HISCOX

Aanvraagformulier
CyberClear by Hiscox

Aanvraagformulier CyberClear by Hiscox 2018

A. Algemeen

1. Gegevens aanvrager

Naam:

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, verwerkt en/of opgeslagen:

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

- Medisch ☐
- Financieel ☐

  (Loon, belasting, BSN nummer, IBAN nummer, etc.)
- Intellectueel eigendom/ handels- en bedrijfsgeheimen ☐
- (Bijzondere) persoonsgegevens** zoals maar niet beperkt tot godsdienst of levensovertuiging , ras , politieke voorkeur of gezondheid* ☐

Aantal	(bijzondere) Persoonsgegevens**	Creditcardgegevens
0 - 20.000	☐	☐
20.001 - 100.000	☐	☐
100.001 - 250.000	☐	☐
250.001 - 500.000	☐	☐
500.001 - 1.000.000	☐	☐
> 1.000.000	☐	☐

* met gegevensaantal wordt bedoeld het aantal records: bijvoorbeeld een naam en e-mailadres zijn 2 records.

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

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 ____ %

   Bedrijfsschade

   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?

   €

   Toelichting:

HISCOX

Aanvraagformulier CyberClear by Hiscox 2018

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 (2 factor autorisatie)? 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. AVG

13. Is uw onderneming AVG compliant? Ja ☐ Nee ☐

    Zo niet: welke stappen heeft u wel genomen?:

14. Worden de personeelsleden met toegang tot persoonsgegevens regelmatig getraind op het gebruik hiervan en geïnformeerd over wet- en regelgeving? Ja ☐ Nee ☐
15. 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 ☐
16. Deelt u persoonsgegevens met derden Ja ☐ Nee ☐

    Zo ja: Heeft deze derde partij een (contractuele) verplichting om AVG compliant te zijn? Ja ☐ Nee ☐
17. Heeft u toegang tot persoonsgegevens beperkt tot de gebruikers voor wie dit noodzakelijk is om hun taken uit te voeren en deze toelating wordt regelmatig herbekeken? Ja ☐ Nee ☐

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

Uw organisatie en informatiebeveiliging

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

    Uitgevoerd door:

22. Worden er ICT activiteiten uitbesteed aan derden? Denk aan hosting, systeembeheer, Cloud computing etc. Ja ☐ Nee ☐

23. 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.)

24. Heeft u een schriftelijke bewerkersovereenkomst met deze dienstverleners? Ja ☐ Nee ☐

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

Ja ☐ Nee ☐

26. 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 ☐

27. 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

28. 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

29. Hoe vaak wordt deze software ge-update?

☐ dagelijks

☐ wekelijks

☐ maandelijks

☐ anders, ter weten:

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

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

32. Beschikt uw organisatie over firewalls, die up-to-date zijn, voor alle Ja ☐ Nee ☐

internettoegangen en bestaan er procedures over de inrichting van genoemde firewalls?

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

Indien nee, graag een toelichting

34. 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?

35. 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

F. Gewenste dekking (en)

36. 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** €

Wilt u het verzekerde bedrag verhogen tot maximaal twee maal de aanspraak per verzekeringsjaar? Ja ☐ Nee ☐

HISCOX

Aanvraagformulier CyberClear by Hiscox 2018

Uitbreidingen

Wilt u dekking voor Cyberfraude- en bedrog door opzettelijke misleiding, bedrog/fraude als gevolg van social engineering, de pretext-techniek, phishing, spear phishing of een andere vertrouwenstruc die wordt overgebracht middels e-mail, sms, een chatapplicatie, telefoon of ander elektronische media door een persoon die zich valselijk uitgeeft als een handelspartner of klant van de verzekerde of als werknemer, bestuurder, toezichthouder, gevolmachtigde of vergelijkbare functionaris van verzekeringnemer en/of haar dochtervennootschappen en/of haar deelnemingen, hetgeen een overmaking, betaling of overdracht van geld en/of effecten door verzekerde tot gevolg heeft?. Ja ☐ Nee ☐

Wilt u dekking voor de kosten en bedrijfsschade als gevolg van een hack, inbreuk of systeemstoring bij bedrijven die zaken doen met u en waar u voor een deel van afhankelijk bent (inbreuken en systeem storing/falen bij andere bedrijven dan uw bedrijf)? Ja ☐ Nee ☐

37. Gewenste ingangsdatum:

/ /

38. **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?	☐	☐

39. **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):		

HISCOX

Aanvraagformulier CyberClear by Hiscox 2018

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:

In te sturen stukken:

☐ Audit/ recente ICT Security Scan (indien beschikbaar)

☐ Opgave medeverzekerden (organogram)

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.

De verklaringen vormen, tezamen met de overige aan Hiscox Nederland 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.

Ondertekening

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

Plaats

Handtekening

/ /

Datum

Privacy

Hiscox is een handelsnaam voor een aantal bedrijven van Hiscox. Het specifieke bedrijf dat optreedt als verwerkingsverantwoordelijke van uw persoonsgegevens staat aangegeven in de documentatie die wij aan u verstrekken. Wanneer u vragen hebt kunt u altijd contact met ons opnemen door te bellen naar 020-5170700 of door ons te mailen op hiscox.underwriting@hiscox.nl. Wij verzamelen en verwerken gegevens over u om verzekeringspolissen te verstrekken en claims 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 met, en kunnen gegevens over u worden verkregen van, onze groepsmaatschappijen en derden, waaronder verzekeringsmakelaars, schaderegelaars, kredietinformatiebureaus, dienstverleners, professionele adviseurs, onze 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