Bitte per Telefax oder E-Mail an Hiscox
Fax-Nr.: 089/54 58 01-199
E-Mail: hiscox.underwriting@hiscox.de

Fragebogen CyberClear

Mit diesem Fragebogen möchten wir Sie und Ihr Unternehmen gerne kennenlernen. Aufgrund der von Ihnen gemachten Angaben besteht für keine Partei die Verpflichtung zum Abschluss eines Versicherungsvertrages.

Bitte beantworten Sie die folgenden Fragen vollständig und verwenden Sie falls notwendig ein Beiblatt.

I. GENERELLE INFORMATIONEN

Vermittlername | Vermittlernummer

1. Unternehmensangaben

Name | Homepage

Straße, Nr. | Tätigkeitsbeschreibung (Branche und Geschäftstätigkeit)

PLZ, Ort, Land

2. Unternehmenskennzahlen

Konsolidierte Kennzahlen für alle mitzuversichernden Gesellschaften aus dem letzten Geschäftsjahr

	Gesamt	davon EWR	davon USA/Kanada	davon restliche Länder
Umsatz in €				
davon Onlineumsatz in €				
Rohertrag in €				
Anzahl Mitarbeiter				
Anzahl Kunden				

Gesamtumsatz aktuelles Geschäftsjahr in € _____

3. Mitzuversichernde Gesellschaften

Tochtergesellschaften außerhalb des Europäischen Wirtschaftsraumes (EWR) und/oder mitzuversichernde Gesellschaften im In- und Ausland inkl. Tätigkeit und Umsatz (ggf. auf separatem Blatt).

Name	Anschrift	Umsatz in €	Tätigkeit (falls abweichend)

Bitte fügen Sie dem Fragebogen ggf. ein aktuelles Organigramm der Unternehmensstruktur bei.

Hinweis: Die nachfolgenden Fragen bitte für die Gesamtheit der zu versichernden Unternehmen beantworten.
Bei Abweichungen bitten wir um weitere Informationen auf einem separaten Blatt.

4. Versicherungsumfang

Versicherungs-summe	☐ € 500.000	☐ € 1.000.000	☐ € 3.000.000	☐ € 5.000.000	☐ € _____
Selbstbehalt	☐ € 5.000	☐ € 10.000	☐ € 25.000	☐ € 50.000	☐ € _____

HISCOX

Bitte per Telefax oder E-Mail an Hiscox
Fax-Nr.: 089/54 58 01-199
E-Mail: hiscox.underwriting@hiscox.de

Ist eine Absicherung von Cyber-Diebstahl und/oder Cloud-Ausfall und/oder Vertragsstrafen wegen verzögerter Leistungserbringung gewünscht? **Wenn keine Absicherung gewünscht, bitte mit 5. Zusatzfragen fortfahren.**

Diese Frage ist nur zu beantworten, wenn die Erweiterung Cyber-Diebstahl gewünscht wird.

1. Haben Sie bei Ihren Telefonanlagen und Anrufbeantwortern die Passwörter & PINs von der Werkseinstellung geändert? ☐ Ja ☐ Nein
2. Haben Sie ein verpflichtendes Vier-Augen-Prinzip ab einer Überweisungshöhe von € 25.000 implementiert? ☐ Ja ☐ Nein

Diese Fragen sind nur zu beantworten, wenn die Erweiterung Betriebsunterbrechung bei Cloud-Ausfall gewünscht wird.

1. Welche kritischen Geschäftsprozesse haben Sie in die Cloud ausgelagert? _____
2. Welche Verfügbarkeit haben Sie mit ihrem Cloud-Anbieter vereinbart? Zugesicherte Betriebszeit _____ %

☐ Tier Level 1 ☐ Tier Level 2 ☐ Tier Level 3 ☐ Tier Level 4

☐ TUViT Level 1 ☐ TUViT Level 2 ☐ TUViT Level 3 ☐ TUViT Level 4

3. Welche zusätzlichen Zertifizierungen werden von Ihrem Cloud-Anbieter vorgehalten?

☐ ISO27001 ☐ IT Grundschutz ☐ BSI C5 ☐ Andere _____

Wünschen Sie die Erweiterung um Vertragsstrafen wegen verzögerter Leistungserbringung? ☐ **Ja** ☐ **Nein**
Falls ja, fügen Sie die vertragliche Vereinbarung bitte dem Fragebogen an.

5. Zusatzfragen

Können Ihre Kunden bei Ihnen mit Kreditkarte zahlen? ☐ Ja ☐ Nein
Falls ja, dann beantworten Sie bitte die Fragen zur Kreditkartenzahlung auf Seite 1 des Zusatzfragebogens.

Generieren Sie Onlineumsätze über Ihre Website? ☐ Ja ☐ Nein
Falls ja, dann beantworten Sie bitte die Fragen zum Online Shop auf Seite 2 des Zusatzfragebogens.

Betreiben Sie Industrie-Steuerungsanlagen mithilfe automatisierter Kontrollsysteme (ICS/SCADA) z.B. Produktion oder Logistik? ☐ Ja ☐ Nein
Falls ja, dann beantworten Sie bitte die Fragen zu Industrie-Steuerungsanlagen auf Seite 3 des Zusatzfragebogens.

II. DATEN

1. Datenschutz

1. Bitte kreuzen Sie die Spanne der sensiblen personenbezogenen Datensätze an, die Ihr Unternehmen sammelt, verarbeitet und speichert: **(Zutreffendes bitte ankreuzen)**

Sensible personenbezogene Daten sind 1. Sozialversicherungs-, Führerschein- und Ausweisdaten 2. Steuer und Finanzdaten, wie Bank- oder Kreditkartenkonten 3. Informationen zu Strafverfahren und Ordnungswidrigkeiten 4. Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben.

☐ 0 – 20.000 ☐ 20.001 – 100.000 ☐ 100.001 – 250.000

☐ 250.001 – 500.000 ☐ 500.001 – 1.000.000 ☐ > 1.000.000

Bei Datenmengen größer 1.000.000 bitten wir um eine genauere Aufschlüsselung (in 1. bis 4.) und die konkrete Anzahl.

2. Führen Sie ein Verfahrensverzeichnis (BDSG) bzw. Verzeichnis von Verarbeitungstätigkeiten (EU-DSGV) bezüglich des Umgangs mit personenbezogenen Daten? ☐ Ja ☐ Nein
3. Sind jährliche Reports des Datenschutzbeauftragten vorhanden? ☐ Ja ☐ Nein
4. Gibt es in Ihrem Unternehmen eine Prüfung ob datenschutzrechtliche Vorgaben eingehalten werden?

☐ Nicht regelmäßig ☐ Nur bei kritischen Änderungen ☐ Mindestens einmal jährlich

Bitte per Telefax oder E-Mail an Hiscox
Fax-Nr.: 089/54 58 01-199
E-Mail: hiscox.underwriting@hiscox.de

2. Datenverarbeitung

1. Sind Sie im Rahmen der Auftragsdatenverarbeitung für Dritte tätig? ☐ Ja ☐ Nein

2. Nutzen Sie Dienstleister zur Auftragsdatenverarbeitung? ☐ Ja ☐ Nein

Nr.	Name des Dienstleisters	E-Mail	Hosting	Abrechnung	Sonstige	Sofern Haftungsfreistellungen vereinbart, in welcher Form?
1.		☐	☐	☐		
2.		☐	☐	☐		
3.		☐	☐	☐		

Wenn genutzt bitte in der Tabelle aufführen, wenn nicht bitte mit Teil III. fortfahren (ggf. auf separatem Blatt).

3. Halten sich Ihre Dienstleister mindestens an das Datenschutzniveau aus Ihrem Unternehmen und überprüfen Sie dies regelmäßig durch Auditierungen?

☐ Nein bzw. unbekannt ☐ Ja, wir lassen uns dies regelmäßig durch eine Selbstauskunft bestätigen ☐ Ja, wir überprüfen dies regelmäßig durch die Prüfung eines Auditors ☐ Ja, unser Dienstleister ist zertifiziert. Benennung Zertifikat: _____

4. Regeln Sie in Ihren Dienstleistungsverträgen die Verfügbarkeit, Updates und das Beheben von Sicherheitslücken? ☐ Ja ☐ Nein

III. INFORMATIONSSICHERHEITS-MANAGEMENT

1. ISMS Zertifizierung

1. Ist in Ihrem Unternehmen ein Informationssicherheits-Management-System (ISMS) etabliert? ☐ Ja ☐ Nein
Wenn ja, von wem wird das ISMS überprüft und angepasst?

☐ Eigene IT-Abteilung ☐ Interne(r) Informationssicherheitsbeauftragte(r) ☐ Interne Revision

☐ Externer Wirtschaftsprüfer ☐ Sonstige _____

2. Sind Sie nach einem der folgenden Standards oder Normen zertifiziert? ☐ Ja ☐ Nein

Wenn vorhanden, bitte angeben und mit Teil IV. fortfahren.

☐ VdS 3473 ☐ ISO27001 ☐ IT-Grundschutz ☐ Cloud C5 Anforderung Katalog - Testat nach BSI C5

Bis wann ist diese Zertifizierung gültig? _____ Ist eine Verlängerung beabsichtigt? ☐ Ja ☐ Nein

2. Technische Sicherheitsmaßnahmen

1. Verfügen alle informationsverarbeitenden Systeme über einen Virenschutz mit aktuellen Virensignaturen? ☐ Ja ☐ Nein

2. Betreiben Sie Firewallstrukturen an allen Netzübergängen zu externen Netzen? ☐ Ja ☐ Nein

3. Wer (Position) ist in Ihrem Unternehmen für die IT-Sicherheit verantwortlich?

☐ GeschäftsführerIn ☐ IT-Sicherheitsbeauftragte(r) / CISO ☐ IT-LeiterIn ☐ Sonstige _____

4. Haben Sie eine Richtlinie implementiert, die durchgehend das automatische oder zeitnahe Einspielen von Sicherheitsupdates regelt (Patch-Management-Prozess)? ☐ Ja ☐ Nein

- Sind hiervon auch Plug-Ins (Webbrowser und Frameworks) erfasst? ☐ Ja ☐ Nein

5. Sind die IT-Systeme die mit Außen kommunizieren in einem separaten Segment gebündelt? (Demilitarisierte Zone (DMZ)) ☐ Ja ☐ Nein

- Ist das interne Netz noch weiter segmentiert (Client, Server, Multifunktionsgeräte)? ☐ Ja ☐ Nein
- Erfolgt zwischen den Segmenten eine Filterung der Kommunikation? ☐ Ja ☐ Nein

HISCOX

Bitte per Telefax oder E-Mail an Hiscox
Fax-Nr.: 089/54 58 01-199
E-Mail: hiscox.underwriting@hiscox.de

6. Sie haben eine IT-Sicherheitsrichtlinie umgesetzt, in der die folgenden Elemente geregelt werden: **(Zutreffendes bitte ankreuzen)**

- ☐ Wir haben keine schriftliche IT-Sicherheitsrichtlinie
- ☐ Benutzerindividuelle Zugänge mit erzwungenen individuellen Passwörtern
- ☐ Alle Standardnutzer und Standardpasswörter werden durch starke individuelle Daten ersetzt
- ☐ Definierte Mindestanforderungen an die Passwortstärke
- ☐ Zugriffsbeschränkungen, sodass jeder Mitarbeiter nur auf die Ressourcen (Daten und Programme) Zugriff hat, die für das jeweilige Aufgabenspektrum benötigt werden
- ☐ Prozess zur regelmäßigen Überprüfung der Zugriffsrechte (z.B. bei Beförderung oder Kündigung)
- ☐ Administrative Zugänge werden ausschließlich zur Erledigung administrativer Tätigkeiten genutzt. Für die alltägliche Nutzung (insbesondere Surfen im Internet) wird ein Benutzer-Konto ohne Admin-Rechte verwendet
- ☐ Dauer der Speicherung von Protokollierungsdaten
- ☐ Authentifizierungsverfahren wie Mehr-Faktor-Authentifizierung, Zertifikate, Hard-Token, Einmalpasswörter
- ☐ Sichere Vernichtung von sensiblen Daten
- ☐ Regelung oder Verbot der privaten Nutzung der dienstlichen IT Infrastruktur
- ☐ Vorhalten eines aktuellen Netzplans (Strukturplan des IT-Systems)

7. Welche Maßnahmen haben Sie zur Erkennung von Angriffen und Sicherheitsvorfällen implementiert? **(Zutreffendes bitte ankreuzen)**

- ☐ Wir haben keine entsprechenden Maßnahmen implementiert
- ☐ Automatische Auswertung von Protokolldaten
- ☐ Angriffserkennungssystem (Intrusion-Detection und -Prevention)
- ☐ Schutzmaßnahmen gegen unerwünschten Datenabfluss (Data Loss Prevention)
- ☐ System zum Umgang mit sicherheitsrelevanten Ereignissen (Security Information und Event Management (SIEM))
- Ist sichergestellt, dass bei Feststellung unmittelbar eine Bewertung und Lösung umgesetzt wird? ☐ Ja ☐ Nein

8. Wurde in der Vergangenheit ein Penetrationstest durchgeführt? ☐ Ja ☐ Nein
Wenn ja, wann zuletzt? _____

9. Sie haben in Ihrem Unternehmen folgende Schutzmaßnahmen bei Fernwartungszugängen und Fernzugriffen umgesetzt: **(Zutreffendes bitte ankreuzen)**

- ☐ Fernwartungszugänge und Fernzugriffe sind nicht möglich
- ☐ Dokumentation der eingerichteten Fernwartungszugänge und Fernzugriffe
- ☐ Geeignete VPN-Verschlüsselung (Virtual Private Networks)
- ☐ Personenbezogene Zugänge
- ☐ Zwei-Faktor-Authentifizierung
- ☐ Protokollierung des Verbindungsaufbaus und Archivierung der Daten
- ☐ Protokollierung aller Tätigkeiten beim Zugriff durch Externe
- ☐ Beobachtung externer Wartungszugriffe durch eigene Mitarbeiter
- ☐ Interne individuelle Freischaltung nur für Dauer und Zweck der Fernwartung

10. Sie haben in Ihrem Unternehmen eine Mobilgeräteverwaltung (Mobile-Device-Management (MDM)) implementiert, das die folgenden Schutzmaßnahmen umsetzt: **(Zutreffendes bitte ankreuzen)**

- ☐ Wir haben kein MDM umgesetzt
- ☐ Fernlöschung der Geräte
- ☐ Sichere VPN Verbindung (beschränkt, protokolliert, autorisiert)
- ☐ Verschlüsselung (Full-disk-encryption)
- ☐ Abgetrennte Container für dienstliche Daten auf mobilen Geräten
- ☐ Es gibt eine Bring-Your-Own-Device-Policy (BYOD) - Regelung zur dienstlichen Nutzung privater Geräte

3. Datensicherung

1. Führen Sie mindestens täglich eine automatische Sicherung durch? ☐ Ja ☐ Nein
Wenn nein, dann _____

2. Wird die Datensicherung von der Betriebsumgebung getrennt gespeichert? ☐ Ja ☐ Nein

Bitte per Telefax oder E-Mail an Hiscox
Fax-Nr.: 089/54 58 01-199
E-Mail: hiscox.underwriting@hiscox.de

3. Ist die Datensicherung durch Verschlüsselung und beschränkte Zugriffsrechte vor Manipulation geschützt? ☐ Ja ☐ Nein

4. In welchem Turnus wird die Wiederherstellung dieser Daten getestet?

☐ Gar nicht ☐ Unregelmäßig ☐ Jährlich ☐ Quartalsweise ☐ Monatlich

IV. NOTFALLMANAGEMENT

1. Haben Sie kritische IT-Systeme und Anwendungen für Ihr Unternehmen definiert und diese redundant aufgestellt? ☐ Ja ☐ Nein

2. Haben Sie die für Ihr Unternehmen kritischen bzw. sensiblen Daten definiert? ☐ Ja ☐ Nein

3. Sie betreiben Business Continuity Management (BCM) inkl. IT-Notfallplan und Wiederanlauf-Konzept der betriebsnotwenigen Systeme in Ihrem Unternehmen und setzen dabei Folgendes um: **(Zutreffendes bitte ankreuzen)**

☐ Wir haben kein BCM umgesetzt
☐ Schriftlich fixiertes BCM
☐ Benannte verantwortliche Person(en) für BCM
☐ Regelmäßige inhaltliche Überprüfung
☐ Regelmäßige praktische Tests
☐ Ausgerichtet an einer Norm (BSI 100-4 oder ISO22301)
☐ ISO22301 zertifiziert

V. VORSCHÄDEN

1. Hat eine Aufsichtsbehörde, staatliche Stelle oder Verwaltungsbehörde Klage gegen Sie oder eine mitversicherte Person eingereicht, Ermittlungen eingeleitet oder Auskünfte angefordert, was den Umgang mit sensiblen Daten angeht? ☐ Ja ☐ Nein

2. Sind Ihnen aus den letzten 5 Jahren Netzwerksicherheitsverletzungen (wie Hacker-Angriffe, Denial-of-Service-Angriffe oder Vorfälle durch Schadprogramme), Bedienfehler, Datenrechtsverletzungen oder Cyber-Erpressungen o.ä. bekannt, die einen Schaden bei Ihnen oder einen Schadenersatzanspruch eines Dritten hervorgerufen haben oder sind Ihnen Umstände bekannt, die zu einem Cyber-Versicherungsfall führen könnte? ☐ Ja ☐ Nein

Wenn mindestens eine der beiden vorstehenden Fragen nicht mit „Nein“ beantwortet wurden, bitten wir um Details zu jedem Vorfall.

- Was ist konkret passiert (Detailbeschreibung)?
- Welche einzelnen Kosten sind Ihnen durch den Vorfall entstanden?
- Kam es zu einem Systemausfall/Betriebsausfall (vollständig oder teilweise), und wenn ja wie lange?
- Welche Maßnahmen wurden ergriffen um solche Vorfälle zukünftig möglichst zu vermeiden?

Datenschutz

Der Versicherungsnehmer willigt ein, dass der Versicherer im erforderlichen Umfang Daten, die sich aus den Antragsunterlagen oder der Vertragsdurchführung (Prämien, Versicherungsfälle, Risiko-/Vertragsänderungen) ergeben, an Rückversicherer sowie zur Beurteilung des Risikos und der Ansprüche an andere Versicherer/Gutachter/Rechtsanwälte etc. und/oder den HUK-Verband zur Weitergabe dieser Daten an andere Versicherer übermitteln darf. Diese Einwilligung gilt auch unabhängig vom Zustandekommen des Versicherungsvertrages sowie für entsprechende Prüfungen bei anderweitig beantragten Versicherungsverträgen und bei künftigen Anträgen.
Diese ausgefüllte Erklärung sowie eventuelle Anlagen werden bei Abschluss eines Versicherungsvertrages der Verletzung vorvertraglicher Anzeigepflichten verweisen wir auf die Regelung des Versicherungsvertragsgesetzes (VVG).
Mit Ihrer Unterschrift bestätigen Sie, dass vorstehende Angaben vollständig und richtig sind.

Name	Position im Unternehmen	Unterschrift Geschäftsleitung oder befugten Vertreters/Firmenstempel	Datum