

Chubb Cyber Enterprise Risk Management

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. Als het beveiligingsbeleid voor informatiesystemen van de te verzekeren ondernemingen/dochtermatenschappen per bedrijf verschilt, dient voor elk daarvan een afzonderlijke vragenlijst te worden ingevuld.

Bedrijfsgegevens

Naam van de moedermaatschappij:

Adres, postcode en plaats:

Oprichtingsjaar:

Aantal werknemers:

Website:

Beschrijf de hoofdactiviteiten van de te verzekeren onderneming(en) inclusief nevenactiviteiten.

Bedrijfsprofiel

1. Geconsolideerde bruto jaaromzet of exploitatiesom

Omzet	Voorafgaand aan huidig boekjaar	Omzetverwachting huidig boekjaar	Omzetverwachting volgend boekjaar
Jaaromzet	€	€	€
Percentage van de wereldwijde omzet gegenereerd in de USA/ Canada			%
Percentage van de wereldwijde omzet die door online verkoop gegenereerd wordt			%

2. Heeft uw onderneming dochtermatenschappen buiten Nederland? *

Ja Nee

a. Zo ja, voeg dit dan toe als bijlage.

* Als sprake is van een vestiging/dochteronderneming/deelneming of joint venture of andere zaken (met partijen) in Syrië, Cuba, Soedan, Iran, Myanmar, Venezuela, De Krim en/of Noord-Korea, dan kunnen wij geen verzekeringsmogelijkheden bieden.

Data Privacy

1. Voor hoeveel dossiers met persoonsgegevens bent u verantwoordelijk?
2. Voor hoeveel dossiers met **gevoelige data** bent u verantwoordelijk?
3. Verwerkt, bewerkt of beheert u gegevens voor of namens een derde? Ja Nee
 - a. Zo ja? Gelieve toe te lichten:
4. Wordt betaalkaartinformatie verwerkt, verzameld, beheerd of bewerkt? Ja Nee
 - a. Indien ja, worden deze activiteiten uitbesteed?
 - b. Beschrijf het niveau van uw (of uw outsourcer/uitbesteede) **PCI DSS** compliance, het aantal transacties, aantal betaalkaarten waarvan u informatie heeft, de naam van de betalingsverwerker en of de betalingsverwerker u schadeloos stelt in geval van schade.

Niveau 1 (meer dan 6M)

Niveau 2 (1M tot 6M)

Niveau 3 (20.000 tot 1M)

Niveau 4 (minder dan 20.000)

Data- en informatiebeveiliging

1. Welke van de volgende punten heeft u (geef indien uitbesteed, uw provider aan) geïmplementeerd om uw bedrijf te beschermen tegen een mogelijk **cyber-incident** of **datalek**.

Beleid	Bescherming en technologie	Bedrijfscontinuïteit
Functionaris gegevensbescherming	Firewalls & Antivirus	Bedrijfscontinuïteitsplan
Medewerker die verantwoordelijk is voor de IT beveiliging	Kwetsbaarheidsscan	Crisis herstelplan (Disaster Recovery Plan)
Privacy beleid goedgekeurd en geïmplementeerd	Endpoint protection	Systeemback-up: Dagelijks Wekelijks Maandelijks
Regelmatig trainingen op het gebied van privacy en cyber	Indringer detectie systeem	
Maatregelen genomen om te (blijven) voldoen aan toepasselijke privacywetgeving, waaronder de AVG	Encryptie van gevoelige data	Back-ups zijn in een offline omgeving opgeslagen en zijn niet verbonden met het netwerk
Een Cyber incident response plan dat regelmatig getest wordt	Multi-factor authentication 2FA	Duplicatie en redundantie van kritieke systemen in een offline omgeving
Kritische updates en patches worden binnen één maand doorgevoerd	Jaarlijks een externe pentest	
Gebruik van Threat Intelligence		
Authorisatiebeheer voor systemen		
Testen van back-ups		
Overige (gelieve te omschrijven):		

Systemen

1. **Noodzaak van informatiesystemen** – Van welke systemen bent u het meest afhankelijk (inclusief uitbesteede IT-diensten) en de gevolgen die het niet beschikbaar zijn voor elk van hen heeft.

Naam IT dienstverlener (noteer 'intern' als deze niet is uitbesteed)	Activiteiten, zoals data opslag, netwerk infrastructuur, PaaS, SaaS, back-ups, ERP, beveiliging.	Hersteltermijn (Recovery time objective) In uren	Geschatte bedrijfsschade Per uur
			€
			€
			€
			€
			€

- | | | | |
|-----------|--|----|-----|
| 2. | Voert u beoordelingen, assessments of audits uit om ervoor te zorgen dat IT-dienstverleners voldoen aan de beveiligingsvereisten van uw bedrijf? | Ja | Nee |
| 3. | Neemt u afstand van uw verhaalsrecht tegen één van de hierboven genoemde aanbieders in geval van onderbreking/tekortkoming van de dienstverlening? | Ja | Nee |

Media

- | | | | |
|-----------|--|----|-----|
| 1. | Is het gebruik van handelsmerken en dienstmerken gescreend, inclusief het gebruik van domeinnamen en metatags, om te verzekeren dat er geen inbreuk op intellectuele eigendomsrechten van anderen wordt gemaakt? | Ja | Nee |
| 2. | Verkrijgt u schriftelijke toestemming of vrijwaring van externe content providers, waaronder freelancers, of andere belanghebbenden voor publicatie? | Ja | Nee |
| 3. | Wint u juridisch advies in bij het beoordelen van een publicatie voorafgaand aan de publicatie? | Ja | Nee |
| 4. | Sluit u contracten af met derden, waaronder advertentie- of marketingbureaus, om namens u inhoud te creëren of te beheren? | Ja | Nee |
| a. | Zo ja, eist u een vrijwaring of vergoeding in geval van schade? | Ja | Nee |
| 5. | Zijn uw privacybeleid, gebruikersvoorwaarden, servicevoorwaarden en Algemene Voorwaarden door een juridisch adviseur beoordeeld? | Ja | Nee |
| 6. | Gemiddels aantal unieke bezoekers van uw websites per maand: | | |

Schadeverleden

- | | | | |
|-----------|--|----|-----|
| 1. | Heeft u in de afgelopen drie jaar te maken gehad met een vermoedelijk of daadwerkelijk datalek, cyber-incident of media-aansprakelijkheidscclaim of heeft u te maken gehad met de Autoriteit Persoonsgegevens of een vergelijkbare toezichthouder? | Ja | Nee |
|-----------|--|----|-----|

a. Indien ja, graag voorzien van:

Beschrijving eventuele claims/incidenten en datum van het voorval.

Beschrijving van de financiële gevolgen.

Welke maatregelen heeft u getroffen om dergelijke incidenten in de toekomst te voorkomen of beperken?

- | | | | |
|-----------|---|----|-----|
| 2. | Bent u op de hoogte van feiten of omstandigheden die mogelijk te kwalificeren zijn als een datalek, cyberincident of media-aansprakelijkheid? | Ja | Nee |
|-----------|---|----|-----|

a. Zo ja, beschrijf:

Dekking

1. Gelieve hieronder het verzekerde bedrag aan te geven waarvoor u een offerte wilt ontvangen.

€

€

€

2. Gelieve hieronder het eigen risico aan te geven waarvoor u een offerte wilt ontvangen.

€

Verklaring

De informatie die in dit overzicht is opgenomen is voor ons van belang voor: 1) onze beslissing omtrent acceptatie van deze verzekering; 2) het bepalen van de voorwaarden die op deze verzekering van toepassing zijn; 3) het bepalen van de verzekeringspremie.

Wij vertrouwen op deze informatie bij het accepteren van deze verzekering. Het feit dat specifieke vragen gesteld en beantwoord zijn, neemt niet weg dat de verzekerde ons dient te informeren over alle zaken die de acceptatie of beoordeling van het risico door ons wezenlijk zou beïnvloeden.

Ondergetekende verklaart voorgaande vragen juist en volledig te hebben beantwoord. Indien sprake is van vooraf ingevulde antwoorden verklaart ondergetekende deze antwoorden op juistheid en volledigheid te hebben gecontroleerd. Wij zijn ontslagen van iedere uitkeringsplicht indien blijkt dat verzekeringnemer bij het aanvragen van de verzekering onjuiste of onvolledige informatie heeft verstrekt en wij de verzekering niet of niet onder dezelfde voorwaarden zouden hebben gesloten, indien wij de juiste feiten gekend hadden.

Naam:

Functie / Titel:

Datum van ondertekening (DD/MM/JJJJ):

Optioneel: additionele dienstverlening

Chubb is een samenwerking aangegaan met een aantal pre-incident dienstverleners, die u kunnen helpen bij het beter beheersbaar maken van uw cyberrisico's. Om u van deze diensten te kunnen voorzien kunt u een paar vragen hieronder beantwoorden.

Meer informatie over onze Pre Incident Diensten kunt u vinden via de volgende link: www.chubb.com/cyber-services

- | | | | |
|----|---|----|-----|
| 1. | Organiseert u regelmatig phishing trainingen voor uw medewerkers? | Ja | Nee |
| 2. | Maakt u gebruik van een password manager? | Ja | Nee |
| 3. | Maakt u uw medewerkers bewust van cyberrisico's? | Ja | Nee |

Begrippenlijst

Autorisatiebeheer voor Systemen - Access Management Controls omvat het management van gebruikersnamen, wachtwoorden en toegang tot systemen en informatie.

Cyber-incident- Cyber-incident betekent ongeautoriseerde toegang tot computer systemen, hacking, malware, virus, cyber afpersing, distributed denial of service-aanval, misbruik door voorkennis, menselijke fout of programmeerfout of een andere aan cyber gerelateerde gebeurtenis.

Datalek- Een datalek betekent dat er een incident heeft plaatsgevonden waarbij gevoelige persoonsgegevens of bedrijfsgevoelige informatie is gestolen, kwijtgeraakt of bekeken bij of door een onbevoegde partij.

Encryptie – Encryptie is een methode om data vanuit een leesbare format te converteren naar een gecodeerde format. Het kan alleen weer leesbaar worden (worden geopend) met behulp van een sleutel.

Endpoint Protection – Endpoint Protection zorgt voor de bescherming en bewaking van de eindpunten in uw netwerk. Eindpunten omvatten desktop-en laptopcomputers, tablets, mobiele telefoons, servers en elk ander apparaat dat verbonden is met uw netwerk.

Gevoelige data– Onder gevoelige data wordt o.a. verstaan gezondheids-of medische dossiers van werknemers of klanten, door de overheid uitgegeven identificatienummers, gebruikersnamen en wachtwoorden, e-mailadressen, creditcardnummers, intellectueel eigendom of andere persoonlijk identificeerbare informatie.

Indringer Detectie Systeem – Is een apparaat of software dat een netwerk monitort op kwaadwillige activiteiten of beleidsschendingen.

Media-aansprakelijkheid – Media-aansprakelijkheid omvat ieder claim voor het kleineren, smaad, laster in handelsbetrekkingen, schijnvertoning, plagiaat of iets dergelijks van uw website of social media accounts.

PCI DSS -Payment Card Industry Data Security Standard. Dit is een 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.

Recovery Time Objective - De beoogde tijdsduur waarbinnen het bedrijfsproces moet worden hersteld na een storing of verstoring om onaanvaardbare gevolgen te vermijden die samenhangen met een onderbreking van de bedrijfscontinuïteit.

Threat Intelligence– Bedreigingsinformatie is informatie over huidige beveiligingsbedreigingen, kwetsbaarheden, doelen, slechte actoren en implicaties die kunnen worden gebruikt om beveiligingsbeslissingen.

Contact

Chubb European Group SE
Nederlands bijkantoor Marten
Meesweg 8-10 3068 AV Rotterdam
T: 0800-22 55 223
www.chubb.com/nl

Verwerking persoonsgegevens

De verzekeraar maakt gebruik van door verzekeringnemer aan hem verstrekte persoonsgegevens voor het accepteren en beheren van deze overeenkomst, waaronder begrepen daaruit voortvloeiende aanspraken.

De ingezamelde gegevens omvatten basiscontactgegevens zoals naam, adres en polisnummer, maar kunnen tevens meer gedetailleerde informatie bevatten (bijvoorbeeld leeftijd, medische gegevens, vermogenssituatie of schadehistorie) voor zover dit relevant is voor het door verzekeraar te verzekeren risico, de door verzekeraar te verlenen diensten of voor de door verzekerde in te dienen aanspraken.

De verzekeraar maakt deel uit van een wereldwijd concern, en de persoonsgegevens kunnen met zijn groepsmaatschappijen in andere landen worden gedeeld, voor zover dit nodig is voor de dekking van de polis of het opslaan van de gegevens. De verzekeraar maakt daarnaast ook gebruik van erkende dienstverleners, die toegang hebben tot de persoonsgegevens met inachtneming van verzekeraars instructies en zeggenschap.

De verzekerde heeft een aantal rechten met betrekking tot de verstrekte persoonsgegevens, waaronder begrepen inzage-rechten en in bepaalde gevallen het recht op verwijdering en doorhaling.

In dit onderdeel is in het kort uitgelegd op welke manier de verzekeraar gebruik maakt van de persoonsgegevens. Voor meer informatie raadt de verzekeraar de verzekerde ten eerste aan om zijn Algemene Privacybeleid te raadplegen, dat hier kan worden ingezien:

<https://www.chubb.com/benelux-nl/footer/privacy-policy.aspx>. Verzekerde kan de verzekeraar altijd vragen om een papieren versie van het Privacybeleid door een e-mail te sturen naar dataprotectionoffice.europe@chubb.com.

Bij het verwerken van persoonsgegevens binnen Nederland houdt de verzekeraar zich tevens aan de Gedragscode Verwerking Persoonsgegevens van het Verbond van Verzekeraars, die verzekerde kan raadplegen via de website van het Verbond van Verzekeraars, www.verzekeraars.nl, of die opgevraagd kan worden bij het Verbond van Verzekeraars, Postbus 93450, 2509 AL Den Haag, telefoon 070-3338500.

Beknopt privacystatement Turien & Co. Assuradeuren

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

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.