LIGA LÖFFLER VERSICHERUNGSMAKLER

Fragebogen Cyberversicherung

VERSICHERUNGSNEHMER/ANTRAGSSTELLER

Name:	
Anschrift:	
Homepage:	
Branche/Unternehmenstätigkeit:	Gründungsjahr:
Tochtergesellschaften mit Sitz in Deutschland:	Mitarbeiteranzahl:

Firma und Rechtsform	Hauptsitz	Beteiligung in %

1. UMSATZANGABEN

Geschäftszahlen	Letztes Geschäftsjahr	Aktuelles Geschäftsjahr	Folge Geschäftsjahr
(konsoldierter) Bruttojahresumsatz			
davon EU/EWR			
davon USA/Kanada			
davon E-Commerce (Online-Umsätze)			

Höhe des IT-Budgets im aktuellen Geschäftsjahr? _____ Euro (ohne Personenkosten)

2. ART UND MENGE VON DATEN

Art der Daten	Menge der gespeicherten und/oder verarbeiteten Datensätze in Ihrem UN		
Personenbezogene sensible Daten	Weniger als 1.000 Personen ☐	Weniger als 10.000 Personen ☐	Mehr als 10.000 Personen ☐
Geschützte Gesundheitsdaten (medizin. Patientendaten)	Weniger als 1.000 Personen ☐	Weniger als 5.000 Personen ☐	Mehr als 5.000 Personen ☐

3. DATENVERARBEITUNG

3.1. Nutzen Sie hauptberufliche externe Dienstleister für die folgenden IT-Leistungen (insbesondere: Betreuung der eigenen IT-Systeme, Sicherung, Sicherheit und Datenauslagerungen)? ☐ ja ☐ nein

Wenn ja, bitte geben Sie den/die Namen der Dienstleister, deren Tätigkeit und Internetadresse an:

Falls nein, bitte um Angabe der Anzahl der Mitarbeiter in der internen IT-Abteilung auf VZ-Basis und deren jeweilige Qualifikation und Berufserfahrung in Jahren

3.2. Ist im Vertrag mit jedem in Frage 3.1 genannten Dienstleister die Erreichbarkeit während den Geschäfts- bzw. Produktionszeiten bei Störungen der Verfügbarkeit des IT-Systems und die Reaktionszeit bei Ausfällen geregelt? ☐ ja ☐ nein

3.3. Enthält der Vertrag mit dem/die Dienstleister Haftungsfreistellungen und/oder Haftungsausschlüsse? ☐ ja ☐ nein

3.4. Ist sichergestellt, dass das IT-Sicherheitsniveau der/des beauftragten Dienstleister/s mindestens dem Sicherheitsstandard Ihres Unternehmens entspricht? ☐ ja ☐ nein

3.5. Werden Datensätze an Subunternehmer weitergegeben? ☐ ja ☐ nein
Wenn ja, bitte beschreiben Sie die Art und Menge der weitergegebenen Datensätze

Ist sichergestellt, dass die weitergebenen Daten jederzeit verschlüsselt werden? ☐ ja ☐ nein

4. NETZWERKSICHERHEIT IHRES UNTERNEHMENS

4.1. Werden alle Internet Zugangspunkte durch Firewall geschützt? ☐ ja ☐ nein

4.2. Werden alle Systeme und Anwendungen durch eine Antivirussoftware und Anti-Malware-Software gesichert? ☐ ja ☐ nein
Wird diese Software jeweils automatisch aktualisiert? ☐ ja ☐ nein
Wenn nein, wie erfolgt die Aktualisierung?

4.3. Sind Drahtlosnetzwerke nach WPA/WPA2 Verschlüsselungsstandard gesichert? ☐ ja ☐ nein

4.4. Wird Ihr Netzwerk/Betriebssystem neben der Firewall ununterbrochen durch weitere Systeme zur Angriffserkennung/Angriffsvorbeugung (Intrusion/Prevention Detection - IPS, DMZ) überwacht? ☐ ja ☐ nein

4.5. Wie wird das Patch/Update Management (Fehlerkorrekturen für Systeme und Anwendungen) durchgeführt?

- ☐ automatisch
- ☐ zeitnahe manuelle Implementierung

4.6. Welche Schutzmaßnahmen bei Fernwartungszugängen und Fernzugriffen auf Ihr Netzwerk haben Sie umgesetz (auch mehrfach Nennung möglich)

- ☐ VPN-Verschlüsselung (Virtual Private Networks)
- ☐ Zwei-Faktor-Authentifizierung
- ☐ Personenbezogene Zugänge
- ☐ Dokumentation der Fernwartungszugänge
- ☐ Beobachtung externer Wartungszugriffe durch eigene Mitarbeiter
- ☐ Freischaltung von Fernwartungszugriffe durch eigene Mitarbeiter

5. INFORMATIONS- UND DATENSICHERHEIT

5.1. Ist eine Datenschutzrichtlinie in Ihrem Unternehmen umgesetzt? ☐ ja ☐ nein

5.2. Ist eine IT-Sicherheitsrichtlinie in Ihrem Unternehmen umgesetzt? ☐ ja ☐ nein

5.3. Wann wurden die Datenschutz- und IT-Sicherheitsrichtlinie zum letzten Mal aktualisiert?

Datum

5.4. Ist ein abgestuftes Rechtskonzept in Ihrem Unternehmen umgesetzt (Mitarbeiterberechtigungen nach Einsatzbereichen der Mitarbeiter, Administratorenberechtigung)? ☐ ja ☐ nein

5.5. In welchen zeitlichen Intervallen werden getrennte Datensicherungen durchgeführt (Backup)

- ☐ täglich
- ☐ wöchentlich
- ☐ individuelles Intervall (bitte angeben)

5.6. In welchen zeitlichen Intervallen werden Wiederherstellungstests durchgeführt (Test der Backups und der getrennten Datensicherung)?

- ☐ monatlich
- ☐ individuelles Intervall (bitte angeben)

5.7. Haben Sie einen Krisen- oder Notfallplan nach Störfällen bei denen es zur Verletzung von Datenschutz und/oder zum Eindringen in Ihr Netzwerk und/oder zu einer IT-Virus-Infektion Ihres Netzwerkes kommt? ☐ ja ☐ nein

5.8. Wird der Zugriff auf personenbezogene oder sonstige sensible Daten durch sichere Passwörter geschützt? ☐ ja ☐ nein

5.9. Haben Sie eine Passwortrichtlinie und setzen Sie komplexe und regelmäßig zu ändernde Passwörter durch? ☐ ja ☐ nein

5.10. Werden die Mitarbeiter regelmäßig persönlich zur IT-Sicherheit geschult, insbesondere zu den Themen Datenschutz, IT-Sicherheit? ☐ ja ☐ nein
Wenn ja, bitte geben Sie an in welchem Abstand

5.11. Haben alle internen und externen Mitarbeiter sowie externen Dienstleister eine schriftliche Vertraulichkeitserklärung (z.B. im Arbeitsvertrag) abgegeben? ☐ ja ☐ nein

6. ZAHLUNGSKARTEN (KREDITKARTEN UND EC-KARTENZAHLUNGEN)

6.1. Akzeptieren Sie Kreditkartenzahlungen?

6.2. Wie viele Transaktionen mit Bezahlkarten (Kreditkarten, EC-Karten) führen Sie jährlich durch? ☐ ja ☐ nein

- ☐ weniger als 20.000
- ☐ 20.001 bis 50.000
- ☐ mehr als 50.000 (bitte Anzahl angeben)

6.3. Welches Händlerniveau nach der PCI Definition erfüllen Sie (PCI DSS Level)?

6.4. Verwenden Sie softwaregesteuerte Anlagen (z.B. SCADA, ICS) und sind diese segmentiert (physisch oder virtuell getrenntes Netzwerk)? ☐ ja ☐ nein

6.5. In welchem Zeitraum können Sie Ihr IT-System/Netzwerk nach einem Cyberangriff und/oder einem Ausfall wieder vollständig in Betrieb nehmen und bestimmungsgemäß nutzen (Wiederanlaufzeit)?

- ☐ weniger als 12h
- ☐ 12h bis 24h
- ☐ mehr als 1 Tag

7. VORSCHADENINFORMATION

7.1. Trifft es zu, dass keine Aufsichtsbehörde oder sonstige Behörde bereits einmal eine Klage gegen das Unternehmen oder mitversicherte Unternehmen eingereicht oder Ermittlungen wegen dem Umgangs mit sensiblen Daten eingeleitet hat? ☐ ja ☐ nein

7.2 Trifft es zu, dass es in den letzten 5 Jahren keine Schäden durch Datenrechtsverletzungen, Hacker-Angriffe, Denial-of-Service-Attacken oder Schadsoftware gegeben hat und dass Ihnen aktuell keine Umstände bekannt sind, die zu solchen Ereignissen führen könnten? ☐ ja ☐ nein

Der ausgefüllte Fragebogen ist die Grundlage der Versicherung und wird Bestandteil des Versicherungsvertrages. Die vorstehend gemachten Risikoangaben sind vorvertragliche Angaben im Sinne der §§ 19 ff. VVG. Die Mitteilung nach § 19 Absatz 5 VVG über die Folgen einer Verletzung der gesetzlichen Anzeigepflicht werden zur Kenntnis genommen.
Der Unterzeichner bestätigt, die vorstehenden Fragen vollständig und wahrheitsgemäß beantwortet zu haben. Unrichtige oder unvollständige Angaben können zum Verlust des Versicherungsschutz führen.

Ort, Datum	Unterschrift Antragsteller

Angaben zum gewünschten Versicherungsumfang

Versicherungssumme:

- ☐ 100.000 Euro
- ☐ 250.000 Euro
- ☐ 500.000 Euro
- ☐ 1.000.000 Euro
- ☐ Andere:

Mit Ertragsausfall/Betriebsunterbrechung ☐ ja ☐ nein

Die Absicherung für Ertragsausfallschäden durch den Cloud-Ausfall bei DDoS-Angriffen gegen den Cloud-Dienstleister wird gewünscht? ☐ ja ☐ nein