HISCOX

Bitte per Telefax oder E-Mail an
ALT + PARTNER
Fax-Nr.: 03142-21240
E-Mail: office@alt-partner.at

ALT+PARTNER
VERSICHERUNGSLÖSUNGEN

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.

Nähere Erläuterungen zu cyberspezifischen Begriffen finden Sie in unserem Cyber-Glossar unter **www.hiscox.de/blog/cyber-glossar**.

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/UK	davon USA/Kanada	davon restliche Länder
Umsatz in €				
davon Onlineumsatz in €				
Rohertrag in €				
Anzahl Mitarbeiter				
Anzahl Mitarbeiter mit Zugang zu Emails				
Anzahl Kunden				

Gesamtumsatz aktuelles Geschäftsjahr in € _____

3. UNTERNEHMENSSTRUKTUR

Gibt es Tochtergesellschaften oder Niederlassungen **innerhalb** des EWRs? ☐ Nein ☐ Ja

Wenn **Ja**, nennen Sie uns bitte diese sowie die Länder, in denen sich diese befinden und die dort erwirtschafteten Umsätze.

Name/Firmierung/Anschrift	Umsatz
	€
	€
	€
	€

Bitte per Telefax oder E-Mail an
ALT + PARTNER
Fax-Nr.: 03142-21240
E-Mail: office@alt-partner.at

Gibt es Tochtergesellschaften oder Niederlassungen **außerhalb** des EWRs? ☐ Nein ☐ Ja

Wenn **Ja**, nennen Sie uns bitte diese sowie die Länder, in denen sich diese befinden und die dort erwirtschafteten Umsätze.

Name/Firmierung/Anschrift	Umsatz
	€
	€
	€
	€

Gibt es sonstige verbundene Unternehmen? ☐ Nein ☐ Ja

Wenn **Ja**, nennen Sie uns bitte diese sowie die Länder, in denen sich diese befinden sowie die dort erwirtschafteten Umsätze.

Name/Firmierung/Anschrift/Art der Verbindung	Umsatz
	€
	€
	€

4. Versicherungsumfang

Versicherungssumme	☐ € 500.000	☐ € 1.000.000	☐ € 3.000.000	☐ € 5.000.000	☐ € _____
Selbstbehalt	☐ € 5.000	☐ € 10.000	☐ € 25.000	☐ € 50.000	☐ € _____

Sie wünschen ein Angebot für die folgenden Zusatz-Bausteine:

Cyber-Betrug (Ziff. II.2.6. CyberClear 03/2019) ☐ Ja

Vertragsstrafen wegen verzögerter Leistungserbringung (Ziff. II.2.10. CyberClear 03/2019) ☐ Ja

Falls ja, fügen Sie bitte den entsprechenden Teil der vertraglichen Vereinbarung diesem Fragebogen an.

Cyber-Betriebsunterbrechung bei Cloud-Ausfall (Ziff. II.5.6. CyberClear 03/2019) ☐ Ja

Cyber-Betriebsunterbrechung bei Technischen Problemen (Ziff. II.5.7. CyberClear 03/2019) ☐ Ja

Diese Fragen sind nur zu beantworten, wenn die Erweiterung Cyber-Betrug gewünscht wird.

1. Gibt es ein verpflichtendes 4-Augenprinzip bei Überweisungen über € 10.000? ☐ Ja ☐ Nein
2. Sensibilisieren Sie alle Mitarbeiter mit Überweisungsvollmachten mindestens halbjährlich zur Erkennung und Vermeidung von Betrugsmaschen, wie CEO-Fraud und Lieferanten-Betrug. ☐ Ja ☐ Nein
3. Wie viele Mitarbeiter dürfen im Namen Ihres Unternehmens eigenständig Überweisungen tätigen / bei der Bank anweisen? _____ Mitarbeiter

HISCOX

Bitte per Telefax oder E-Mail an
ALT + PARTNER
Fax-Nr.: 03142-21240
E-Mail: office@alt-partner.at

ALT+PARTNER
VERSICHERUNGSLÖSUNGEN

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

1. Welche kritischen Geschäftsprozesse haben Sie in die Cloud / an ein externes Rechenzentrum ausgelagert? _____

2. Führen Sie ein Verzeichnis über Ihre Cloud-Anbieter und externe Rechenzentren, und wofür Sie diese in Ihrem Unternehmen nutzen? ☐ Ja ☐ Nein

3. Welche Verfügbarkeit haben Sie mit ihrem Cloud-Anbieter / externen Rechenzentrum 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

4. Welche zusätzlichen Zertifizierungen werden von Ihrem Cloud-Anbieter oder externen Rechenzentrum vorgehalten?

☐ ISO27001 ☐ IT Grundschutz ☐ BSI C5 ☐ Andere _____

Diese Frage ist nur zu beantworten, wenn die Erweiterung Betriebsunterbrechung bei Technischen Problemen gewünscht wird.

1. Werden kritische Systemänderungen wie die Installation und Veränderung von Software vor der Ausführung im Live-System erfolgreich in einer Testumgebung eingespielt? ☐ Ja ☐ Nein

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, Leitstände/Leitwarten, Gebäudeleittechnik 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 besonderen personenbezogenen **Datensätze** an, die Ihr Unternehmen sammelt, verarbeitet und speichert (ein **Datensatz** kann dabei mehrere Daten zu einer Person enthalten): **(Zutreffendes bitte ankreuzen)**

Besondere 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. Sind die besonderen personenbezogenen Daten in Ihrem Unternehmen sowohl „in transit“ (z.B. beim Versenden von Emails) als auch „at rest“ (z.B. bei der Speicherung auf einem Server) zu jederzeit verschlüsselt? ☐ Ja ☐ Nein

3. Führen Sie ein Verzeichnis von Verarbeitungstätigkeiten (gem. DSGVO) bezüglich des Umgangs mit personenbezogenen Daten? ☐ Ja ☐ Nein

4. Sind jährliche Reports des Datenschutzbeauftragten vorhanden? ☐ Ja ☐ Nein

5. Wird in Ihrem Unternehmen das Recht auf Löschung (Art.17 DSGVO – „Recht auf Vergessenwerden“) umgesetzt? ☐ Ja ☐ Nein

6. Existiert in Ihrem Unternehmen eine schriftliche Richtlinie die den Schutz und die Aufbewahrung von personenbezogenen Daten regelt? ☐ Ja ☐ Nein

Bitte per Telefax oder E-Mail an
ALT + PARTNER
Fax-Nr.: 03142-21240
E-Mail: office@alt-partner.at

7. In welchem Abstand werden Ihre Mitarbeiter in Bezug auf Datenschutz- und IT-Risiken geschult?
☐ gar nicht
☐ unregelmäßig
☐ mind. jährlich

2. Datenverarbeitung

1. Sind Sie im Rahmen der Auftragsverarbeitung von personenbezogenen Daten für Dritte tätig? ☐ Ja ☐ Nein
2. Nutzen Sie Dienstleister zur Auftragsverarbeitung von personenbezogenen Daten? ☐ 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, das Beheben von Sicherheitslücken und den Datenschutz? ☐ 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 zum Internet? ☐ Ja ☐ Nein
3. Sie haben eine Telefonanlage ohne Anrufbeantworter mit PIN-Zugang oder haben bei Ihren Telefonanlagen und Anrufbeantwortern die Passwörter & PINs von der Werkseinstellung geändert. ☐ Ja ☐ Nein

Wenn die Antragsfrage mit „Nein“ beantwortet wird, wird Ziffer II.2.5. der CyberClear Bedingungen (Cyber-Diebstahl) vom Versicherungsschutz ausgeschlossen.)

HISCOX

Bitte per Telefax oder E-Mail an
ALT + PARTNER
Fax-Nr.: 03142-21240
E-Mail: office@alt-partner.at

ALT+PARTNER
VERSICHERUNGSLÖSUNGEN

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

☐ GeschäftsführerIn ☐ IT-SicherheitsbeauftragteR / CISO ☐ IT-LeiterIn ☐ Sonstige _____

5. Spielen Sie automatisch bzw. durchgehend und zeitnah Sicherheitsupdates ein (Patch-Management-Prozess)? ☐ Ja ☐ Nein

- Sind hiervon auch Plug-Ins (Webbrowser und Frameworks) erfasst? ☐ Ja ☐ Nein
- Betreiben Sie, sofern vorhanden, nicht mehr patchbare Altsysteme ausschließlich in einer komplett isolierten Umgebung? ☐ Ja ☐ Nein
- Werden Sicherheitsupdates vor der Ausführung im Live-System erfolgreich in einer Testumgebung eingespielt? ☐ Ja ☐ Nein

6. 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
- Ist eine Netzwerksegmentierung zwischen den einzelnen Standorten umgesetzt? ☐ Ja ☐ Nein
- Hat Ihr Unternehmen den Internetzugang auf einen redundanten Zugang zentralisiert? ☐ Ja ☐ Nein

7. 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 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)

8. 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

9. Wurde in der Vergangenheit ein Penetrationstest durchgeführt? ☐ Ja ☐ Nein

Wenn ja, wann zuletzt? _____

Welche identifizierten Maßnahmen wurden danach noch nicht umgesetzt? _____

10. Sie haben 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 urch Externe
☐ Beobachtung externer Wartungszugriffe durch eigene Mitarbeiter
☐ Interne individuelle Freischaltung nur für Dauer und Zweck der Fernwartung

11. Sie haben 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
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? ☐ Ja ☐ Nein
2. Haben Sie kritische IT-Systeme und Anwendungen redundant aufgestellt? ☐ Ja ☐ Nein
3. Wie werden Ihre kritischen IT-Systeme und Anwendungen primär gehostet? ☐ intern ☐ extern ☐ gemischt
4. Haben Sie die für Ihr Unternehmen kritischen bzw. sensiblen Daten definiert? ☐ Ja ☐ Nein
5. Sie haben einen Business Continuity Plan (BCP) in Ihrem Unternehmen und setzen dabei Folgendes um **(Zutreffendes bitte ankreuzen)**

☐ Wir haben keinen BCP
☐ Schriftlich fixierter BCP
☐ Regelmäßige inhaltliche Überprüfung
☐ Regelmäßige praktische Tests

6. Sie haben ein IT-Notfall- und Wiederanlaufkonzept der betriebsnotwendigen Systeme in Ihrem Unternehmen und setzen dabei folgendes um **(Zutreffendes bitte ankreuzen)**

☐ Wir haben kein IT-Notfall- und Wiederanlaufkonzept
☐ Schriftlich fixiertes IT-Notfall- und Wiederanlaufkonzept
☐ Regelmäßige inhaltliche Überprüfung
☐ Regelmäßige praktische Tests

7. Wie schnell können Sie Ihre betriebsnotwendigen Syteme nach einem Cyber-Vorfall wieder in den (Not-) Betrieb nehmen?

☐ < 8 Stunden ☐ < 24 Stunden ☐ < 3 Tage ☐ < 1 Woche ☐ > 1 Woche

8. Welchen umsatzrelevanten Anteil Ihres Geschäftsbetriebes könnten Sie bei einem IT-Ausfall im Notbetrieb aufrechterhalten?

☐ 100% ☐ 99 - 90% ☐ 90 - 75% ☐ 75 - 50% ☐ 50 - 25 % ☐ < 25%

HISCOX

Bitte per Telefax oder E-Mail an
ALT + PARTNER
Fax-Nr.: 03142-21240
E-Mail: office@alt-partner.at

ALT+PARTNER
VERSICHERUNGSLÖSUNGEN

V. VORSCHÄDEN

1. In den letzten fünf Jahren gab es keine Netzwerksicherheitsverletzungen (wie Hacker-Angriffe, Denial-of-Service-Angriffe oder Vorfälle durch Schadprogramme), Bedienfehler, Datenrechtsverletzungen oder Cyber-Erpressungen, die insgesamt bereits zu Schäden und Kosten von über EUR 1.000 geführt haben. Darüber hinaus sind Ihnen keine Umstände bekannt, die zu einem Schaden oder Kosten führen könnten. ☐ Ja ☐ Nein

Wenn die vorstehende Frage mit „Nein“ beantwortet wurde, 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?

Mit einer Vorversichereranfrage erkläre ich mich einverstanden!

Diese ausgefüllte Erklärung sowie eventuelle Anlagen werden bei Abschluss eines Vertrages Grundlage und Bestandteil des Versicherungsvertrages. Die Risikoangaben sind vorvertragliche Anzeigen. Hinsichtlich der Folgen bei der Verletzung vorvertraglicher Anzeigep ichten 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