

Disclaimer en privacy statements

1. Disclaimer Website

Bij het maken van deze website is de grootst mogelijke zorgvuldigheid in acht genomen. Wij staan echter niet in voor de gevolgen van activiteiten die worden ondernomen op basis van gegevens ontleend aan deze website.

Dit onder andere vanwege het feit dat de gegevens op deze site doorgaans aan veroudering onderhevig zijn en omdat in de meeste gevallen specifieke informatie nodig is om de toepasbaarheid van bepaalde regels en/of regelingen te kunnen bepalen.

Wij verwijzen op onze website naar internetpagina's van derden. Wij staan niet in voor de juistheid, volledigheid, betrouwbaarheid e.d. van de gegevens die daarop worden getoond.

Elke aansprakelijkheid op basis van deze website en doorverwezen websites wijzen wij hiermee van de hand. Indien u wilt weten of u specifiek voor bepaalde regels en/of regelingen in aanmerking komt, verzoeken wij u contact met ons op te nemen.

Een bezoeker van de site mag geen auteursrechtelijke beschermde werken of andere in de site opgeslagen informatie openbaar maken of op enige wijze verveelvoudigen zonder onze toestemming. Hieronder wordt tevens verstaan het verveelvoudigen van informatie en of delen daarvan door de publicatie op een elektronisch (computer-) netwerk.

2. Privacy statement

Wij respecteren de privacy van alle gebruikers van onze website en dragen er zorg voor dat de persoonlijke informatie die u ons verschaft vertrouwelijk wordt behandeld. Wij gebruiken uw gegevens om uw vraag, aanvraag of aanmelding zo snel mogelijk af te handelen. Wij zullen deze gegevens uitsluitend gebruiken met uw toestemming. Wij zullen uw persoonlijke gegevens niet aan derden verkopen en zullen deze uitsluitend aan derden ter beschikking stellen wanneer zij zijn betrokken bij het uitvoeren van uw (aan)vraag of aanmelding. Onze werknemers en de door ons ingeschakelde derden zijn verplicht om de vertrouwelijkheid van uw gegevens te respecteren.

3. Meldplicht datalekken

Vanaf 1 januari 2016 geldt in Nederland de Wet Meldplicht Datalekken. Deze wet houdt in dat een datalek met een kans op ernstige nadelige gevolgen voor de persoonsgegevens moet worden gemeld bij de toezichthouder, de Autoriteit Persoonsgegevens (voorheen College Bescherming Persoonsgegevens).

Wat is een datalek? De Autoriteit Persoonsgegevens geeft hiervoor de volgende definitie: Bij een datalek is sprake van een inbreuk op de beveiliging waardoor persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking. Onder een datalek valt dus niet alleen het vrijkomen (lekken) van persoonsgegevens, maar ook vernietiging daarvan en andere vormen van onrechtmatige verwerking. Een datalek kan bijvoorbeeld zijn: een gestolen laptop, een verloren usb-stick met

persoonsgegevens, een ex-werknemer met toegang tot persoonsgegevens, een e-mailbericht waarin alle geadresseerden zichtbaar zijn of een inbraak in een databestand door een hacker.

Een datalek moet volgens de wet bij de toezichthouder worden gemeld als dit 'leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens'. Wij volgen hierin de beleidsregels van de Autoriteit Persoonsgegevens. In lijn met deze beleidsregels zal de melding zo mogelijk niet later dan 72 uur na de ontdekking van het datalek gedaan worden.

Wanneer wij zijn ingeschakeld als derde partij (bewerker) van persoonsgegevens hoeven wij de datalek niet te melden bij de toezichthouder. Uw eigen organisatie is dan primair verantwoordelijk voor het melden van een datalek.

Als wij een ernstig datalek hebben geconstateerd stellen wij onze relaties daarvan zo snel mogelijk op de hoogte, zo mogelijk uiterlijk binnen 36 uur na het constateren ervan.

Om te kunnen voldoen aan de wettelijk aan ons gestelde eisen maakt ons kantoor gebruik van een intern handboek Datalekken waarin onze werkwijze geregeld is.

4. Wet ter voorkoming van Witwassen en Financiering van Terrorisme (WWFT)

De wet WWFT brengt verplichtingen met zich mee voor onder andere banken, verzekeraars en accountants. Ook ons administratiekantoor dient hier zijn medewerking aan te verlenen. In dit kader moeten wij de identiteit van onze klanten vaststellen. Wij vragen nieuwe klanten om een kopie van hun identiteitsbewijs in te leveren en wij dienen vast te stellen dat de identiteit van de klant overeenkomt met die op het identiteitsbewijs. Tevens dienen wij bij ondernemingen uw eigendoms- en zeggenschapsstructuur in kaart te brengen en de risico's vast te leggen. Indien wij dat noodzakelijk achten doen wij een uitgebreider onderzoek.

In geval van een rechtspersoon kunnen wij normaal gesproken volstaan met een uittreksel van de kamer van Koophandel en identificatie van de eigenaar met een belang van 25% of meer.

In het kader van de WWFT zijn wij verplicht ongebruikelijke transacties te melden. Hieronder vallen onder meer kastransacties verricht aan of via ons kantoor van € 15.000 of meer. Ook andere transacties die op witwassen of financiering van terrorisme duiden zijn wij verplicht te melden aan de overheid. Overigens zult u hier -normaal gesproken- niet mee te maken krijgen.

Om te kunnen voldoen aan de wettelijk aan ons gestelde eisen maakt ons kantoor gebruik van een intern handboek WWFT waarin onze werkwijze geregeld is.

5. Contactgegevens bij vragen

- E-mailadres: info@twanvandewiel.nl
- Telefoonnummer: 0416-337793
- Contactpersoon: Twan van de Wiel