



Dit risico inventarisatie formulier is bedoeld om informatie te verzamelen over uw cyber- en privacy risico's.

Naast de informatie in dit formulier maken wij in het kader van onze acceptatie beoordeling ook gebruik van openbare externe bronnen zoals BitSight en Company.info.

Wij vragen u dit formulier in te vullen om een goed beeld te krijgen van uw bedrijf.

Het invullen verplicht geen van beide partijen een verzekeringsovereenkomst aan te gaan dan wel te continueren.

De informatie die u in dit formulier verstrekt moet volledig, juist en niet misleidend zijn. Het betekent verder dat u ons over alle feiten en omstandigheden dient te informeren die van belang kunnen zijn voor ons besluit om al dan niet een verzekeringsovereenkomst met u aan te (blijven) gaan. Als er tussen Hiscox en u een verzekeringsovereenkomst wordt of is gesloten, dan gebeurt dat op basis van dit risico inventarisatie formulier, een aanvraagformulier, eventuele aanvullende vragen(lijsten) en alle verdere informatie die door of namens u aan ons wordt verstrekt in mondelinge, schriftelijke of andere vorm*.

Dit formulier dient te worden ondertekend door een bestuurder, partner, directeur of andere tekeningsbevoegde van de aanvrager en hij of zij dient bij collega-bestuurders, -partners, -directeuren of medewerkers alle informatie in te winnen die nodig is om de vragen juist te kunnen beantwoorden.

Privacy

Hiscox is een handelsnaam voor een aantal Hiscox-vennootschappen. Het specifieke bedrijf dat optreedt als verwerkingsverantwoordelijke van uw persoonsgegevens staat aangegeven in de documentatie die wij aan u verstrekken.

Wanneer u vragen heeft kunt u altijd contact met ons opnemen door te bellen naar +31(0)20 517 0700 of door ons te mailen op hiscox.underwriting@hiscox.nl.

Wij verzamelen en verwerken gegevens over u om verzekeringen te verstrekken, te beheren en schade te behandelen. Uw gegevens worden ook voor zakelijke doeleinden gebruikt, zoals fraudepreventie en -opsporing en financieel beheer. In dit kader kunnen uw gegevens worden gedeeld en kunnen gegevens over u worden verkregen van onze vennootschappen van de Groep en derden, waaronder verzekeringsadviseurs en -intermediairs, schade-experts, advocaten, kredietinformatiebureaus, dienstverleners, herverzekeraars, professionele adviseurs, toezichthouders of bureaus voor fraudepreventie.

Wij kunnen telefoongesprekken opnemen om ons te helpen de dienst die wij aanbieden te monitoren en te verbeteren.

Voor meer informatie over de wijze waarop uw gegevens worden gebruikt en over uw rechten in verband met uw gegevens, zie onze privacyverklaring op www.hiscox.nl.

Ik geef Hiscox toestemming om mijn gegevens te gebruiken als hierboven omschreven

* Deze informatie is de grondslag voor en vormt een integraal onderdeel van de verzekeringsovereenkomst

A. Algemeen

Gegevens aanvrager:

1A. Naam te verzekeren bedrijf:

Polisnummer:

1B. Adres:

1C. Deelnemingen met meer dan 50% aandeel:

1D. Heeft u een vestiging buiten de Europese Economische Ruimte (EER) ja nee of het Verenigd Koninkrijk?

Naam entiteit	Land van vestiging	Adres en vestigingsplaats

1E. Geef een beschrijving van uw bedrijfsactiviteiten in uw eigen woorden, inclusief eventuele specialisaties:

1F. Vermeld alle websites die eigendom zijn van uw organisatie:

1G. Contactpersoon/risk manager:

Naam	Functie	E-mailadres

2A. Omvang en herkomst van uw omzet of exploitatiesom (a.) en bruto winst (b.) excl. BTW:

Herkomst omzet	Vorig boekjaar, eindigend op ___ / ___ / _____	Lopend boekjaar, eindigend op ___ / ___ / _____	Schatting volgend boekjaar, eindigend op ___ / ___ / _____
a. Nederland	€	€	€
a. EER en UK	€	€	€
a. USA/Canada	€	€	€
a. Rest van de wereld	€	€	€
a. Totale omzet of exploitatiesom	€	€	€
b. Bruto winst	€	€	€

2B. Wat is uw verdeling van de totale omzet (off- en online)?

Offline % Online %

2C. Wat is uw gemiddelde brutowinstmarge over de afgelopen 3 jaar? %

3. Aantal medewerkers:

	Vorig boekjaar, eindigend op ___ / ___ / _____	Lopend boekjaar, eindigend op ___ / ___ / _____	Schatting volgend boekjaar, eindigend op ___ / ___ / _____
Nederland			
EER en UK			
USA/Canada			
Rest van de wereld			

B. Toelichting op uw activiteiten en de hoeveelheid van uw data

4. Hoeveel gegevens/data heeft u, zowel elektronisch als fysiek?

Aantal records*	Persoonsgegevens**	Bijzondere persoonsgegevens***	Creditcardgegevens
0 - 20.000	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
20.001 - 100.000	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
100.001 - 250.000	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
250.001 - 500.000	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
500.001 - 1.000.000	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.000.001 - 6.000.000	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
> 6.000.000	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

* De hoeveelheid data uitgedrukt in het aantal "records" die het bedrijf onder zich heeft. Een record is een verzameling gegevens van één persoon.

** Voor hoeveel personen (waaronder klanten, medewerkers en leveranciers) verwerkt, verwerkt of bewaart u basisprofielgegevens (naam, adres, e-mailadres, telefoonnummer)?

*** Zoals, maar niet beperkt tot, godsdienst of levensovertuiging, ras, politieke voorkeur, medisch, financieel (anders dan creditcard). Een organisatie mag geen gevoelige persoonsgegevens gebruiken, tenzij daarvoor in de wet een uitzondering is gemaakt.

5. Zijn uw (kritische) bedrijfsprocessen gekoppeld aan het bedrijfsnetwerk of het internet? Het gaat hier bijvoorbeeld om: productiemachines, orderpicksystemen, webshops.

nee gedeeltelijk ja

Bedrijfsschade:

6. Wat is naar uw inschatting de financiële schade per dag indien er sprake is van onderbreking of ernstige belemmering van uw bedrijfsactiviteiten als gevolg van een cyberrisico?

€

7. Stel: U wordt getroffen door een cyberincident waardoor uw systemen (ICT en/of productiemachines) niet beschikbaar zijn voor gebruik. Wanneer komen uw (kritische) bedrijfsprocessen in gevaar?:

- Binnen één dag
 Binnen twee dagen
 Na één week
 Na twee weken of langer

C. AVG

8. Is uw onderneming AVG compliant? ja nee

Zo niet, welke stappen heeft u wel genomen?

9. Worden de personeelsleden met toegang tot persoonsgegevens jaarlijks getraind op het gebruik hiervan en geïnformeerd over wet- en regelgeving? ja nee

10. Heeft u toestemming gevraagd aan de personen waarvan u data opslaat en biedt u de mogelijkheid deze data in te zien en op verzoek te verwijderen? ja nee

11. Deelt u persoonsgegevens met derden? ja nee

Zo ja, heeft/hebben deze derde partij(en) een (contractuele) verplichting om AVG compliant te zijn?

ja nee

12. Heeft u toegang tot persoonsgegevens beperkt tot de gebruikers voor wie dit noodzakelijk is om hun taken uit te voeren en wordt deze toelating regelmatig opnieuw bekeken? ja nee

D. Toelichting op uw organisatie- en informatiebeveiliging

13. Hoeveel fysieke en virtuele servers heeft uw bedrijf?

14. Hoeveel medewerkers gebruiken een PC of een laptop voor hun dagelijkse werkzaamheden?

15. Is er sprake van fysieke beveiligingsmaatregelen om ongeoorloofde toegang tot computersystemen en datacentra te voorkomen en op te sporen? ja nee

- 16A. Krijgen uw medewerkers jaarlijks training op het gebied van cyberbeveiliging? ja nee

- 16B. En zo ja; (vink alle opties aan die van toepassing zijn):

- Alle medewerkers krijgen ten minste eenmaal per jaar trainingen en/of bijscholingen over het omgaan met vertrouwelijke gegevens en cyberrisico's
 Het personeel krijgt af en toe training over de omgang met vertrouwelijke gegevens en cyberrisico's
 Er worden jaarlijkse phishingtests uitgevoerd
 Geen van de bovenstaande

Beveiligingssoftware en versleuteling:

17. Maakt u gebruik van een information security management system (ISMS)? ja nee

18. Heeft u een van de volgende certificeringen? (zo ja, graag aanvinken)

Cyber- en informatiebeveiliging:

- ISO 27001 (Informatiebeveiliging)
- ISO 27002 (Informatiebeveiliging)
- ISO 27017 (Informatiebeveiliging security controls for cloud services)
- ISO 27018 (Informatiebeveiliging bescherming persoonsgegevens in de cloud)
- ISAE 3402

Privacy:

- ISO 27701 (privacy management)

Onderwijs:

- IBHO (Informatiebeveiliging hoger onderwijs)
- saMBO ICT

Zorg:

- NEN7510 (Informatiebeveiliging zorg)
- NEN7512 (Informatiebeveiliging zorg, vertrouwensbasis voor gegevensuitwisseling)
- NEN7513 (Informatiebeveiliging zorg logging - Vastleggen van acties op elektronische patientendossiers)

Business Continuity:

- ISO 22301 (business continuity)

19. Beschikt uw organisatie over up-to-date firewalls en bestaan er procedures over de inrichting van genoemde firewalls? ja nee

20. Met betrekking tot uw firewalls, welke van onderstaande situaties zijn op uw ICT omgeving van toepassing?

- Er zijn firewalls in gebruik in alle network gateways
- Op alle desktops, laptops en terminals zijn firewalls in gebruik
- Web application firewalls (WAF) zijn in gebruik
- Firewalls worden ingezet tussen verschillende netwerksegmenten
- Firewalls worden ingezet tussen de draadloze toegang voor gasten en de rest van uw IT-landschap
- Er zijn geen firewalls in gebruik

21A. Wordt er gebruik gemaakt van antivirus software en zijn er procedures voor het installeren en implementeren van updates op alle desktops, laptops, mobiele telefoons, tablets, e-mailsystemen, servers etc. om worms, spyware, ransomware en andere malware tegen te gaan? ja nee

Zo niet, graag een toelichting:

21B. Hoe vaak wordt deze software ge-updatet? dagelijks
 wekelijks
 maandelijks
 automatisch
 anders, te weten:

22. Heeft u applicatie-whitelisting geïmplementeerd in uw organisatie? ja nee

23. Bestaat er binnen uw organisatie een methode om alle vertrouwelijke informatie en persoons-gegevens te versleutelen met minimaal 256 bit encryptie, ongeacht waar deze informatie zich bevindt binnen het netwerk (zoals op opslag- apparaten, mobiele apparaten (inclusief laptops en smartphones), servers en andere eindpunten)? ja nee

Zo niet, op welke manier vindt de versleuteling dan plaats?

Back-ups:

24. Maakt u minimaal wekelijks back-ups van al uw kritische gegevens en kritische systemen? ja nee

Zo ja, voldoen deze o.a. aan het volgende:

- Ten minste één fysieke back-up die losgekoppeld is van uw systemen op elk gegeven moment tijd en/of; ja nee

- Inzet van een van de volgende cloud gebaseerde back-upoplossingen: Microsoft OneDrive, Google Drive, iCloud of Azure Recovery Services Vault, Amazon. ja nee

- En houdt u 1 fysieke back-up (bijvoorbeeld op tape) los van het netwerk in een (brand)veilige omgeving. ja nee

Eventuele toelichting:

25. Wordt er periodiek gecontroleerd of back-ups volledig en betrouwbaar zijn? ja nee

Zo ja, hoe vaak?

per kwartaal

per jaar

per 2 jaar

anders namelijk:

Toegangsbeheer:

26. Zijn de gebruikersrechten van werknemers in uw ICT systeem gelimiteerd tot enkel datgene wat zij nodig hebben om hun functie uit te kunnen oefenen? ja nee

27. Hebben alle admins twee accounts: één voor dagelijks gebruik zonder administratieve taken zoals het checken van e-mails? ja nee

28. Heeft u een procedure voor autorisatiebeheer geïmplementeerd in uw bedrijfsvoering? ja nee

29. Wordt de toegang van werknemers systematisch ontzegd wanneer werknemers de organisatie verlaten? ja nee

* Met kritische gegevens en kritische systemen wordt bedoeld gegevens en systemen die ertoe leiden dat uw inkomsten verliest als ze langer dan 24 uur offline of niet beschikbaar zijn of waren.

Legacy systems (verouderde systemen):

30. Gebruikt u in uw netwerkomgeving(en) nog besturingssystemen die niet langer door de fabrikant worden ondersteund? Denk bijvoorbeeld aan Windows XP, Windows 7 of Windows Server 2008? ja nee

Zo ja, welke?

- Legacy systemen zonder verdere maatregelen
- Legacy systemen met extra beveiliging
- Legacy systemen gesegmenteerd en los van internet
- Legacy systemen met gekochte extra ondersteuning (extended support)

Eventuele toelichting:

31. Worden alle IT systemen en firewalls binnen 30 dagen geüpdatet nadat de fabrikant een patch uitgeeft? ja nee

Zo niet, graag uw toelichting:

Remote access (inloggen op afstand):

32. Wordt binnen uw netwerk twee- of multi factor authenticatie* (2FA) gebruikt om de toegang tot alle web-based (mail)accounts te beheren (bijvoorbeeld Office365, Gsuite, Azure, AWS, Salesforce) en om in te loggen op afstand in uw systemen? ja nee

Segmentatie:

33. Zijn internetgerichte systemen zoals web en email servers in een DMZ** geplaatst? ja nee

34. Heeft u dochterondernemingen? ja nee

Zo ja,

Maken alle dochterondernemingen gebruik van hetzelfde IT systeem? ja nee

Maken alle dochterondernemingen gebruik van dezelfde systeembeheerders? ja nee

Heeft elke dochteronderneming een eigen netwerk welke is gesegmenteerd van de anderen? ja nee

Zo ja, hoe?

35. Zijn er gasten- of klanten wifi netwerken in een onafhankelijk netwerk gesegmenteerd? ja nee

* Naast het invoeren van een gebruikersnaam en wachtwoord, heeft de gebruiker een tweede factor nodig om in te loggen. Bijvoorbeeld in de vorm van een code die per sms naar de smartphone wordt toegestuurd.

** Een demilitarized zone (DMZ) is een netwerksegment dat zich tussen het interne en externe netwerk bevindt. DMZ is feitelijk een andere naam voor extranet.

36. Maakt u gebruik van operational technologies (OT) zoals, maar niet beperkt tot, industrial control systems (ICS), distributed control systems (DSC), SCADA systemen of internet of things (IoT)? ja nee

Zo ja, zijn uw operational technologies in een netwerk geplaatst die is gesegmenteerd van uw bedrijfsnetwerk? ja nee

Zo ja, hoe?

Indien u vraag 36 met JA heeft beantwoord vragen wij u ook om het aanvullende Hiscox CyberClear formulier in te vullen.

Betalingen:

37A. Dient uw onderneming/ organisatie te voldoen aan de PCI DSS normering (Payment Card Industry Data Security Standaard)? ja nee
 Voor toelichting: <https://www.pcisecuritystandards.org/>.

Zo ja, aan welke versie voldoet u?

37B. Maakt u gebruik van een betalingsdientaanbieder die daar wel aan voldoet? ja nee n.v.t

Vermeld hieronder de naam van de betalingsdienst aanbieder die u gebruikt:

37C. Heeft u Verified by Visa geïmplementeerd voor online betalingen? ja nee

E. Externe dienstverleners

38. Worden er ICT- of business services uitbesteed aan derden? ja nee

Zo ja, graag een opgave van uw belangrijkste providers:

Naam dienstverlener	Soort dienstverlening*

39. Host u zelf bedrijfskritische IT services**? ja nee

Zo niet, worden uw bedrijfskritische IT services gehost door twee of meer verschillende data centers die meer dan 350 km uit elkaar liggen? ja nee

* Denk hier aan: betalingsdiensten, back-up data herstel, databeheer en archivering, klantenservice, internal audits, marketing en verkoopactiviteiten, HR, business development, etc.

** Een bedrijfskritische IT-dienst wordt gedefinieerd als elke persoon of entiteit die u op grond van een schriftelijk contract computer- en elektronische technologiediensten zoals IaaS, PaaS, SaaS of webhostingdiensten (maar met uitzondering van een internetprovider of telecommunicatieprovider) levert die tot inkomstenderving zou leiden als deze langer dan 24 uur niet beschikbaar zou zijn.

Deze vraag moet worden beantwoord indien bedrijfskritische IT-services zijn uitbesteed en u overweegt om de optionele dekking (sublimiet) **Bedrijfsstagnatie van uw aanbieder van informatietechnologiediensten** mee te verzekeren:

40. Worden de door de verzekerde(n) uitbesteede bedrijfskritische IT-services geleverd door een van de volgende bedrijven:
- AWS, Google, IBM, Alibaba, Salesforce, Microsoft of Oracle? ja nee n.v.t

Is dit niet bij een van deze bedrijven, wilt u dan aangeven welke van de volgende opties van toepassing zijn op de door u uitbesteede bedrijfskritische IT-services?
(vink alle opties aan die van toepassing zijn)

Deze services worden geleverd door een aanbieder:

- Met wie u een SLA heeft die u een uptime garandeert die gelijk is aan of groter is dan 99,9%
 Die minimaal in het bezit is van een ISO27001-certificering
 En die uw gegevens of diensten hosten in twee of meer geografisch gescheiden datacenters

41. Heeft u een schriftelijke bewerkersovereenkomst met deze dienstverleners? ja nee

Zo ja, bevat deze overeenkomst de mogelijkheid om directe schade voortvloeiende uit een datalek of een tekortkoming in de dienstverlening te verhalen? ja nee

Bevat de bewerkersovereenkomst hiernaast:

- a. Voorschriften ten aanzien van de beveiliging? ja nee
b. Afspraken over de bewaking en monitoring van een eventuele inbreuk? ja nee
c. Een verplichting tot het melden bij verantwoordelijken na ontdekking of vermoeden van een datalek? ja nee

F. Aanvullende vragen

42. Worden patches en nieuwe code in een separate testomgeving getest (user acceptance testing environment) voordat deze in een liveomgeving geplaatst worden? ja nee

Detectie:

43. Hoe lang bewaart u logbestanden en notificaties over mogelijke cyberveiligheidsgebeurtenissen?

44. Welk van de volgende analyses gebruikt u om logbestanden en veiligheidswaarschuwingen te analyseren?

- SIEM
 Interne Security Operation Centre (SOC)
 Externe Security Operation Centre (SOC)
 Anders (leg uit):

- Er wordt geen analyse uitgevoerd

45. Maakt u een back-up van de logbestanden en waarschuwingen voor mogelijke cyberveiligheidsgebeurtenissen die u verzamelt? ja nee

46. Heeft u de volgende technologieën ingezet om u te helpen bij het opsporen van aanvallen?
- | | | |
|---------------------------------------|-----------------------------|------------------------------|
| a. Intrusion detection systems (IDS) | <input type="checkbox"/> ja | <input type="checkbox"/> nee |
| b. Intrusion prevention systems (IPS) | <input type="checkbox"/> ja | <input type="checkbox"/> nee |
| c. Data loss prevention (DLP) | <input type="checkbox"/> ja | <input type="checkbox"/> nee |
| d. Integriteitscontrole | <input type="checkbox"/> ja | <input type="checkbox"/> nee |
| e. Change control | <input type="checkbox"/> ja | <input type="checkbox"/> nee |

Verantwoordelijkheid IT-beveiliging:

47. Heeft u een dedicated IT-beveiligingsrol binnen uw organisatie? ja nee

- Toegewijde rol
 Specifieke rol (hoofd informatiebeveiliging of CISO)
 Een specifieke rol (hoofd informatiebeveiliging of CISO met zichtbaarheid in het bestuur)
 Anders (leg uit):

- 48A. Wanneer is voor het laatst een audit uitgevoerd in verband met ICT- beveiliging?

- 48B. Wat voor soort beveiligingsaudit is/wordt er uitgevoerd op uw netwerk? (vink alle opties aan die van toepassing zijn)

- Kwetsbaarheidsscans, minder dan jaarlijks
 Kwetsbaarheidsscans, ten minste jaarlijks
 Penetratietests, minder dan jaarlijks
 Penetratietests, ten minste eenmaal per jaar
 Geen van de bovenstaande

- 48C. En door wie is deze uitgevoerd?

- 48D. Worden de uit de audits voortvloeiende aanbevelingen geïmplementeerd? ja nee

49. Heeft u een Business Continuity of Disaster Recovery Plan dat betrekking heeft op cyberscenario's, inclusief ransomware-aanvallen? ja nee

Zo ja, hoe vaak wordt dit plan getest?

G. Gewenst verzekerd bedrag

50. Gewenste verzekerd bedrag per aanspraak / schade:

- | | |
|--------------------------------------|---------------------------------------|
| <input type="checkbox"/> € 1.000.000 | <input type="checkbox"/> € 2.000.000 |
| <input type="checkbox"/> € 2.500.000 | <input type="checkbox"/> € 5.000.000 |
| <input type="checkbox"/> € 7.500.000 | <input type="checkbox"/> € 10.000.000 |

Anders:

51. Wilt u het verzekerde bedrag verhogen tot maximaal tweemaal de aanspraak per verzekeringsjaar? ja nee

52. Wilt u de de volgende optionele dekking **Bedrijfsstagnatie bij een informatietechnologiedienstverlener waar u afhankelijk van bent** meeverzekeren?* ja nee n.v.t

Zo ja, heeft u ook de vragen beantwoord bij 40?

53. Wilt u ook een hogere sublimiet **“Cyberfraude en Cyberbedrog”** meeverzekeren*. ja nee n.v.t

Zo ja, dan dient u vragen 54 t/m 61 te beantwoorden:

54. Zijn twee of meer personen verplicht om betalingen boven de €10.000,- in waarde te controleren en te autoriseren?

- Ja, dat is het geval
 Nee, dubbele autorisatie is nooit vereist
 Nee, dubbele autorisatie is vereist, maar wel voor transacties boven € in waarde

55. Hoeveel systeemgebruikers zijn gerechtigd om betalingen te autoriseren?

56. Zijn er maatregelen getroffen om e-mails te identificeren waarmee identiteitsfraude wordt geprobeerd te plegen? Zo ja, welke?

57. Hebben het bestuur en de werknemers een formele training gehad van een externe-partij over het risico van cyberfraude en -bedrog?

58. Is er een intern proces geïmplementeerd om contactinformatie dan wel rekeningnummerinformatie van klanten/leveranciers te verifiëren?

59. Geldt dit ook wanneer er een verzoek tot wijziging ervan wordt ontvangen?

60. Is er bij nieuwe of buitenlandse klanten/leveranciers nog sprake van aanvullende verificatiemaatregelen?

ja nee

Zo ja, welke?

61. Houd u een overzicht/archief bij van frauduleuze verzoeken?

ja nee

H. Toezicht en claims

Toezicht:

62. Is verzekeringnemer/verzekerde de afgelopen vijf jaar onderwerp geweest van een onderzoek in verband met persoonsgegevens, inclusief maar niet beperkt tot betaalkaartgegevens, op het gebied van privacy?

ja nee

63. Is verzekeringnemer/verzekerde ooit verzocht informatie te verstrekken aan een toezichthoudende of vergelijkbare instantie met betrekking tot persoonsgegevens op het gebied van privacy?

ja nee

64. Is er ooit een klacht tegen u ingediend over de wijze waarop verzekeringnemer/verzekerde met persoonsgegevens omgaat? ja nee

Schadeclaims:

- 65A. Heeft verzekeringnemer /verzekerde de afgelopen drie jaar schade geleden als gevolg van een IT beveiligingsincident, privacyschending of soortgelijke omstandigheden of is er afgelopen vijf jaar een aanspraak ingediend op het gebied van privacy of cyber aansprakelijkheid? ja nee

Zo ja, vermeld hieronder de bijzonderheden:
(indien nodig kunt u op een aparte bijlage aanvullende bijzonderheden verstrekken)

- 65B. Heeft verzekeringnemer / verzekerde schade geleden als gevolg van fraude, elektronische diefstal van geld of eigendommen of de frauduleuze gebruik van uw elektronische identiteit in de afgelopen 3 jaar? ja nee

Zo ja, vermeld hieronder de bijzonderheden:
(indien nodig kunt u middels een aparte bijlage aanvullende bijzonderheden verstrekken)

66. Is verzekeringnemer/verzekerde op de hoogte van enige omstandigheid of (cyber)incident die er toe kan leiden dat er dekking onder de polis nodig zal zijn? ja nee

Zo ja, vermeld hieronder de bijzonderheden:
(indien nodig kunt u middels een aparte bijlage aanvullende bijzonderheden verstrekken)

I. Belangrijke informatie en ondertekening

U wordt verzocht alle informatie te verstrekken die relevant kan zijn voor de beoordeling van uw aanvraag. Bij twijfel of bepaalde informatie relevant is, wordt u verzocht bijzonderheden te verstrekken.

Verzekeringsadviseur:

In te sturen stukken:

- Audit/ recente ICT Security Scan (indien beschikbaar)
- Opgave medeverzekerden: organogram incl. eigendomsverhoudingen

Slotverklaring:

De verzekeringnemer bevestigt/verklaart mede gelet op de inhoud van artikel 7:928 BW, dat de gegeven informatie/ verklaringen juist en volledig is/zijn en dat mededeling is gedaan (na gedegen onderzoek) van de feiten en omstandigheden die voor Hiscox van belang zijn voor de beoordeling van zowel het te verzekeren risico als ten aanzien van de verzekeringnemer en verzekerden.

Artikel 7:928 BW bepaalt dat de verzekeringnemer verplicht is voor het sluiten van de overeenkomst alle feiten mee te delen die hij kent of behoort te kennen en waarvan, naar hij weet of behoort te begrijpen, de beslissing van de verzekeraar of, en zo ja, op welke voorwaarden, hij de verzekering zal willen sluiten afhangt of kan afhangen. Dit geldt ook voor de derden wiens belangen de verzekering dekt of mede dekt. Indien de mededelingsplicht niet of onvoldoende wordt nagekomen, kan de verzekeraar daar op grond van artikel 7:930 BW, afhankelijk van het verzuim, gevolgen aan verbinden waaronder het met onmiddellijke ingang opzeggen van de verzekering, het beperken van de dekking en het weigeren of beperken van een schadevergoeding op grond van de verzekering.

Ondertekening:

Ondergetekende verklaart verzekeringnemer bevoegd te vertegenwoordigen, zoals directeur, partner, of bevoegd manager.

Naam: Functie: Plaats: Handtekening: Datum: