Turien & Co. Assuradeuren B.V.

(laatste update:17-05-2018)

Verwerking

Registratienummer	T&C02	
Naam verwerking	Verzekeringsadministratie Verzuimverzekeringen (aangaan en uitvoeren verzuimverzekeringen)	
Verantwoordelijke	Turien & Co. Assuradeuren B.V.	
	James Wattstraat 11 1817 DC Alkmaar Nederland	Postbus 216 1800 AE Alkmaar Nederland
Doel(en) van verwerking	1. Aangaan en uitvoeren van een verzekeringsovereenkomst. Hieronder valt onder meer het beoordelen en accepteren van (potentiële) cliënten en het afwikkelen van schadeclaims en het betalingsverkeer. Hieronder valt tevens het beheren van de uit de overeenkomst voortvloeiende relaties; 2. Integriteit en veiligheid dienstverlening. Hieronder vallen onder meer fraudebestrijding en sanctielijsttoetsingen; 3. Verlenen van service in verband met genoemde verzekeringen en het beheersen van schadelast (waaronder verhaal van schade); 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 de kwaliteit van de dienstverlening, 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 betrokkene tot stand te brengen en/of met een cliënt 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; 9. Profilering (onderzoek naar kenmerken en voorkeuren van betrokkenen); 10. Bijhouden van hoe en wanneer wij contact met betrokkene hebben, bijvoorbeeld ter verbetering van de communicatie, als bewijs, of voor training van onze medewerkers. In dit kader kunnen wij ook telefoongesprekken opnemen.	
Grondslag(en) van verwerking	• De betrokkene heeft voor de verwerking zijn ondubbelzinnige toestemming verleend; • 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; • De gegevens zijn noodzakelijk om een wettelijke verplichting na te komen waaraan de verantwoordelijke onderworpen is; • De gegevens zijn noodzakelijk ter vrijwaring van een vitaal belang van de betrokkene; • 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
Verzekeringnemers, oud-verzekeringnemers en	NAW-gegevens
	Telefoon, fax, e-mail
	Bedrijfsgegevens

potentiële verzekeringnemers	KvK-nummer
	Polisnummer en polisgegevens
	Premiegegevens
	Cliëntnummer
	Bankrekeningnummer en betaalgegevens
	Contactpersoon (naam en contactgegevens)
	Voor communicatie benodigde gegevens
	Verzuimpercentage afgelopen drie jaar
	Verzameling loonstaten
	Loonsom
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**
Assurantietussen-personen	NAW-gegevens
	Telefoon, fax, e-mail
	Contactgegevens
	Bedrijfsgegevens
	Relatienummer
Hoedanigheid betrokkene	**Categorieën van persoonsgegevens**
Werknemer (verzekerde)	NAW-gegevens
	Telefoon, email
	Geslacht
	Geboortedatum
	Nationaliteit
	Burgerlijke staat
	Soort diensteverband
	Fulltime of parttime en uren per week werkzaam
	Functie
	Salaris / inkomensgegevens
	Beroepsklasse
	Datum in dienst
	Datum uit dienst
	Arbeidshandicap
	1e ziektedag
	Meldingsdatum bij verzekeraar
	Percentage arbeidsongeschiktheid
	Vangnet / WAO aanwezig
	Sprake van ene ongeval? (ja/nee)
	Interventie ingezet? (ja/nee)
	Is er een opbouwschema of zijn er werkhervatting afspraken? (ja/nee)
	Is er ene plan van aanpak inzake re-integratie? (ja/nee)
	Prognose bedrijfsarts inzake verzuimduur
	Hersteldatum
	Mogelijkheid tot regres
Hoedanigheid betrokkene	**Categorieën van persoonsgegevens**
Externe Deskundigen (Waaronder Arbodienstverlener)	NAW-gegevens
	Telefoon, fax, e-mail
	Bedrijfsgegevens
	Bankrekeningnummer en betaalgegevens
	Declaraties en declaratiegegevens
	Voor communicatie benodigde gegevens

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, 2, 3, 4, 8
	Medisch adviseur en personen behorende tot diens medische staf	1, 3
	Leidinggevenden van de betrokken teams en afdelingen	1, 2, 3, 4, 5, 8, 10
	Medewerkers en leidinggevenden van Marketing	4, 5, 6, 9, 10
	Internal Auditer, Risk officer & Compliance officer	2, 4, 5, 8
	Afdeling BI en Reporting	2, 3, 4, 5, 6, 7, 8, 9, 10
	Afdeling Verzekeringstechniek	1, 3, 5, 7, 9
	Functionaris gegevensbescherming	4, 8
	Fraudecoördinator	1, 2, 4, 5
	Managers	1, 2, 3, 4, 5, 8, 10
	Directieleden	1, 4, 8
	Categorieën van (mogelijke) ontvangers	**Doel(en)**
Extern	Betrokkene zelf	1, 2, 3, 6, 8
	Volmachtgever van de betreffende verzekering	1, 2, 3, 4, 5, 7, 8
	Verwerkers, die de organisatie ondersteuning bij de uitvoering van haar werkzaamheden, zoals Friss ten behoeve van Sanctielijstcontrole en Postex voor digitale postverwerking.	1, 2, 4, 6, 7
	Andere met de verantwoordelijke samenwerkende organisaties, één en ander ten behoeve van de uitvoering van de verzekeringsovereenkomsten (bijvoorbeeld een schadebehandelingsbureau en de medisch adviseur)	1
	Externe deskundigen ter vaststelling van de schade of de toedracht van de schade (ARBO dienst)	1, 2
	Verzuimcoaches	3
	Assurantietussenpersonen	1, 2, 3
	Collectiviteiten	1, 3
	Onderzoeksinstituten	7
	Toezichthouders als de Nederlandse Bank en de Autoriteit Financiële markten	8
	Personen en instanties die op grond van wettelijke verplichting(en) geïnformeerd moeten of mogen worden	8
	Klachtinstanties	1
	Centraal informatiesysteem van de in Nederland werkzame verzekeringsmaatschappijen (Stichting CIS)	1, 2
	Belangenbehartigers van de betrokkene of wederpartij (bijvoorbeeld een advocaat of schuldsaneringsbureau)	1

Doorgifte

Binnen EU	Ja (Buitenlandse verzekeraar als 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 verzekering of –indien dat later is- de einddatum van het schadedossier of het financiële dossier. De bewaartermijn van 7 jaar is een wettelijke fiscale bewaarverplichting.

Uitzondering op de 7 jaar bewaartermijn vormen letselschadedossiers waarbij nog geen eindregeling is getroffen. Deze schadedossiers en daarbij behorende persoonsgegevens bewaren wij maximaal 30 jaar.

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).