Firma und Anschrift	
Internetadresse	
Weitere zu versichernde Unternehmen	
Hinweis: Bitte beantworten Sie die nachstehenden Fragen für die Gesamtheit der zu versichernden Unternehmen. Sofern sich für die einzelnen Mitzuversichernden unterschiedliche Aussagen ergeben, beantworten Sie diese Abschnitte für die betreffenden Unternehmen bitte jeweils separat.	
Umsatz	TEUR
Hinweis: Bitte geben Sie an, ob die nachfolgenden Aussagen für Ihr Unternehmen (und ggfs. weitere mitzuversichernde Unternehmen) zutreffend sind. Zu den Aussagen, die nicht als „zutreffend“ bejaht werden können, geben Sie bitte auf einem Beiblatt eine kurze Erläuterung.	
Wir erwirtschaften derzeit keine direkten USA-/ Kanada-Umsätze oder erbringen Leistungen in den USA/Kanada.	☐ Ja, zutreffend. ☐ Nein
Wir haben keine rechtlich selbstständigen Tochtergesellschaften außerhalb des Europäischen Wirtschaftsraumes (EWR)	☐ Ja, zutreffend. ☐ Nein
Unsere Geschäftstätigkeit umfasst nicht eine der folgenden Sparten/Berufe: • Zahlungsabwicklung, Inkassodienstleistung • Agentur für Kredit-Rating, Datensammlung und –speicherung • Finanzdienstleistungssektor, insbesondere die Vermittlung und Beratung von Versicherungen und Bankprodukten, sowie Vermögensverwaltung • Franchisenehmer, Franchisegeber, Direktmarketing, Call Center • Produzent und/oder Anbieter von pornografischen Inhalten oder Glückspielen • Behörde oder sonstige staatliche Einrichtungen • Hersteller von mobilen Applikationen • Betreiber von sozialen Netzwerken • Fluggesellschaft • öffentliche Versorgungsunternehmen	☐ Ja, zutreffend. ☐ Nein
Akzeptieren Sie Kreditkartenzahlungen?	☐ Ja ☐ Nein
Falls ja: Wir (einschließlich aller unserer rechnergestützten Geräte und Computer) bearbeiten, speichern oder übermitteln im Jahr nicht mehr als 20.000 Kreditkartendaten und bestätigen hiermit, dass wir die Standards gemäß PCI DSS (Payment Card Industry Data Security Standard) einhalten.	☐ Ja, zutreffend. ☐ Nein
Wir betreiben mindestens die folgenden IT-Schutzmaßnahmen: • Durchgängiger Virenschutz mit aktuellen Virensignaturen • Firewallstrukturen an allen Netzübergängen zu externen Netzen • Abgestuftes Rechtekonzept mit administrativen Kennungen ausschließlich für IT-Verantwortliche • Regelmäßige (mindestens tägliche) Datensicherung auf separierten Systemen oder Datenträgern	☐ Ja, zutreffend. ☐ Nein
Keine Aufsichtsbehörde, staatliche Stelle oder Verwaltungsbehörde hat Klage gegen uns oder eine mitversicherte Person eingereicht, Ermittlungen eingeleitet oder Auskünfte angefordert, was den Umgang mit sensiblen Daten angeht.	☐ Ja, zutreffend. ☐ Nein
Aus den letzten 5 Jahren sind uns keine Schäden durch eine Daten- oder Cyberrechtsverletzung, Hacker-Angriff, Denial-of-Service-Angriff oder Cyber-Erpressung bekannt, es sind uns auch keine Umstände bekannt die zu einem Cyber-Versicherungsfall führen könnten.	☐ Ja, zutreffend. ☐ Nein
Haben Sie geschäftskritische IT-Prozesse in eine Cloud oder ein externes Rechenzentrum ausgelagert?	☐ Ja ☐ Nein
Falls ja: Diese externen Rechenzentrums- oder Cloud-Services werden entgeltlich genutzt und es wurde vertraglich vereinbart, dass permanent mindestens eine der folgenden Zertifizierungen vorzuhalten ist: Tier Level 3-4, TÜViT Level 3-4 oder ISO27001	☐ Ja, zutreffend. ☐ Nein
Antwort nur erforderlich, sofern Mitversicherung Baustein „Cyber-Diebstahl“ gewünscht wird: Bei unseren Telefonanlagen und Anrufbeantwortern sind Passwörter und PIN´s von der Werkseinstellung geändert?	☐ Ja, zutreffend. ☐ Nein

Datum, Unterschrift

Hinweise zu den abgefragten IT-Schutzmaßnahmen im Antragsmodell

• Durchgängiger Virenschutz mit aktuellen Virensignaturen

Das installierte Antivirenprogramm muss als Echtzeitscanner aufgesetzt sein und über eine automatische Aktualisierung (Live-Update) verfügen, über die automatisiert aktuelle Virensignaturen beim Hersteller heruntergeladen werden – so bleibt das Programm auf dem aktuellen Stand.

So ein Programm muss auf allen Clients (Desktop-Computer oder Laptop) sowie auf allen Serversystemen eingesetzt werden, auf denen potenziell mit Schadsoftware behaftete Dateien verarbeitet oder gespeichert werden. Dies umfasst insbesondere Datei-Server und E-Mail-Server.

Ein Server, oder auch Hostrechner, ist ein Computer, der Dienste für andere Computer erbringt (zB Web-Server, Applikations-Server).

Ein Client, oder auch Endgerät, ist ein Computer, der Dienste von anderen Computern in Anspruch nimmt.

Erfolgt der Betrieb der Server durch Dritte (Cloud-Computing), so kann eine entsprechende Virenschutzlösung auch vom Betreiber bereitgestellt werden.

• Firewallstrukturen an allen Netzübergängen zu externen Netzen

An der Schnittstelle zwischen internen und externen Netzen muss eine Firewallstruktur betrieben werden, die unerwünschte eingehende und ausgehende Kommunikationsverbindungen unterbindet.

Externe Netze sind alle IT-Netze, die nicht von den versicherten Unternehmen selbst betrieben werden, insbesondere das Internet, Netze der Telekommunikationsanbieter sowie Netze von Partnerunternehmen und externen Rechenzentrumsbetreibern.

Eine Firewallstruktur ist ein System aus einer oder mehreren Firewalls, die den Kommunikationsfluss kontrollieren und filtern und ggf. Netzbereiche mit unterschiedlichen Schutzanforderungen (zB für besonders sensible Daten oder kritischen Anwendungen) voneinander abtrennen.

• Abgestuftes Rechtekonzept mit administrativen Kennungen ausschließlich für IT-Verantwortliche

Ein der Größe des Unternehmens angemessenes Berechtigungskonzept, sodass jeder Mitarbeiter nur auf die Ressourcen Zugriff hat, die für das jeweilige Aufgabenspektrum benötigt werden.

Ein IT-Administrator sollte bei nicht-systemrelevanten Aktivitäten, wie zB der Recherche im Internet oder der E-Mail-Bearbeitung, nicht mit administrativen Berechtigungen ausgestattet sein.

Für einen Einzelunternehmer mit einem Computer reicht es, wenn ein separates Administrationskonto für Systemarbeiten (z. B. Softwareinstallation) angelegt wird und die normale Arbeit mit einem Benutzerkonto mit eingeschränkten Rechten erfolgt.

• Regelmäßige (mindestens tägliche) Datensicherung auf separierten Systemen oder Datenträgern

Die Datensicherung muss täglich an einem Ort gespeichert werden, auf den im Regelbetrieb und ohne administrative Rechte nicht zugegriffen werden kann.

In kleinen Unternehmen kann dies eine externe Festplatte oder ein netzgebundener Speicher (NAS) sein, der direkt an den Server angeschlossen ist und die Datensicherung durchführt, aber keine Freigaben im internen Netz bereitstellt.

Bei der Einrichtung der eigenen Datensicherung sollten Sie die 3-2-1 Backup Regel berücksichtigen:
https://www.ithelps.at/die-3-2-1-backup-regel-nie-wieder-datenverlust