Antragsmodell für eine Cyber-Versicherung

für Transport-, Logistik- und Speditionsunternehmen in Österreich

Vermittlerangaben		
Vermittlernummer:		
Vermittlername:		
Allgemeine Angaben		
Versicherer:	Beazley Insurance Designated Activity Company	
Geschäftstätigkeit:	Transport-, Logistik und/oder Speditionsunternehmen Anderslautende Tätigkeiten können nicht über dieses Antragsmodell abgebildet werden und müssen individuell angefragt werden.	
Name der Versicherungsnehmerin*des Versicherungsnehmers:		
Anschrift der Versicherungsnehmerin*des Versicherungsnehmers:		
Beginn: Der Beginn darf nicht in der Vergangenheit liegen. Sofern dies gewünscht wird, erfolgt eine individuelle Prüfung. / Es handelt sich um **Jahresverträge**.		
Abweichende Hauptfälligkeit:		
Zahlweise: Es erfolgt kein Unterjährigkeitszuschlag. Halbjährlich, vierteljährlich oder monatlich ist nur mittels SEPA möglich.	☐ jährlich ☐ vierteljährlich	☐ halbjährlich ☐ monatlich
Zahlart:	☐ Überweisung	☐ Abbucher (Sepa)
E-Mailadresse für die Befüllung des Sepa-Mandates: Der entsprechende Link wird nach Abschluss des Vertrages an die angeführte E-Mailadresse übermittelt und dort sind die Daten entsprechend auszufüllen und zu übermitteln.		

Risikodaten		
Hat der Versicherungsnehmer eine Internet Domain?	☐ ja	☐ nein
Internet Domain des Versicherungsnehmers: *Hinweis: Der Check der Internet Domain muss bei Abschluss positiv sein. Diese Prüfung erfolgt durch Beazley.*		

Bitte bestätigen Sie, dass nachstehende Aussagen zutreffen (*ansonsten ist der Abschluss über dieses Antragsmodell nicht möglich – bitte fragen Sie dann individuell bei Carl Rieck Österreich unter info@carlrieck.at an):*		
Umsatz des letzten Geschäftsjahres:	EUR	
Das versicherte Unternehmen besteht seit mindestens zwei Jahren	☐ ja	☐ nein
Umsätze in USA/Kanada machen nicht mehr als 25 % des Gesamtumsatzes aus:	☐ ja	☐ nein
Keines der versicherten Unternehmen war Gegenstand von Ansprüchen oder hatte Schäden, die von dem gewählten Versicherungsschutz gedeckt wären. Den versicherten Unternehmen sind keine Sachverhalte bekannt, die zu einer Inanspruchnahme unter der beantragten Deckung führen könnten.	☐ ja	☐ nein
Sie durchlaufen eine mündliche Authentifizierung bei der Einrichtung oder Änderung von Zahlungsempfängerdaten: *„Mündliche Authentifizierung" wird definiert als „Erhalt einer mündlichen Bestätigung durch ein direktes, persönliches Gespräch mit dem Zahlungsempfänger ODER durch ein telefonisches Gespräch mit dem Zahlungsempfänger über eine Festnetznummer (ausgenommen Sprachnachrichten)".* *Überweisungen beinhalten alle manuellen Zahlungen oder alle Zahlungen, bei denen ein manueller Eingriff erforderlich ist, nicht jedoch regelmäßige automatische Zahlungen, bei denen kein manueller Eingriff erfolgt und sich keine Einzelheiten geändert haben."* *„Zahlungsempfänger" wird definiert als „jedes Konto, auf das das versicherte Unternehmen Gelder zu überweisen beabsichtigt".*	☐ ja	☐ nein

Antragsfragen von € 1 Mio. Umsatz bis zu einem Umsatz von € 4.999.999,-		
Sie verwenden Multi-Faktor-Authentifizierung (MFA) für: - den Zugang aller Benutzer zu webbasierten E-Mails - alle Benutzer, die aus der Ferne auf Ihr Netzwerk zugreifen *Hinweis: MFA nutzt eine zweite Information zur Authentifizierung des Zugangs, also mehr als nur ein Passwort. Passwörter allein bieten nicht mehr genügend Sicherheit, insbesondere für Dienste, die über das Internet zugänglich sind (z.B. Microsoft 365, Google Workspace u.s.w.).*	☐ ja	☐ nein
Sie sichern regelmäßig kritische Daten und Systeme. *Hinweise: Die Regelmäßigkeit, mit der Backups erstellt und getestet werden, hängt von der Größe des Backups und der Häufigkeit der Aktualisierungen/Änderungen der kritischen Daten ab. Wenn z. B. große Mengen kritischer Daten vorhanden sind und sich die kritischen Daten täglich ändern, sollten tägliche Backups in Betracht gezogen und die Backups mindestens jeden Monat/alle paar Monate getestet werden.*	☐ ja	☐ nein
Sie schulen regelmäßig alle Benutzer, die Zugang zum Netzwerk Ihres Unternehmens oder zu vertraulichen Informationen/ personenbezogenen Daten haben, in Sachen Cybersicherheit, einschließlich Anti-Phishing. *Hinweis: Neue Benutzer sollten mindestens innerhalb der ersten drei Monate geschult werden, idealerweise früher. Die Häufigkeit der Schulungen hängt von der Anzahl der Benutzer und der Größe des Netzwerks/der Daten ab. Bei vielen Benutzern und/oder einem großen Netzwerk sollten Schulungen z. B. mindestens zweimal pro Jahr erfolgen. Wenn es sich um ein kleines Netzwerk und einen kleinen Datensatz handelt, ist ein jährlicher Rhythmus ausreichend.*	☐ ja	☐ nein

Antragsfragen von € 5.000.000 Mio. Umsatz bis zu einem Umsatz von € 15.000.000,-		
Sie verwenden Multi-Faktor-Authentifizierung (MFA) für: - den Zugang aller Benutzer zu webbasierten E-Mails - alle Benutzer, die aus der Ferne auf Ihr Netzwerk zugreifen *Hinweis: MFA nutzt eine zweite Information zur Authentifizierung des Zugangs, also mehr als nur ein Passwort. Passwörter allein bieten nicht mehr genügend Sicherheit, insbesondere für Dienste, die über das Internet zugänglich sind (z.B. Microsoft 365, Google Workspace u.s.w.).*	☐ ja	☐ nein
Sie sichern regelmäßig kritische Daten und Systeme und bewahren die Datensicherungen an einem Offline-/sicheren Speicherort auf, der von einer Kompromittierung Ihrer Umgebung nicht betroffen wäre. Ihre Datensicherungen werden regelmäßig getestet, um sicherzustellen, dass diese wiederherstellbar sind. *Hinweis: Geeignete Lösungen umfassen beispielsweise „kalte" bzw. „Offline"-Backups oder Cloud-Backups mit separater Authentifizierung und MFA-Schutz. Lösungen, die unveränderliche Backups ermöglichen, oder Backups bei externen Cloud-Anbietern sind ebenfalls geeignet. Die Regelmäßigkeit, mit der Backups erstellt und getestet werden, hängt von der Größe des Backups und der Häufigkeit der Aktualisierungen/Änderungen der kritischen Daten ab. Wenn z. B. große Mengen kritischer Daten vorhanden sind und sich die kritischen Daten täglich ändern, sollten tägliche Backups in Betracht gezogen und die Backups mindestens jeden Monat/alle paar Monate getestet werden. Zu den kritischen Daten und Systemen gehören Geschäftsdaten und zugrundeliegende Systeme, die für Ihren täglichen Betrieb erforderlich sind oder die sensible oder große Mengen an risikoreichen Daten wie personenbezogene Daten enthalten (z. B. SharePoint, CRM, HR-Systeme, ERP).*	☐ ja	☐ nein
Sie schulen regelmäßig alle Benutzer, die Zugang zum Netzwerk Ihres Unternehmens oder zu vertraulichen Informationen/ personenbezogenen Daten haben, in Sachen Cybersicherheit, einschließlich Anti-Phishing. *Hinweis: Neue Benutzer sollten mindestens innerhalb der ersten drei Monate geschult werden, idealerweise früher. Die Häufigkeit der Schulungen hängt von der Anzahl der Benutzer und der Größe des Netzwerks/der Daten ab. Bei vielen Benutzern und/oder einem großen Netzwerk sollten Schulungen z. B. mindestens zweimal pro Jahr erfolgen. Wenn es sich um ein kleines Netzwerk und einen kleinen Datensatz handelt, ist ein jährlicher Rhythmus ausreichend.*	☐ ja	☐ nein

Prämienberechnung. Die ausgewiesenen Prämien sind inkl. 11 % Versicherungssteuer					
Umsatz-staffelung		**Versicherungssumme je Versicherungsfall und Versicherungsjahr**			
		€ 1.000.000,-		**€ 2.000.000,-**	
ab	€ 1.000.000,-	€ 650,- € 585,59 netto	☐	€ 850,- € 765,78 netto	☐
bis	€ 2.500.000,-	€ 1.000,- € 900,91 netto	☐	€ 1.350,- € 1.216,22 netto	☐
bis	€ 3.499.000,-	€ 1.400,- € 1.261,27 netto	☐	€ 1.700,- € 1.531,54 netto	☐
bis	€ 4.999.999,-	€ 1.700,- € 1.531,54 netto	☐	€ 2.100,- € 1.891,90 netto	☐
bis	€ 7.500.000,-	€ 2.450,- € 2.207,21 netto	☐	€ 3.100,- € 2.792,80 netto	☐
bis	€ 10.000.000,-	€ 2.800,- € 2.522,53 netto	☐	€ 3.500,- € 3.153,16 netto	☐
bis	€ 12.500.000,-	€ 3.100,- € 2.792,80 netto	☐	€ 4.000,- € 3.603,61 netto	☐
bis	€ 15.000.000,-	€ 3.400,- € 3.063,07 netto	☐	€ 4.500,- € 4.054,06 netto	☐
ab	€ 15.000.001,- bis € 20.000.000,- Jahresnettoumsatz grundsätzlich abschließbar aber anfragepflichtig			Bitte Ihre Anfrage an info@carlrieck.at	

Selbstbehalt: € 1.000,- fix // Der Selbstbehalt entfällt für den Baustein *Breach Response Service* gemäß der Ziffern A.1. (iv), (v), (i), (ii), (iii), (vi), (vii)

12 Stunden Wartefrist (zeitlicher Selbstbehalt). Sobald die Wartefrist abgelaufen ist, gilt die volle Deckung ab Stunde null.

☐ 10 % Nachlass bei einem Selbstbehalt von € 2.500,00

☐ 15 % Nachlass bei einem Selbstbehalt von € 5.000,00

Gesamtprämie inkl. Steuer	€
Nachlass bei Erhöhung des Selbstbehaltes	€
Gesamtprämie inkl. Steuer abzüglich Nachlass	**€**

Hinweis: Das PDF ist nicht selbstrechnend. Bitte die Prämienberechnung daher händisch bzw. im PDF-Antrag mittels Tastatur einfügen.

Deckungsbausteine und Sublimits		
Breach Response Service: Breach Response Services gemäß der Ziffern A.1. (i), (ii), (iii), (vi), (vii)	€ 500.000,00 zusätzlich zu der oben genannten Versicherungssumme	Für alle Computer-Expertendienstleistungen, juristische Dienstleistungen und Dienstleistungen für Öffentlichkeitsarbeit und Krisenmanagement insgesamt
Breach Response Services gemäß der Ziffern A.1. (iv), (v) Benachrichtigungen infolge einer Datenschutzverletzung	max. 50.000 betroffene Personen	Grenzwert betroffener Personen ab welchem die Breach Response Services greifen: 50
Ist eines oder beide der genannten Zusatzlimits erschöpft, werden die Kosten die unter dem Deckungsbaustein Ziffer A.1. Breach Response Services entstehen, auf die obige Versicherungssumme gemäß Ziffer 1 dieses Versicherungsvertrages angerechnet, soweit diese noch nicht aufgebraucht ist.		
Breach Response Services Hotline 24/7: +49 89 452 054 992; eMail: BBRdeutsche@beazley.com		

Nachstehende Sublimits: Die angegebenen Sublimits sind Teil der vorstehenden Versicherungssumme und stehen nicht zusätzlich zur Verfügung. Unterfällt eine der Schadenpositionen verschiedenen Sublimits, so findet ausschließlich das jeweils niedrigste Sublimit Anwendung		
Eigenschaden „Betrügerisches Verhalten“ (eCrime):	€ 50.000,-	Eigenschaden durch betrügerische Beauftragung
	€ 50.000,-	Eigenschaden durch Zahlungsverkehrsbetrug
	€ 50.000,-	Eigenschaden durch Telefonbetrug
Haftpflichtansprüche	Gem. gewählter Versicherungssumme	Daten-, Informationssicherheitsverletzung Verletzung der Datenschutzerklärung Medienhaftpflicht Vertretung in behördlichen Verfahren Vertretung in behördlichen Verfahren
Eigenschäden		*Betriebsunterbrechungsschaden*
	Gem. gewählter Versicherungssumme	Als unmittelbare Folge einer Informationssicherheitsverletzung
	€ 250.000,-	Als unmittelbare Folge eines Ausfalls des Computersystems
		Abhängiger Betriebsunterbrechungs-schaden
	€ 1.000.000	Als unmittelbare Folge einer abhängigen Informationssicherheitsverletzung
	€ 100.000	Als unmittelbare Folge eines abhängigen Ausfalls des Computersystems
	Gem. gewählter Versicherungssumme	Cyber-Erpressung
	Gem. gewählter Versicherungssumme	Datenwiederherstellungskosten
	€ 250.000,-	PCI-Vertragsstrafen
	€ 150.000,-	Reputationsfolgeschaden
	€ 150.000,-	Computeraustauschkosten
	€ 300.000,-	Freiwillige Selbstabschaltung
	€ 10.000,-	Kosten Schadenaufstellung gemäß Ziffer G.3.1.(iii)
Informationen über Straftaten	€ 50.000,-	Aufwendungen für Informationen über Straftaten

Versicherungsbedingungen: Es gilt die Exklusivvereinbarung zwischen Beazley und Carl Rieck / +Simple Österreich als vereinbart.	Cyber-Versicherung Beazley Breach Response: BBR2.0 MBDE BIdac v2.2 Allgemeine Regelungen für Österreich Sideletter für + Simple Österreich

Hinweis zu den Versicherungsbedingungen:

Abweichende Vereinbarungen zum Versicherungsvertrag: Allgemeine Regelungen für Österreich
Anzuwendendes Recht und Gerichtsstand
Abweichend von den Bedingungen gilt für Streitigkeiten aus diesem Vertrag ausschließlich österreichisches Recht. Sofern die zugrundeliegenden Bedingungen Bezug nehmen auf BGB und VVG wird hiermit klargestellt, dass ABGB und VersVG gemeint sind.
Zuständig für alle Streitigkeiten aus und im Zusammenhang mit diesem Versicherungsvertag sind ausschließlich österreichische Gerichte. Sachliche und örtliche Zuständigkeit richten sich nach den gesetzlichen Vorgaben.

Erklärung	
Der Unterzeichner 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. Diese ausgefüllte Erklärung sowie die beigefügten Anlagen werden bei Abschluss eines Versicherungsvertrages dessen Grundlage und Bestandteil. Die Risikoangaben sind vorvertragliche Anzeigen.	☐ ja

Ort, Datum

Unterschrift der Versicherungsnehmerin*des Versicherungsnehmers