# Turien & Co.

(laatste update:18-05-2018)

## Verwerking

| | | |
|---|---|---|
| *Registratienummer* | ALG02 | |
| *Naam verwerking* | Relatiebeheer tussenpersonen (aangaan en uitvoeren samenwerking met tussenpersonen) | |
| *Gezamenlijke Verantwoordelijken* | • Turien & Co. Assuradeuren B.V. (primair verantwoordelijke, ook richting de betrokkene en naar buiten toe)<br>• Ansvar Verzekeringsmaatschappij N.V. | |
| | James Wattstraat 11<br>1817 DC Alkmaar<br>Nederland | Postbus 216<br>1800 AE Alkmaar<br>Nederland |
| *Doel(en) van verwerking* | 1. Aangaan en uitvoeren van een samenwerking met assurantietussenpersonen.<br>2. Integriteit en veiligheid dienstverlening. Hieronder vallen onder meer fraudebestrijding en sanctielijsttoetsingen;<br>3. Verlenen van service in verband met genoemde samenwerking;<br>4. Verantwoorde uitoefening van de bedrijfsdoelstellingen van de organisatie mede ten behoeve van samenwerkingsverbanden;<br>5. Genereren van management- en beleidsinformatie, onder meer ten behoeve van product- en dienstenontwikkeling alsmede ten behoeve van het bepalen van algemene strategie en beleid;<br>6. Marketingactiviteiten en relatiemanagement. Uitvoeren van (gerichte) marketingactiviteiten teneinde een relatie met een tussenpersoon tot stand te brengen en/of met een tussenpersoon in stand te houden dan wel uit te breiden;<br>7. Analyses voor historische, statistische en wetenschappelijke doeleinden, onder andere middels profilering;<br>8. Voorschriften uit wet- en regelgeving. Hiermee wordt bedoeld het voldoen aan wettelijke verplichtingen, waaronder sanctielijstcontrole en het inwinnen van verplichte informatie over de betrokkene. Maar ook wettelijk verplichte informatieverstrekking aan toezichthouders en opsporingsautoriteiten valt hieronder. | |
| *Grondslag(en) van verwerking* | • De betrokkene heeft voor de verwerking zijn ondubbelzinnige toestemming verleend;<br>• De gegevens zijn noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of voor het nemen van precontractuele maatregelen naar aanleiding van een verzoek van de betrokkene en die noodzakelijk zijn voor het sluiten van een overeenkomst;<br>• De gegevens zijn noodzakelijk om een wettelijke verplichting na te komen waaraan de verantwoordelijke onderworpen is;<br>• De gegevens zijn noodzakelijk ter vrijwaring van een vitaal belang van de betrokkene;<br>• De gegevens zijn noodzakelijk voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke of van een derde aan wie de gegevens worden verstrekt. | |

## Betrokkene(n)

| Hoedanigheid betrokkene | Categorieën van persoonsgegevens |
|---|---|
| *Bedrijfsgegevens* | NAW-gegevens |
| | Telefoon, fax, e-mail |
| | KvK-nummer |
| | Kopie Kifid inschrijving |
| | AFM nummer |
| | Paspoortgegevens eigenaar |
| | Bankrekeningnummer en betaalgegevens |
| | Voor communicatie benodigde gegevens |
| | Website adres |
| | Bezoekgegevens en -verslagen |

| | |
|---|---|
| | Betalingsverkeer (waaronder rekeningcourant en borderellen en betalingsachterstanden) |
| **Hoedanigheid betrokkene** | **Categorieën van persoonsgegevens** |
| *Uiteindelijke belanghebbende van de onderneming (UBO)* | Naam |
| | Geboortedatum |
| | Geslacht |
| | Nationaliteit |
| | Percentage belang in de onderneming |
| | Vermelding op één of meerdere sanctielijsten |
| **Hoedanigheid betrokkene** | **Categorieën van persoonsgegevens** |
| *Contactperso(o)n(en) tussenpersoon* | Naam |
| | Geslacht |
| | Telefoon, e-mail |
| | Contactgegevens |

## Ontvangers

| | **Categorieën van (mogelijke) ontvangers** | **Doel(en)** (zie de eerste tabel 'Verwerking' bij 'Doeleind(en) verwerking voor de betekenis van de nummers) |
|---|---|---|
| *Intern* | Medewerkers acceptatie, schade, financieel | 1, 3, 4 |
| | Leidinggevenden van de betrokken teams en afdelingen | 1, 3, 4 |
| | Medewerkers en leidinggevenden van Marketing | 1, 2, 3, 4, 5, 6, 7, 8 |
| | Internal Auditer, Risk officer & Compliance officer | 2, 4, 5, 8 |
| | Afdeling BI en Reporting | 5, 6, 7, 8 |
| | Fraudecoördinator | 2, 8 |
| | Managers | 1, 3, 4, 5, 8 |
| | Directieleden | 1, 3, 4, 5, 8 |
| | **Categorieën van (mogelijke) ontvangers** | **Doel(en)** |
| *Extern* | Betrokkene zelf | 1, 3, 6 |
| | Volmachtgever | 1, 4 |
| | Bewerkers die de organisatie ondersteuning bij de uitvoering van haar werkzaamheden, zoals Friss en CIS ten behoeve van Sanctielijst- en fraude | 1, 2, 3, 4, 8 |
| | Onderzoeksinstituten | 7 |
| | Toezichthouders als de Nederlandse Bank en de Autoriteit Financiële markten | 4, 8 |
| | Personen en instanties die op grond van wettelijke verplichting(en) geïnformeerd moeten of mogen worden | 8 |
| | Klachtinstanties | 1, 4 |
| | Centraal informatiesysteem van de in Nederland werkzame verzekeringsmaatschappijen (Stichting CIS) | 1, 2 |
| | Belangenbehartigers van de betrokkene of wederpartij (bijvoorbeeld een advocaat of schuldsaneringsbureau) | 1, 4 |

1. Aangaan en uitvoeren van een samenwerking met assurantietussenpersonen.
2. Integriteit en veiligheid dienstverlening. Hieronder vallen onder meer fraudebestrijding en sanctielijsttoetsingen;
3. Verlenen van service in verband met genoemde samenwerking;
4. Verantwoorde uitoefening van de bedrijfsdoelstellingen van de organisatie mede ten behoeve van samenwerkingsverbanden;
5. Genereren van management- en beleidsinformatie, onder meer ten behoeve van product- en dienstenontwikkeling alsmede ten behoeve van het bepalen van algemene strategie en beleid;
6. Marketingactiviteiten en relatiemanagement. Uitvoeren van (gerichte) marketingactiviteiten teneinde een relatie met een tussenpersoon tot stand te brengen en/of met een tussenpersoon in stand te houden dan wel uit te breiden;
7. Analyses voor historische, statistische en wetenschappelijke doeleinden, onder andere middels profilering;

8. Voorschriften uit wet- en regelgeving. Hiermee wordt bedoeld het voldoen aan wettelijke verplichtingen, waaronder sanctielijstcontrole en het inwinnen van verplichte informatie over de betrokkene. Maar ook wettelijk verplichte informatieverstrekking aan toezichthouders en opsporingsautoriteiten valt hieronder.

## Doorgifte

| | |
|---|---|
| *Binnen EU* | Ja (buitenlandse volmachtgever) |
| *Buiten EU* | Nee |
| *Internationale organisaties* | Nee |
| *Passend* | N.v.t |

## Bewaartermijnen

Persoonsgegevens worden 7 jaar bewaard, te rekenen vanaf de einddatum van de actieve relatie met betrokkene. Dit kan de einddatum zijn van de samenwerking of –indien dat later is- de einddatum van het financiële dossier. De bewaartermijn van 7 jaar is een wettelijke fiscale bewaarverplichting.

Nadat de toepasselijke bewaartermijn is verstreken, zullen wij de persoonsgegevens anonimiseren. Dit betekent dat de bij ons aanwezige persoonsgegevens niet meer te herleiden zijn naar de betrokkene als individu.

## Algemene beschrijving technische en organisatorische beveiligingsmaatregelen

De bescherming van persoonsgegevens valt onder het informatiebeveiligingsbeleid van de organisatie. Dit informatiebeveiligingsbeleid is gebaseerd op negen pijlers:

- risicoanalyses, gericht op het bepalen van een beveiligingsclassificatie voor een (business)applicatie en eisen voor specifieke application controls;
- onderhouden van een basisbeveiligingsniveau voor de werkstations, netwerken, servers en storage. Hierbij valt te denken aan clear screen policy (schermbeveiliging), cryptografische versleuteling bij data-uitwisseling met externe partijen; beveiligde serverruimte; bescherming tegen kwaadaardige software.
- logische toegangsbeveiliging, gericht op het onderhouden van een set van regels voor het verlenen van toegang tot netwerk- en computersystemen, waaronder beveiliging van het netwerk middels een inlogprocedure (persoonlijke inlognaam en wachtwoord waarbij wachtwoorden periodiek dienen te worden gewijzigd);
- fysieke beveiliging, gericht op het weren van onbevoegden (toegangsbeveiliging en fysieke beveiliging van gebouw en omgeving);
- integriteitmanagement, gericht op het vaststellen van de betrouwbaarheid van het personeel bij het in dienst nemen van personeel, tijdens de uitvoering van het dienstverband en het einde dienstverband;
- bedrijfscontinuïteitsplannen met betrekking tot informatie in geval van calamiteiten (waaronder maken van back-ups);
- Incidentenmanagement, gericht op de registratie, analyse, escaleren, oplossen en voorkomen van beveiligingsincidenten.
- Autorisatiemanagement, gericht op het voorkomen van ongeoorloofde toegang tot applicaties en onderliggende data.
- Awareness, om de medewerkers regelmatig te wijzen op de rol die zij zelf spelen in de informatiebeveiliging en bescherming van de persoonsgegevens (o.a. Clean desk policy).