlijk verantwoordelijk voor het opstellen van deze GEB.

Vennootschappen en andere juridische entiteiten en beheerders van trusts en soortgelijke juridische constructies kunnen worden aangemerkt als verstrekkers van UBO-informatie. Zij moeten deze informatie immers verstrekken aan de Kamer van Koophandel.

De gewijzigde vierde anti-witwasrichtlijn verplicht tot het instellen van een terugmeldplicht voor instellingen die onder de werking van de Wwft vallen en voor aangewezen bevoegde autoriteiten. Deze terugmeldplicht houdt in dat Wwft-instellingen en – onder omstandigheden, voor zover dat hun werkzaamheden niet doorkruist – bevoegde autoriteiten verplicht zijn om melding aan de Kamer van Koophandel te doen van iedere discrepantie die zij aantreffen tussen de informatie over uiteindelijk belanghebbenden in de UBO-registers en de informatie over uiteindelijk belanghebbenden waarover zij beschikken. Wwft-instellingen en aangewezen bevoegde autoriteiten kunnen dan ook worden aangemerkt als verstrekkers van informatie aan de Kamer van Koophandel.

Als ontvangers van de persoonsgegevens kunnen worden aangemerkt degenen die de UBO-registers mogen raadplegen voor het verkrijgen van UBO-informatie.

6. Belangen bij de gegevensverwerking

Het belang van de gegevensverwerking is het voorkomen van het gebruik van het financiële stelsel voor het witwassen van geld en het financieren van terrorisme. Andere belangen zijn een goede toepassing van (internationale) sancties en wettelijke verplichtingen voor autoriteiten om UBO-informatie te kennen.

7. Verwerkingslocaties

De voorgenomen gegevensverwerking zal in Nederland plaatsvinden.

8. Technieken en methoden van de gegevensverwerkingen

Er is bij de verwerking van UBO-informatie door de Kamer van Koophandel geen sprake van geautomatiseerde besluitvorming, profilering of big data.

9. Juridisch en beleidsmatig kader

De gewijzigde vierde anti-witwasrichtlijn bevat in hoofdstuk 5 bepalingen inzake het bewaren van gegevens en gegevensbescherming.

In de Wwft is de wettelijke verplichting voor vennootschappen en andere juridische entiteiten opgenomen om UBO-informatie in te winnen en bij te houden over wie hun uiteindelijk belanghebbenden zijn. Vennootschappen en andere juridische entiteiten moeten deze informatie 'in huis' hebben.

In de Handelsregisterwet 2007 is de verplichting opgenomen dat vennootschappen en andere juridische entiteiten hun UBO-informatie moeten registreren in het handelsregister. Het niet 'in huis' hebben van deze informatie, alsmede het niet registreren van deze informatie, is een economisch delict dat strafbaar wordt gesteld in de Wet op de economische delicten. In het Burgerlijk Wetboek wordt een specifieke bepaling voor stichtingen opgenomen.

In de Implementatiewet registratie uiteindelijk belanghebbenden van trusts en soortgelijke juridische constructies is de verplichting opgenomen dat de trustee ten behoeve van registratie in het register langs elektronische weg opgave doet van persoonsgegevens met betrekking tot die trust en de uiteindelijk belanghebbenden daarvan.

Voor het overige zijn de Algemene verordening gegevensbescherming (Avg) en de Uitvoeringswet AVG (Uavg) van toepassing.

10. Bewaartermijnen

UBO-informatie zal gedurende een termijn van 10 jaar na het schrappen van de entiteit uit de registers worden bewaard, overeenkomstig de bepaling hieromtrent in de gewijzigde vierde anti-witwasrichtlijn. De gewijzigde richtlijn bepaalt dat UBO-informatie verplicht minimaal 5 en maximaal 10 jaar na het schrappen van de entiteit uit de registers moet worden bewaard. Het bewaren van UBO-informatie gedurende een termijn van 10 jaar is nodig gelet op het doel waarvoor de UBO-gegevens zijn verzameld en worden gebruikt: het voorkomen van het gebruik van het financieel stelsel voor witwassen of terrorismefinanciering. Voor de bevoegde autoriteiten die betrokken zijn bij de bestrijding van witwassen of terrorismefinanciering – met name de opsporingsinstanties – is het noodzakelijk dat historische gegevens betreffende de uiteindelijk belanghebbende gedurende geruime tijd beschikbaar zijn. Opsporingsonderzoeken richten zich immers tot gebeurtenissen in het verleden. Bij het in kaart brengen van eigendoms- en zeggenschapsstructuren is het dan ook van belang om historische UBO-gegevens te kunnen inzien.

B. Beoordeling rechtmatigheid gegevensverwerkingen

11. Rechtsgrond

De gegevensverwerking op grond van het onderhavige wetsvoorstel vindt plaats als gevolg van de implementatie van de UBO-bepalingen uit de gewijzigde vierde Europese anti-witwasrichtlijn in de Nederlandse wet- en regelgeving (Handelsregisterwet 2007, Implementatiewet registratie uiteindelijk belanghebbenden van trusts en soortgelijke juridische constructies, Wwft, Burgerlijk Wetboek, Wed). Op grond van deze gewijzigde vierde anti-witwasrichtlijn moet elke EU-lidstaat centrale registers opzetten met daarin informatie over uiteindelijk belanghebbenden van vennootschappen en andere juridische entiteiten en trusts en soortgelijke juridische constructies. Met dit wetsvoorstel wordt de toegang tot de informatie in de UBO-registers beperkt tot de categorieën hierboven beschreven.

Voorts is in artikel 43 van de gewijzigde vierde anti-witwasrichtlijn bepaald dat de verwerking van persoonsgegevens op grond van deze richtlijn moet worden beschouwd als een taak van algemeen belang. Immers, accurate en actuele informatie over uiteindelijk belanghebbenden is een belangrijke factor bij het opsporen van criminelen, die hun identiteit achter vennootschappen en andere juridische entiteiten en trusts kunnen verbergen. Door deze informatie meer transparant te maken kan misbruik van vennootschappen en andere juridische entiteiten en trusts beter worden tegen gegaan. Zodoende wordt het gebruik (misbruik) van het financiële stelsel voor het witwassen van geld of terrorismefinanciering bestreden. Dit is een taak van algemeen belang.

Voor sanctieautoriteiten geldt dat het van groot belang is voor een goede toepassing van sancties dat zij weten wie achter juridische entiteiten en juridische constructies zitten voor een goede toepassing van sancties en het internationaal recht.

Om deze redenen is er sprake van de volgende grondslagen:

- i) de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust;
- ii) de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen.

12. Bijzondere persoonsgegevens

Hierboven onder punt 2 staat omschreven dat de Handelsregisterwet 2007 en de Implementatiewet voorzien in de verwerking van bijzondere persoonsgegevens, te weten de nationaliteit (in combinatie met de naam en geboorteplaats), en de foto op het identificatiedocument. Er worden geen strafrechtelijke persoonsgegevens verwerkt.

13. Doelbinding

In artikel 41, tweede lid, van de gewijzigde vierde anti-witwasrichtlijn komt het beginsel van doelbinding tot uitdrukking. Op grond van dit artikel kunnen persoonsgegevens alleen worden verwerkt met het oog op het voorkomen van witwassen en financieren van terrorisme.

Persoonsgegevens mogen niet verder worden verwerkt op een manier die niet verenigbaar is met dat doel. De gewijzigde vierde anti-witwasrichtlijn specificeert dat commerciële doelen in elk geval niet met dit doel verenigbaar zijn. Dit beginsel is in de Wwft geïmplementeerd in artikel 34a.⁴

Persoonsgegevens worden uit hoofde van de Handelsregisterwet 2007 en de Implementatiewet registratie uiteindelijk belanghebbenden van trusts en soortgelijke juridische constructies verwerkt en kunnen alleen voor een ander doel worden verwerkt, indien dat doel verenigbaar is met het doel waarvoor de persoonsgegevens aanvankelijk zijn verzameld: het voorkomen van het gebruik van het financiële stelsel voor het witwassen van geld of financieren van terrorisme.

Een belangrijk element ten aanzien van het begrip legitiem belang is dat er sprake moet zijn van een doelbinding met de doelstellingen uit de anti-witwasrichtlijn. De verzoeker zal moeten aantonen dat activiteiten worden ontplooid in het kader van de doelstellingen van de richtlijn, dus met het voorkomen of bestrijden van witwassen en het financieren van terrorisme, of daarmee verband houdende gronddelicten. De afbakening en toetsing hiervan wordt bij algemene maatregel van bestuur uitgewerkt.

14. Noodzaak en evenredigheid

Op grond van de Uitvoeringswet algemene verordening gegevensverwerking dient de verwerking van persoonsgegevens, waarin dit wetsvoorstel voorziet, noodzakelijk te zijn voor het doeleinde waarvoor de persoonsgegevens worden verwerkt. De verwerkingsdoeleinden staan omschreven in onderdeel 4.

Zoals eerder in deze GEB is aangegeven, verplicht de gewijzigde vierde anti-witwasrichtlijn tot centrale registers van uiteindelijk belanghebbenden van vennootschappen en andere juridische entiteiten en trusts en soortgelijke juridische constructies. Het verplichte deel van de UBO-informatie zal alleen toegankelijk zijn voor Wwft-instellingen, bevoegde autoriteiten en de FIU en personen en organisaties die een legitiem belang kunnen aantonen. De richtlijn biedt daarnaast de mogelijkheid om aanvullende UBO-gegevens te registreren. Van deze mogelijkheid wordt gebruik gemaakt. Deze aanvullende UBO-gegevens zijn alleen raadpleegbaar door specifiek aangewezen bevoegde autoriteiten en de FIU-Nederland.

De gegevens die ingevolge de richtlijn ten minste geregistreerd moeten worden zijn: de naam, de geboortemaand, het geboortjaar, de nationaliteit, de woonstaat en de aard en omvang van het door de uiteindelijk belanghebbende gehouden economische belang.

De aanvullende UBO-gegevens – de geboortedag, de geboorteplaats, het geboorteland, het woonadres, BSN en/of TIN en de onderliggende documentatie waaruit de identiteit van de UBO en de precieze aard en omvang van het door de UBO gehouden economische belang blijkt – zijn uitsluitend toegankelijk voor bevoegde autoriteiten en de FIU-Nederland. De bevoegde autoriteiten en de Financiële inlichtingen eenheid kennen in dit verband een geheimhoudingsplicht. Ditzelfde geldt voor de autoriteiten die belast zijn met het toezicht op de naleving van de Sanctiewet 1977 en autoriteiten die worden aangewezen in verband met een wettelijke taak. Daarbij kunnen in de

⁴ Wetsvoorstel tot wijziging van de Wet ter voorkoming van witwassen en financieren van terrorisme en enige andere wetten in verband met de implementatie van richtlijn (EU) 2015/849 van het Europees Parlement en de Raad van 20 mei 2015 inzake de voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld of terrorismefinanciering, tot wijziging van Verordening (EU) nr. 648/2012 van het Europees Parlement en de Raad en tot intrekking van Richtlijn 2005/60/EG van het Europees Parlement en de Raad en Richtlijn 2006/70/EG van de Commissie (PbEU 2015, L 141), alsmede in verband met de uitvoering van verordening (EU) 2015/847 van het Europees Parlement en de Raad van 20 mei 2015 betreffende bij geldovermakingen te voegen informatie en tot intrekking van Verordening (EG) nr. 1781/2006 (PbEU 2015, L 141) (Implementatiewet vierde anti-witwasrichtlijn)

algemene maatregel van bestuur voorwaarden worden verbonden aan de verstrekking van de gegevens.

De bevoegde autoriteiten en de Financiële inlichtingen eenheid dienen op grond van de richtlijn onbeperkte toegang tot alle gegevens in de registers te krijgen. De bevoegde autoriteiten die toegang krijgen tot alle gegevens betreffende een UBO zijn bij algemene maatregel van bestuur aangewezen. Het betreft hier dus een afgebakende, wettelijk vastgelegde groep:

Wwft-toezichthouders

De Nederlandsche Bank
Autoriteit Financiële Markten
Bureau Financieel Toezicht
Bureau Toezicht Wwft
Kansspelautoriteit
Dekens van de Orde van Advocaten

Financiële Inlichtingen Eenheid (FIU)

Belastingdienst

Opsporingsinstanties

Douane
Dienst Justis
Bureau Bibob
Nationale Politie
Openbaar Ministerie
Algemene inlichtingen- en veiligheidsdienst
Militaire inlichtingen- en veiligheidsdienst
Koninklijke Marechaussee
Fiscale inlichtingen- en opsporingsdienst

Inspecties

Inspectie Sociale Zaken en Werkgelegenheid (ISZW-DO)
Inlichtingen- en opsporingsdienst van de Nederlandse Voedsel- en Warenautoriteit (NVWA-IOD)
Inspectie Leefomgeving en Transport (ILT/IOD)
de Rijksrecherche

Bureau Economische Handhaving

Toegang voor de bevoegde autoriteiten en de FIU-Nederland tot alle UBO-gegevens is relevant voor hun werkzaamheden in het kader van opsporing van strafbare feiten en toezicht. Alleen de bevoegde autoriteiten en de FIU-Nederland kunnen UBO-gegevens, gerangschikt op natuurlijke personen, inzien. De overige afnemers van UBO-informatie (zie hieronder) kunnen niet op natuurlijke personen in de registers zoeken, maar uitsluitend op (de naam van de) vennootschap of juridische entiteit of trust.

Alle overige afnemers die onder de categorie 'toegang op grond van de richtlijn' vallen (dus afnemers anders dan bevoegde autoriteiten en de FIU-Nederland) krijgen alleen toegang tot de openbare UBO-gegevens. Deze categorie 'overige afnemers' kan opgesplitst worden in twee categorieën:

- i) meldingsplichtige instellingen in de zin van de Wwft;
- ii) personen en organisaties die een legitiem belang kunnen aantonen.

Ad i).

Meldingsplichtige instellingen in de zin van de Wwft zijn de poortwachters van het financiële systeem en dienen op grond van de richtlijn toegang te krijgen tot UBO-gegevens. Aan deze groep afnemers wordt uitsluitend toegang gegeven tot deze UBO-gegevens en niet tot de aanvullende gegevens. Inzage in de aanvullende UBO-gegevens, waaronder adresgegevens en BSN en/of TIN, wordt niet gegeven omdat die inzage risico's van bijvoorbeeld identiteitsfraude of kidnaping met zich kan brengen. Toegang tot alleen de openbare set UBO-gegevens is ook in lijn met de verplichting die de richtlijn voorschrijft: Wwft-instellingen mogen zich bij hun cliëntenonderzoek niet uitsluitend verlaten op de UBO-informatie uit het centraal register. Omdat UBO-informatie niet meer volledig openbaar is, zullen voor raadplegers van de registers strengere toegangseisen gelden. Identificatie en autorisatie van raadplegers zullen op niveau substantieel vormgegeven worden (e-Herkenning 3 en DigiD Substantieel).

Ad ii).

Voor de categorie personen en organisaties die een legitiem belang kunnen aantonen, is in dit wetsvoorstel aangegeven dat dit bij lagere regelgeving vorm zal krijgen. In het kader van die regelgeving zal ook gekeken worden naar consequenties ten aanzien van de verwerking van persoonsgegevens.

Tot slot wordt toegang tot UBO-informatie verleend aan autoriteiten die op grond van Sanctieregelgeving moeten weten wie achter juridische entiteiten en juridische constructies zitten. Dit om een goede toepassing van sancties en het internationaal recht te garanderen.

15. Rechten van de betrokkenen

Beschrijf de procedure waarmee invulling wordt gegeven aan de rechten van de betrokkenen. Als de rechten van de betrokkene worden beperkt, beschrijf op grond van welke wettelijke uitzondering dat is toegestaan.

C. Beschrijving en beoordeling risico's voor de betrokkenen

16. Risico's voor betrokkenen

Het onderhavige wetsvoorstel brengt privacyrisico's met zich. Dat wil zeggen: risico's dat het verwerken van persoonsgegevens op grond van dit wetsvoorstel gevolgen heeft voor de rechten en vrijheden van betrokkenen.

Er bestaat een kans op een datalek of wederrechtelijke toegang tot de UBO-informatie in de registers.

D. Beschrijving voorgenomen maatregelen

17. Maatregelen

De voorgenomen maatregelen om bovenstaande risico's te voorkomen of te mitigeren zijn:

- i) Toegang tot informatie uit de UBO-registers wordt beperkt tot de hierboven genoemde categorieën;
- ii) Raadplegers worden geïdentificeerd via autorisaties en identificatiemiddelen op niveau Substantieel;
- iii) Alleen specifiek aangewezen autoriteiten en de FIU-Nederland krijgen inzage in de aanvullende UBO-gegevens;
- iv) Indien de UBO door het beschikbaar maken van diens gegevens blootgesteld wordt aan een onevenredig risico, een risico op fraude, ontvoering, chantage, geweld, pesterijen of intimidatie kan om afscherming van zijn of haar gegevens worden verzocht;
- v) Informatiebeveiliging door de Kamer van Koophandel.

- vi) UBO's kunnen hun eigen gegevens inzien evenals het aantal keer dat hun gegevens is ingezien.

Ad i)

Naar aanleiding van de uitspraak van het Europees Hof van Justitie is informatie uit de UBO-registers niet meer toegankelijk voor eenieder, maar wordt de toegang tot UBO-informatie beperkt met dit wetsvoorstel.

Ad ii)

De toegang voor de genoemde categorieën wordt gewaarborgd via autorisaties afgegeven door de Kamer van Koophandel en identificatie van raadplegers via identificatiemiddelen op niveau Substantieel.

Ad iii)

De aanvullende gegevens zijn alleen toegankelijk voor bevoegde autoriteiten en de FIU-Nederland, autoriteiten die belast zijn met het toezicht op de naleving van de Sanctiewet 1977 en specifiek aangewezen autoriteiten die in het kader van een taak noodzakelijkerwijs over UBO-informatie moeten beschikken. Zij kennen in dit verband een geheimhoudingsplicht.

Ad iv)

In de gewijzigde richtlijn is opgenomen dat lidstaten in uitzonderlijke omstandigheden en per geval kunnen voorzien in een uitzondering op de toegang tot UBO-informatie indien de UBO door het beschikbaar maken van diens gegevens blootgesteld wordt aan een onevenredig risico, een risico op fraude, ontvoering, chantage, afpersing, pesterijen, geweld of intimidatie, of indien de UBO minderjarig is of anderszins handelingsonbekwaam. In het onderhavige wetsvoorstel verandert er niets aan deze mogelijkheid tot afscherming van gegevens.

De beoogde afscherming ziet op naam, geboortemaand en -jaar, nationaliteit en woonstaat, met uitzondering van de aard en omvang van het door de uiteindelijk belanghebbende gehouden economische belang (weergegeven, waar het gaat om percentages aandelen, stemrecht of eigendom, in bandbreedtes van 25% tot 50%, van 50% tot 75% en van 75% tot en met 100%). Voor het niet afschermen van laatstgenoemd persoonsgegeven is gekozen omdat dit geen gegeven betreft dat leidt tot directe herleidbaarheid van de UBO.

Opgemerkt dient te worden dat de afscherming – uit hoofde van de richtlijn – niet zal gelden indien banken, andere financiële instellingen of notarissen toegang vragen tot deze informatie. Zij zullen dus altijd inzage hebben in alle gegevens, gelet op hun taakuitoefening. De afscherming kan ook niet worden ingeroepen tegen de aangewezen bevoegde autoriteiten en de FIU-Nederland, wanneer zij om toegang tot UBO-informatie vragen.

De UBO kan een verzoek tot afscherming van zijn UBO-informatie indienen bij de Kamer van Koophandel. Hij zal daarbij moeten aantonen dat één van de in de richtlijn genoemde situaties aan de orde is: blootstelling aan een onevenredig risico, een risico op fraude, ontvoering, chantage, afpersing, pesterijen, geweld of intimidatie, of dat sprake is van minderjarigheid of handelingsonbekwaamheid. Het besluit van de Kamer van Koophandel op een verzoek tot afscherming van de UBO-informatie is een besluit in de zin van artikel 1:3 van de Algemene wet bestuursrecht, waar bezwaar en beroep tegen open staat.

Om dit regime effectief te laten zijn, zullen de UBO-gegevens niet openbaar zijn tijdens de periode die nodig is om de UBO in staat te stellen een verzoek in te dienen, de Kamer van Koophandel om daarover te besluiten en – indien het verzoek wordt afgewezen – bezwaar en beroep af te handelen.

Het regime voor afscherming is nader uitgewerkt in het Handelsregisterbesluit 2008.

Ad v)

Bij de Kamer van Koophandel zijn daartoe speciaal opgeleide en geautoriseerde medewerkers belast met beheer van de UBO-registers, waaronder invoer en wijziging van (persoons)gegevens.

Dit gebeurt onder verantwoordelijkheid van het management van de Kamer van Koophandel. De medewerkers werken volgens vaste protocollen en instructies.

De UBO-gegevens zijn goed beschermd tegen onbevoegde toegang; de UBO-informatie valt onder datzelfde regime van bescherming. De Kamer van Koophandel heeft een integraal beveiligingsbeleid en privacybeleid dat is vastgesteld door de Raad van Bestuur van de Kamer van Koophandel. In het kader van de ISO27001 certificering en de maatregelen die in de ISO 27002 worden beschreven, heeft de Kamer van Koophandel een Information Security Managementsystem (ISMS) ingericht. De Kamer van Koophandel heeft een IBC in dienst en een team van Security Officers die ieder op hun 'eigen' hoofdstuk(ken) van het ISMS zorg dragen voor handhaving van de daarin beschreven maatregelen. Onderdelen hiervan zijn specifiek gericht op gegevensbescherming en -beveiliging.

De Kamer van Koophandel heeft een procedure Meldplicht Datalekken ingericht en dit aan haar medewerkers kenbaar gemaakt. Meldingen van beveiligingsincidenten worden via een intern systeem vastgelegd en doorgezet naar de Functionaris Gegevensbescherming. Deze treedt in overleg met de IBC en andere relevante interne partijen en beoordeelt of er sprake is van een meldingsplichtig datalek. Alle beveiligingsincidenten worden vastgelegd en gedocumenteerd.

De informatiebeveiliging van Kamer van Koophandel voldoet aan internationale standaarden op dit gebied. De Kamer van Koophandel is ISO 27001 gecertificeerd. Het certificaat is een bevestiging dat de Kamer van Koophandel voldoet aan de internationale standaarden voor informatiebeveiliging. De norm regelt zowel de inrichting van processen en procedures rond informatiebeveiliging als de naleving, controle, toetsing en permanente verbetering daarvan. Deze norm voorziet ook in specifieke maatregelen waar het de bescherming van persoonsgegevens betreft, dit zijn maatregelen van zowel organisatorische als technische aard.

Ad vi)

UBO's hebben toegang tot de gegevens die over hen zijn geregistreerd. Daarnaast kunnen zij een opvraag doen over het aantal keer dat hun gegevens is geraadpleegd. Hierin worden de raadplegingen van de autoriteiten niet meegenomen.

Voor beide registers zijn twee afzonderlijk Data Protection Impact Assessments (DPIA) opgesteld in het kader van de uitvoering. Deze documenten zullen naar aanleiding van de hofuitspraak en onderhavig wetsvoorstel worden geactualiseerd waar nodig.