TURIEN&CO ASSURADEUREN

Aanvraagformulier CyberClear by Hiscox

A. Algemeen

1. Gegevens aanvrager

Naam bedrijf:

Adres:

Deelnemingen 50% aandeel of meer:

Heeft u een vestiging in de Verenigde Staten van Amerika/Canada ? Ja ☐ Nee ☐

Graag een omschrijving van uw activiteiten:

Graag een opgave van uw website(s):

2. Omzet of exploitatiesom

	Jaar eindigend op / /	Lopend jaar	Schatting komend jaar
Totale omzet of exploitatiesom	€	€	€
Waarvan in VS/Canada	€	€	€

3. Aantal medewerkers

	Jaar eindigend op / /	Lopend jaar	Schatting komend jaar
Nederland			€
Waarvan in VS/Canada			€
Rest van de Wereld			€

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

4. Graag uw toelichting op de activiteiten in relatie tot uw Cyber en Data risico's:

Welke soort gegevens worden door u verzameld, bewerkt en/of opgeslagen:

- Persoons-, vertrouwelijke bedrijfs- en klant(en)gegevens Ja ☐ Nee ☐
  (Naam, adres, emailadressen)

Graag hieronder aangeven over hoeveel gegevens u bij benadering beschikt:	
< 100.000	☐
100.001 - 500.000	☐
500.001 - 1.000.000	☐
> 1.000.000	☐

TURIEN&CO ASSURADEUREN

Aanvraagformulier CyberClear by Hiscox

- Medische gegevens Ja ☐ Nee ☐
- Financiële gegvens Ja ☐ Nee ☐

  (Loon, belasting, BSN nummer, IBAN nummer, etc.)
- Intellectueel eigendom/ handels- en bedrijfsgeheimen Ja ☐ Nee ☐
- Bijzondere persoonsgegevens zoals maar niet beperkt tot godsdienst of levensovertuiging, ras, politieke voorkeur of gezondheid* *(kruis hieronder het aantal geschatte records aan)* Ja ☐ Nee ☐

0 - 20.000	☐
20.001 - 100.000	☐
100.001 - 250.000	☐
250.001 - 500.000	☐
500.001 - 1.000.000	☐
1.000.000 - 6.000.000	☐
> 6.000.000	☐

- Creditcardgegevens: Ja ☐ Nee ☐
  (kruis hieronder het aantal geschatte records aan)

0 - 20.000	☐
20.001 - 100.000	☐
100.001 - 250.000	☐
250.001 - 500.000	☐
500.001 - 1.000.000	☐
1.000.000 - 6.000.000	☐
> 6.000.000	☐

- Andere data, zoals Ja ☐ Nee ☐

*Een organisatie mag geen bijzondere persoonsgegevens gebruiken, tenzij daarvoor in de wet een uitzondering is.

5. Worden door u online verkopen gedaan waarbij tevens betalingsgegevens zoals rekeningnummers en/of creditcardgegevens (al dan niet tijdelijk) worden opgeslagen op uw netwerk? Ja ☐ Nee ☐

   Zo ja, wat is uw verdeling van de totale omzet (off- en online)?

   Offline ____ % Online ____ %

   A. Offline business interruption

   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?

   EUR

   Toelichting

   B. Online business interruption

   Wat is naar uw inschatting de financiële schade gemiddeld per dag indien er sprake is van onderbreking of ernstige belemmering van uw internetactiviteiten (online) met omzetverlies tot gevolg als gevolg van een cyberrisico?

   EUR

TURIEN&CO ASSURADEUREN

Aanvraagformulier CyberClear by Hiscox

Toelichting

C. Beleid en Bewustwording

6. Is er een geformaliseerd privacy beleid en is deze verankerd in uw bedrijfsvoering? Ja ☐ Nee ☐
7. Is er een geformaliseerd beveilingsbeleid en is deze verankerd in uw bedrijfsvoering? Ja ☐ Nee ☐
8. Krijgen uw medewerkers regelmatig een beveiliging / privacy en bewustwording training? Ja ☐ Nee ☐
9. Vereist toegang tot uw ICT systeem identificatie en verificatie van de gebruiker? Ja ☐ Nee ☐
10. Worden de wachtwoorden regelmatig gewijzigd en hebben deze de nodige moeilijkheidsgraad?

    (Het wachtwoord bestaat uit cijfers, letters én leestekens, er wordt minimaal 1 hoofdletter, 1 kleine letter en 1 cijfer gebruikt, het wachtwoord is minimaal 8 karakters lang) Ja ☐ Nee ☐
11. Zijn de gebruikersrechten op uw ICT systeem gebaseerd op gebruikersprofielen? Ja ☐ Nee ☐
12. Heeft u een procedure voor autorisatiebeheer geïmplementeerd in uw bedrijfsvoering? Ja ☐ Nee ☐

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

Uw organisatie en informatiebeveiliging

13. Is er sprake van fysieke beveiligingsmaatregelen om ongeoorloofde toegang tot computersystemen en datacentra te voorkomen en op te sporen? Ja ☐ Nee ☐
14. Worden er periodieke audits uitgevoerd ten aanzien van het beleid en de procedures op het gebied van informatiebeveiliging? Ja ☐ Nee ☐
15. Worden de uit de audits als genoemd onder vraag 14, voortvloeiende aanbevelingen geïmplementeerd? Ja ☐ Nee ☐
16. Wanneer is voor het laatst een audit uitgevoerd in verband met ICT-beveiliging en door wie? / /

    Uitgevoerd door:
17. Worden er ICT activiteiten uitbesteed aan derden? Denk aan hosting, systeembeheer, etc. Ja ☐ Nee ☐
18. Verstrekt u data aan externe gegevensverwerkers/outsourcing (zoals maar niet beperkt tot een cloud-leverancier) Ja ☐ Nee ☐

    Indien ja, graag een opgave van de betrokken dienstverleners in verband met uitbestede werkzaamheden:

    (Denk aan: betalingsdiensten, back-up data herstel, ISP, databeheer en archivering, klantenservice, internal audits, marketing en verkoopactiviteiten, HR, Business Development, etc.)
19. Heeft u een schriftelijke bewerkersovereenkomst met deze dienstverleners? Ja ☐ Nee ☐

TURIEN&CO ASSURADEUREN

Aanvraagformulier CyberClear by Hiscox

20. Indien ja, bevat deze overeenkomst de mogelijkheid om directe schade voortvloeiende uit een datalek of een tekortkoming in de dienstverlening te verhalen? Ja ☐ Nee ☐

21. Bevat de bewerkersovereenkomst hiernaast:
    - voorschriften ten aanzien van de beveiliging? Ja ☐ Nee ☐
    - afspraken over de bewaking en monitoring van een eventuele inbreuk? Ja ☐ Nee ☐
    - een verplichting tot het melden bij verantwoordelijken na ontdekking of vermoeden van een datalek? Ja ☐ Nee ☐

22. Worden door u aan de bedrijven of hulppersonen waaraan diensten worden uitbesteed eisen gesteld t.a.v. de mate van gegevensbescherming? Ja ☐ Nee ☐

Beveiligingssoftware en versleuteling

23. Wordt 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 ☐

    Indien nee, graag een toelichting

24. Hoe vaak wordt deze software ge-update?
    - ☐ dagelijks
    - ☐ wekelijks
    - ☐ maandelijks
    - ☐ anders, ter weten:

25. Wordt er regelmatig een controle op de juistheid van de back-ups uitgevoerd? Ja ☐ Nee ☐

26. Wordt er periodiek een restore test (herstel na crash of hardware storing) uitgevoerd? Ja ☐ Nee ☐

27. Beschikt uw organisatie over firewalls, die up-to-date zijn, voor alle internettoegangen en bestaan er procedures over de inrichting van genoemde firewalls? Ja ☐ Nee ☐

28. Zijn er firewalls aanwezig tussen draadloze toegangspunten en systemen welke persoonlijke informatie opslaan dan wel verwerken? Ja ☐ Nee ☐

    Indien nee, graag een toelichting

29. Bestaat er binnen uw organisatie een methode om alle vertrouwelijke informatie en persoonsgegevens te versleutelen? (zoals bijv. encryptie) Ja ☐ Nee ☐

    Zo ja, op welke wijze vindt deze versleuteling plaats?

TURIEN&CO ASSURADEUREN

Aanvraagformulier CyberClear by Hiscox

30. 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 ☐

A. Zo ja, aan welk niveau voldoet uw organisatie:

- **Niveau 1:**
  Indien uw onderneming in een periode van 12 maanden meer dan 6 miljoen kaarttransacties uitvoert.
- **Niveau 2:**
  Indien uw onderneming in een periode van 12 maanden 1 tot 6 miljoen kaarttransacties via e-commerce uitvoert.
- **Niveau 3:**
  Indien u in een periode van 12 maanden tussen 20.000 en 1 miljoen kaarttransacties via e-commerce uitvoert.
- **Niveau 4:**
  Indien u in een periode van 12 maanden minder dan 20.000 kaarttransacties via e-commerce uitvoert.

Niveau ☐

B. Wilt u eventuele boetes / kosten of opgelegde maatregelen opgelegd door PCI DDS meeverzekeren binnen uw Cyber en Data Risks verzekering ? Ja ☐ Nee ☐

E. Gewenste dekking en eigen risico

31. Gewenste verzekerd bedrag per aanspraak / schade :

- ☐ **EUR 1.000.000**
- ☐ **EUR 2.000.000**
- ☐ **EUR 2.500.000**
- ☐ **EUR 3.000.000**
- ☐ **EUR 5.000.000**
- ☐ **EUR 10.000.000**
- ☐ **Anders EUR** ☐

Optionele uitbreiding van de dekking:

32. Wilt u verzekeringsdekking voor business interruption offline? Ja ☐ Nee ☐

33. Wilt u verzekeringsdekking voor boetes/kosten/maatregelen opgelegd door PCI DDS? Ja ☐ Nee ☐

34. Wilt u het dekkings- en rechtsgebied uitbreiden met de Verenigde Staten van Amerika? Ja ☐ Nee ☐

35. Gewenste ingangsdatum:

/ /

36. **Toezicht**

	Ja	Nee
a. 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?	☐	☐
b. Is verzekeringnemer/verzekerde ooit verzocht informatie te verstrekken aan een toezichthoudende of vergelijkbare instantie met betrekking tot persoonsgegevens op het gebied van privacy?	☐	☐
c. Is er ooit een klacht tegen u ingediend over de wijze waarop verzekeringnemer/verzekerde met persoonsgegevens omgaat?	☐	☐

37. **Schadeclaims**

	Ja	Nee
a. 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 ?	☐	☐
Indien Ja, vermeld hieronder de bijzonderheden (indien nodig kunt u op een aparte bijlage aanvullende bijzonderheden verstrekken):		

	Ja	Nee
b. 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?	☐	☐
Indien Ja, vermeld hieronder de bijzonderheden (indien nodig kunt u op een aparte bijlage aanvullende bijzonderheden verstrekken):		

Belangrijke informatie

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:

Beknopt privacystatement
Hieronder treft u ons verkorte privacystatement aan met de belangrijkste onderwerpen. Voor ons volledige privacystatement verwijzen wij u naar onze website www.turien.nl/privacystatement. Ook kunt u bij ons een exemplaar van het volledige privacystatement opvragen.

Waarvoor gebruiken wij uw gegevens?
Bij de aanvraag, uitvoering of wijziging van een verzekering of financiële dienst vragen wij om persoonsgegevens en andere gegevens. Deze gegevens gebruiken wij voor het aangaan en uitvoeren van uw verzekeringsovereenkomst of financiële dienst, het beheren van de daaruit voortvloeiende relaties, het verlenen van service en schadelastbeheersing, om u te informeren over onze diensten en producten, voor activiteiten gericht op het vergroten van het klantenbestand, voor (statistische) analyses, onderzoek en managementinformatie, om te kunnen voldoen aan wettelijke verplichtingen en in het kader van het waarborgen van de veiligheid en integriteit van de financiële sector, onze organisatie, medewerkers en cliënten. De verkregen persoonsgegevens kunnen worden verwerkt door derden, teneinde ons te ondersteunen voor de hierboven vermelde doeleinden.

Uw rechten
U heeft het recht om uw persoonsgegevens in te zien, aan te passen of te verwijderen. Ook heeft u het recht om bezwaar te maken tegen de verwerking van die gegevens, de verwerking ervan te beperken en uw persoonsgegevens over te dragen naar een andere organisatie. Wilt u hier meer over weten, raadpleeg dan ons uitgebreide privacystatement.

Aanvraagformulier CyberClear by Hiscox

Gedragscode
Op de verwerking van persoonsgegevens is de 'Gedragscode Verwerking Persoonsgegevens Verzekeraars' van toepassing. De volledige tekst van de gedragscode kunt u raadplegen via de website van het Verbond van Verzekeraars (www.verzekeraars.nl). U kunt de gedragscode ook opvragen bij het Verbond van Verzekeraars (Postbus 93450, 2509 AL Den Haag, telefoonnummer 070 333 85 00).

Bijzondere persoonsgegevens
Wij kunnen bijzondere persoonsgegevens van u nodig hebben. U kunt hierbij denken aan medische gegevens of strafrechtelijke gegevens. Deze gegevens kunnen van belang zijn voor de aanvraag van een verzekering, voor de afhandeling van een uitkeringsverzoek, voor het invorderen van een claim of voor het voorkomen van fraude. Bijzondere persoonsgegevens worden door ons extra zorgvuldig verwerkt: slechts een beperkte groep van medewerkers heeft toegang tot deze gegevens.

Stichting CIS
Voor een verantwoord acceptatie-, risico- en fraudebeleid raadplegen en registeren wij uw gegevens in het Centraal Informatie Systeem van de in Nederland werkzame verzekeringsmaatschappijen (CIS), Bordewijklaan 2, 2591 XR te Den Haag.

Doelstelling van de verwerking van persoonsgegevens bij CIS is voor verzekeraars en gevolmachtigden risico's te beoordelen en te beheersen en verzekeringscriminaliteit tegen te gaan. De gegevens die wij bij CIS vastleggen, worden verder gebruikt voor statistische analyses en het waarborgen van de veiligheid en integriteit van de financiële sector. Uw klantgegevens worden bovendien apart centraal vastgelegd om in geval van ernstige calamiteiten, incidenten (zoals verzekeringsfraude) of opsporingsactiviteiten door politie en justitie de verzekeraars en gevolmachtigden bij personen, bedrijven, objecten en risicoadressen te kunnen vinden. Zie voor meer informatie www.stichtingcis.nl. Hier vindt u ook het CIS privacyreglement.

Verklaring

Ik/Wij verkla(a)r(en) dat (a) dit aanvraagformulier na het vereiste onderzoek volledig is ingevuld, (b) de inhoud daarvan juist en nauwkeurig is en (c) alle feiten en omstandigheden die relevant kunnen zijn voor de behandeling van deze verzekeringsaanvraag, volledig zijn verstrekt.

Ik/wij verbind(en) mij/ons om, alvorens een verzekeringsovereenkomst af te sluiten, u te informeren over eventuele wezenlijke veranderingen in de verstrekte informatie of van nieuwe feiten of omstandigheden die relevant kunnen zijn voor de beoordeling van deze verzekeringsaanvraag.

Ik/Wij aanvaard(en) dat het niet bekendmaken of het geven van misleidende voorstelling van zaken van een wezenlijk feit of wezenlijke zaak Turien & Co. Assuradeuren het recht geeft deze verzekering te ontbinden.

Ik/Wij ga(an) ermee akkoord dat dit aanvraagformulier en alle overige schriftelijke informatie die is verstrekt, worden opgenomen in en de basis vormen van de verzekeringsovereenkomst.

Slotverklaring
De verzekeringnemer bevestigt, mede gelet op de inhoud van artikel 7:928 BW, dat de gegeven **antwoorden en verklaringen juist en volledig** zijn en dat mededeling is gedaan van de feiten en omstandigheden die voor ons van belang zijn voor de beoordeling van zowel het te verzekeren risico als ten aanzien van de verzekeringnemer en verzekerden. De verklaringen vormen, tezamen met de overige aan ons verstrekte informatie in dit formulier, de grondslag voor en vormt een integraal onderdeel van de verzekeringsovereenkomst.

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 dadelijke ingang opzeggen van de verzekering, het beperken van de dekking en het weigeren of beperken van een schadevergoeding op grond van de verzekering.

Naam Lastgever/Partner/Directeur	Functie
Handtekening Lastgever/Partner/Directeur	Datum / /