Assekuranzmakler
LAHRES

Fragebogen zur Risikoerfassung ByteProtect

A Allgemeine Angaben zum Unternehmen (Versicherungsnehmerin)

Name und Rechtsform: _____

Internetadresse: www._____ Kontaktperson: _____ Telefon _____

Anschrift: _____

Sind Sie bereits Kunde der Assekuranzmakler LAHRES? ( ) nein ( ) ja, Art der Versicherung: _____

Versicherungsschein-Nr.: _____ Jahr der Unternehmensgründung: _____

Zu welcher Branche ist Ihr Unternehmen zu rechnen (z. B. nach NACE)? _____

Betriebsbeschreibung

Mitzuversichernde **Tochterunternehmen** und **Betriebsstätten** (ggf. auf separatem Blatt auflisten):

Firma/ Ort/ Land	Umsatz	Tätigkeiten

Bitte machen Sie Angaben zu Ihrem konsolidierten **Gesamtumsatz** und Ihrer Umsatzentwicklung:

Jahr	Gesamtumsatz	Davon in den USA	Jahresüberschuss / Jahresfehlbetrag
Letztes Geschäftsjahr			
Aktuelles Geschäftsjahr (Erwartungswert)			
Geplanter Umsatz nächstes Geschäftsjahr			

Anteil des Umsatzes, der online (z. B. über Web-Shops) erzielt wird: _____ %

Unterliegt der Umsatz saisonalen Schwankungen? ( ) Nein

( ) Ja, Begründung: _____

Umsatz in dem Monat mit höchstem Umsatz: _____

Wie viele **Mitarbeiter** arbeiten in Ihrem Unternehmen im Jahresdurchschnitt?

Gesamt _____, freie Mitarbeiter _____, Studenten _____

Kundenstruktur: Wer sind Ihre 3 **Hauptkunden**? _____

Haben Sie mit einem von diesen einen Umsatzanteil von mehr als 50 %?
( ) nein ( ) ja, _____ % mit _____

Sind Sie **mit Ihren Auftraggebern/ Abnehmern** durch Personalunion, Gesellschaftsverhältnisse oder Beteiligungen **verbunden**? ( ) nein ( ) ja, mit _____

Anteil privater Kunden _____ %; Anteil Körperschaften des öffentlichen Rechts____ %

Werden von Ihnen **personenbezogene Daten** gespeichert?

( ) Nein ( ) ja, und zwar folgende _____

Anzahl aktuell gespeicherter Datensätze: _____

B Bestehender/ gewünschter Versicherungsschutz und Schadenverlauf

Gewünschte Deckungsbausteine

Bausteine	Versicherungs-summe	Versicherungswunsch	
		Ja	Nein
A Ertragsausfall (nur in Verbindung mit Vereinbarung von Baustein D!) aufgrund folgender Ereignisse:	(max. 5 Mio. €)		
Ausfall des Internetzugangs des Versicherungsnehmers durch ein Ereignis außerhalb der Einflusssphäre des Versicherungsnehmers. Nicht versichert ist, wenn die Ursache in einer zu geringen Bandbreite der Datenleitung begründet ist.			
Ausfall des internen Netzwerkes durch eine Fehlbedienung eines Mitarbeiters (Human Error)			
DoS-Attacke			
Zielgerichtete Hacker-Angriffe (auch bei Erpressung) auf die Webseite, EDV-Systeme, Netzwerk bzw. gespeicherte Daten und Programme von außen			
Manipulation von Daten und Programmen durch interne Mitarbeiter			
Ausfall einer ausgelagerten IT-Dienstleistung (z. B. Cloud Computing) Die IT-Dienstleister sind namentlich zu benennen. Die Deckung ist auf diese beschränkt.			
B Sachverständigenkosten aufgrund folgender Ereignisse:	(max. 100 T€)		
Betriebsunterbrechung nach Baustein A			
DoS-Attacke, auch ohne dass es zur Betriebsunterbrechung nach Baustein A gekommen ist			
Entdeckung von Wirtschaftsspionage			
Befall der EDV mit Schadprogrammen			
Entdeckung der Manipulation von Daten, Webseiten und Programmen durch eigene Mitarbeiter			
Verletzung von Datenschutzgesetzen (vorsätzlich oder grob fahrlässig)			
Entdeckung der Manipulation von Daten, Webseiten und Programmen durch Dritte			
C Datenwiederherstellung aufgrund folgender Ereignisse:	(max. 2 Mio. €)		
Unmittelbare Manipulation/ Löschung durch Dritte (Hacker-Angriff)			
Befall von Schadprogrammen (Malware)			

Bausteine	Versicherungs-summe	Versicherungswunsch	
		Ja	Nein
D Rufschädigung / Krisenmanagement aufgrund folgender Ereignisse:			
Eine Betriebsunterbrechung nach Baustein A			
Hacker- und DoS-Attacken, ohne dass es zur Betriebsunterbrechung nach Baustein A gekommen ist			
Verletzung von Datenschutzgesetzen (nur in Verbindung mit Vereinbarung von Baustein E!)			
Entdeckung von Wirtschaftsspionage über das Internet			
Erpressung nach Baustein G			
Identitätsdiebstahl			
E Datenschutzverletzung aufgrund folgender Ereignisse:			
Unberechtigter Zugriff durch Dritte auf die EDV des Versicherungsnehmers bzw. auf dessen Daten, auch wenn diese bei einem Dienstleister gespeichert sind			
Verlust von Datenträgern durch Einbruch bzw. Diebstahl			
Verlust von Datenträgern aus anderen Gründen (z. B. verlorener Laptop)			
F Internet-Betrug aufgrund folgender Ereignisse:			
Manipulation der Web-Seite der VN (z. B. Angebotstools, Web-Shops)			
Manipulation des Online-Bankings bzw. von Online-Zahlungssystemen/ Anwendungsprogrammen bei der VN			
Betrug mit Hilfe von Phishing, Pharming oder Identitätsdiebstahl			
G Erpressung/Lösegeld (nur in Verbindung mit Vereinbarung von Baustein D!) aufgrund folgender Ereignisse:			
Erpressung bei Zugangssperrung zu Daten und Programmen oder Störung von EDV- oder internetbasierten Leistungen oder der Webseite der VN			
Erpressung bei unberechtigtem Zugriff auf geschützte Daten (personenbezogene Daten, Betriebsgeheimnisse)			
H Cyber Liability Haftpflichtansprüche in Folge eines Datenverlustes, einer Cyber-Attacke oder einer Datenschutzverletzung			
Jahreshöchstentschädigung			

Sollen **SCADA-Systeme** in den Versicherungsschutz einbezogen werden? ( ) nein ( ) ja

Aktuell bestehende Versicherungen

Bezeichnung	Anbieter	Deckungs-summe	Relevante Deckungsbausteine
Haftpflicht			
Vertrauensschaden			
Elektronik			

Zum Schadenverlauf

Beschreibung der einzelnen Schäden/ Vorfälle, sofern diese einen Zusammenhang mit der EDV, dem Internet bzw. schutzbedürftigen Daten zu tun haben.

Beschreibung des Schadens (Ursache, Ablauf etc.)	Eintritts-jahr	Aufwand
Haftpflichtschäden		
Eigenschäden		

Welche IT-relevanten Sicherheitsvorfälle haben sich in Ihrem eigenen Unternehmen in den letzten drei Jahren ereignet, auch wenn diese zu keinem versicherten Schaden geführt haben (z. B. IT-Ausfälle, Schadsoftware-Befall, DoS-Attacke, Hacking der Webseite, Verlust von sensiblen Daten, Beanstandungen von Datenschutzbehörden)?

Beschreibung des Vorfalls (Ursache, Ablauf etc.)	Jahr	Aufwand

Sind Ihnen Umstände bekannt, die zu einem Schadenersatz gegen Sie oder zu einem Schaden führen könnten?

( ) Nein; ( ) Ja und zwar folgende:

Wo sehen Sie selber Ihr höchstes Risiko? Bitte erläutern: _____

C Eigene IT-Infrastruktur

Ihr Unternehmen verfügt über:

( ) eigene IT-Abteilung mit _____ Mitarbeiter

( ) externe IT-Dienstleister für folgende Leistungen:

( ) Datenspeicherung und –sicherung

( ) Web-Hosting

( ) Cloud Computing (für folgende Dienste: _____ - Umsatz _____ €)

( ) Administration, technischen Support, Hotline

( ) _____

( ) Mit diesen wurden schriftliche Dienstleistungsverträge abgeschlossen.
Bitte legen Sie Auszüge zu haftungsrechtlichen Regelungen bei.

( ) Es wurden keine Regressverzichtserklärungen bzw. Freistellungen ausgesprochen
(wenn doch, bitte Dokumente vorlegen)

( ) Von den beauftragten IT-Dienstleistern wurden Bestätigungen über vorhandene
IT-Haftpflichtversicherung eingeholt

Folgende Ausnahmen: _____

( ) eigenes Rechenzentrum (Ort: _____)

( ) eigene oder gemietete Server, Anzahl: _____,
für folgende Dienste: _____

Server-Betriebssysteme: _____

( ) PC-Arbeitsplätze, Anzahl: _____

( ) Notstromversorgung, sichergestellt durch: _____ -

Sicherstellung des Strombedarfs in Vollast über einen Zeitraum von _____ h

( ) eine unterbrechungsfreie Stromversorgung (USV-Anlage)

( ) internes Firmennetzwerk, das alle Standorte und Mitarbeiter zentral versorgt

( ) Einwahlmöglichkeit für Mitarbeiter in das interne Netzwerk über VPN
(Anzahl der Mitarbeiter mit einer derartigen Berechtigung: _____)

( ) eigene Webseite, die

( ) vom eigenen Server gehostet wird

( ) von _____ gehostet wird

( ) für das Web-Design und Aktualisierungen ist verantwortlich: _____

( ) Voice Over IP (VoIP)

( ) Ausstattung der Mitarbeiter mit folgender Hardware ausgestattet: _____

( ) Erlaubnis der Mitarbeiter, dass eigene Geräte eingebunden werden können (BYOD)

( ) die Möglichkeit, dass Kunden über das Internet bei Ihnen Käufe tätigen können

( ) Hierbei werden Kreditkartenzahlungen zugelassen

Wenn ja, welcher Sicherheitsstandard ist hierbei gewährleistet? _____
( ) dieser Standard ist zertifiziert seit _____

Werden Kreditkartendaten auf Ihren IT-Systemen gespeichert? ( ) Ja; ( ) Nein

D Schutzmaßnahmen zur IT- bzw. Informationssicherheit

Sie haben in Ihrem Unternehmen folgende Maßnahmen zum Schutz Ihrer Daten und IT-Systeme ergriffen:

( ) Informationssicherheits-Managementsystem (ISMS) ist seit _____ im Unternehmen eingeführt
( ) Zertifizierung nach ISO/IEC 27001, IT-Grundschutz oder vergleichbaren IT-Standards

( ) COBIT ( ) ITIL ( ) _____

( ) Zertifiziertes Qualitätsmanagementsystem (QMS) nach ISO 9001

Bitte weisen Sie Zertifizierungen durch entsprechende Kopien nach.

( ) Schriftliche Security Policy (Festlegung von Sicherheitszielen und einer Sicherheitspolitik)

( ) Bestellung eines Sicherheitsbeauftragten für IT-/Informationssicherheit

( ) Bestellung eines Datenschutzbeauftragten : ( ) intern ( ) extern

( ) Einrichtung eines Patch-Managements

( ) Sensible Daten werden vor unberechtigtem Zugriff durch Verschlüsselung geschützt (Speicherung, Emails etc.)

( ) Mobile IT-Geräte wie Notebooks, USB-Sticks etc. werden standardmäßig verschlüsselt (zumindest sensible Daten)

( ) Zugriff auf Daten erfolgt über dokumentierte und abgestufte Berechtigungen

( ) Regelmäßige Datensicherung

( ) Es erfolgen mindestens täglich Datensicherungen

( ) Die Datensicherungen werden getrennt und geschützt z. B. vor Brand gelagert

( ) Es werden regelmäßig Restore-Tests der Datenbestände durchgeführt

( ) Etablierung eines Informationssicherheitsprozesses (ISP)

( ) Schutzbedarfsanalyse ist erfolgt (zuletzt: _____)

( ) Schulungsplan zur Sicherstellung eines ausreichenden Bewusstseins der Mitarbeiter für das Thema Informationssicherheit (Awareness-Schulungen)

( ) Installation eines Intrusion Prevention-Systems – Beschreibung: _____

( ) Schutz vor Einbruch/Diebstahl durch folgende Maßnahmen: _____

( ) Zugangssicherung zu Rechenzentren und Serverräumen durch _____

( ) Es werden Log-Files erstellt, über die ein Zugriff auf Daten nachvollzogen werden kann. Aufbewahrungszeit der Log-Files: ____ Tage

( ) Durchführung von IT-Sicherheitsaudits durch _____, zuletzt am _____

( ) Personenbezogene Daten, die an Subunternehmer weitergegeben werden, sind zu jeder Zeit verschlüsselt

( ) Penetrationstest durch einen externen Sachverständigen, zuletzt am _____

( ) Sie verfügen über einen aktuellen Notfallplan, der Maßnahmen beschreibt um Krisensituation bzw. Sicherheitsvorfälle aus der IT zu bewältigen (z. B. Cyber-Angriff, Ausfall des Internets etc.)

Der Notfallplan wurde eingeführt am: _____

Der Notfall wurde zuletzt geprobt am: _____

Bitte Kopie des Notfallplanes vorlegen.

Der Versicherer behält sich eine zusätzliche Risikoaufnahme vor Ort durch einen technischen Sachverständigen ausdrücklich vor.

E Bausteinspezifische Fragen

Eine Beantwortung der Fragen ist nur erforderlich, falls der jeweilige Baustein mit versichert werden soll.

Baustein A – Ertragsausfall

( ) Business Impact Analyse (BIA), zuletzt durchgeführt am _____

Maximal tolerierbare Ausfallzeit: _____

Prozess mit der geringsten tolerierbaren Ausfallzeit: _____

( ) Business Continuity Management (BCM) wurde eingeführt am _____

( ) nach ISO 22301

( ) nach folgendem Standard: _____

Nach Ihrer Einschätzung dauert der Wiederanlauf aller Geschäftsprozesse nach einem vollständigen Netz- bzw. Serverausfall maximal _____ Stunden

Ist ein „Notbetrieb“ vorgesehen bzw. möglich? ( ) Nein ( ) Ja, in folgendem Umfang: _____

Die letzte Notfallübung mit Simulation eines Ausfalls des internen bzw. externen Netzes bzw. eines vollständigen Datenverlustes erfolgte zuletzt _____

Bei folgenden externen IT-Dienstleistern werden Daten bzw. Programme gespeichert und sollen in die Deckung aufgenommen werden:

_____

Anmerkung: Voraussetzung für die Deckung ist u. a. der Nachweis einer Haftpflichtversicherung entsprechend den Versicherungsbedingungen ByteProtect.

Baustein D – Krisenmanagement

Bitte benennen Sie einen **externen Berater**, der Ihnen in Krisenfällen kurzfristig zur Verfügung steht:

Name: _____ Ansprechpartner: _____

Adresse: _____

Kontaktdaten: _____

Wer berät Sie bezüglich **rechtlicher Fragen** im Krisenfall?

Name: _____ Ansprechpartner: _____

Adresse: _____

Kontaktdaten: _____

Wer berät Sie bezüglich **Fragen** der externen Kommunikation im Krisenfall?

Name: _____ Ansprechpartner: _____

Adresse: _____

Kontaktdaten: _____

Baustein E - Datenschutzverletzung

Sie verfügen über

( ) eine schriftliche Datenschutzrichtlinie

( ) die von einem Rechtsanwalt geprüft wurde

( ) die Auskunft darüber gibt, an wen Daten ggf. weitergegeben werden

( ) eine Datensicherheitsrichtlinie

( ) eine Prozessanweisung wie im Falle eines Datenschutzverstoßes Informationen erfolgen sollen

Das letzte externe Datenschutzaudit ist erfolgt am _____ durch _____

Baustein F – Internet-Betrug

Ist bei Ihnen sichergestellt, dass der Online-Banking-Standard HBCI mit elektronischer Signatur eingehalten wird?

( ) Ja ( ) Nein, Erläuterung: _____

Wichtig für den Antragsteller:

Bitte beantworten Sie die Fragen vollständig und richtig. Sonst ist der Versicherungsschutz gefährdet.

Mit der nachfolgend abgedruckten datenschutzrechtlichen Einwilligungserklärung bin ich einverstanden.

Außerdem erklären Sie hiermit, dass Sie einen Datenschutzbeauftragten entsprechend der gesetzlichen Vorschriften bestellt haben, mindestens täglich Ihre Daten sichern und professionelle Antivirensoftware und Firewalls einsetzen.

_____ _____

Ort, Datum Firma, Name, Unterschrift(en)

Funktion im Unternehmen: _____

Sofern vorhanden, möchten wir Sie bitten, folgende Unterlagen dem ausgefüllten Fragebogen in Kopie beizufügen.

Unterlage	Liegt bei	Entfällt
Organigramm / Organisationsdarstellung		
Firmen- und Produktbroschüren, ggf. Kataloge		
Aktueller Geschäftsbericht		
Haftungsrechtlich relevante Regelungen mit IT-Dienstleistern		
Zertifikate von Dritten		
Security Policy		
Notfallplan		

Einwilligungserklärung zur Datenverwaltung nach dem Bundesdatenschutzgesetz

I. Bedeutung dieser Erklärung und Widerrufsmöglichkeit

Ihre personenbezogenen Daten benötigen wir insbesondere zur Einschätzung des zu versichernden Risikos (Risikobeurteilung), zur Verhinderung von Versicherungsmissbrauch, zur Überprüfung unserer Leistungspflicht, zu Ihrer Beratung und Information sowie allgemein zur Antrags-, Vertrags- und Leistungsabwicklung.
Personenbezogene Daten dürfen nach geltendem Datenschutzrecht nur erhoben, verarbeitet oder genutzt werden (Datenverwendung), wenn dies ein Gesetz ausdrücklich erlaubt oder anordnet oder wenn eine wirksame Einwilligung des Betroffenen vorliegt.
Nach dem Bundesdatenschutzgesetz (BDSG) ist die Verwendung Ihrer allgemeinen personenbezogenen Daten (z.B. Alter oder Adresse) erlaubt, wenn es der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses dient (§ 28 Abs. 1 Nr. 1 BDSG). Das gleiche gilt, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt (§ 28 Abs. 1 Nr. 2 BDSG). Die Anwendung dieser Vorschriften erfordert in der Praxis oft eine umfangreiche und zeitintensive Einzelfallprüfung. Auf diese kann bei Vorliegen dieser Einwilligungserklärung verzichtet werden. Zudem ermöglicht diese Einwilligungserklärung eine Datenverwendung auch in den Fällen, die nicht von den Vorschriften des Bundesdatenschutzgesetzes erfasst werden.
Die Einwilligung ist ab dem Zeitpunkt der Antragstellung wirksam. Sie wirkt unabhängig davon, ob später der Versicherungsvertrag zustande kommt. Es steht Ihnen frei, diese Einwilligung mit Wirkung für die Zukunft jederzeit ganz oder teilweise zu widerrufen. Dies lässt aber die gesetzlichen Datenverarbeitungsbefugnisse unberührt. Sollte die Einwilligung ganz oder teilweise verweigert werden, kann das dazu führen, dass ein Versicherungsvertrag nicht zustande kommt.

II. Erklärung zur Verwendung Ihrer allgemeinen personenbezogenen Daten

Hiermit willige ich ein, dass meine personenbezogenen Daten unter Beachtung der Grundsätze der Datensparsamkeit und der Datenvermeidung verwendet werden

1. a) zur Risikobeurteilung, zur Vertragsabwicklung und zur Prüfung der Leistungspflicht;

   b) zur Weitergabe an den/die für mich zuständigen Vermittler, soweit dies der ordnungsgemäßen Durchführung meiner Versicherungsangelegenheiten dient;

2. zur Risikobeurteilung durch Datenaustausch mit dem Vorversicherer, den ich bei Antragstellung genannt habe;

3. zur gemeinschaftlichen Führung von Datensammlungen, um die Anliegen im Rahmen der Antrags-, Vertrags- und Leistungsabwicklung schnell, effektiv und kostengünstig bearbeiten zu können (z.B. richtige Zuordnung Ihrer Post oder Beitragszahlungen). Diese Datensammlungen enthalten Daten wie Name, Adresse, Geburtsdatum, Kundennummer, Versicherungsnummer, IBAN, BIC, Art der bestehenden Verträge, sonstige Kontaktdaten;

4. zur Risikobeurteilung und Abwicklung der Rückversicherung. Dies erfolgt durch Übermittlung an und zur Verwendung durch die Rückversicherer, bei denen mein zu versicherndes Risiko geprüft oder abgesichert werden soll. Eine Absicherung bei Rückversicherern im In- und Ausland dient dem Ausgleich der vom Versicherer übernommenen Risiken und liegt damit auch im Interesse der Versicherungsnehmer. In einigen Fällen bedienen sich Rückversicherer weiterer Rückversicherer, denen sie - sofern erforderlich - ebenfalls entsprechende Daten übermitteln;

5. durch andere Unternehmen / Personen (Dienstleister), denen der Versicherer oder ein Rückversicherer Aufgaben ganz oder teilweise zur Erledigung überträgt und die im Internet einsehbar sind oder mir auf Wunsch mitgeteilt werden. Diese Dienstleister werden eingeschaltet, um die Antrags-, Vertrags- und Leistungsabwicklung möglichst schnell, effektiv und kostengünstig zu gestalten. Eine Erweiterung der Zweckbestimmung der Datenverwendung ist damit nicht verbunden. Die Dienstleister sind im Rahmen ihrer Aufgabenerfüllung verpflichtet, ein angemessenes Datenschutzniveau sicher zu stellen, einen zweckgebundenen und rechtlich zulässigen Umgang mit den Daten zu gewährleisten sowie den Grundsatz der Verschwiegenheit zu beachten;

6. zum Betrieb des Hinweis- und Informationssystems für die Versicherungswirtschaft (HIS) der informa IRFP GmbH, das eine genauere Risiko- und Leistungsfalleinschätzung bezweckt. Die Sachversicherer melden erhöhte Risiken und Auffälligkeiten, die auf Versicherungsbetrug hindeuten könnten, in das HIS ein oder fragen Daten aus dem HIS ab. Dies gilt unabhängig davon, ob der Vertrag zustande gekommen ist oder nicht. Die Kontaktdaten von informa IRFP GmbH sind:

   informa Insurance Risk and Fraud Prevention GmbH
   Rheinstraße 99 / 76532 Baden-Baden

   Eine Beschreibung des HIS finden Sie im Internet unter www.informa-irfp.de

7. zur Beratung und Information über Versicherungs- und sonstige Finanzdienstleistungen durch

   a) den Versicherer und den für mich zuständigen Vermittler sowie zur Datenverarbeitung durch den von diesem Vermittler zur ordnungsgemäßen Durchführung meiner Versicherungs- und Finanzangelegenheiten ggf. eingeschalteten Maklerpool bzw. technischen Dienstleister (Betreiber von Vergleichssoftware, Maklerverwaltungsprogrammen) oder sonstigen Dienstleister, den ich bei meinem Vermittler erfragen kann;

   b) Kooperationspartner des Versicherers (die im Internet einsehbar sind oder mir auf Wunsch mitgeteilt werden); soweit aufgrund von Kooperationen mit Gewerkschaften/Vereinen Vorteilskonditionen gewährt werden, bin ich damit einverstanden, dass der Versicherer zwecks Prüfung, ob eine entsprechende Mitgliedschaft besteht, mit den Gewerkschaften/Vereinen einen Datenabgleich vornimmt;

8. zur Antrags-, Vertrags- und Leistungsabwicklung, indem der Versicherer Informationen über mein allgemeines Zahlungsverhalten einholt. Dies kann auch erfolgen durch eine Auskunftei (z.B. Bürgel, Infoscore, Creditreform, SCHUFA);

9. zur Antrags-, Vertrags- und Leistungsabwicklung, indem der Versicherer oder eine Auskunftei eine auf der Grundlage mathematisch-statistischer Verfahren erzeugte Einschätzung meiner Zahlungsfähigkeit bzw. der Kundenbeziehung (Scoring) einholt.