Risikoanalyse Cyberversicherung

exzellent Versicherungsmakler

1. ALLGEMEINE INFORMATIONEN ZUM VERSICHERUNGSNEHMER

Name und Firmierung:	
Straße u. Hausnummer:	
Postleitzahl und Ort:	
Firmen-Website:	www.
Gründungsdatum:	
Mitarbeiteranzahl:	

2. UNTERNEHMENSSTRUKTUR

Gibt es Tochtergesellschaften?	Ja	☐	Nein	☐

Wenn ja, bitte Folgendes angeben (gegebenenfalls ein Organigramm dem Fragebogen anfügen):

Name und Firmierung	Land	Umsatz

3. WEITERE UNTERNEHMENSINFORMATIONEN

a) Beschreibung der Geschäftstätigkeit der Gesellschaft und etwaiger Tochtergesellschaften:

b) Konsolidierter Jahresumsatz (inkl. mitzuversichernder Tochtergesellschaften):			
	letztes Geschäftsjahr	aktuelles Geschäftsjahr	kommendes Geschäftsjahr
Deutschland	€	€	€
Europa	€	€	€
USA / Kanada	€	€	€
Rest der Welt	€	€	€
Umsatz insgesamt	€	€	€
Umsatz aus online-Verkäufen oder online-Dienstleistungen?	€	€	€
c) Bilanzsumme	€	€	---

d) Wurden in den letzten drei Jahren Firmen übernommen (M&A), Tochtergesellschaften gegründet oder ist dieses aktuell geplant?	
Nein ☐	Ja ☐ Bitte geben Sie hierzu weitere Details an:

4. AUSGEGLIEDERTE DIENSTLEISTUNGEN UND PROZESSE

Bitte kreuzen Sie an, welche der folgenden Dienstleistungen outgesourct sind:

Abrechnungs- oder Zahlungsdienste (inkl. Lohn-abrechnungen)	Sicherung und Wiederherstellung von Daten	Hosting eines Webservers	Internetdienst-anbieter (Internet Service Provider (ISP))	Management der Informations-sicherheit (ISMS)
☐	☐	☐	☐	☐
Finanzdienst-leistungen und Zahlungsverkehr	Datenvernichtung	Datenverwaltung und -archivierung	Cloud-Dienste	
☐	☐	☐	☐	

5. INFORMATIONEN ZUM RISKO / RISIKOANALYSE

a) Art und Menge der Daten

Welche der folgenden Daten werden von Ihnen auf Ihren oder in Ihre EDV-Systeme übertragen, bearbeitet oder gespeichert?			Anzahl/Menge:
- Kreditkartendaten?	Ja ☐	Nein ☐	
Bei Speicherung von Kreditkartendaten:			
Vollständige Speicherung der Kreditkartennummer?	Ja ☐	Nein ☐	
Speicherung des Card Validation Codes (CVC)?	Ja ☐	Nein ☐	
- EC-Kartendaten?	Ja ☐	Nein ☐	
- Kundendaten?	Ja ☐	Nein ☐	
- Steuer- und Finanzdaten?	Ja ☐	Nein ☐	
- Sozialversicherungs- und Ausweisdokumente?	Ja ☐	Nein ☐	
- Kenn- oder Passwörter?	Ja ☐	Nein ☐	
- Sonstige Daten (bitte angeben):			

b) Informationen zur elektronischen Zahlungsabwicklung (payment processing):

1. Akzeptieren Sie Kreditkartenzahlungen?	Ja ☐	Nein ☐		
2. Finden die aktuell geltenden Payment Card Industry Data Security Standards (PCI DSS) bei Ihnen Anwendung?	Ja ☐	Nein ☐		
3. Falls „Ja“, in welche Händlerkategorie (Level 1-4) sind Sie eingestuft?	1 ☐	2 ☐	3 ☐	4 ☐

LEVEL 1 bis 4

	TRIFFT ZU AUF	ANFORDERUNGEN
LEVEL 1	1 Organisationen, die jährlich mehr als 6 Millionen Transaktionen über Visa oder MasterCard; oder mehr als 2,5 Millionen Transaktionen über American Express abwickeln; oder 2 Eine Datenschutzverletzung erfahren haben; oder 3 Werden von allen Kartenverbänden (Visa, Mastercard usw.) als Level 1 eingestuft	1 Jährlicher Konformitätsbericht (ROC) durch einen qualifizierten Sicherheitsprüfer (Qualified Security Assessor) (QSA) - auch bekannt als Level 1- Standortprüfung oder interne Prüfung, wenn einer der Unternehmensleiter unterschreibt 2 Vierteljährlicher Netzwerk-Scan durch anerkannten Scan-Anbieter (Approved Scan Vendor) ASV 3 Konformitätsbescheinigung (AOC) für Standortprüfungen - es gibt bestimmte Formulare für Händler und Service-Anbieter
LEVEL 2	Organisationen, die jährlich zwischen 1 und 6 Millionen Transaktionen abwickeln.	1 Jährlicher PCI DSS Selbstbewertungsfragebogen (Self-Assessment Questionnaire) SAQ - in der Tabelle unten werden die 9 bestehenden SAQ-Typen kurz beschrieben 2 Vierteljährlicher Netzwerk-Scan durch anerkannten Scan-Anbieter (Approved Scan Vendor) (ASV) 3 Konformitätsbescheinigung (AOC) - es gibt ein entsprechendes Formular für jeden der 9 Selbtbewertungsfragebögen
LEVEL 3	1 Organisationen, die jährlich insgesamt **zwischen 20.000 und einer Million** Transaktionen abwickeln 2 Organisationen, die jährlich insgesamt **weniger als eine Million** Transaktionen abwickeln	
LEVEL 4	1 Organisationen, die jährlich insgesamt **weniger als 20.000** Transaktionen abwickeln; oder 2 Organisationen, die jährlich **insgesamt** bis zu einer Million Transaktionen abwickeln	

c) Datenschutz

1. Werden von Ihnen Unternehmensrichtlinien in Bezug auf Datensicherheit, Datenschutz und Umgang mit Firmeneigentum durchgesetzt, die von allen Personen befolgt werden müssen, die Zugriff auf Ihr Netzwerk oder auf Ihnen anvertraute sensible Informationen/Daten haben? Ja ☐ Nein ☐

2. Bieten Sie mindestens einmal jährlich IT-Sicherheitstrainings für jeden Ihrer Mitarbeiter bzw. für alle Personen an, die Zugriff auf Ihr Netzwerk oder auf Ihnen anvertraute sensible Daten haben? Ja ☐ Nein ☐

d) Netzwerksicherheit

1. Wird in allen ITK-(Informations- und Kommunikations-) Systemen Folgendes regelmäßig aktualisiert?

- Anti-Viren-Programme Ja ☐ Nein ☐
- Firewalls Ja ☐ Nein ☐

	Täglich?	Wöchentlich?	Monatlich?	In Intervallen > 1 Monat?
2. Wie oft implementieren Sie aktuelle Sicherheits-Updates /Sicherheits-Patches in Ihren ITK-Systemen?	☐	☐	☐	☐

3. Ersetzen Sie umgehend werksseitige Standardkonfigurationen, um zu gewährleisten, dass Ihre ITK-Systeme ausreichend sicher konfiguriert sind? Ja ☐ Nein ☐

4. Findet mindestens einmal jährlich von Ihnen eine Neubewertung Ihrer Risikosituation in Bezug auf Informationssicherheit und Datenschutzverletzungen statt und erhöhen Sie als Reaktion auf mögliche Änderungen Ihre Risikokontrollen? Ja ☐ Nein ☐

5. Sofern Sie ein drahtloses Netzwerk (WLAN) benutzen, richten Sie für dieses alle gängigen Sicherheitsstandards (wie. z.B. Username + Passwort) ein? Ja ☐ Nein ☐

6. Gibt es einen schriftlich festgelegten Notfallplan (Business Continuity Plan), der sicherstellt, dass Sie Netzwerkstörungen, unberechtigte Netzwerkzugriffe, Netzwerkattacken und -vorfälle (z.B. durch Viren, Malware, unbefugtes Eindringen (Hacking) oder Denial-of-Service-Angriffe (Dos)), Datenverlust und Verstöße gegen den Datenschutz sicher bewältigen können? Ja ☐ Nein ☐

7. Wenn ja, wird dieser Notfallplan einmal im Jahr überarbeitet und fortgeschrieben? Ja ☐ Nein ☐

8. Wie lange dauert es, bis Ihre Systeme nach einer Hackerattacke oder einem Datenverlust wieder komplett verfügbar sind? _____ Stunden

9. Kontrollieren und verfolgen Sie alle Veränderungen in Ihrem Netzwerk, um auf Störfaktoren und Fehler reagieren und weiterhin die Sicherheit gewährleisten zu können? Ja ☐ Nein ☐

10. Findet bei Ihnen keine Entwicklungsaktivität (wie z.B. Programmierung) in Ihrer IT-Produktionsumgebung statt und implementieren Sie neue Technologien erst nach einem Proof-of-Concept Verfahren in einer Testumgebung? Ja ☐ Nein ☐

11. Haben Sie in Ihrem Unternehmen einen eigenen IT-Security Verantwortlichen? Ja ☐ Nein ☐

12. Haben Sie im Rahmen Ihrer Informationssicherheit die DIN-Norm ISO 27001 umgesetzt? Ja ☐ Nein ☐

13. Falls „nein“, welche anderen Normen (z.B. DS484, ISA 3000) haben Sie berücksichtigt?	Normen:

e) Zugriffsrechte

1.Existieren geeignete Unternehmensrichtlinien über die Komplexität von Passwörtern?	Ja	☐	Nein	☐
2. Beschränken Sie den Zugriff auf den Personenkreis, der Zugriff auf die Daten benötigt?	Ja	☐	Nein	☐
3. Erfolgt ein Fernzugriff („remote access“) auf Ihre IT-Systeme mittels Authentifizierung und Verschlüsselung und ist gewährleistet, dass dieser Zugriff genauso sicher ist wie von unternehmenseigenen Systemen und werden diese Zugriffe auch gemonitort und regelmentiert?	Ja	☐	Nein	☐
4. Haben Sie die Möglichkeit, nichtautorisierte Zugriffe oder Zugriffsversuche auf sensible Informationen/Daten aufzuspüren, zu protokollieren und ggf. umgehend zu unterbinden?	Ja	☐	Nein	☐

f) Datensicherheit

1. Ist in Ihrem Unternehmen ein betrieblicher Datenschutzbeauftragter gesetzlich ordentlich bestellt worden?	Ja	☐	Nein	☐
2. Setzen Sie zum Schutz von sensiblen und unternehmenskritischen Daten geeignete Sicherungsverfahren ein (z.B. Verschlüsselung)?	Ja	☐	Nein	☐

Wenn ja, welche Verfahren werden eingesetzt?

3. Setzen Sie in Ihrem Unternehmen eine „clean desk policy“ um?	Ja	☐	Nein	☐
4. Setzen Sie in Ihrem Unternehmen eine „clean screen policy“ um?	Ja	☐	Nein	☐
5. Wissen Sie wie Sie Einzelpersonen bzw. Ihre Kunden jeweils kontaktieren, falls Datenschutzverletzungen vorliegen?	Ja	☐	Nein	☐
6. Beim Transport von Wechseldatenträgern (z.B. Laufwerke, USB-Sticks, Laptops oder Mobiltelefone) mit sensiblen Informationen/Daten, ist sichergestellt, dass:				
1) die sensiblen Informationen/Daten verschlüsselt sind	Ja	☐	Nein	☐
2) der mobile Datenträger ständig unter der direkten physischen Kontrolle einer Einzelperson ist, die eine Zugriffsberechtigung auf die gespeicherten Informationen/Daten hat (das heißt, der mobile Datenträger ist niemals unbeaufsichtigt).	Ja	☐	Nein	☐
7. Stellen Sie beim Transport von sensiblen Informationen/Daten in Papierform sicher, dass die schriftlichen Aufzeichnungen ständig unter der direkten physischen Kontrolle einer Einzelperson sind, die eine Zugriffsberechtigung auf die schriftlichen Aufzeichnungen hat (das heißt, die schriftlichen Aufzeichnungen sind niemals unbeaufsichtigt)?	Ja	☐	Nein	☐
8. Wenn Sie sensible Daten an Dritte weitergeben,				
1) regeln Sie vertraglich, dass die Daten von dem Dritten mit Sicherungsmaßnahmen geschützt werden, die mindestens den Ihren entsprechen oder prüfen Sie, ob die Sicherheitsstandards des Dritten bzgl. des Umgangs mit vertraulichen Daten mindestens Ihren eigenen Standards entsprechen?	Ja	☐	Nein	☐
2) regeln Sie vertraglich, dass man Ihr Unternehmen freistellt bzw. schadlos hält, falls eine Vertraulichkeitsverletzung oder eine Datenschutzverletzung von dem Dritten begangen wird?	Ja	☐	Nein	☐

3) fordern Sie, dass der Dritte entweder über ausreichende Geldmittel verfügt oder eine Versicherung mit ausreichender Deckungssumme abgeschlossen hat, die bei Verstößen gegen den Datenschutz Deckung bietet? Ja ☐ Nein ☐

g) Datensicherung

1.Bewahren Sie nicht öffentliche, persönliche und andere sensible Informationen/Daten nur solange auf, wie sie tatsächlich gebraucht bzw. verwendet werden und löschen oder zerstören Sie diese nach abschließender Verwendung irreversibel und stellen sicher, dass keinerlei Datenrückstände verbleiben? Ja ☐ Nein ☐

2. Wie oft erfolgt die Datensicherung (Back-Up) Ihrer Netzwerkdaten und Konfigurationsdateien?	Täglich?	Wöchentlich?	Monatlich?	In Intervallen > 1 Monat?
	☐	☐	☐	☐

3. Wird die Datenwiederherstellung regelmäßig simuliert? Ja ☐ Nein ☐

6. SCHADENVERLAUF

a) Eigenschadenhistorie:

	Ja	Nein
Haben Sie im Hinblick auf Ihr Netzwerk in den letzten 5 Jahren Erfahrungen gemacht, die zu einer Inanspruchnahme bzw. zu einem Versicherungsfall gem. unserer NetProtect - Cyber Versicherung geführt hätten?	☐	☐

Falls „Ja“, bitte beschreiben Sie die Einzelheiten auf dem im Anhang angefügten Zusatzblatt. Bitte beschreiben Sie das Ereignis unter Berücksichtigung der folgenden Gesichtspunkte:

(1) Wie ist es passiert? (2) Was war beeinträchtigt? (3) Welcher Schaden ist Ihnen entstanden? (4) Wie haben Sie reagiert? (5) Welche Maßnahmen haben Sie unternommen, um Schäden dieser Art künftig zu vermeiden?

b) Dritt- bzw. Haftpflichtschaden:

	Ja	Nein
Sind gegen Sie Beschwerden, Ansprüche oder Schäden geltend gemacht worden im Hinblick auf Inhaltsverletzungen, Persönlichkeitsverletzungen, Identitätsdiebstahl, Dos- oder DDos-Angriffen, Virenbefall, Diebstahl von Informationen Dritter, Beschädigungen anderer Netzwerke oder die Möglichkeit anderer, auf Ihr Netzwerk zurückzugreifen?	☐	☐

Wenn ja, wie oft kam dies in den letzten fünf Jahren vor? Anzahl:

Falls ja, bitte beschreiben Sie die Einzelheiten auf dem im Anhang angefügten Zusatzblatt.

c) Bisherige Schadenmeldungen:

	Ja	Nein

Haben Sie schon einmal Ereignisse, Schadenersatzansprüche oder Verluste an Versicherer gemeldet, die Versicherungsverträge mit (teilweise) gleichen Deckungsinhalten wie denen der NetProtect-Cyber Versicherung betrafen?	☐	☐

Falls ja, bitte beschreiben Sie die Einzelheiten auf dem im Anhang angefügten Zusatzblatt.

d) Kenntnisse von Umständen und Beschwerden:

	Ja	Nein
Sind Ihnen Umstände bekannt, die zu einem Schadenersatzanspruch gegen Sie oder einem Schaden (Datenverlust, Betriebsunterbrechung, etc.) führen könnten?	☐	☐

Falls ja, bitte beschreiben Sie die Einzelheiten auf dem im Anhang angefügten Zusatzblatt.

7. GEWÜNSCHTE DECKUNGSBAUSTEINE

	Gewünscht				Versicherungs-summe	Selbstbehalt / zeitlicher Selbstbehalt
Cyber Haftpflichtversicherung:	Ja	☐	Nein	☐	€	€

Cyber-Eigenschadendeckung:	Ja	☐	Nein	☐	€	€
Cyber-Betriebsunterbrechungsschaden						Stunden

Kumulierte Versicherungssumme / Gesamtversicherungssumme:				€
Rückwärtsdeckung gewünscht? (nur bei Vorversicherung möglich)	Beginn:			
Verteidigungs- und Abwehrkosten	Inklusive	☐	Zusätzlich	☐

8. ERKLÄRUNG / AUTORISIERTE UNTERSCHRIFT

Der Unterzeichner dieses Fragebogens bestätigt, dass die oben genannten Erklärungen vollständig und wahrheitsgemäß beantwortet wurden und keine für die Übernahme dieser Versicherung wichtigen Aspekte verschwiegen oder nicht richtig wiedergegeben wurden. Der Unterzeichner verpflichtet sich, Änderungen, die sich vor oder nach dem Abschluss des Vertrages ergeben haben, unverzüglich dem Versicherer mitzuteilen.

Datum

Unterschrift u. Firmenstempel

Position im Unternehmen

Zusatzblatt zur Beantwortung der Fragen

8a)

8b)

8c)

Weitere ergänzende Anmerkungen zu anderen Fragen: