Identificatie

Naam & Rechtsvorm Aanvrager					
Ondernemingsnummer					
Datum van oprichting					
Adres	Straat & Nummer				
	Postcode		Gemeente	Land	

Aantal werknemers	
Bedrijfsactiviteiten	

	Vorig Boekjaar	Huidig Boekjaar
Jaaromzet (in Euro)		
Geografische spreiding van de jaaromzet (%)		
• België		
• EU		
• US/Canada		
• Rest van de wereld		
Opsplitsing van de jaaromzet **per activiteit** (%)		
•		
•		
•		
•		
•		
•		

Indien voor de beantwoording van de vragen onvoldoende ruimte beschikbaar is, verzoeken wij u de complete antwoorden in een bijlage mee te zenden.

System, Security & Privacy

1. **Welke soort persoonsgegevens** worden door u verzameld, bewerkt en/of opgeslagen en in welke aantallen?

Bedrijfs- en klanteninformatie		
Medische gegevens		
Belastinggegevens		
Credit Card Informatie		
Financiële gegevens		
Intellectuele eigendom / Handels- en bedrijfsgeheimen		
Andere, te weten:		

2. Vindt **outsourcing** van primaire bedrijfsfuncties aan derden plaats?	**Ja**		**Nee**	
Indien **Ja**, graag aangeven welke bedrijfsfuncties:				
Personeelszaken				
Klantenservice				
Marketing en verkoop				
Business Development				
IT				
Interne audits				
Andere, te weten:				

3. Wordt **(gevoelige) informatie** (zoals persoonsgegevens) **gedeeld** met business partners, leveranciers of andere derden, voor de levering van producten en/of diensten?	**Ja**		**Nee**	
4. Worden bedrijven of hulppersonen waaraan diensten worden uitbesteed **verplicht** een cyber en/of beroepsaansprakelijkheids**verzekering** te hebben?	**Ja**		**Nee**	
5. Worden aan de bedrijven of hulppersonen waaraan diensten worden uitbesteed **eisen** gesteld ten aanzien van de mate van **gegevensbescherming**?	**Ja**		**Nee**	
6. Wordt in contracten overeengekomen dat de bedrijven of hulppersonen waaraan diensten worden uitbesteedt u in geval van aanspraken zullen **vrijwaren**?	**Ja**		**Nee**	

7. Graag ontvangen wij een overzicht van de **IT** gerelateerde activiteiten die worden **uitbesteedt** aan derden:

Soort IT-dienst	**Naam leverancier**

8. Is er een **medewerker verantwoordelijk** voor gegevensbescherming, informatiebeveiliging, privacy en gerelateerde zaken?	**Ja**		**Nee**	
Indien Ja, graag aangeven welke functie dit betreft:				
Chief Privacy Officer				
Chief Information Security Officer				
Anders, functie:				

9. Is er een schriftelijke procedure aanwezig op het gebied van **gegevensbeschermingsbeleid**?	**Ja**		**Nee**	
Zo **Ja**, graag bijvoegen.			**bijgevoegd**	

10. Zijn er maatregelen genomen met betrekking tot **cyber-awareness** bij werknemers? (bv. phishing campagnes)	**Ja**		**Nee**	
Zo **Ja**, welke?				
11. Dient uw organisatie te voldoen aan de Payment Card Industry Data Security Standard (**PCI DSS** v1.2)?	**Ja**		**Nee**	
Zo **Ja**, aan welk niveau? **1.** **2.** **3.** **4.**				
Graag ontvangen wij een kopie van het laatste certificaat.		**bijgevoegd**		
12. Beschikt uw organisatie over **firewalls**, die up-to-date zijn, voor alle internettoegangen en hanteert u een gestandaardiseerde configuratie?	**Ja**		**Nee**	
13. Zijn er firewalls aanwezig tussen draadloze toegangspunten en systemen die persoonlijke informatie opslaan of verwerken?	**Ja**		**Nee**	
14. Beschikken alle gebruikers van systemen en applicaties die persoonlijke informatie opslaan of verwerken over een **unieke gebruikersidentiteit**?	**Ja**		**Nee**	
15. Gebruikt uw organisatie **antivirussoftware** op alle systemen, zoals desktops, laptops, mobiele apparaten, emailsystemen en servers?	**Ja**		**Nee**	
Zo **Ja**, hoe vaak worden deze geüpdatet?				
Dagelijks		Wekelijks		Maandelijks		Anders, nl.:		
16. Zijn er procedures aanwezig om zwakke plekken in de **netwerkbeveiliging** te identificeren en op te sporen?	**Ja**		**Nee**	
17. Worden **administrator-accounts** extra beveiligd? (bv. MFA, PAM-software…)	**Ja**		**Nee**	
18. Beschikt uw organisatie over schriftelijke procedures ten aanzien van het **verwijderen en vernietigen van persoonlijke informatie**?	**Ja**		**Nee**	
19. Beschikt uw organisatie over **back-up- en herstelprocedures**?	**Ja**		**Nee**	
Hoe vaak wordt er een back-up gemaakt?				
Wordt er een periodieke controle op deze back-ups uitgevoerd?	**Ja**		**Nee**	
Worden er periodieke *'restore tests'* uitgevoerd?	**Ja**		**Nee**	
Hoe lang worden back-ups bewaard?				
Zijn er meerdere datacenters?	**Ja**		**Nee**	
Kunnen ze afzonderlijk van elkaar werken?	**Ja**		**Nee**	
Worden de back-up- en herstelprocedures regelmatig getest?	**Ja**		**Nee**	
Zo **Ja**, hoe frequent?				
Hoelang duurt een volledige herstelprocedure?				
Worden ook offline kopieën op tapes bijgehouden	**Ja**		**Nee**	

20. Bestaat er binnen uw organisatie een methode om alle vertrouwelijke informatie en persoonlijke informatie te **versleutelen**?	**Ja**		**Nee**	
Zo **Ja**, op welke wijze en wanneer wordt dergelijke informatie versleuteld?				
21. Zijn er procedures en/of maatregelen om **fraude te voorkomen**? (bv. vier-ogenprincipe bij betalingen)	**Ja**		**Nee**	
Zo **Ja**, welke?				
22. Beschikt uw organisatie over een **incidentenbeleid**?	**Ja**		**Nee**	
Zo ja, omvat dit beleid de volgende elementen:				
- formele aanstelling contactpersonen?	**Ja**		**Nee**	
- stappenplan na een incident?	**Ja**		**Nee**	
- een communicatieplan?	**Ja**		**Nee**	
Graag ontvangen wij een kopie.		**toegevoegd**		
23. Beschikt uw organisatie over een **bedrijfscontinuïteitsplan**?	**Ja**		**Nee**	
Zo **Ja**, graag bijvoegen.		**toegevoegd**		
24. Bestaat het netwerk uit meerdere **hubs**?	**Ja**		**Nee**	
Zo **Ja**, kan een cyberincident in een van de hubs een negatieve impact hebben op andere hubs?	**Ja**		**Nee**	
Zo **Ja**, graag overzicht van het netwerk inclusief beschrijving van de afhankelijkheid tussen hubs toevoegen.		**toegevoegd**		
25. Inschatting van de verzekeringsnemer met betrekking tot de mogelijke **impact van een cyberincident** op bedrijfscontinuïteit:				
Kan een cyberincident een volledige stilstand veroorzaken?	**Ja**		**Nee**	
Na hoeveel uur wordt de situatie kritisch?				
Is er een noodprocedure/mogelijke by-pass opties? (bv. als website plat ligt)?	**Ja**		**Nee**	

Claims Informatie

26. Heeft er de afgelopen 5 jaar een gebeurtenis plaatsgevonden, waarbij digitale informatie werd verloren, ontvreemd, beschadigd of gemanipuleerd als gevolg van een computervirus, hacker, of andere oorzaak?	**Ja**		**Nee**	
Zo ja, graag uw toelichting:				
27. Is uw organisatie het onderwerp geweest van een onderzoek of audit met betrekking tot de bescherming van (persoons)gegevens door de Gegevens-beschermingsautoriteit of andere regulerende instantie?	**Ja**		**Nee**	
Zo ja, graag uw toelichting:				
28. Is een soortgelijke verzekering al eens afgewezen of geweigerd?	**Ja**		**Nee**	
Zo ja, graag uw toelichting:				
29. Zijn de rechtspersoon, één van haar meerderheidsdeelnemingen en/of de bestuurders op de hoogte van feiten, waarvan kan worden aangenomen dat deze kunnen leiden tot een aanspraak onder de aangevraagde verzekering?	**Ja**		**Nee**	
Zo ja, graag uw toelichting:				

Handtekening

Dit document dient te worden ondertekend door een (gedelegeerde) bestuurder, zaakvoerder, productie- of financieel directeur van de aanvrager, of gelijkwaardige positie.

Datum	/ /
Ik verklaar dat de verklaringen en informatie in dit voorstelformulier, met inbegrip van eventuele bijlagen, na onderzoek waarheidsgetrouw zijn en dat geen enkele materiële feiten onjuist zijn, verkeerd zijn weergegeven of zijn achtergehouden. Ik ga ermee akkoord dat dit voorstelformulier de basis vormt van een eventueel verzekeringscontract tussen de Verzekeraar en de Aanvrager.	
Handtekening	