Aanvraagformulier CyberEdge

1. Voor het verkrijgen van een offerte is het van belang dat het formulier volledig wordt ingevuld.
2. Indien er onvoldoende ruimte aanwezig is voor de beantwoording van de vragen, gaarne op uw eigen papier de beantwoording bijvoegen.
3. Het aanvraagformulier dient getekend en gedateerd te worden door een daartoe bevoegd persoon.

Invulling en ondertekening van het formulier verplicht de aanvragende onderneming of verzekeraar niet om de verzekeringsovereenkomst aan te gaan.

Algemene gegevens van de aanvrager

1. Bedrijf _____
2. Website _____
3. Hoofdadres _____
4. Bedrijfsactiviteiten _____
5. Omzet en geografische verdeling:

	20..	20..
Totale omzet		
Verdeling van de omzet per regio (%)		
NL		
Overige EU		
US / Canada		
Rest van de wereld		

6. Gewenste dekking:
   ❑ CyberEdge ` ❑ Cyber Afpersing ❑ Media Aansprakelijkheid ❑ Netwerkonderbreking

   Gewenste limiet : EUR_____
   Gewenst eigen risico : EUR_____

Beleid rondom informatiebeveiliging en privacybescherming

7. Is er een geschreven informatiebeveiligings- en privcaybeleid aanwezig binnen het bedrijf? ❑Ja ❑Nee

Indien "Ja", graag bijvoegen. Indien "Nee", dan ontvangen wij graag een toelichting op de uitvoering van een risicoanalyse, betrouwbaarheidseisen van informatiesystemen en beveiligingseisen en -maatregelen van het bedrijf.

_____
_____
_____
_____
_____

8. Krijgt iedere (ingehuurde) medewerker en externe gebruiker een kopie (en updates) van het informatiebeveiligingsbeleid en dienen zij naleving ervan te bevestigen? ❑Ja ❑ Nee
Indien "Nee" graag uitleg:

_____
_____

9. Wanneer is het informatiebeveiligingsbeleid voor het laatst gecontroleerd en door wie?

_____

10. Wat doet het bedrijf eraan om naleving en awareness voor informatiebeveiliging te borgen en hoe wordt de naleving ervan gecontroleerd?

_____
_____
_____
_____

11. Is er sprake van verwerking of doorgifte van persoonsgegevens buiten Nederland? ❑Ja ❑Nee
Indien "Ja", hoe wordt de informatiebescherming en privacy gewaarborgd?

_____
_____

12. Is er een Chief Compliance Officer / Gegevensbeveiligingsofficier of een interne afdeling / medewerker die verantwoordelijk is voor gegevensbescherming en gerelateerde zaken? ❑Ja ❑Nee
Indien "Nee" , wie is er dan verantwoordelijk voor zaken rondom informatiebeveiliging en privacy?

_____

Beveiligingseisen- en maatregelen

13. Gebruikt het bedrijf firewalls om ongeoorloofde toegang vanaf externe netwerken en computers op de systemen te voorkomen? ❑Ja ❑Nee

Indien "Ja", zijn alle computersystemen, mobiele apparatuur en websites voorzien van een firewall of een toegangpreventiesysteem?

_____

14. Gebruikt het bedrijf antivirussoftware en -procedures op alles desktops, emailsystemen en belangrijke servers om virussen, worms, spyware en andere malware tegen te gaan? ❑Ja ❑Nee
Indien "Ja", hoe vaak worden deze geupdate?

☐ Dagelijks ☐ Wekelijks ☐ Maandelijks ☐ Anders, namelijk:

15. Zijn er procedures aanwezig om zwakke plekken in de netwerkbeveiliging te identificeren en op te sporen?

❑Ja ❑Nee

Graag uitleg:

_____

_____

_____

16. Monitort het bedrijf het netwerk en de computersystemen voor inbreuken op de informatiebeveiliging? Wordt hier een logbestand van bijgehouden? ❑Ja ❑Nee

17. Is er sprake van fysieke beveiliging om ongeoorloofde toegang tot uw computersystemen en data center te voorkomen en op te sporen? ❑Ja ❑Nee

18. Verzamelt, bewaart of beheert het bedrijf credit card gegevens of andere persoonlijke gevoelige informatie?

☐ Credit Card

☐ (gevoelige) persoonsgegevens

☐ (gevoelige) bedrijfsinformatie, namelijk_____

Indien "Credit Card" is aangevinkt hierboven, is het bedrijf compliant met PCI-DSS? ❑Ja ❑Nee

Indien een van de opties is aangevinkt hierboven, graag een indicatie van het aantal en het soort datarecords per jaar en een toelichting op hoe de toegang tot deze gegevens beperkt wordt?

_____

_____

_____

_____

Wie hebben er toegang?

_____

19. Verwerkt het bedrijf betalingen namens anderen (inclusief eCommerce transacties)? ❑Ja ❑Nee

Indien "Ja", voor hoeveel klanten worden deze betalingen verwerkt per jaar en wat is de gemiddelde transactiesom?

_____

20. Heeft het bedrijf voorschriften op het gebied van versleuteling voor data-in-transit en data-at-rest voor de bescherming van de integriteit van gevoelige informatie (inclusief data op draagbare media, zoals laptops, USB sticks en dergelijke)?

❑Ja ❑Nee

Indien "Ja", graag een omschrijving van waar deze versleuteling wordt gebruikt:

_____

_____

21. Heeft het bedrijf back-up en herstel procedures voor alle:

i) bedrijfskritieke systemen? ❑Ja ❑Nee

ii) data en informatie? ❑Ja ❑Nee

Indien "Ja", zijn deze gegevens versleuteld? ❑Ja ❑Nee

Hoe vaak worden back-ups uitgevoerd?

☐ Dagelijks ☐ Wekelijks ☐ Maandelijks ☐ Anders, namelijk:

22. Wordt er een antecedentenonderzoek uitgevoerd voor alle medewerkers en ingehuurde consultants?

❑Ja ❑Nee

23. Worden gebruikers op afstand geauthentiseerd alvorens ze toegang krijgen tot het interne netwerk en computersystemen? ❑Ja ❑Nee

Uitbesteding van activiteiten

24. Wordt (een deel van) het netwerk, de computersystemen of informatiebeveiligingsfuncties uitbesteed?

❑Ja ❑Nee

Indien "Ja", aan wie wordt dit uitbesteed?

_____

25. Wordt gegevensverzameling en/of gegevensbeheer uitbesteed? ❑Ja ❑Nee
Indien "Ja", graag een toelichting op de functies die worden uitbesteed en aan wie:

_____

_____

26. Welke eisen worden gesteld aan de insourcers of (sub)bewerkers rondom beveiligingseisen, standaarden en procedures en hoe wordt de kwaliteit ervan gewaarborgd en gecontroleerd?

_____

_____

_____

_____

27. Verplicht het bedrijf dat insourcers hun eigen Cyber Aansprakelijkheidsverzekering hebben? ❑Ja ❑Nee

28. Verlangt het bedrijf een vrijwaring voor aanspraken van derden van de insourcers? ❑Ja ❑Nee

29. Hoe worden de insourcers geselecteerd en gemanaged?

_____

30. Worden insourcers verplicht om te voldoen aan het informatiebeveiligingsbeleid van het bedrijf? ❑Ja ❑Nee

31. Is het bedrijf zich bewust van en voldoet men aan de eisen vanuit de nieuwe CBP richtsnoeren voor de beveiliging van persoonsgegevens? ❑Ja ❑Nee

Claims Informatie

32. Is het bedrijf onderwerp geweest van een onderzoek of audit met betrekking tot de bescherming van (persoons) gegevens door het College bescherming persoonsgegevens (Cbp) of andere regulerende instantie? ❑Ja ❑Nee

Indien "Ja", graag details

_____

33. Heeft het bedrijf ooit een verzoek tot inzage ontvangen van een betrokkene? ❑Ja ❑Nee

Indien "Ja", graag details

_____

34. Heeft het bedrijf ooit een dwangbevel met betrekking tot de bescherming van (persoons)gegevens ontvangen van het Cbp of andere regulerende instantie? ❑Ja ❑Nee

Indien "Ja", graag details

_____

35. Is de aanvrager zich bewust van een omstandigheid welke mogelijkerwijs aanleiding zou kunnen geven tot een claim onder deze polis? ❑Ja ❑Nee

36. Is er ooit schade geweest voor iets wat onder deze polis gedekt zou zijn? ❑Ja ❑Nee

Indien "Ja" graag details

_____

_____

Ondergetekende, bevoegd voor de onderneming te tekenen, verklaart de vorenstaande vragen volledig en naar waarheid te hebben beantwoord en geen voor de acceptatie van deze verzekering belangrijke aspecten te hebben verzwegen of niet geheel juist te hebben voorgesteld.

Dit aanvraagformulier dient als basis van de verzekering en zal derhalve onderdeel uitmaken van de verzekeringsovereenkomst.

Ondergetekende zegt hierbij toe de verzekeraar op de hoogte te stellen van iedere wezenlijke verandering in de in dit aanvraagformulier vermelde gegevens, of deze nu voor of na de afsluiting van de verzekeringsovereenkomst plaatsvindt.

Naam van de aanvrager: _____

Handtekening bevoegd persoon: _____

Titel: _____

Plaats: _____ Datum: _____