Aanvraagformulier Cyberverzekering

Digitale ontwikkelingen gaan razendsnel. Maar naast alle mogelijkheden, brengt dit ook complexe uitdagingen mee. Zoals cybersecurity. In deze snel veranderende wereld helpt onze cyberverzekering uw cyberrisico's te beheersen en steeds een stap voor te zijn.

Cyber incidenten

Een cyberincident kan door verschillende oorzaken ontstaan. Bijvoorbeeld als door een beveiligingslek data wordt gestolen, of als uw complete netwerk wordt platgelegd met gijzelsoftware.

Dekking

Met de AIG Cyberverzekering helpen wij de gevolgen van het incident te beperken, zo goed mogelijk op te lossen en gevolg schade te vergoeden. Denk bijvoorbeeld aan:

Kosten voor experts die u helpen het incident te onderzoeken, op te lossen en het systeem te herstellen. Zo kunt u zo snel mogelijk uw bedrijfsvoering hervatten.

Bedrijfsschade (verlies van omzet) door een Cyberincident, ook als dat komt door uitbestede IT systemen.

Datalekken en eventuele notificatie naar toezichthouders en betrokkenen.

Aansprakelijkheid als gevolg van bovengenoemde gebeurtenissen.

Systeemfalen is een optionele module voor onopzettelijke en onvoorziene uitval van het computer systeem van verzekerde. Systeemfalen biedt dekking voor het verlies door een netwerkonderbreking die niet het gevolg is van een cyber incident. Met deze aanvulling ontstaat een Cyber allrisk dekking voor bedrijfsschade.

First Response bij noodgevallen

Al bij het vermoeden van een cyberincident kunt u 24/7 de CyberEdge hotline bellen. Tijdens de eerste cruciale 48 uur krijgt u de beste internationale hulp ten aanzien van IT security, juridische vraagstukken en PR. Hiervoor geldt geen eigen risico en de kosten hebben geen impact op de limiet.

Waarom de cyberverzekering van AIG?

Gratis preventieve tools en services
Wij bieden kosteloos diverse beveiligingsmaatregelen aan waaronder bewustwordingstrainingen voor personeel (tot 10.000 werknemers en beschikbaar in >30 talen), kwetsbaarheden scans, identity security assessment en nog veel meer.

Ruime dekking

- Standaard alle dekkingsrubrieken meeverzekerd
- Vrijwillige uitschakeling van IT systeem vanwege een (mogelijk) cyberaanval
- 365 dagen bedrijfsschade + 90 dagen na oplossen incident
- Kosten van specialistische losgeld onderhandelingen en vergoeding eventuele losgeldbetalingen
- Dekking voor wijdverspreide incidenten en end-of-life-software

Jarenlange wereldwijde ervaring
Wij verzekeren al meer dan 20 jaar cyberrisico's en zijn experts als het gaat om acceptatie en behandeling van schades.

Cyberverzekering

Voor wie is dit formulier?

Dit aanvraagformulier is bedoeld voor organisaties met een totale groepsomzet tot 500M. Voor organisaties hogere omzet dan 500M of activiteiten in sectoren met een verhoogd risicoprofiel hanteren wij een ander aanvraagformulier. Zie hiervoor www.aiginsurance.nl. De volgende sectoren worden beschouwd als sectoren met een verhoogd risico: Luchtvaartmaatschappijen, Financiële instellingen, Ziekenhuizen, Advocatenkantoren, Managed Service (security) Providers (M(S)SP), Payment processors, overheidsinstanties (waaronder Gemeenten) en Scholen.

Invulinstructie

Voor het verkrijgen van een offerte is het van belang dat het formulier volledig wordt ingevuld. Het aanvraagformulier dient getekend en gedateerd te worden door een daartoe bevoegd persoon.
Het invullen en ondertekenen van het formulier verplicht de verzekeringnemer of verzekeraar niet om de verzekeringsovereenkomst aan te gaan.

"***Organisatie***" verwijst individueel en collectief naar elke persoon of entiteit die verzocht wordt onder deze verzekering te vallen.
Verzekeraar" betekent de verzekeringsmaatschappij die gelieerd is aan American International Group, Inc. en die de polis uitgeeft aan de organisatie op basis van deze aanvraag. AIG Europe S.A. is een verzekeringsmaatschappij naar Luxemburgs recht met R.C.S. Luxemburgs nummer B218806. AIG Europe S.A. heeft zijn hoofdkantoor op 35D Avenue J.F. Kennedy, L-1855 Luxemburg. http://www.aig.lu/.

Algemene informatie

Naam (kandidaat)verzekeringnemer (Organisatie):	
(kandidaat)verzekeringnemer is:	◯ Moederonderneming (holding) ◯ Dochteronderneming
Website:	
Aantal werknemers:	
Jaarinkomsten (omzet en/of baten):	

Omzetverdeling Geografisch

Totaal % van inkomsten moet gelijk zijn aan 100% (selecteer alles wat van toepassing is).

Australië en Nieuw-Zeeland	%	Rusland	%
Canada	%	Mexico, Centraal-Amerika en Caraïben	%
Verenigde Staten	%	Zuid-Amerika	%
Oost-Azië	%	Verenigd Koninkrijk (UK)	%
Europe (ex UK)	%	Zuid-Afrika	%
Centraal- en Zuid-Azië	%		
Midden-Oosten en Noord-Afrika	%	**Totaal**	**%**

Cyberverzekering

Gegevens Chief Information Security Officer (CISO) van de ***organisatie***, of gelijkwaardige werknemer, die verantwoordelijk is voor het handhaven van de cyberbeveiliging van de ***organisatie***.

Naam:	
Functie:	
E-mail:	

*De **verzekeraar** kan, maar is nooit verplicht om, (1) extern waarneembare gegevens over het computernetwerk van de **organisatie** te onderzoeken, en (2) contact op te nemen met de Chief Information Security Officer (CISO) van de **organisatie** (of een andere hierboven aangewezen persoon) in verband met een omstandigheid waarvan de **verzekeraar** redelijkerwijs denkt dat deze kan leiden tot een toekomstig cyberincident waarvoor dekking kan worden verleend onder de Cyberverzekering. De **verzekeraar** zal blijven observeren en rapporteren, zoals hierboven beschreven, gedurende de looptijd van de Cyberverzekering van de **organisatie**.*

Data

Vul onderstaand het aantal unieke gegevens (geschat) in die de ***organisatie*** in bezit heeft, verwerkt, opslaat en/of overdraagt, met inbegrip van gegevens verzameld, verwerkt, of opgeslagen door anderen (uitbesteed).

Persoonsgegevens van eigen personeel, klanten of andere derden:		
Medische gegevens van eigen persoon, klanten of andere derden:	of	◯ N.v.t.
Betaalkaarttransacties per jaar (PCI):	of	◯ N.v.t.
Biometrische gegevens:	of	◯ N.v.t.

Sector

Selecteer in welke van de onderstaande sector(en) de ***organisatie*** actief is of welke activiteiten worden verricht.
Totaal % van inkomsten moet gelijk zijn aan 100%.

Accountancy	%	Media of gerelateerde activiteiten	%
Landbouw, bosbouw, mijnbouw, visserij en jacht	%	Payment processing	%
Advocatuur	%	Vastgoed	%
Incasso bureau	%	Detailhandel (incl. webshops)	%
Bouw	%	(ICT) Informatie, communicatie en technologie (excl. payment processing)	%
Kredietbeoordelaar	%	Telemarketing	%
Horeca	%	Uitzendbureau, werving & selectie en payrolling	%
Educatie (gerelateerd)	%	Management van bedrijven en ondernemingen	%
Financiële instelling	%	Transport, logistiek en opslag	%
Financiële dienstverlening (anders dan financiële instellingen)	%	Reisbureau	%
Dienstverlening: adviserende, wetenschappelijke en technische diensten	%	Groothandel	%
Gaming en kansspelen	%	Nutsvoorzieningen	%
Overheidsactiviteiten (o.a. gemeentes etc.)	%	Afvalbeheer en saneringsdiensten, en gerelateerde diensten	%
Ziekenhuis, gezondheidszorg en sociale zekerheid	%	Niet vermeld, namelijk:	%
Hotel	%		
Productie / Fabricage	%	**Totaal**	**%**

IT omgeving

a. Maakt de ***organisatie*** gebruik van Microsoft Active Directory Domain Services ("ADDS"), op locatie, gehost of in een hybride configuratie? Om misverstanden te voorkomen: met ADDS wordt uitdrukkelijk NIET Azure Active Directory ("Azure AD") of Microsoft Entra ID bedoeld. Ja ◯ Nee ◯

b. Maakt de ***organisatie*** gebruik van Microsoft Exchange, eventueel in een "hybride implementatie"? Ja ◯ Nee ◯

c. Maakt de ***organisatie*** gebruik van niet-ondersteunde/ legacy software ('unsupported software' waarvoor de leverancier geen beveiligingspatches meer levert)? Ja ◯ Nee ◯

Beveiligingsmaatregelen

De volgende vragen zien toe op de beveiligingsmaatregelen binnen de IT omgeving van de ***organisatie***. Hiervoor betekent 'IT omgeving', zowel de interne als het uitbestede deel van de IT van de ***organisatie***. Mocht een antwoord niet 100% passen bij de situatie van de ***organisatie***, selecteer dan "Nee" en geef aanvullende informatie over de nuances binnen de open tekstvakken in het formulier of in een apart document.

1. Backups and herstelmogelijkheden

a. Er bestaat een proces voor het maken van regelmatige back-ups (zelfs als dit niet gedocumenteerd en/of ad hoc is). Ja ◯ Nee ◯

b. De back-upstrategie omvat regelmatige offline back-ups (onsite of offsite). Ja ◯ Nee ◯

c. Back-ups zijn geïsoleerd en gescheiden van het productiedomein (d.w.z. cloudback-ups met MFA-bescherming) of ze zijn 'immutable'. Ja ◯ Nee ◯

d. Er is een gedocumenteerd incident response plan. Ja ◯ Nee ◯

2. Remote access (selecteer één antwoord)

Alleen een geldige gebruikersnaam en wachtwoord (single factor authenticatie) is nodig om op afstand toegang te krijgen tot de IT omgeving. ◯

Multi-factor authenticatie (MFA) is ingeschakeld voor verbindingen voor werknemers om op afstand toegang te krijgen tot de IT omgeving, alle uitzonderingen hierop worden bijgehouden. ◯

Multi-factor authenticatie (MFA) is ingeschakeld voor alle verbindingen (werknemers, opdrachtgevers, IT partners etc.) om op afstand toegang te krijgen tot de IT omgeving, alle uitzonderingen hierop worden bijgehouden. ◯

Er wordt geen toegang op afstand geboden. ◯

3. Wachtwoordbeleid

a. Er is een password manager ter beschikking gesteld aan alle werknemers. Ja ◯ Nee ◯

b. Er is een beleid tegen hergebruik van wachtwoorden (voor applicaties op de IT omgeving worden unieke wachtwoorden gebruikt). Ja ◯ Nee ◯

c. Serviceaccounts (accounts die door machines/ software - niet door mensen - worden gebruikt voor het uitvoeren van applicaties en processen) hebben een wachtwoordlengte van tenminste 25 tekens. Ja ◯ Nee ◯

Aanvullende toelichting beantwoorde vragen

4. Monitoring & detectie

a. Er is een SIEM-tool (Security Information and Event Monitoring) in gebruik. Ja ◯ Nee ◯

b. Het netwerkverkeer wordt gemonitord op abnormale of mogelijk verdachte gegevensoverdrachten. Ja ◯ Nee ◯

c. Er is een "Security Operations Center" oftewel SOC aanwezig om beveiligingsincidenten te monitoren, eventueel intern en/of verzorgd door een MSSP (Managed Security Services Provider). Ja, 24/7 ◯ Ja, maar niet 24/7 ◯ Nee ◯

d. Er is een gedocumenteerd incident response plan met specifieke aandacht voor Cyber incident management. Ja ◯ Nee ◯

5. Phishing beveiliging: organisatorisch

a. Medewerkers krijgen tenminste één keer per jaar een bewustwordingstraining over beveiliging, met specifieke aandacht voor phishing. Ja ◯ Nee ◯

b. Ten minste jaarlijks worden gesimuleerde phishing-aanvallen uitgevoerd om het bewustzijn van werknemers te monitoren. Ja ◯ Nee ◯

c. Er is een gedocumenteerd proces om verdachte e-mails te melden aan een (intern) beveiligingsteam voor onderzoek. Ja ◯ Nee ◯

6. Phishing beveiliging: technisch

a. Extern ontvangen e-mails worden als 'extern' gemarkeerd of getagd. Ja ◯ Nee ◯

b. Er is een e-mailfilteroplosing die bekende kwaadaardige bijlagen en verdachte bestandstypen blokkeert, inclusief 'executable' bestanden. Ja ◯ Nee ◯

c. Er is een webfilteringsoplossing waardoor werknemers bekende kwaadaardige of verdachte webpagina's niet kunnen bezoeken. Ja ◯ Nee ◯

d. De webfiltermogelijkheden zijn voor alle systemen, ook indien deze zich niet op de omgeving van de organisatie bevinden (systemen welke bijvoorbeeld zijn geconfigureerd om cloudbased webfilters te gebruiken of een VPN-verbinding vereisen om op het internet te surfen). Ja ◯ Nee ◯

7. Endpoint security tools

a. Er wordt gebruik gemaakt van beveiligingssoftware (antivirus) op werkstations met heuristische mogelijkheden en/of tools met detectie van ongebruikelijk gedragspatronen en misbruik (exploit) bescherming. Ja ◯ Nee ◯

b. Er wordt gebruik gemaakt van 'endpoint threat detection and response (ETDR of EDR)' software die het volgende doet: controleren op dreigingsindicatoren; patronen identificeren die overeenkomen met bekende dreigingen; automatisch reageren door dreigingen te verwijderen of in te perken; beveiligingspersoneel waarschuwt bij incidenten; forensische en analysemogelijkheden biedt om analisten in staat te stellen op dreigingen te reageren. Ja ◯ Nee ◯

Aanvullende toelichting beantwoorde vragen

8. Scope van Endpoint security tools

a. De in vraag 7 benoemde beveiligingssoftware wordt op alle werkstations (desktop en laptops) gebruikt. Ja ◯ Nee ◯

b. De in vraag 7 benoemde beveiligingssoftware wordt op alle servers gebruikt. Ja ◯ Nee ◯

c. Automatische updates zijn ingeschakeld voor bovenstaande beveiligingssoftware. Ja ◯ Nee ◯

d. De benoemde beveiligingssoftware is ingesteld zodat verdachte processen/ bestanden geblokkeerd worden (i.p.v. alleen gemeld worden). Ja ◯ Nee ◯

9. Patching

a. Wat is de termijn waarbinnen patches met de hoogste prioriteit worden uitgevoerd buiten het reguliere periodieke patchbeleid /-processen om? (bijvoorbeeld in het geval van een in-the-wild-exploitatie van software waarvoor een out-of-band patch beschikbaar is)? 0-3 dagen ◯ 3-7 dagen ◯ >7 dagen ◯

b. Wordt er regelmatig een 'vulnerability scan' op de extern blootgestelde IT omgeving uitgevoerd? Ja ◯ Nee ◯

10. Segmentatie en bescherming

a. Er zijn netwerk- en/of hostfirewallregels geïmplementeerd die het gebruik van RDP (Remote Desktop Protocol) om extern in te loggen op werkstations voorkomt. Ja ◯ Nee ◯

b. Alle serviceaccounts (accounts die door machines/ software - niet door mensen - worden gebruikt voor het uitvoeren van applicaties en processen) worden bijgehouden op een lijst. Ja ◯ Nee ◯ Wij hebben geen service accounts ◯

c. Netwerkfirewalls zijn geïmplementeerd op alle locaties van de ***organisatie***. Ja ◯ Nee ◯

11. Data Beveiliging

Gegevens worden versleuteld op apparaten van gebruikers om gegevens te beveiligen tegen verlies van apparaten. Voorbeelden zijn Windows Bitlocker, Apple FileVault en Linux dm-crypt. Ja ◯ Nee ◯

Aanvullende toelichting beantwoorde vragen

Cyberverzekering

Service Providers Section

Geef de naam van de externe dienstverleners die u gebruikt voor elk van de volgende categorieën. Indien de ***organisatie*** geen gebruik maakt van dienstverleners en uitsluitend interne IT omgeving gebruikt, of indien de categorie niet van toepassing is, vink dan het vakje n.v.t. aan voor deze categorie. Als er andere externe dienstverleners zijn die van invloed zijn en die niet in de lijst zijn opgenomen, gebruik dan het vakje "Anders".

Hosting Services

- ◯ N.v.t.
- ◯ Accenture
- ◯ Akamai
- ◯ Amazon AWS
- ◯ Atos
- ◯ AT&T
- ◯ CloudFlare
- ◯ Dell
- ◯ Equinix
- ◯ Fujitsu
- ◯ F5 Networks
- ◯ Gandi SAS
- ◯ Google
- ◯ HCL Technologies
- ◯ Hewlett Packard
- ◯ IBM
- ◯ Microsoft
- ◯ Newfold Digital
- ◯ OVH SAS
- ◯ Rackspace
- ◯ Siemens
- ◯ Telefonica
- ◯ United Internet AG
- ◯ Verizon
- ◯ Oipro
- ◯ Anders:

E-Mail (services)

- ◯ N.v.t.
- ◯ Amazon AWS SES
- ◯ AppRiver, LLC
- ◯ Barracuda Networks
- ◯ CyrenCorporation
- ◯ GoDaddy
- ◯ Google
- ◯ Intuit Mailchimp
- ◯ MailChannels
- ◯ McAfee, Inc
- ◯ Microsoft
- ◯ Mimecast
- ◯ Proofpoint
- ◯ Rackspace
- ◯ SendGrid, Inc
- ◯ Symantec
- ◯ United Internet AG
- ◯ Anders:

Relatiemanagement / CRM Software

- ◯ N.v.t.
- ◯ Aptean
- ◯ Astute
- ◯ Atos
- ◯ Deltek
- ◯ eGain
- ◯ Gainsight
- ◯ Google
- ◯ Infor
- ◯ Medallia Inc
- ◯ Microsoft
- ◯ Oracle
- ◯ Sage Group
- ◯ Salesforce.com
- ◯ SAP
- ◯ Veeva Systems
- ◯ Zoho Corporation
- ◯ Anders:

HR Management

- ◯ N.v.t.
- ◯ ADP
- ◯ Avature Recruiting
- ◯ Ceridian
- ◯ Cornerstone
- ◯ Fujitsu
- ◯ HCL Technologies
- ◯ iCIMS
- ◯ IBM
- ◯ Jobvite
- ◯ Kronos
- ◯ NICE Systems
- ◯ Oracle
- ◯ PeopleAdmin
- ◯ PeopleFluent
- ◯ SAP
- ◯ WorkDay
- ◯ Xactly Corporation
- ◯ Anders:

E-Commerce & betaaldiensten

- ◯ N.v.t.
- ◯ Adyen
- ◯ Amazon AWS
- ◯ Apple
- ◯ Atos
- ◯ BlueSnap
- ◯ CCBill
- ◯ EverCommerce
- ◯ Fidelity National Information Services
- ◯ Fujitsu
- ◯ Ingenico
- ◯ Klarna AB
- ◯ NCR Corporation
- ◯ PayPal
- ◯ Recurly
- ◯ Square
- ◯ Stripe
- ◯ VeriFone Systems
- ◯ Anders:

Industrial Control

- ◯ N.v.t.
- ◯ ABB
- ◯ Bosch
- ◯ Emerson
- ◯ GE
- ◯ Honeywell
- ◯ Metso
- ◯ Mitsubishi Electric
- ◯ Rockwell Automation
- ◯ Rolls Royce
- ◯ Schneider
- ◯ Siemens
- ◯ Toshiba
- ◯ Yokogawa
- ◯ Anders:

IT Security Services

- ◯ N.v.t.
- ◯ Accenture
- ◯ Akamai
- ◯ Atos
- ◯ Carbon Black
- ◯ Cisco
- ◯ CloudFlare
- ◯ Comodo Group
- ◯ CrowdStrike
- ◯ Dell
- ◯ DigiCert
- ◯ Fujitsu
- ◯ GMO GlobalSign
- ◯ HCL Technologies
- ◯ Hewlett Packard
- ◯ IBM
- ◯ Let's Encrypt
- ◯ McAfee
- ◯ Microsoft
- ◯ Okta
- ◯ Palo Alto
- ◯ Sentinel One
- ◯ Siemens
- ◯ Symantec
- ◯ Tenable Network
- ◯ TrustWave Holdings
- ◯ Unisys
- ◯ Verizon
- ◯ Wipro
- ◯ Anders:

Cyberverzekering

Slotvragen

1. Heeft de ***organisatie*** in de afgelopen 5 jaar een of meerdere van de onderstaande beveiligingsincidenten ervaren:

a. Ransomware — Ja ◯ Nee ◯

b. Significante datalekken / privacy schendingen met aanzienlijke gevolgen — Ja ◯ Nee ◯

c. Andere beveiligingsincidenten met aanzienlijke gevolgen — Ja ◯ Nee ◯

*** Indien ja, graag de volgende informatie aanleveren:**

- Een samenvatting van het incident en de rootcause (of hoofdoorzaak) van het incident.
- Welke beveiligingsmaatregelen zijn er getroffen een soortgelijk incident in de toekomst te voorkomen?
- Heeft u forensisch onderzoek uitgevoerd naar de oorzaak? Zo ja, dan ontvangen we graag een kopie van het rapport.
- Welke schade uitgedrukt in een bedrag (EUR) heeft u als gevolg van dit incident geleden (denk hierbij aan kosten van externe experts, herstel en gevolgschade zoals bedrijfsschade)

2. Heeft de ***organisatie*** een vestiging, dochteronderneming, deelneming of joint venture in en/of doet de ***organisatie*** zaken (met partijen) in een land waarop de Verenigde Naties, de Verenigde Staten, de Europese Unie of Nederland een sanctieregeling van toepassing heeft verklaard? Ja ◯ Nee ◯

3. Is in de afgelopen 5 jaar:

a. aan ***verzekeringnemer*** een verzekeringsovereenkomst geweigerd? Ja ◯ Nee ◯

b. een verzekeringsovereenkomst van ***verzekeringnemer*** opgezegd? Ja ◯ Nee ◯

c. aan ***verzekeringnemer*** een verzekeringsovereenkomst onder beperkende of bijzondere voorwaarden voorgesteld? Ja ◯ Nee ◯

d. een aanspraak op dekking van ***verzekeringnemer*** geheel of gedeeltelijk afgewezen? Ja ◯ Nee ◯

e. door een verzekeraar van ***verzekeringnemer*** schade teruggevorderd in verband met onware opgave? Ja ◯ Nee ◯

4. Is ***verzekeringnemer*** of een andere belanghebbende bij deze verzekering, in de laatste 8 jaar, als verdachte of ter uitvoering van een opgelegde (straf)maatregel, in aanraking geweest met politie of justitie in verband met: Ja ◯ Nee ◯

- wederrechtelijk verkregen of te verkrijgen voordeel, zoals diefstal, verduistering, bedrog, oplichting, valsheid in geschrifte of poging(en) daartoe en enige (andere vorm) van fraude;
- wederrechtelijke benadeling van anderen, zoals vernieling of beschadiging, mishandeling, afpersing en bedreiging of enig misdrijf gericht tegen de persoonlijke vrijheid of tegen het leven of poging(en) daartoe; overtreding van de Wet wapens en munitie, de Opiumwet, de Wet op de economische delicten, de Wet ter voorkoming van witwassen en financieren van terrorisme of enige met het voorgaande vergelijkbare wet-of regelgeving in een andere jurisdictie?

Zo ja, geef dan aan om welk strafbaar feit het ging, of het tot een rechtszaak is gekomen, wat het resultaat daarvan was en of eventuele (straf)maatregelen al ten uitvoer zijn gelegd. Indien het niet tot een rechtszaak is gekomen, geef dan aan of er sprake is geweest van een schikking met het Openbaar Ministerie, en zo ja, tegen welke voorwaarden de schikking tot stand kwam.

5. Hieronder kan een toelichting op bovenstaande Slotvragen worden gegeven als deze met “ja” zijn beantwoord. Indien er onvoldoende ruimte aanwezig is voor de beantwoording van de vragen, dan graag op uw eigen papier aanvullende beantwoording bijvoegen.

Cyberverzekering

No-claim verklaring

Is de ***organisatie*** bekend met een gebeurtenis, voorval of omstandigheid (zoals o.a. een beveiligingsincident, datalek of ander privacy gerelateerd evenement), welke mogelijkerwijs aanleiding zou kunnen geven tot een claim onder deze polis?

- ◯ Ja
- ◯ Nee
- ◯ Niet van toepassing (de gevraagde verzekering is een verlenging van de dekking met de verzekeraar)

Er wordt in verband met het bovenstaande overeengekomen dat indien zulke gebeurtenissen, voorvallen of omstandigheden zich hebben voorgedaan, of als daarover kennis bestaat, de daaruit voortvloeiende schade of claims uitgesloten worden van de dekking.

Ondertekening

Ondergetekende is bevoegd de ***organisatie*** in deze te vertegenwoordigen.
Ondergetekende verklaart hierbij ook dat hij / zij de disclaimer in dit formulier heeft gelezen en daarmee akkoord gaat.

Naam:	Handtekening:
Functie:	
E-mailadres:	
Plaats:	
Datum:	

DISCLAIMER

Alle geschreven verklaringen, al het materiaal of alle documenten die samen met dit formulier aan verzekeraar worden verstrekt, ongeacht of deze documenten al dan niet bij de polis worden gevoegd, worden geacht onderdeel uit te maken van de verzekeringsaanvraag.

Juridische informatie en handtekeningen

Lees, vóór u dit formulier ondertekent, deze mededelingen aandachtig en bespreek ze met uw bemiddelaar of verzekeringsadviseur als u vragen heeft.

Ten behoeve van de verzekeringsaanvraag verklaart ondergetekende, die bevoegd is de onderneming te vertegenwoordigen:

- dat alle gegevens vermeld in dit formulier en in alle bijlagen juist en volledig zijn;
- dat hij/zij na een deugdelijk onderzoek binnen haar organisatie dit formulier volledig en naar waarheid heeft beantwoord en geen belangrijke aspecten die voor de verzekeraar van belang zijn voor de acceptatie van deze verzekeringsovereenkomst heeft verzwegen of niet geheel juist heeft voorgesteld.

Ten behoeve van deze aanvraag verklaart ondergetekende dat hij/zij de verzekeraar onmiddellijk op de hoogte stelt van iedere wezenlijke verandering (materiele wijziging) in de gegevens die in deze verzekeringsaanvraag zijn vermeld, of deze nu voor of na de afsluiting van de verzekeringsovereenkomst plaatsvindt.

Het ondertekenen van dit formulier verbindt u of de verzekeraar er niet toe om de verzekering af te sluiten. Als de verzekering wel wordt afgesloten, vormt dit formulier en alle informatie die hier wordt gegeven, de basis van de verzekering, en voornoemde informatie maakt daardoor onderdeel uit van de verzekering.

Indien u vragen heeft over de verzekering, neem dan contact op met uw bemiddelaar of verzekeringsadviseur. Deze verzekering kan alleen tot stand worden gebracht door bemiddeling van een bemiddelaar.

Als (kandidaat-)***verzekeringnemer*** bent u verplicht de gestelde vragen in dit formulier zo volledig mogelijk te beantwoorden. Dit geldt ook voor feiten en omstandigheden die betrekking hebben op een bij het sluiten van deze verzekeringsovereenkomst bekende derde, wiens belangen worden meeverzekerd. Bij de beantwoording is bovendien niet alleen de eigen wetenschap van de ***verzekeringnemer*** bepalend, maar ook die van de andere belanghebbenden bij deze verzekering.

De vragen die gericht zijn op het schadeverleden gelden ook voor de leden van de maatschap, de (commanditaire) vennoten van de vennootschap onder firma (VOF), de statutair directeur(en)/bestuurder(s) van de rechtspersoon en de aandeelhouder(s) met een belang van 33,3% of meer en – zo deze zelf een rechtspersoon is (zijn) – hun statutair directeur(en)/bestuurder(s) en aandeelhouders(s) met een belang van 33,3% of meer.

Feiten en omstandigheden die u bekend worden nadat u deze verzekeringsaanvraag heeft ingezonden, maar voordat u bent bericht over de definitieve beslissing over het al dan niet accepteren door de verzekeraar van het door u aangeboden risico, moet u alsnog onmiddellijk aan de verzekeraar mededelen indien deze vallen onder de vraagstelling in dit formulier. De verzekeraar heeft het recht om op basis van deze nieuwe feiten en omstandigheden het risico niet te accepteren of een reeds gedaan (voorlopig) voorstel te wijzigen of in te trekken.

Vragen waarvan u het antwoord al bij de verzekeraar bekend veronderstelt, moet u toch zo volledig mogelijk beantwoorden. Indien u niet (volledig) aan uw mededelingsplicht heeft voldaan, kan dit ertoe leiden dat het recht op uitkering wordt beperkt of zelfs vervalt. Indien u met opzet tot misleiden van de verzekeraar heeft gehandeld of de verzekeraar bij kennis omtrent de ware stand van zaken de verzekeringsovereenkomst niet zou hebben gesloten, heeft de verzekeraar tevens het recht de verzekeringsovereenkomst op te zeggen.

In afwijking van het bepaalde in artikel 7:928, lid 6, BW gelden ten aanzien van de mededelingsplicht voor deze verzekering bovendien de volgen uw organisatie uitgangspunten:

- een niet beantwoorde of open gelaten vraag wordt geacht ontkennend te zijn beantwoord;
- de slotvragen dient volledig te worden beantwoord. Een slotvraag wordt geacht onvolledig te zijn beantwoord, indien daarbij feiten en omstandigheden zijn verzwegen of verkeerd voorgesteld waarvan aanvrager, bijvoorbeeld op grond van de overige op het aanvraagformulier gestelde vragen en/of de aard van de aangevraagde verzekering in relatie tot hetgeen niet is opgegeven of verkeerd is voorgesteld, in redelijkheid moest begrijpen dat deze voor de beoordeling van het ter verzekering aangeboden risico van belang konden zijn.

Stichting CIS

In verband met een verantwoord acceptatie-, risico- en fraudebeleid kunnen wij uw gegevens raadplegen en vastleggen in het Centraal informatiesysteem van de in Nederland werkzame verzekeringsmaatschappijen (Stichting CIS), Bordewijklaan 2, 2591 XR te Den Haag. Doelstelling van de verwerking van persoonsgegevens bij Stichting CIS is voor verzekeraar en gevolmachtigd agenten risico's te beheersen en fraude tegen te gaan. Zie voor meer informatie ***www.stichtingcis.nl***. Hier vindt u ook het privacyreglement van Stichting CIS.

NL FINCY 1010 0923