

Bedrijfsbeleid inzake Preventie van Witwassen van Geld

Laatste update: januari 2024

Inhoudsopgave

1. DOELSTELLING 3
2. DEFINITIES 3
3. REIKWIJDTE 4
4. ALGEMENE PRINCIPES 5
5. IMPLEMENTATIE VAN HET BELEID 6
 - 5.1 Zorgvuldigheidsonderzoek 6
 - 5.1.1 Herkenning van Derde Partijen 7
 - 5.1.2 Controle van Derde Partijen 7
 - 5.2 Het Sluiten van Contracten 8
 - 5.3 Continue Monitoring 9
 - 5.4 Verzoeken van Derde Partijen 10
 - 5.5 Opleiding 10
 - 5.6 Audit 10
6. BEVOEGDHEDEN EN VERANTWOORDELIJKHEDEN 10
7. WIJZIGINGSGESCHIEDENIS 11

1. DOELSTELLING

Het doel van het bedrijfsbeleid inzake de preventie van witwassen ("Beleid") is om een algemeen kader vast te stellen voor de implementatie van Know Your Customer (KYC)-principes en de preventie van het witwassen van criminele opbrengsten binnen het bedrijf Van Eck Trailers B.V. ("Bedrijf") om het witwassen van criminele opbrengsten te voorkomen en de strijd tegen de financiering van terrorisme te ondersteunen.

2. DEFINITIES

- "Klant" verwijst naar natuurlijke personen of rechtspersonen die producten of diensten van het Bedrijf afnemen of gebruiken.
- "Compliance Manager" betekent de onafhankelijke compliance manager van het Bedrijf.
- "FATF" verwijst naar de internationale Financial Action Task Force.
- "Financiering van Terrorismen" verwijst naar het opzettelijk verstrekken of verzamelen van fondsen en andere activa, op welke manier dan ook, direct of indirect, met het oog op het gebruik van dergelijke middelen, geheel of gedeeltelijk, door een terroristische organisatie of voor een terroristische daad.
- "FIU" verwijst naar de Financial Intelligence Unit van Nederland.
- "GWG" verwijst naar de Wet van de Bondsrepubliek Duitsland inzake de Preventie van Witwassen van Geld (Geldwäschegesetz).
- "Know Your Customer-principes" verwijst naar de grondige herkenning van een natuurlijke persoon of rechtspersoon die voor het eerst contact heeft opgenomen met het Bedrijf en een belangrijke rol speelt bij het elimineren van de risico's in verband met witwassen van criminele opbrengsten, financiering van terrorisme, corruptie, fraude, omkoping en andere illegale activiteiten waarmee het Bedrijf te maken kan krijgen door deze personen.
- "Witwassen van criminele opbrengsten" is het proces waarbij illegaal gegenereerde opbrengsten legaal worden aangetoond, zoals vastgelegd in internationale regelgeving zoals Wwft, MASAK, GwG en FATF-aanbevelingen. Het proces omvat meestal de fasen van plaatsing, scheiding en integratie. Eerst worden illegitieme fondsen in contante vorm heimelijk in een legitiem financieel systeem geïntroduceerd. Vervolgens wordt het geld verplaatst binnen het systeem via meerdere rekeningen om de traceerbaarheid van het geld te voorkomen. Uiteindelijk worden de criminele opbrengsten, losgekoppeld van hun illegale bron, witgewassen in het financiële systeem van het land via legale procedures.
- "Management" verwijst naar de raad van bestuur of de algemeen directeur, afhankelijk van wie de hoogste beslissingsbevoegdheid heeft binnen het Bedrijf.
- "MASAK" verwijst naar de Financial Crimes Investigation Board van de Republiek Turkije.

- "Overheidsfunctionaris" verwijst naar een persoon die permanent, tijdelijk of voor een bepaalde periode betrokken is bij het uitvoeren van een openbare taak door benoeming of verkiezing.
- "Politiek Blootgestelde Persoon" (PEP) verwijst naar een persoon die is toegewezen aan of belast is met een belangrijke openbare functie. Politiek blootgestelde personen omvatten, maar zijn niet beperkt tot:
 - Regeringsleiders, ministers en plaatsvervangend ministers;
 - Parlementsleden;
 - Leden van hoge rechtbanken, constitutionele rechtbanken of andere hoge gerechtelijke organen waarvan de beslissingen in uitzonderlijke gevallen niet verder kunnen worden aangevochten;
 - Rechter;
 - Bestuursleden van centrale banken;
 - Ambassadeurs;
 - Hooggeplaatste officieren in het leger;
 - Leden van administratieve, management- of toezichhoudende organen van overheidsbedrijven of personen die in vergelijkbare posities werkzaam zijn; en
 - Familieleden en nauwe zakenpartners van de bovengenoemde personen.
- "Risk Manager" verwijst naar een objectieve en onafhankelijke adviespersoon binnen het Bedrijf, die is ontworpen om waarde toe te voegen aan de operaties van de organisatie en om de processen te verbeteren.
- "Sanctielijsten" verwijst naar de lijsten van gesanctioneerde personen, entiteiten of regeringen.
- "Systeem" verwijst naar het onpartijdige en onafhankelijke informatiesysteem dat geïntegreerd werkt met de ERP-software van het Bedrijf en analyseert volgens de bestaande internationale sanctielijsten, beslissingen en nieuws in overeenstemming met de vereisten van de Know Your Customer-principes.
- "Leverancier" verwijst naar een natuurlijke persoon of rechtspersoon die goederen en diensten aan het Bedrijf levert. Deze natuurlijke personen/ rechtspersonen maken deel uit van de toeleveringsketen van het Bedrijf en kunnen een groot deel van de waarde vertegenwoordigen in de producten van het Bedrijf.
- "Derde" verwijst naar elke natuurlijke persoon of rechtspersoon die handelt namens het Bedrijf of in verband staat met het Bedrijf, zoals een distributeur, dealer, tussenpersoon, adviseur, vertegenwoordiger, aannemer of onderaannemer.
- "Wwft" verwijst naar de Wet ter voorkoming van witwassen en financieren van terrorisme in Nederland.

3. REIKWIJDTE

Het Bedrijf zet zich in voor de hoge normen die wereldwijd worden geaccepteerd bij de preventie van het witwassen van criminele opbrengsten. Alle Derden, medewerkers en managers zijn verplicht zich aan deze normen te houden en verantwoordelijk te zijn voor de implementatie van dit Beleid om te voorkomen dat het handelsmerk van het Bedrijf, evenals de producten en diensten, worden gebruikt voor het witwassen van criminele opbrengsten of de financiering van terrorisme.

Dit Beleid is opgesteld op basis van, maar niet beperkt tot, de onderstaande regelgeving en standaarden, en de normen in overeenstemming met wereldwijde praktijken zijn ook geïnspecteerd:

- Wwft;
- FIU-wetgeving;
- GwG;
- Basel Principles Declaration on the Prevention of the Use of the Banking System for Money Laundering Purposes;
- Financial Action Task Force (FATF) 40 Aanbevelingen;
- Wolfsberg-standaarden; en
- MASAK-wetgeving.

4. ALGEMENE PRINCIPES

Voor zover redelijk en haalbaar, houdt het Bedrijf regelmatig en continu toezicht op zijn activiteiten in overeenstemming met internationale praktijken, regelgeving en verdragen met betrekking tot de preventie van het witwassen van criminele opbrengsten en werkt het Beleid dienovereenkomstig bij. In dit kader heeft het Bedrijf dit Beleid vastgesteld.

Door een passend kader te creëren voor het witwassen van criminele opbrengsten, streeft het Bedrijf ernaar de kans op blootstelling aan verschillende risico's voor zowel het Bedrijf als zijn werknemers te minimaliseren, waaronder maar niet beperkt tot:

- **Reputatierisico:** Verlies dat voortvloeit uit een aanzienlijke invloed op de reputatie van het Bedrijf. Reputatieverlies kan leiden tot schade aan de goede naam die het Bedrijf heeft opgebouwd door zijn activiteiten in overeenstemming met lokale en internationale wetgeving met al zijn medewerkers en belanghebbenden sinds de oprichting. Dit kan morele en daaropvolgende financiële schade voor het Bedrijf veroorzaken.
- **Compliance-risico:** Verlies als gevolg van niet-naleving van lokale en internationale wetgeving. Compliance-risico kan ertoe leiden dat het Bedrijf en/ of zijn werknemers

worden geconfronteerd met sancties, zoals directe boetes, opschorting van activiteiten, gevangenisstraf voor werknemers en managers, evenals opname op sanctielijsten.

- **Financieel risico:** Materiële schade als gevolg van een van de bovengenoemde risico's of een combinatie daarvan, die een nadelige financiële impact op het Bedrijf veroorzaakt.

² <https://www.hmb.gov.tr/aklama-sucu-uluslararasi-mevzuat>

³ <https://ms.hmb.gov.tr/uploads/2019/01/FATF-Tavsiyeleri-2012.pdf>

⁴ <https://ms.hmb.gov.tr/uploads/2019/01/1-1.pdf>

⁵ <https://www.hmb.gov.tr/aklama-sucu-ulusal-mevzuat>

Het Bedrijf en zijn werknemers, evenals derden die verbonden zijn aan het Bedrijf, worden geacht de Compliance Manager en/of Risk Manager onmiddellijk schriftelijk (e-mail) te informeren als zij informatie hebben of vermoeden dat zij betrokken zijn bij een relatie die verband houdt met het witwassen van criminele opbrengsten.

Van een werknemer van het Bedrijf wordt verwacht dat hij/zij dit Beleid onder geen enkele omstandigheid schendt. Het Bedrijf hanteert een nultolerantiebeleid voor schendingen van het Beleid. Elke werknemer die wordt betrapt op het overtreden van dit Beleid, zal onderworpen worden aan diverse sancties, waaronder ontslag.

In het geval dat dit Beleid door derden wordt geschonden, moeten de bestaande contracten onmiddellijk worden beëindigd en moeten de noodzakelijke juridische meldingen worden gedaan.

Indien derden, met name onze werknemers, twijfels hebben over de naleving van een bepaalde activiteit met dit Beleid, wordt van hen verwacht dat zij dergelijke vermoedens melden aan het Bedrijf, anoniem of door hun persoonlijke gegevens te delen via <https://www.app.faceup.com/nl/c/vanecktrailers>.

Voor gedetailleerde informatie over dit onderwerp, raadpleeg het Bedrijfsbeleid inzake Informantenbescherming.

5. IMPLEMENTATIE VAN HET BELEID

Het Bedrijf is sterk toegewijd aan zakelijke ethiek en nalevingsnormen. Het Bedrijf implementeert wereldwijd geaccepteerde standaarden in elk gebied waar het actief is en voert regelmatig controles uit om de risico's met betrekking tot het witwassen van criminele opbrengsten te verminderen.

5.1 Zorgvuldigheidsonderzoek

De principes voor het herkennen van Derden waarmee we samenwerken, zoals onze zakenpartners en klanten, vormen een zeer kritisch proces bij de beoordeling van risico's met betrekking tot Derden en zijn ook onvermijdelijk om te voldoen aan de relevante lokale en internationale regelgeving.

Het acceptatieproces van Derden bestaat uit onderzoeksprocessen die onder meer, maar niet uitsluitend, de volgende stappen omvatten: (i) identificatie, (ii) onderwerp van de activiteit, (iii) doel van de transactie, (iv) bron van activa, (v) zakelijke geschiedenis, (vi) geografie waar de activiteiten worden uitgevoerd, en (vii) reputatieonderzoek.

Derden moeten worden onderzocht volgens de bovenstaande stappen en er moet een zorgvuldigheidsonderzoek op hen worden uitgevoerd. Dit onderzoek is van het grootste belang om het Bedrijf te beschermen tegen Derden die betrokken zijn bij illegale

activiteiten, zoals het witwassen van criminele opbrengsten. In dit verband is het vereist ervoor te zorgen dat onderzoeken naar Derden en alle in dit verband ontvangen informatie en documenten correct worden verstrekt tijdens het acceptatieproces.

Er zijn enkele punten waar rekening mee moet worden gehouden voordat er een zakelijke relatie wordt aangegaan met Derden, waaronder personeelswervingsprocessen. Vooral de volgende situaties, maar niet beperkt tot, vereisen meer aandacht en een grondiger beoordeling:

- Bedrijfslijnen en landen van zakelijk activiteit;
- Financiële positie en reputatie;
- Historische controles;
- Ethiek- en nalevingsbeleid;
- Personen en instellingen die actief zijn in hoogrisicogebieden;
- Politiek blootgestelde personen;
- Personen en instellingen die contante transacties gebruiken of willen gebruiken;
- Personen en instellingen die weigeren informatie en documenten te verstrekken;
- Personen over wie negatieve berichten zijn gepubliceerd in de pers;
- Personen en instellingen die als verdacht worden beschouwd op internationale lijsten.

Het uit te voeren zorgvuldigheidsonderzoek zal direct worden uitgevoerd door het Systeem door de benodigde informatie in te voeren.

5.1.1 Herkenning van Derde Partijen

Het zorgvuldigheidsonderzoek zal worden gestart door de handelsnaam en andere documenten (zoals handelsregistratie, belastingaangifte) te verstrekken voor rechtspersonen van derden en de volledige voor- en achternaam op het identiteitsdocument van natuurlijke personen van derden. Deze informatie en documenten, indien beschikbaar, die van de Derde Partij worden verkregen, zullen zonder vertraging in het Systeem worden ingevoerd en de eerste stap van het zorgvuldigheidsonderzoek zal direct door het Systeem worden uitgevoerd.

5.1.2 Controle van Derde Partijen

De volgende zaken moeten worden gecontroleerd, namelijk:

- Negatief nieuws;
- Politiek blootgestelde personen (PEP's);
- Verdachte lijsten; en
- Geografie van de activiteiten

⁶[http://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/?hf=10&b=0&s=desc\(fatf_releasedate\)](http://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/?hf=10&b=0&s=desc(fatf_releasedate))

⁷It is the responsibility of the Risk Manager to check the up-to-dateness of high-risk countries. ⁸The results obtained as the result of a simple search on search engines such as Google and Yandex are examined.

worden door het Systeem gescand en het resultaat wordt automatisch gearchiveerd. In gevallen waarin geen waarschuwing in het Systeem wordt weergegeven, wordt de beslissing om een contract af te sluiten genomen door de afdeling die direct met de betreffende Derde Partij zal werken (zoals Human Resources bij het afsluiten van een arbeidsovereenkomst, of de Sales-afdeling bij het afsluiten van een verkoopcontract met klanten).

Als er een waarschuwing in het Systeem verschijnt, stuurt het Systeem onmiddellijk schriftelijke informatie (e-mail) naar de Risk Manager. In dat geval moet de afdeling die direct contact heeft met de Derde Partij, op verzoek van de Risk Manager, alle informatie en documenten onmiddellijk doorsturen naar de Risk Manager.

De Risk Manager zal de waarschuwing uit het Systeem verwijderen als hij/ zij na beoordeling van alle relevante informatie en documenten concludeert dat er geen schending is van de wetgeving, mondiale normen en/of dit Beleid. Zo niet, dan zal de Risk Manager, indien nodig, juridisch advies inwinnen en zijn/ haar evaluatie samen met de voorgestelde administratieve herzieningsperioden ter goedkeuring voorleggen aan de manager(s). In dergelijke gevallen mag de beslissing om een contract af te sluiten met de betreffende Derde Partij alleen door de manager(s) worden genomen.

Als bij de acceptatie van Derde Partijen blijkt dat de partners of managers van de betreffende personen of bedrijven Politiek Blootgestelde Personen zijn, wordt er redelijk onderzoek gedaan om de bron van de activa van de betrokken partijen vast te stellen en zal de Risk Manager beoordelen of het aangaan van een zakelijke relatie met hen een risico vormt voor het Bedrijf. Op basis van de gemaakte evaluaties zal het Management de uiteindelijke beslissing schriftelijk nemen.

Alle resultaten van het zorgvuldigheidsonderzoek naar Derde Partijen, de relevante informatie en documenten moeten worden bewaard in overeenstemming met de toepasselijke lokale wetgeving. Tenzij anders bepaald in de lokale wetgeving, moeten de gegevens minimaal acht (8) jaar worden bewaard, op een duidelijke en begrijpelijke manier, zodat ze beschikbaar zijn voor eventuele interne en/ of externe audits.

5.2 Het afsluiten van contracten

Na het zorgvuldigheidsonderzoek dat door het Bedrijf is uitgevoerd om voldoende informatie te verkrijgen over de Derde Partijen waarmee het zaken zal doen, wordt een schriftelijk contract opgesteld en ondertekend in gevallen waarin is besloten om met deze Derde Partijen samen te werken.

Om het Bedrijf te beschermen tegen de risico's die samenhangen met het witwassen van criminele opbrengsten door Derde Partijen, moeten tijdens het contractproces de relevante beschermende clausules aan het contract worden toegevoegd. In dit kader

Van Eck Trailers B.V.

moeten bepalingen over het recht om Derde Partijen te controleren, ter plaatse te inspecteren of het contract te beëindigen in overweging worden genomen. Om ervoor te zorgen dat alle contracten die met Derde Partijen worden gesloten de relevante bepalingen bevatten, moet de schriftelijke goedkeuring (e-mail) van de juridische afdeling van het Bedrijf worden verkregen voor de ondertekende versie van het betreffende contract.

5.3 Continue monitoring

Het is niet voldoende om Derde Partijen waarmee het Bedrijf samenwerkt alleen vóór de ondertekening van het contract te controleren. Derde Partijen met wie een ononderbroken zakelijke relatie bestaat, moeten continu en regelmatig worden gemonitord, inclusief financiële transacties, in overeenstemming met hun risicoprofielen en in overeenstemming met de wereldwijde normen en dit Beleid.

Wat betreft de Derde Partijen die tijdens het acceptatieproces als risicoloos worden beschouwd, moeten deze natuurlijke personen of rechtspersonen minstens één keer per jaar door de Risk Manager worden gecontroleerd, waarbij wordt gedocumenteerd:

- (i) of zij voorkomen op internationale sanctielijsten, en
- (ii) of er negatief nieuws over hen in de pers is verschenen.

Na een waarschuwing in het systeem zal de frequentie van het regelmatige zorgvuldigheidsonderzoek voor Derde Partijen, waarmee wordt besloten om samen te werken of door te gaan met samenwerken volgens de beslissing van de manager(s) van het Bedrijf, worden bepaald door de Risk Manager op basis van de omvang van het risico. Deze frequentie zal minimaal elke zes (6) maanden zijn. Voor dergelijke beoordelingen zullen de volgende punten door het systeem worden uitgevoerd door middel van onderzoek van openbare bronnen:

- (i) zoeken naar negatief nieuws in de pers over de betreffende natuurlijke personen en rechtspersonen, hun bedrijfspartners en senior managers;
- (ii) scannen van internationale sanctielijsten;
- (iii) volgen van veranderingen in de activiteitensectoren; en
- (iv) volgen van landen waar buitenlandse handel wordt uitgevoerd.

Het onderzoek in dit verband zal worden uitgevoerd door de Risk Manager.

Op basis van dit onderzoek zal de beslissing om door te gaan met werken bij het ontstaan van een nieuw risico dat voorheen niet bestond, alleen worden genomen door de manager(s) van het Bedrijf, indien nodig na het verkrijgen van juridisch advies. De beslissing van de manager(s) van het Bedrijf zal worden toegevoegd aan het advies van de Risk Manager en, indien van toepassing, de juridische afdeling voor archiveringsdoeleinden. In gevallen waarin wordt geoordeeld dat er geen nieuw risicofactor is gevormd, zal het

zorgvuldigheidsonderzoek worden voortgezet met de frequentie die is bepaald door de Risk Manager.

5.4 Verzoeken van Derden

Verschillende instellingen kunnen documenten en informatie opvragen met betrekking tot hun transacties met het Bedrijf of Derde Partijen. Als een medewerker van het Bedrijf de ontvanger is van een dergelijk verzoek, moet hij/ zij dit verzoek zonder vertraging delen met de Risk Manager. De antwoorden op dergelijke verzoeken moeten zonder uitzondering worden goedgekeurd door de Risk Manager en mogen geen onjuiste of onvolledige informatie bevatten. Bovendien moet alle interne en externe correspondentie met betrekking tot dit verzoekproces, indien aanwezig, fysiek en in elk geval in elektronische vorm worden vastgelegd en opgeslagen.

5.5 Opleiding

Om ervoor te zorgen dat wordt voldaan aan lokale en internationale regelgeving met betrekking tot het witwassen van criminele opbrengsten en om het bewustzijn te vergroten over de risico's die verband houden met het relevante beleid en de regels van de instelling, moeten alle relevante medewerkers regelmatig trainingen volgen. Alle medewerkers van het Bedrijf moeten bij indiensttreding een training volgen over de preventie van witwassen van criminele opbrengsten en ten minste één keer per jaar aan deze training deelnemen. Bovendien kan het Bedrijf, indien het dit nodig acht, bewustwordingstrainingen aanbieden over de regelingen ter preventie van witwassen van criminele opbrengsten, of verzoeken dat werknemers op eigen kosten elders trainingen volgen over deze kwesties. De organisatie en opvolging van de trainingen wordt uitgevoerd door de afdeling Human Resources van het Bedrijf, samen met de Risk Manager.

5.6 Audit

Externe auditors zullen minstens één keer per jaar en/of op verzoek van het Management een algemene audit uitvoeren van de activiteiten met betrekking tot de preventie van witwassen van criminele opbrengsten in het Bedrijf en de resultaten van de audit rapporteren aan de manager(s).

6. BEVOEGDHEDEN EN VERANTWOORDELIJKHEDEN

Het updaten van dit Beleid is de verantwoordelijkheid van de Risk Manager.

Werknemers en managers van het Bedrijf zijn verplicht zich aan dit Beleid te houden, en van zakenpartners van het Bedrijf wordt verwacht dat zij dit Beleid zoveel mogelijk naleven. Als er een verschil is tussen dit Beleid en de lokale wetgeving die van kracht is in de landen waar het Bedrijf actief is, zal de meest restrictieve van kracht zijn.

Indien medewerkers van het Bedrijf getuige zijn van een transactie die in strijd is met dit Beleid, de toepasselijke wetgeving of de Gedragscode van het Bedrijf volgens de hierboven genoemde artikelen, zijn zij persoonlijk verplicht de vermoedelijke schending te melden via <https://www.app.faceup.com/nl/c/vanecktrailers>.

Werknemers kunnen ook te allen tijde vragen stellen aan het Management en/of de Compliance Manager over de preventie van het witwassen van criminele opbrengsten en de implementatie van dit Beleid.

De Risk Manager is verantwoordelijk voor het uitvoeren van audits die de kans vergroten dat mogelijke schendingen worden gedetecteerd, en ervoor te zorgen dat risicobeperkende controles met betrekking tot de geïdentificeerde risico's binnen het hele Bedrijf worden geïmplementeerd.

Zoals hierboven uitvoeriger vermeld, kunnen in geval van een schending van dit Beleid strafrechtelijke sancties worden opgelegd, waaronder het ontslag van werknemers en de beëindiging van het contract met Derde Partijen.

7. WIJZIGINGSGESCHIEDENIS

Dit Beleid is in werking getreden op 31 januari 2024.

Herziening	Datum	Beschrijving
No.1	31.01.2024	Er werden updates gemaakt als gevolg van de nieuwe informantienregeling zoals bepaald in Richtlijn (EU) 2019/ 1937 van het Europees Parlement en de Raad van 23 oktober 2019 over de bescherming van personen die inbreuken op het recht van de Unie melden.