Allianz Versicherungs-AG

Vermittlernummer / /

B-Nr. b

Versicherungsscheinnummer (Beispiel: AS-1234567890)

—

Allianz CyberSchutz – Kurzfragebogen für Unternehmen mit Umsatz bis einschließlich 5.000.000 EUR

Dieser Fragebogen dient der Ermittlung betriebsbezogener Daten zur Erstellung eines Angebotes.
Die Vorschriften des Bundesdatenschutzgesetzes werden beachtet. Fettgedruckte Begriffe werden im Glossar beschrieben.

Antragsteller ☐ Herr ☐ Frau ☐ Firma Anredezusätze _____

Zuname, Vorname _____

bzw. Firmierung _____

Straße, Haus-Nr. _____

Postleitzahl, Ort _____ | — | _____

Straßen-, Ortszusatz _____

Risikoanschrift: Str., Haus-Nr. _____

Postleitzahl, Ort _____ | — | _____

Telefon * _____ Fax * _____ E-Mail * _____

www. * _____

Gesprächspartner * _____

Telefon, Fax, E-Mail des Vermittlers (soweit vorhanden)

_____

* freiwillige Angaben

Geschäftstätigkeit

Tätigkeitsbereich _____

Jahresumsatz/Haushaltssumme _____

Anzahl der Mitarbeiter (Angestellte Mitarbeiter, Mitarbeiter von Zeitarbeitsfirmen und freie Mitarbeiter, sofern sie in den Betrieb eingegliedert sind)

_____

Davon als IT-Administratoren beschäftigt

_____

Mitzuversichernde Tochtergesellschaften (bitte eigenen Fragebogen einreichen, wenn diese abweichende IT-Sicherheitsstrukturen aufweisen)

_____

Anzahl der gespeicherten Datensätze (siehe Glossar)

_____

Anzahl gespeicherter, bearbeiteter oder übermittelter Kreditkartendaten

_____

Sofern Kreditkartendaten vorhanden sind: Einhaltung der **PCI DSS** Standards? ☐ ja ☐ nein

Können Sie einen Betriebsunterbrechungsschaden durch den Ausfall einer Ihrer IT-Dienstleister erleiden? ☐ ja ☐ nein

Sofern der Ausfall einer Ihrer IT-Dienstleister mitversichert werden soll, bitte namentliche Nennung der/s IT-Dienstleister/s und Beschreibung der Dienstleistung/en.

_____

_____

PESVA03035

FH---0003Z0 (02) PDF.2.18

Vorschäden/Vorversicherung

Wurden gegen Sie oder mitversicherte Personen im Zusammenhang mit Ihrer oben beschriebenen Tätigkeit Ansprüche geltend gemacht, oder sind Ihnen Umstände bekannt, welche zu Ansprüchen führen könnten? ☐ ja ☐ nein

Wenn ja, welche: _____

Wurden gegen Sie oder mitversicherte Personen durch eine Behörde Klage erhoben, Ermittlungen eingeleitet oder Auskünfte angefordert bezüglich des Umgangs mit sensiblen Daten? ☐ ja ☐ nein

Wenn ja, welche: _____

Gab es schon Betriebsunterbrechungen wegen erfolgreicher Cyber Angriffe? ☐ ja ☐ nein

Wenn ja, wie lange hat die Betriebsunterbrechung gedauert? _____

Besteht bereits eine eigenständige Versicherung von Cyber Risiken? ☐ ja ☐ nein

Wenn ja:
Versicherungsgesellschaft _____ Versicherungsnummer _____

Gekündigt? ☐ nein ☐ ja, zum _____ durch ☐ Versicherungsnehmer ☐ Versicherer

Allianz

Individuelle Risikobeurteilung

Sicherheit und Verantwortung durch Mitarbeiter

1. Ist ein (auch externer) Datenschutzbeauftragter bestellt?
   ☐ ja, intern ☐ ja, extern
   ☐ nein, da rechtlich nicht erforderlich
   ☐ nein, wird nachgeholt

2. Werden Mitarbeiter regelmäßig (mindestens 1x jährlich) zur Informationssicherheit und Cyber-Sicherheit sensibilisiert/geschult? ☐ ja ☐ nein
   (Sensibilisierungsmaßnahmen können persönlich, per Mail bzw. Newsletter oder per web-based-training erfolgen.)

3. Sind Verantwortlichkeiten und Stellvertretungen im Bereich der IT-Sicherheit fest zugewiesen? ☐ ja ☐ nein
   (Ob diese Stelle von einer einzelnen Person, einer Personengruppe oder in Teilzeit wahrgenommen wird, hängt von der Größe des Unternehmens, der vorhandenen Ressourcen und dem angestrebten Sicherheitsniveau ab. Die Hauptaufgabe des IT-Sicherheitsbeauftragten besteht darin die Unternehmensleitung bei der Wahrnehmung deren Aufgaben bezüglich der IT-Sicherheit zu beraten und bei deren Umsetzung zu unterstützen. I.d.R. ist die Funktion direkt der Unternehmensleitung unterstellt.)

4. Existieren Richtlinien oder Vorgaben zum Umgang mit Passwörtern? ☐ ja ☐ nein

Netzwerksicherheit

5. Wird eine Firewall verwendet und deren Einstellungen bei Bedarf überprüft und aktualisiert? ☐ ja ☐ nein

6. Wird eine Anti-Schadcode-Software verwendet, die durch anbieterseitige Updates aktualisiert wird? ☐ ja ☐ nein

7. Werden externe Zugriffe zum Netzwerk (z.B. für Fernwartungen, IT-Support/Helpdesk , Go to meeting) erst auf Anforderung vergeben und nach Gebrauch wieder entfernt bzw. deaktiviert? ☐ ja ☐ nein

8. Existiert ein geregelter und/oder automatisierter Prozess zum Aufspielen von Updates, Patches und Servicepacks zur Schließung von Sicherheitslücken (**Patch-Management**)? ☐ ja ☐ nein
   (Im Bereich der Standardsoftware wie Mac OS X und Windows gibt es hierfür automatisierte Verfahren, bei Individualsoftware kann auch ein proaktives Handeln notwendig sein, um an Patches zu gelangen.)

Backups

9. Existieren Prozesse, wie Backups zu erstellen und aufzubewahren sind? ☐ ja ☐ nein

10. Werden sporadisch (mindestens 1x p.a.) Wiederherstellungstests von Backups durchgeführt? ☐ ja ☐ nein

Versicherungsumfang

Gewünschte Versicherungssumme:

- ☐ 250.000 EUR
- ☐ 500.000 EUR
- ☐ 1.000.000 EUR
- ☐ _____

Gewünschter Selbstbehalt:

(Standard)
- ☐ 2.500 EUR
- ☐ 5.000 EUR
- ☐ 10.000 EUR
- ☐ _____

Deckungserweiterungen:

Datenmanipulation: ☐ ja ☐ nein

(Sublimit)
- ☐ 50.000 EUR
- ☐ 150.000 EUR
- ☐ 500.000 EUR

Erpressung: ☐ ja ☐ nein

(Sublimit)
- ☐ 50.000 EUR
- ☐ 150.000 EUR
- ☐ 500.000 EUR

Anmerkungen

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Ort, Datum

_____

Unterschrift Antragssteller

_____

Unterschrift Vermittler

Allianz

Glossar

Datensätze

Bei Datensätzen handelt es sich um eine Gruppe von inhaltlich zusammenhängenden Datenfeldern, welche Daten sowohl von privaten und als auch juristischen Personen enthalten. Zu diesen gehören bspw. Namen, Adressen, Sozialversicherungsdaten, Kontodaten, Projektdaten oder Produktdaten von Geschäftspartnern, Mitarbeitern, Kunden, Patienten und anderen Dritten.

Härtung

Erhöhung der Sicherheit von IT-Systemen

Das Bundesamt für Sicherheit in der Informationstechnik bezeichnet als Härten in der IT-Sicherheit „[…] die Entfernung aller Softwarebestandteile und Funktionen, die zur Erfüllung der vorgesehenen Aufgabe durch das Programm nicht zwingend notwendig sind." Ziel ist es, ein System zu schaffen, das von vielen, auch weniger vertrauenswürdigen Personen benutzt werden kann.

Patch-Management

Bereitstellen und Verwalten von Softwareaktualisierungen

Patch-Management ist der Bereich des Systemmanagements, der sich mit der Beschaffung, dem Testen und der Installation von Patches (Codeänderungen) auf einem verwalteten Computersystem beschäftigt. Die Aufgaben im Patch-Management sind unter anderem: Pflege des aktuellen Wissensstands über verfügbare Patches, die Entscheidungsfindung in Bezug auf die für ein bestimmtes System geeigneten Patches, Sicherstellen, dass Patches korrekt installiert werden, Testen der Systeme nach der Installation und Dokumentation aller damit verbundenen Prozeduren wie beispielsweise die erforderlichen Detailkonfigurationen.

PCI DSS

Payment Card Industry Data Security Standard

Regelwerk im Zahlungsverkehr, das sich auf die Abwicklung von Kreditkartentransaktionen bezieht und von allen wichtigen Kreditkartenorganisationen unterstützt wird. Handelsunternehmen und Dienstleister, die Kreditkarten-Transaktionen speichern, übermitteln, oder abwickeln, müssen die Regelungen erfüllen. Halten sie sich nicht daran, können Strafgebühren verhängt, Einschränkungen ausgesprochen, oder ihnen letztlich die Akzeptanz von Kreditkarten untersagt werden.

Tochtergesellschaft

Wird eine Gesellschaft mit gleichem Betriebscharakter durch Erwerb oder Gründung während der Versicherungszeit zu einer Tochtergesellschaft, erstreckt sich der Versicherungsschutz automatisch auch auf diese, es sei denn die Gesellschaft hat ihren Sitz außerhalb der Europäischen Union Versicherungsschutz besteht ab dem Zeitpunkt der Gründung bzw. Übernahme im gleichen Rahmen und Umfang wie für die bereits versicherten Gesellschaften. Ab diesem Zeitpunkt ist auch der Beitrag zu entrichten. Der Versicherungsnehmer ist verpflichtet, dem Versicherer die neu hinzukommenden Tochtergesellschaften spätestens drei Monate nach Beginn der auf den Zugang folgenden Versicherungsperiode anzuzeigen (Meldezeitraum). Unterlässt der Versicherungsnehmer die rechtzeitige Anzeige oder kommt innerhalb Monatsfrist nach Eingang der Anzeige bei dem Versicherer eine Vereinbarung über den Beitrag für die neuen Tochtergesellschaften nicht zustande, so entfällt der Versicherungsschutz rückwirkend ab Gefahreneintritt.

PESVA03035

FH---0003Z0 (02) PDF.2.18