Chubb Insurance Company of Europe SE
Wegalaan 43
2132 JD Hoofddorp

Chubb Cyber ERM Aanvraagformulier

Met deze vragenlijst kan de verzekeringsmaatschappij CHUBB de benodigde informatie verzamelen ter beoordeling van de risico's die zijn verbonden aan de informatiesystemen van de te verzekeren onderneming. Ook biedt deze lijst CHUBB de mogelijkheid haar aanbod beter te laten aansluiten op de verwachtingen van de klant. Let op: het invullen van deze vragenlijst verbindt noch CHUBB, noch de aanvragende onderneming tot het sluiten van een overeenkomst. De aanvragende onderneming is echter wel verplicht om de vragenlijst naar waarheid in te vullen. Als het beveiligingsbeleid voor informatiesystemen van de te verzekeren ondernemingen/dochtermaatschappijen per bedrijf verschilt, dient voor elk daarvan een afzonderlijke vragenlijst te worden ingevuld.

1 GEGEVENS VAN DE AANVRAGENDE ONDERNEMING

Bedrijfsnaam

Adres

Postcode, Plaats

Website(s)

Aantal werknemers

Jaaromzet

Jaarlijkse bruto marge

Percentage van de omzet gegeneerd in

US/Canada:

EU:

Rest of World:

2 PROFIEL VAN TE VERZEKEREN ONDERNEMING(EN)

2.1 Te verzekeren activiteiten

[Beschrijf de hoofdactiviteiten van de te verzekeren onderneming(en). Als e-commerce tot deze activiteiten behoort, verzoeken we u het gegenereerde omzetpercentage te vermelden.]

2.2 Omvang

[De te verzekeren ondernemingen en dochtermaatschappijen. Als de onderneming dochtermaatschappijen buiten de EU heeft, verzoeken we u de gegevens daarvan te vermelden]

2.3 Belangrijkheid van de informatiesystemen

[Beoordeel de uitvalperiode na verloop waarvan uw onderneming aanzienlijke gevolgen voor haar bedrijfsvoering zal ondervinden.]

Applicatie (of Activiteit)	Maximale uitvalperiode vóór ontstaan negatieve impact op bedrijfsvoering				
	Onmiddellijk	> 12 h	> 24 h	> 48 h	> 5 dagen

3 INFORMATIESYSTEMEN

	< 100	101 - 1000	> 1000
Aantal IT gebruikers			
Aantal laptops			
Aantal servers			

	JA	NEE
Heeft u een e-commerce of een online service website?	☐	☐
Indien JA, wat is het percentueel aandeel van de omzet dat hierdoor gegenereerd wordt? (schatting)		

4 BEVEILIGING VAN INFORMATIESYSTEMEN (INFORMATION SYSTEMS SECURITY, ISS)

4.1 Beveiligingsbeleid en risico management

		JA	NEE
1	Er is een geformaliseerd beveiligingsbeleid, dat is goedgekeurd door het management, meegedeeld aan alle personeelsleden en goedgekeurd door de ondernemingsraad.	☐	☐
2	De gebruikers krijgen regelmatig een ISS-bewustwordingstraining.	☐	☐
3	U hebt kritische informatiesystemen geidentificeerd en de nodige voorzorgsmaatregelen genomen om schade te beperken aan deze.	☐	☐
4	Er worden regelmatig audits van de ISS uitgevoerd en de aanbevelingen worden geïmplementeerd.	☐	☐
5	U deelt de IT systemen in volgens hun belangrijkheid en gevoeligheid. Het niveau van beveiliging sluit hier op aan.	☐	☐

4.2 Informatiebescherming en toegangscontrole

		JA	NEE
1	Toegang tot het IT system vereist identificatie en verificatie van de gebruiker. Paswoorden worden regelmatig gewijzigd en hebben de nodige moeilijkheidsgraad.	☐	☐
2	Toegangsrechten zijn gebaseerd op gebruikersprofielen en er is een procedure voor autorisatiebeheer geïmplementeerd. Alleen de minimum authorisatie wordt toegekend.	☐	☐
3	Voorafingestelde configuraties zijn gedefinieerd per werkstation, laptop, server en draagbare apparatuur (smartphones, tablets,...).	☐	☐
4	Het beheer en de configuratie van computer systemen wordt centraal beheerd en gemonitored.	☐	☐
5	De laptops zijn beschermd door persoonlijke firewalls.	☐	☐
6	Er is een antivirusprogramma geïnstalleerd op alle systemen, en de antivirus updates worden gemonitored.	☐	☐
7	De beveiligingspatches worden regelmatig geïnstalleerd.	☐	☐
8	Een Disaster Recovery Plan is uitgewerkt, getest en, indien nodig, jaarlijks geupdated.	☐	☐
9	Data backups worden dagelijks gemaakt, backups worden regelmatig getest en een backup copie wordt regelmatig opgeslagen buiten de bedrijfssite.	☐	☐

4.3. Netwerkbeveiliging en bewerkingen

		JA	NEE
1	Er is een firewall geïnstalleerd tussen het interne netwerk en het internet, en de beveiliging van het inkomend en uitgaand verkeer wordt regelmatig bijgewerkt.	☐	☐
2	Indringingsdetectie/preventie systemen zijn geïnstalleerd, regelmatig bijgewerkt en gemonitored.	☐	☐
3	Gebruikers kunnen op het internet navigeren door middel van een netwerkinrichting (proxy) die is uitgerust met een websitefilter.	☐	☐
4	Het netwerk is gesegmenteerd om de bedrijfskritische gebieden (servers, beheer) te scheiden van de minder bedrijfskritische gebieden (zoals het gebruikersgedeelte...) .	☐	☐
5	Er wordt regelmatig een penetratietestbeoordeling uitgevoerd en een herstelplan geïmplementeerd.	☐	☐
6	Kwetsbaarheidsbeoordeling worden regelmatig uitgevoerd en een herstelplan geïmplementeerd.	☐	☐
7	Er zijn procedures voor veranderings- en incidentbeheer geïmplementeerd.	☐	☐
8	Security events (zoals virus detectie, indringingsspogingen...) worden bijgehouden en nagezien.	☐	☐

9	Er is een proactieve bewaking tegen binnendringing in het netwerk geïmplementeerd door middel van event-correlatiesystemen, loganalyse enz...	☐ ☐

	4.4. Fysieke beveiliging van de computerruimte	JA NEE
1	Bedrijfskritische systemen zijn in minimaal één speciaal daarvoor bestemde, beperkt toegankelijke computerruimte geplaatst.	☐ ☐
2	Het datacenter waar bedrijfskritische systemen zijn ondergebracht, heeft ontdubbelde infrastructuur (energie, cooling, netwerk connecties, ...).	☐ ☐
3	Bedrijfskritische systemen zijn gedupliceerd volgens een Actieve/Passieve- of Actieve/Actieve-architectuur.	☐ ☐
4	Bedrijfskritische systemen zijn gedupliceerd in twee afzonderlijke panden.	☐ ☐
5	Branddetectie en automatische blusinstallaties zijn aangebracht in kritische ruimtes.	☐ ☐
6	De stroomtoevoer is beschermd door een niet-onderbreekbare voeding (UPS) en batterijen; aan beide wordt regelmatig onderhoud gepleegd.	☐ ☐
7	De stroomvoorziening kan worden overgenomen door een elektrische generator die regelmatig wordt onderhouden en getest.	☐ ☐

	4.5. Outsourcing	JA NEE
	[In te vullen als een functie van het informatiesysteem is uitbesteed]	
1	In het contract met het outsourcing bedrijf staan beveiligingsvereisten die de service provider moet observeren.	☐ ☐
2	Er zijn Service Level Agreements met de outsourcer afgesloten waarbij incidenten en veranderingen beheerd worden en waarbij boetes kunnen opgelegd worden indien niet aan de SLA voldaan wordt.	☐ ☐
3	Er is/zijn (een) toezicht- en stuurgroep(en) met de dienstverlener georganiseerd om de dienstverlening te beheren en verbeteren.	☐ ☐
4	Heeft u afstand van verhaal gedaan tegen uw dienstverlener(s) ?	☐ ☐

Welke functies van de informatiesystemen zijn uitbesteed?	JA NEE	Dienstverlener (outsourcer)
Desktopbeheer	☐ ☐	
Serverbeheer	☐ ☐	
Netwerkbeheer	☐ ☐	
Netwerkbeveiligingsbeheer	☐ ☐	
Applicatiebeheer	☐ ☐	
Gebruik van cloud of Software as a service?	☐ ☐	

Overige, te verduidelijken:

VRAGENLIJST CHUBB CYBER ERM

5 PERSOONSGEGEVENS IN HET BEZIT VAN DE ORGANISATIE

5.1. Aantal en soorten dossiers

Het aantal persoonsgegevensdossiers dat in bezit is voor de te verzekeren activiteit: Totaal :

Per regio : Europa(EU): | USA/Canada: | Rest of World:

Categorieën verzamelde/verwerkte persoonsgegevens	JA	NEE	Aantal files
Commerciële en marketing informatie	☐	☐	
Informatie over Payment Card of financiële transacties	☐	☐	
Gezondheidsinformatie	☐	☐	

Overige, te verduidelijken:

Verwerkt u gegevens voor : ☐ uzelf ? ☐ derden ?

	5.2. Beleid voor bescherming van persoonsgegevens	JA	NEE
1	Er is een geformaliseerd privacybeleid, goedgekeurd door het management en/of de beveiligingsregels voor persoonsgegevens zijn gedefinieerd en aangeleerd aan het personeel.	☐	☐
2	De juridische aspecten van dit beleid zijn bekrachtigd door de juridische afdeling en er wordt regelmatig gecontroleerd of de wetten ter bescherming van persoonsgegevens worden nageleefd.	☐	☐
3	Het personeel dat bevoegd is om persoonsgegevens te raadplegen en/of verwerken heeft een training ontvangen in de veiligheidsregels ervan.	☐	☐
4	In uw organisatie is een functionaris voor de bescherming van persoonsgegevens benoemd.	☐	☐
5	Het betreffende personeel heeft een geheimhoudingsovereenkomst of geheimhoudingsclausule in de arbeidsovereenkomst ondertekend.	☐	☐
6	Uw praktijken op het gebied van persoonsgegevens zijn in de afgelopen twee jaar gecontroleerd door een externe revisor.	☐	☐
7	Een Data Breach Response plan is uitgewerkt en gecommuniceerd naar het response team.	☐	☐

	5.3. Verzamelen van persoonsgegevens	JA	NEE
1	U hebt de autoriteit voor gegevensbescherming medegedeeld dat u persoonsgegevens verwerkt in het kader van uw activiteit en/of u hebt toestemming van deze autoriteit ontvangen.	☐	☐
2	Op uw website staat een privacybeleid dat is gecontroleerd door een jurist/juridische afdeling.	☐	☐
3	U hebt de betrokkenen om toestemming gevraagd alvorens hun persoonsgegevens te verzamelen en ze kunnen hun persoonsgegevens raadplegen en waar nodig corrigeren of verwijderen.	☐	☐
4	In het geval van marketingactiviteiten kunnen de betrokkenen zich gemakkelijk terugtrekken ?	☐	☐
5	Draagt u persoonsgegevens over aan derden ?	☐	☐
	Indien persoonsgegevens overgedragen worden aan derden, gelieve dan volgende in te vullen		
6	De betrokken derde (bijv. verwerker) is contractueel verplicht om persoonsgegevens uitsluitend namens u en volgens uw instructies te verwerken.	☐	☐
7	De betrokken derde is contractueel verplicht om voldoende beveiligingsmaatregelen ter bescherming van de persoonsgegevens te nemen.	☐	☐

	5.4. Controle van de bescherming van persoonsgegevens	JA	NEE
1	De toegang tot persoonsgegevens is beperkt tot de gebruikers voor wie dit noodzakelijk is om hun taken uit te voeren en deze toelating wordt regelmatig herbekeken.	☐	☐
2	Persoonsgegevens en hun backups worden versleuteld wanneer ze worden opgeslagen in de informatiesystemen.	☐	☐
3	Persoonsgegevens worden versleuteld wanneer ze via het netwerk worden verzonden.	☐	☐
4	De harde schijven van laptops en smartphones zijn versleuteld.	☐	☐
5	Het is verboden om niet versleutelde persoonsgegevens te kopiëren op verwisselbare opslagmedium (zoals USB stick) of te verzenden via email.	☐	☐

		JA	NEE
	Maakt **betaalkaartinformatie** (Payment Card Information ofwel PCI) deel uit van de persoonsgegevensdossiers ?	☐	☐

Indien JA, aantal kaarttransacties per jaar	< 20K	20K tot 1M	1M tot 6M	> 6M
	☐	☐	☐	☐

1	De betalingsverwerker (uzelf of een derde) voldoet aan PCI DSS Indien NEE:	☐	☐
2	PCI wordt versleuteld opgeslagen of enkel een deel van de betaalkaarnummers wordt bewaard.	☐	☐
3	De bewaartijd van de PCI overschrijdt de duur van de betaling of de wetgeving niet.	☐	☐
4	Het beheer van betaalkaartinformatie wordt uitgevoerd door een derde ?	☐	☐
5	Als dit het geval is, eist u dat de betalingsverwerker u schadeloosstelt bij veiligheidsinbreuken.	☐	☐
6	Noem de naam van de betalingsverwerker, de bewaartijd van de PCI en eventuele aanvullende maatregelen:		

5.5. Incidenten

[Vermeld de incidenten die de afgelopen 12 maanden aanzienlijke gevolgen voor het beheer van persoonsgegevens hadden]

Datum	Beschrijving van het incident

Opmerking:

Contactpersoon voor aanvullende informatie

Naam	
Functie	
Telefoon	
E-Mail	
Ingevuld door	

Ondergetekende bevestigt hierbij dat alle verklaringen in deze vragenlijst volledig en juist zijn. Wijzigingen die na indiening van de vragenlijst of gedurende de looptijd van de verzekering plaatsvinden, dienen onmiddellijk aan Chubb Insurance Company of Europe SE te worden gemeld.

Naam ondergetekende _____ Functie _____

Datum _____ Handtekening _____

6 DEFINITIES

U:
De te verzekeren onderneming(en)

Uw:
van de te verzekeren onderneming(en)

Persoonsgegevens:
Alle geautomatiseerde informatie betreffende een persoon waarmee deze wordt of kan worden geïdentificeerd, direct of indirect, bijv. voornaam, achternaam, e-mailadres, telefoonnummer, functie, gezinssituatie, creditcardinformatie...
Gegevens over een onderneming zijn geen persoonsgegevens (de omzet van een onderneming is bijvoorbeeld geen persoonsgegeven)

Dossier :
Dit is al de persoonsinformatie omtrent 1 individu. Het aantal persoonsgegevendossiers refereereert naar het aantal individuen.

Gevoelige gegevens:
Informatie over ras/etnische afstamming, politieke/levensbeschouwelijke/religieuze opvattingen of vakbondslidmaatschap van personen, gegevens betreffende hun gezondheid of seksuele leven, sofinummer, gegevens over strafbare feiten en veroordelingen, gegevens betreffende sociale problemen van personen, biometrische gegevens.

Datasubject/betrokkene:
Elke persoon van wie de persoonsgegevens door de te verzekeren onderneming worden verzameld/verwerkt (bijv. klanten, prospecten, internetgebruikers...) BEHALVE de eigen werknemers.

Gegevensverwerking:
Alle handelingen of reeks handelingen uitgevoerd op geautomatiseerde persoonsgegevens. Het beheer van klanten bijvoorbeeld impliceert dat er persoonsgegevens over klanten worden verzameld, dat deze worden ingevoerd in een computer en worden bewaard op servers.

Autoriteit voor gegevensbescherming:
Een autoriteit voor gegevensbescherming is een onafhankelijke organisatie belast met: • het bewaken van de verwerking van persoonsgegevens binnen haar rechtsgebied (land, regio of internationale organisatie); • het verstrekken van advies aan bevoegde instanties over wettelijke en administratieve maatregelen betreffende de verwerking van persoonsgegevens; • het aanhoren van klachten ingediend door burgers betreffende hun gegevensbeschermingsrechten.

Recht op informatie:
Iedereen die persoonsgegevens verzamelt/verwerkt moet datasubjecten op de hoogte stellen van: • de identiteit van de controller, • het doel van de informatieverzameling, • de verplichte of optionele aard van de antwoorden, • de gevolgen van niet-beantwoording, • de ontvangers van de informatie, • de rechten van de persoon (voor het raadplegen, corrigeren of verwijderen van zijn persoonsgegevens), • eventuele overdracht van gegevens naar een land buiten de Europese Unie

PCI DSS: Payment Card Industry Data Security Standard (standaard voor gegevensbescherming voor kaartaccepterende bedrijven.
Een standaard voor gegevensbescherming van betaalkaartinformatie. De gevoelige betaalkaartinformatie die moet worden beschermd is het kaartnummer, de vervaldatum, de CVC-code en de naam van de kaarthouder.

PCI DSS-niveau
De handelaren zijn onverdeeld in vier PCI DSS-niveaus, afhankelijk van het aantal kaarttransacties in een periode van 12 maanden.

Niveau 1:	handelaren die jaarlijks meer dan 6 miljoen kaarttransacties uitvoeren
Niveau 2:	handelaren die jaarlijks 1 tot 6 miljoen kaarttransacties via e-commerce uitvoeren
Niveau 3:	handelaren die jaarlijks tussen 20.000 en 1 miljoen kaarttransacties via e-commerce uitvoeren
Niveau 4:	handelaren die jaarlijks minder dan 20.000 kaarttransacties via e-commerce uitvoeren en alle andere handelaren die jaarlijks tot 1 miljoen Visa-transacties uitvoeren