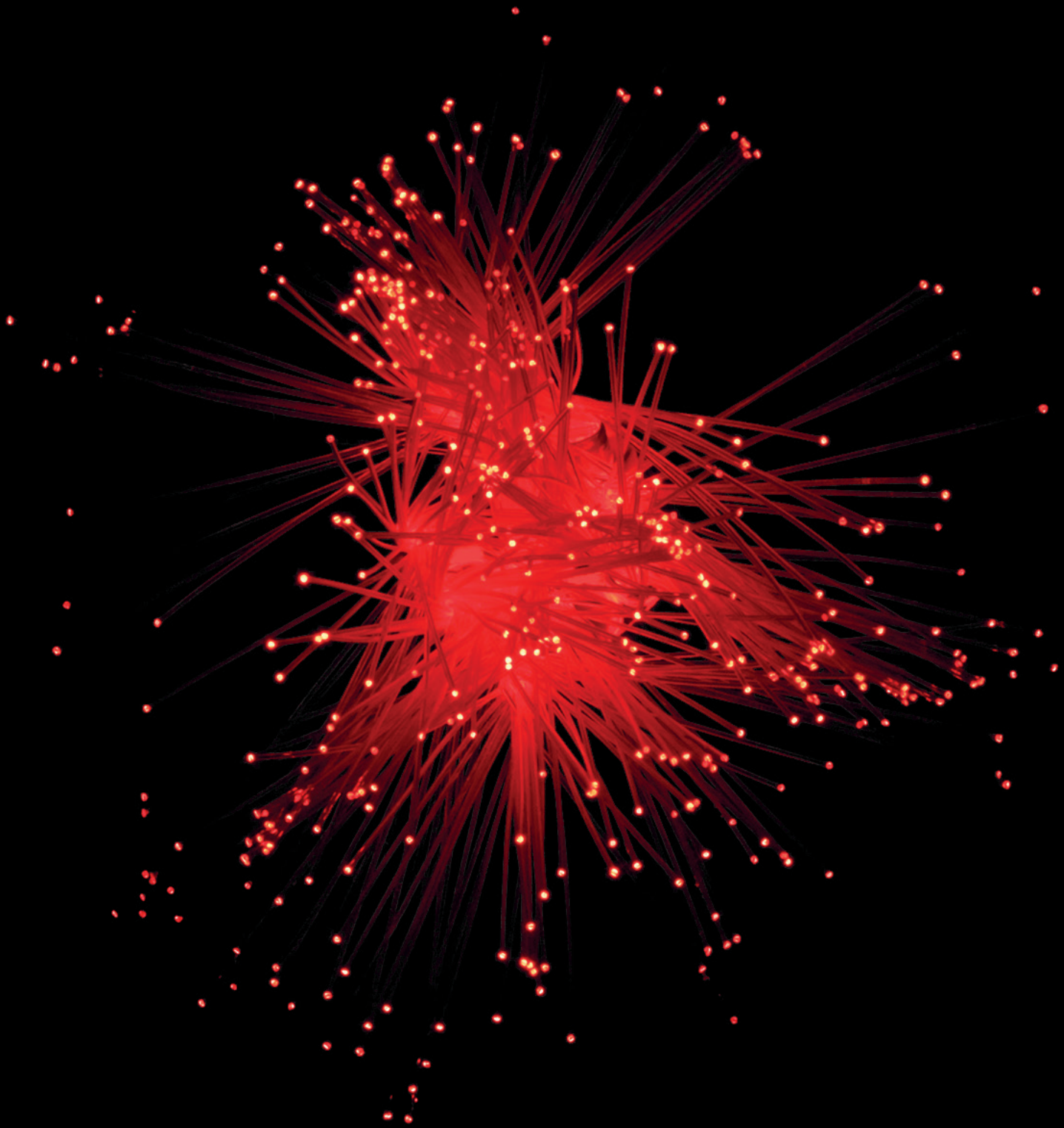
HISCOX

CyberClear by Hiscox
Aanvraagformulier
Cyber & Data Risks verzekering



Dit aanvraagformulier is bedoeld om informatie te verzamelen over uw cyber- en privacy risiso's.

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.

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 gaan.

Als er tussen Hiscox en u een verzekeringsovereenkomst wordt gesloten, dan gebeurt dat op basis van dit 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:

1B. Adres:

1C. Deelnemingen met meer dan 50% aandeel

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

Zo ja, in welk(e) land(en)?

1E. Graag een omschrijving van uw activiteiten:

1F. Graag een opgave van uw website(s):

2. 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	€	€	€

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*	Bijzondere persoonsgegevens**	Creditcardgegevens
0 - 20.000	☐	☐
20.001 - 100.000	☐	☐
100.001 - 250.000	☐	☐
250.001 - 500.000	☐	☐
500.001 - 1.000.000	☐	☐
1.000.001 - 6.000.000	☐	☐
> 6.000.000	☐	☐

* Het aantal unieke individuen wiens data wordt opgeslagen of verwerkt. Bijvoorbeeld als er van 2 personen elk een naam en rekeningnummer worden verwerkt dan zijn het 2 records (niet 4).

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

Offline ☐ % Online ☐ %

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

☐ nee ☐ gedeeltelijk ☐ ja

Bedrijfsschade:

7. 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?

€

8. 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 eeltelijk
☐ Na één week
☐ Na twee weken of langer

C. AVG

9. Is uw onderneming AVG compliant? ☐ ja ☐ nee

Zo niet, welke stappen heeft u wel genomen?

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

11. 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

12. 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

13. 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

14. Hoeveel servers heeft uw bedrijf? ☐

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

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

17. Krijgen uw medewerkers jaarlijks training op het gebied van cyberbeveiliging? ☐ ja ☐ nee

Beveiligingssoftware en versleuteling:

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

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

20. Welke van de volgende stellingen, met betrekking tot uw firewalls, zijn waar?

    ☐ 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
☐ 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 bevind 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 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

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

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 admin-rechten en één voor 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

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, graag uw 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:

* Met kritische gegevens en kritische systemen wordt bedoeld gegevens en systemen die ertoe leiden dat uw inkomsten verliest als ze langer dan 72 uur offline of niet beschikbaar zijn of waren.

** 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.

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

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?

* Als een van deze vragen met "ja" is beantwoord dan dient het aanvullende aanvraagformulier Hiscox CyberClear 2021 ook ingevuld te worden.

Betalingen:

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

    Zo ja, aan welke versie voldoet u?

38. Heeft u Verified by Visa geïmplementeerd voor online betalingen? ☐ ja ☐ nee

E. Externe dienstverleners

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

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

Zo ja, graag een opgave van uw belangrijkste providers:

Zo ja, welke werkzaamheden worden uitbesteed*?

40. 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

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

42. Worden door u aan de bedrijven of hulppersonen waaraan diensten worden uitbesteed eisen gesteld t.a.v. de mate van gegevensbescherming? ☐ ja ☐ nee

43. Voor alle uitbestede bedrijfskritische (cloud)-diensten** waarop u vertrouwt, worden deze diensten geleverd door een serviceprovider bij wie u een SLA hebt die een uptime van 99,9% of meer garandeert, die een ISO27001-certificering heeft en die uw gegevens of diensten in twee of meer geografisch gescheiden datacentra herbergt? ☐ ja ☐ nee

Zo niet, geef dan details over de naam en de geleverde dienst:

F. Aanvullende vragen

Let op! De vragen in deze sectie (F) hoeft u alleen te beantwoorden wanneer de jaarlijkse omzet van uw bedrijf ≥ 50 miljoen euro bedraagt. Indien uw omzet minder dan € 50 miljoen euro per jaar bedraagt, kunt u verder gaan naar de volgende sectie (G).

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

Detectie:

45. Hoe lang bewaard u logbestanden en notificaties over mogelijke cyberveiligheidsgebeurtenissen?

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

** Onder een bedrijfskritische cloud-dienst wordt verstaan: een dienst die zou leiden tot een verlies van inkomsten als deze langer dan 24 uur niet beschikbaar zou zijn.

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

☐ SIEM
☐ Interne SOC
☐ Externe SOC
☐ Anders (leg uit)

☐ Er wordt geen analyse uitgevoerd

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

48. Heeft u de volgende technologieën ingezet om u te helpen bij het opsporen van aanvallen?
a. Intrustion detection systems (IDS) ☐ ja ☐ nee
b. Intrustion prevention systems (IPS) ☐ ja ☐ nee
c. Data loss prevention (DLP) ☐ ja ☐ nee
d. Integriteitscontrole ☐ ja ☐ nee
e. Change control ☐ ja ☐ nee

Verantwoordelijkheid IT-beveiliging:

49. 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)

50A. Wanneer is voor het laatst een audit uitgevoerd in verband met ICT- beveiliging?

50B. Wat voor soort audit werd er uitgevoerd?

☐ Scannen van de kwetsbaarheid
☐ Penetratietesten of red teaming
☐ Anders (leg uit)

50C. En door wie is deze uitgevoerd?

50D. Worden de uit de audits voortvloeiende aanbevelingen geïmplementeerd? ☐ ja ☐ nee

51. 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

52. Gewenste verzekerd bedrag per aanspraak / schade:

☐ € 1.000.000 ☐ € 2.000.000
☐ € 2.500.000 ☐ € 5.000.000
☐ € 7.500.000 ☐ € 10.000.000

☐ Anders:

53. Wilt u het verzekerde bedrag verhogen tot maximaal twee maal de aanspraak per verzekeringsjaar? ☐ ja ☐ nee

H. Toezicht en claims

Toezicht:

54. 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

55. 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

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

Schadeclaims:

57. Heeft verzekeringnemer/verzekerde de afgelopen vijf jaar schade geleden of is er afgelopen vijf jaar een aanspraak ingediend op het gebied van privacy of cyberaansprakelijkheid? ☐ ja ☐ nee

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

58. Is verzekeringnemer/verzekerde op de hoogte van enige omstandigheid of evenement 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:

Adviseur:

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: