EUROPÄISCHE GRUPPE AUF GEGENSEITIGKEIT
VERSICHERUNG UND RISIKOMANAGEMENT

Cyber-Bewertungsfragebogen

Sie erhalten auf der Basis dieses Fragebogens eine erste Sicherheitseinschätzung Ihrer informationsverarbeitenden Systeme. Auf Basis Ihrer Angaben erstellen wir für Sie eine erste, für beide Seiten unverbindliche Indikation. Der Versicherungsvertrag kommt selbstverständlich erst nach formeller Einigung über den Versicherungsumfang, den Beitrag, die Selbstbehalte und ein ggf. noch zu erfüllendes Sicherheitsniveau zustande.

Sie finden zur Orientierung im Fragebogen drei Farbkategorien von Fragen:

- *Rote Fragen = Pflichtangaben (Diese Fragen müssen für eine erste Einschätzung mindestens beantwortet sein.)*
- *Gelbe Fragen = Weitere Angaben zur detaillierteren Darstellung des Sicherheitsreifegrades Ihres Unternehmens (Bei zusätzlicher Beantwortung dieser Fragen, kann die für Sie eine Indikation ausgestaltet werden.)*
- *Grüne Fragen = Vervollständigen das Gesamtbild auf Ihr Unternehmen und den Sicherheitsreifegrad. (Diese Fragen sind obligatorisch für Einrichtungen mit einem Jahresumsatz von mehr als 1 Milliarde EURO.)*

Bitte beachten Sie, dass neben Ihren Antworten auf die Fragen auch die Anzahl der von Ihnen beantworteten Fragen aus den Bereichen unmittelbaren Einfluss auf den Beitrag hat.

IHRE EINRICHTUNG: BETRIEB UND DATEN

FIRMENBEZEICHNUNG

Firmenbezeichnung:
_____

Straße:
_____
Postleitzahl: _____ Ort: ___ _____
Telefon: _____ E-Mail: _____

BETRIEB

Personalkosten/Umsatz p. a.: _____ €

Bruttogewinn: _____

Anzahl der Mitarbeiter: _____

Fragen	Antworten
1. **Wie hoch ist der Anteil der Festangestellten gegenüber den Zeitarbeitskräften?**	Niedrig Hoch Nur Festangestellte

2.	**Wie hoch ist die jährliche Fluktuation Ihres Personals?**	Hoch Durchschnittlich Niedrig
3.	**Sind Sie Teil eines regionalen Krankenhausverbundes in öffentlicher Trägerschaft (beziehungsweise größtenteils in öffentlicher Trägerschaft)?**	Ja, als Mitglied Nein Ja, als Unterstützung
4.	**(Falls private Organisation) Sind Sie mit weiteren Einrichtungen vertraglich verbunden?**	Ja, keine gemeinsame Politik Nein Ja, Sicherheit gleichermaßen abgedeckt
5.	**Umsatzanteil:**	In den USA: ___% In der EU: ___% In anderen Staaten: ___%
6.	**Haben oder hatten Sie eine Cyberversicherung mit einem oder mehreren der zu versichernden Leistungsbausteinen abgeschlossen?**	Nein Ja
7.	**Wurde Ihre Cyberversicherung mit einem oder mehreren der zu versichernden Leistungsbausteine durch den Versicherer gekündigt oder nicht verlängert?**	Nein Ja
8.	**Hatten Sie in den letzten drei Jahren einen bedeutenden Vorfall im Bereich der Informationssicherheit?**	Jeden Tag Jeden Monat Jedes Jahr Niemals
9.	**Waren Sie in den letzten drei Jahren von einer Verletzung des Schutzes personenbezogener Daten betroffen, die zu einer Benachrichtigung der betroffenen Personen führte?**	Nein Ja
10.	**DATEN:**	PCI-Anteil: ____ PHI-Anteil: ____ Gesamtzahl der Daten:____
11.	**Ungefähre Anzahl von Arbeitsplätzen (1), Servern (2), "OT" Geräten (3) und medizinischen Geräten (4)**	1:____ 2:____ 3:____ 4:____
12.	**Verwenden Sie Intrusion Protection ("EDR") für Workstations und Server?**	Nein Ja (nur IT-Desktops) Ja (nur IT-Server) Ja (alle)
13.	**Decken drahtlose Netzwerke alle Gebäude ab?**	Nein Ja, nur medizinische Gebäude Ja, überall
14.	**Sind alle Ihre Zugangspunkte durch einen aktiven EDR gesichert?**	Nein Ja

15. Haben Sie ein Programm zur technologischen Risikominderung initiiert?	Nein Ja, nicht formal Ja, dokumentiert
16. Haben Sie eine formelle Richtlinie zur Informationssicherheit entwickelt und implementiert, die unternehmensweit und dauerhaft für alle Mitarbeiter und relevante externe Dritte verfügbar ist?	Ja, intern Ja, intern und extern Nein
17. Werden Ihre Richtlinien zur Informationssicherheit jährlich überprüft und von der Geschäftsleitung genehmigt?	Ja Nein
18. Unterliegen IT und OT in Ihrer Organisation einer einheitlichen Verwaltung und einem einheitlichen Governance?	Ja Nein
19. Haben Sie einen Verantwortlichen für die Informationssicherheit (z. B. Chief Information Security Officer "CISO") benannt?	Ja Nein
20. Berichtet die für die IT Sicherheit verantwortliche Person regelmäßig an die Geschäftsleitung?	Ja Nein
21. Bieten Sie mindestens einmal jährlich eine Weiterbildung an, um das Sicherheitsbewusstsein Ihrer Nutzer (Mitarbeiter und Auftragnehmer) zu erhöhen und sie darauf vorzubereiten, wachsamer gegen Phishing zu sein?	Nein Ja, alle Mitarbeiter werden geschult. Ja, ein Teil der Mitarbeiter wird geschult.
22. Stellen Sie mindestens einmal im Jahr Informationen zur Verfügung, um das Sicherheitsbewusstsein Ihrer Nutzer (Partner und Anbieter) zu erhöhen und sie darauf vorzubereiten, sich besser gegen Phishing zu wappnen und wachsam zu sein?	Ja, Informationen werden an alle Nutzer weitergegeben Nein
23. Protokollieren Sie die Schulungen zum Sicherheitsbewusstsein und berichten an die Geschäftsleitung?	Ja Nein
24. Haben Sie Personenkreise identifiziert (z. B. privilegierte Nutzer, Administratoren, Führungskräfte), welche spezifische Schulungen zum Sicherheitsbewusstsein benötigen?	Ja Nein
25. Verfügen Sie über eine aktuelle Liste von Behörden und externen Kontakten, die bei einer Informationssicherheitsverletzung informiert werden müssen?	Ja Nein
26. Verfügen Sie über ein aktuelles Inventarverzeichnis an Software (einschl. Betriebssystemen) und Hardware-Beständen in Ihrem Netzwerk? (Alle IT und OT System).	Ja Nein

27.	Verfügen Sie über eine umfassende Konfigurationsmanagement-Datenbank (CMDB), einschließlich aller IT- und öffentlichen Cloud-Ressourcen, Abhängigkeiten, Schwachstellen, verantwortlicher Personen, Software- und Patch-Versionen?	Ja Nein
28.	Verwenden Sie eine Mobile Device Management Lösung (MDM) für alle Laptops und Smartphones?	Ja Nein
29.	Klassifizieren Sie Informationen in Bezug auf deren Vertraulichkeit?	Ja Nein
30.	Klassifizieren Sie Informationen in Bezug auf deren Integritäts- und Verfügbarkeitsanforderungen?	Ja Nein
31.	Haben Sie Verfahren zur Kennzeichnung von Informationen eingeführt, die im Einklang mit dem oben definierten Klassifizierungsschema stehen?	Ja Nein
32.	Haben Sie ein Schema zur technischen Klassifizierung von Informationen umgesetzt?	Ja Nein
33.	Gibt es eine Anleitung zum Umgang mit klassifizierten Informationen?	Ja Nein
34.	Wird der Umgang mit Informationen regelmäßig überprüft, um die Übereinstimmung mit deren Klassifikation sicherzustellen?	Ja Nein
35.	Ist der Zugriff auf Informationen, welche sich auf Wechseldatenträgern wie externen Speichergeräten (z.B. USB-Sticks oder Festplatten) befinden, beschränkt oder sind diese verschlüsselt?	Ja Nein
36.	Ist eine Genehmigung für das Löschen von Medien der Organisation erforderlich und wird für ein Audit-Trail ein Protokoll über solche Löschungen geführt?	Ja Nein
37.	Werden Hardwareanschlüsse für Datenträger (z. B. USB-Anschlussbuchsen) zentral verwaltet oder werden diese grundsätzlich deaktiviert?	Ja Nein
38.	Löschen Sie Datenträger mit sensiblen Informationen, die nicht länger gebraucht werden, auf sichere Art und Weise?	Ja Nein
39.	Verfügen Sie über eine Richtlinie zur dauerhaften und nicht mehr wiederherstellbaren Entfernung von Medien, die nicht mehr benötigt werden?	Ja Nein
40.	Beschränken Sie die Zugriffsrechte von Mitarbeitern auf Basis betrieblicher Notwendigkeit (insbesondere administrative Berechtigungen und Zugriff auf vertrauliche z. B. persönliche Daten)?	Ja Nein

41.	Schränken Sie die Zugriffsrechte von externen Nutzern (insbesondere Administratorrechte und den Zugang zu sensiblen Daten, z. B. personenbezogenen Daten) auf der Grundlage der geschäftlichen Notwendigkeit ein (Mitarbeiter und Auftragnehmer)?	Ja Nein
42.	Erlauben Sie Ihren Mitarbeitern, ihren persönlichen Computer oder Mobilgeräte für die Erledigung ihrer Aufgaben zu nutzen (BYOD)?	Häufig Selten Nein Nicht zutreffend
43.	Erlauben Sie Ihren Mitarbeitern, einen Teil ihrer Aufgaben von zu Hause aus zu erledigen?	Häufig Selten Nein Nicht zutreffend
44.	Fördern Sie die Verwendung von MFA-Authentifizierungsverfahren (CPS-Karte, Hardware-Token)?	Nein Selten Häufig
45.	Verfügen Sie über eine Mehrfaktor-Authentifizierung für den Fernzugriff?	Ja Nein
46.	Verfügen Sie über einen formalen Prozess für die Zuweisung und den Widerruf von Zugriffsrechten?	Ja Nein
47.	Verfügen Sie über ein zentrales Identitäts- und Zugangsmanagementsystem (Identity and Access Management, IAM)?	Ja Nein
48.	Sind lokale Administrationsrechte für Nutzer auf Arbeitsplatzrechnern verboten?	Ja Nein
49.	Ist das Anmelden an einem Desktop für privilegierte Nutzer unterbunden?	Ja Nein
50.	Verwenden Sie ein Managementsystem für privilegierte Nutzer und Benutzerkonten (Privileged Identity and Account Management, PIM, PAM)?	Ja Nein
51.	Wird der Systemzugriff, bzw. Datenzugriff mindestens einmal jährlich überprüft?	Ja Nein
52.	Überprüfen Sie die Zugriffsrechte der Nutzer mindestens einmal jährlich?	Ja Nein
53.	Überprüfen Sie geteilte Benutzerkonten (z. B. für hochprivilegierte Systeme und Anwendungen) mindestens jährlich?	Ja Nein
54.	Überprüfen Sie mindestens einmal jährlich die Berechtigungen für privilegierte Zugangsrechte?	Ja Nein

55. Widerrufen Sie alle Systemzugänge, Benutzerkonten und zugehörigen Rechte nach der Kündigung von Benutzern (inkl. Mitarbeiter, Leiharbeitnehmer, Auftragnehmer oder Lieferanten)?	Ja Nein
56. Haben Sie ein Verfahren zum Entfernen unnötiger Nutzerrechte nach einem Funktionswechsel innerhalb des Betriebes?	Ja Nein
57. Haben Sie eine Kennwortrichtlinie implementiert, welche die Verwendung langer und komplexer Kennwörter in Ihrem Betrieb erzwingt? Lange und komplexe Passwörter werden definiert als: acht oder mehr Zeichen; enthalten keine Wörter aus Wörterbüchern; sind frei von aufeinanderfolgenden identischen, vollständig numerischen oder ausschließlich alphabetischen Zeichen.	Ja Nein
58. Wie oft werden die Passwörter für die Nutzer geändert?	_____
59. Haben Sie die werksseitig eingestellten Passwörter für alle angeschlossenen Komponenten (z.B. Router, IoT usw.) geändert?	Nein Ja, wenn es sich um eine Internetverbindung handelt Ja, bei allen verbundenen IT-Geräten
60. Ändern Sie die werksseitigen Passwörter Ihrer IT, OT und Medizinprodukte, sobald diese in den Normalbetrieb integriert werden?	Nein Nur IT Ja für alle IT-Systeme und IT-Geräte
61. Bieten Sie allen Nutzern einen Kennwortmanager an?	Nein Ja Ja, mit einem hochwertigen Masterpasswort
62. Entsprechen die Passwörter der Nutzer der MINIMAL MS-Komplexität?	Ja Nein
63. Entsprechen die Kennwörter der Microsoft AD-Standardrichtlinie?	Nein Ja
64. Werden wiederholte Passwortfehler für die Anmeldedaten der einzelnen Sitzungen erkannt und neutralisiert (um Brute-Force zu vermeiden, durch automatische - und vorübergehende - Sperrung)?	Ja Nein
65. Werden die Passwörter für die Anwendungen / Software regelmäßig geändert?	Nein, nie N/A SSO Ja, vierteljährlich Ja, halbjährlich Ja, jährlich

66. Werden die Passwörter für die Machine-to-Machine Authentifizierung regelmäßig geändert?	Nein, nie NA, aufgrund einer Zertifizierung Ja, vierteljährlich Ja, halbjährlich Ja, jährlich
67. Verfügen Sie über allgemeine Standardkennungen für neue Mitarbeitergruppen (z. B. neue Mitarbeiter in praktischer Ausbildung oder Praktikanten)?	Nein Nicht zutreffend (N/A) Ja
68. Stellen Sie für Geräte und Systeme, welche über das Internet erreichbar sind oder sich im mobilen Einsatz befinden, zusätzliche Schutzmaßnahmen sicher, beispielsweise Firewall, Mehr-Faktor-Authentifizierung, Verschlüsselung von Datenträgern, Diebstahlsicherung oder ähnliches?	Nein Ja, Teilweise, Ja
69. Sind alle vertraulichen Informationen, die auf mobilen Geräten (z. B. Smartphones und Laptops) gespeichert sind, verschlüsselt?	Nein Ja
70. Sind alle vertraulichen Informationen, die auf allen anderen Geräten gespeichert sind, verschlüsselt?	Nein Ja
71. Verschlüsseln Sie sensible Daten und vertrauliche Informationen, die in Datenbanken und auf Dateiservern gespeichert sind?	Ja Nein N/A
72. Haben Sie eine Richtlinie zur Benutzung, zum Schutz und zur Lebensdauer von kryptographischen Schlüsseln entwickelt und eingeführt?	Ja Nein N/A
73. Wird Ihre Richtlinie von kryptographischen Schlüsseln während der gesamten Lebensdauer regelmäßig überprüft und aktualisiert?	Ja Nein N/A
74. Führen Sie eine Liste von Personen (Mitarbeiter, Fremdfirmen und Besucher), die autorisierten Zutritt zum Betriebsgelände und zu Sicherheitsbereichen haben?	Ja Nein N/A
75. Haben Sie erweiterte Zutrittskontrollsysteme (z. B. biometrische Zugangskontrollen, Vereinzelungsschleusen) installiert?	Ja Nein N/A
76. Haben Sie eine erweiterte Zutrittsüberwachung (z. B. 24-7 Videoüberwachung (CCTV), Dokumentation aller Zutritte) installiert?	Ja Nein N/A
77. Verschlüsselt Ihr Webserver vertrauliche Daten (z. B. HTTPS)?	Ja Nein
78. Schützen Sie Ihre Webserver vor Denial-of-Service-Angriffen (z. B. durch den Einsatz eines Content Delivery Network Provider)?	Ja Nein N/A

79.	**Testen Sie die sicherheitsrelevante Funktionalität von Informationssystemen (inkl. deren IT-Sicherheitsupdates) während des Entwicklungszyklus?**	Ja Nein N/A
80.	**Führen Sie automatisierte Sicherheitstests oder Codeanalysen während der System- oder Softwareentwicklung durch?**	Ja Nein N/A
81.	**Erhalten Sie die Vertraulichkeit bei der Verwendung von Betriebsdaten für Tests aufrecht, um sicherzustellen, dass alle sensiblen Daten durch Entfernen oder Ändern von Einstellungen auch weiterhin geschützt sind?**	Nein Ja, anonymisierte Daten Ja, anonymisierte und geschützte Daten
82.	**Verfügt Ihr IT-Team über die notwendigen Fähigkeiten, um alle in Ihrer Einrichtung vorhandenen Technologien (IT, OT, medizinische Geräte) zu bedienen?**	Nein Ja, nur für IT Ja, für alle IT-Systeme und IT-Geräte
83.	**Von wem werden die Wartungsarbeiten an OT-Geräten und Medizinprodukten durchgeführt?**	Keine Externer Dienst Interner Dienst Hersteller
84.	**Von wem werden die Wartungsarbeiten an Ihrer Telefonanlage (PABX) durchgeführt?**	Keine Externer Dienst Interner Dienst Hersteller
85.	**Haben Sie für kritische Systeme ein Verfahren für das Änderungsmanagement eingeführt?**	Ja Nein N/A
86.	**Umfassen Ihre Verfahren für das Änderungsmanagement Tests, Szenarien zur Wiederherstellung nach Fehlern und ein Berichtswesen?**	Ja Nein
87.	**Berücksichtigen Sie bei Änderung Ihrer IT Umgebung stets die Anforderungen der Geschäftsprozesse?**	Ja Nein
88.	**Ist die IT Umgebung für Entwicklungen und Tests getrennt von der Betriebsumgebung?**	Ja Nein
89.	**Verwenden Ihre Entwickler unterschiedliche Benutzerkonten zum Entwickeln, Testen und für alltägliche Aufgaben?**	Ja Nein

90. Haben Sie Kontrollen gegen Malware-Risiken (Virenschutz, EDR...) für die folgenden Vermögenswerte der IT-SYSTEME unter alleiniger Verantwortung des Versicherten umgesetzt)?	Nein Internet-exponierte Komponenten (Ausnahmen wurden identifiziert und das Risiko gemindert) Nicht-medizinische Server (Ausnahmen mit Risikominderung identifiziert) IT-Endpunkte
91. Haben Sie einen Prozess implementiert, bei dem Sie Hersteller oder Softwareherausgeber über einen möglichen Einsatz von Malware-Schutz auf ihren Systemen befragen?	Nein Ja (nicht formal/mündlich) Ja (Schriftform) Ja (Vereinbarung)
92. Wird eine Datenbank mit Malware-Signaturen automatisch heruntergeladen und installiert?	Nein Ja, ohne Identifizierung der Ausnahmen Ja, mit 100% identifizierten Ausnahmen Ja, überall
93. Wird der Einsatz von Malware regelmäßig überprüft und aktualisiert?	Nein Ja, täglich Ja, monatlich
94. Werden neben der herkömmlichen signaturbasierten Erkennung auch erweiterte heuristik- und verhaltensbasierte Erkennungsmechanismen zum Schutz vor neuer Malware verwendet?	Ja Nein
95. Sind die Backups der Geräte, für die Sie die alleinige Verantwortung tragen, vom Netz getrennt oder gegen unbefugte oder unbeabsichtigte Manipulationen geschützt?	Nein Ja, die Daten sind durch einen logischen Schutz geschützt (zumindest gegen Cryptolocker Ja, die Daten sind gegen logische Manipulationen geschützt (DLP einschließlich Cryptolockers) Ja, die Daten sind durch eine physische Trennung geschützt
96. Halten Sie den Anwendungsbereich Ihrer Sicherung für die Geräte, für die Sie allein verantwortlich sind, auf dem neuesten Stand?	Nein (nie) Ja, täglich Ja, wöchentlich Ja, monatlich

97. Wie oft werden Backups nach Änderungen von Daten, Software oder Konfigurationen an den Geräten durchgeführt, für die Sie die alleinige Verantwortung tragen?	Niemals täglich wöchentlich monatlich
98. Werden die Protokolle der Sicherung betreffend die Geräte, für die Sie die alleinige Verantwortung tragen, analysiert um Probleme zu erkennen und diese zu beheben?	Nein (Nichts) Ja (aus Protokollen) Ja, (aus Protokollen und regelmäßigen Stichproben) Ja, (Automatischer Alarm und Ticketausstellung)
99. Haben Sie für die Geräte, für die Sie die alleinige Verantwortung tragen, eine Liste aller Syteme erstellt, die nicht gesichert werden können, und analysieren Sie, warum?	Nein Ja, technische Schwierigkeiten identifiziert Ja, andere Schwierigkeiten identifiziert
100. Besteht bei Geräten, für die Sie die alleinige Verantwortung tragen, ein "Änderungsmanagementprozess", der die Sicherung der betroffenen Geräte erzwingt?	Nein Ja, vorher Ja, danach Ja, beide
101. Sind die Rückverfolgbarkeitsdaten bei Geräten, für die Sie die alleinige Verantwortung tragen, Teil der Software und sowie der Sicherungskopie der medizinischen Umgebung (mehrere Antworten möglich)?	Nein Ja, Journale (Protokolle) Ja, rechtliche Rückverfolgbarkeit (Audit Trail)
102. Bewahren Sie die Sicherungsmedien physisch getrennt von ihrem Netzwerk (z. B. außerhalb des Betriebsgeländes) auf?	Ja Nein N/A
103. Stellen Sie regelmäßig sicher, dass die Backups vollständig sind und so schnell wie möglich wiederhergestellt werden können, ohne dass dies Auswirkungen auf das Geschäft hat?	Ja Nein N/A
104. In Bezug auf Geräte, für die eine gemeinsame gesetzliche Verantwortung besteht (z. B. Medizinprodukte): kennt und befolgt Ihr Unternehmen die Anforderungen des Herstellers für die Datensicherung, sofern vorhanden?	Nein, ich weiß es nicht Nein, ich kann nicht immer folgen Nein, ich kann nicht immer folgen und diese Ausnahmen sind gerechtfertigt Ja, ich befolge oder mein Anbieter befolgt alle bestehenden Anforderungen fü Backups

105. In Hinblick auf Geräte, für die eine gemeinsame gesetzliche Verantwortung besteht (z. B. Medizinprodukte): überprüfen/aktualisieren Sie die Pläne für die Datensicherung mit relevanten Dritten?	Nein (nie) Ja, wöchentlich Ja, monatlich Ja, jährlich
106. Stellen Sie sicher, dass die Rückverfolgbarkeitsdaten im Hinblick auf Geräte, für die eine gemeinsame gesetzliche Verantwortung besteht (z. B. Medizinprodukte), Bestandteil der Backups sind?	Nein Ja, Protokolle Ja, Audit Trail Journale
107. Erhalten Sie im Hinblick auf Geräte, für die eine gemeinsame gesetzliche Verantwortung besteht (z. B. Medizinprodukte), Berichte über Probleme bei der Datensicherung von relevanten Dritten?	Nein (nie) Ja, wöchentlich Ja, monatlich Ja, jährlich
108. Überprüfen / Aktualisieren Sie bei Anlagen, an denen ein Dritter beteiligt ist (z. B. SCADA/IoT/GTB/GTC), die Pläne für die Datensicherung mit den betreffenden Dritten?	Nein (nie) Ja, wöchentlich Ja, monatlich Ja, jährlich
109. Erhalten Sie bei Anlagen, an denen ein Dritter beteiligt ist (z. B. SCADA/IoT/GTB/GTC), Berichte über Probleme bei der Datensicherung von den betreffenden Dritten?	Nein (nie) Ja, wöchentlich Ja, monatlich Ja, jährlich
110. Erstellen und überprüfen Sie regelmäßig Ereignisprotokolle, in denen Benutzeraktivitäten, Ausnahmen, Fehler und Informationssicherheitsereignisse aufgezeichnet werden (zumindest von Ihren Firewalls und dem Domain Controller)?	Ja Nein
111. Haben Sie die Rückverfolgbarkeit von Zugriffen und Aktionen, die auf den Systemen durchgeführt werden, implementiert (zumindest persönliche Verbindung/Trennung)?	Nein Ja dezentrales Protokoll Ja zentralisiertes Protokoll Ja zentralisiertes und geschütztes Protokoll
112. Verfügen Sie über ein SIEM-System (Security Information and Event Management), das Regeln für die Erstellung von Berichten und Warnungen zur Systemsicherheit enthält?	Ja Nein
113. Haben Sie einen zentralen Prozess zur Softwareinstallation implementiert?	Ja Nein
114. Wenden Sie ein striktes Konfigurationsmanagement an und entwickeln Sie sichere Abbilder, die zur Erstellung aller neu bereitgestellten Arbeitsstationen und Server verwendet werden?	Ja Nein
115. Werden Patches für Betriebssysteme, für die Sie allein verantwortlich sind, maximal 60 Tage nach Verfügbarkeit installiert (mehrere mögliche Antworten)?	Nein Ja, für Desktops Ja, für nicht-medizinische Server Ja, für medizinische Server (oder Ausnahmen werden verwaltet)

116. Soweit Dritte Ihre Geräte verwalten/warten, haben Sie mit diesen vereinbart, dass Sicherheitspatches maximal 60 Tage nach Verfügbarkeit installiert werden (mehrere mögliche Antworten)?	Nein Ja, Desktops Ja, nicht medizinische Server Ja, medizinische Server (oder identifizierte und anderweitig geschützte) Ja, "SCADA/IoT" (oder identifiziert und anderweitig geschützt)
117. Werden Sicherheitspatches für alle Komponenten, die mit dem Internet verbunden sind, maximal 30 Tage nach Verfügbarkeit installiert (die Frist beginnt erneut, wenn eine neuere Version des Patches erscheint)?	Nein Nein, 60 Tage Ja, 30 Tage
118. Befolgen Sie einen Prozess zur Ablösung veralteter Systeme, die keinen Sicherheitspatch erhalten haben?	Nein Ja, mit Ausnahmemana-gemer Ja, mit strikter Isolierung der Systeme
119. Planen Sie die Systeme in Ihrem Verantwortungsbereich, die keine Patches mehr erhalten können, zu ersetzen?	Kein Plan vorhanden Ja, innerhalb von 6 Monaten Ja, innerhalb von 12 Monaten Ja, ohne Frist
120. Planen Sie die Systeme auszutauschen, die keine Patches mehr erhalten und für die eine dritte Partei ebenfalls die Gefahr trägt?	Nein Nein, aber formelle Besprechung Ja, innerhalb von 12 Monaten Ja, ohne Frist
121. Berücksichtigen Sie die von den nationalen Behörden veröffentlichten Warnmeldungen mit hoher Priorität (mehrere Antwortmöglichkeiten, siehe URLs)?	Nein Ja, https://wid.cert-bund.de/portal/wid/start
122. Ergreifen Sie vorübergehende Gegenmaßnahmen gegen Zero-Day-Exploit (falls vorhanden)?	Ja Nein
123. Führen Sie regelmäßig Untersuchungen auf Schwachstellen durch, ermitteln das damit verbundene Risiko und ergreifen geeignete Maßnahmen?	Ja Nein N/A
124. Stellen Sie technisch oder organisatorisch sicher, dass Benutzer keine Software auf ihren Arbeitsplatzrechnern installieren dürfen?	Ja Nein N/A
125. Ist Ihre Firewall nach dem "White - Listing - Prinzip" konfiguriert?	Ja Nein

126. Enthält die zentrale Firewall sowohl für eingehenden als auch für ausgehenden Verkehr im Internet Filterregeln, die den Spezifikationen des Herstellers entsprechen?	Ja Nein
127. Wird der durch die Firewall abgelehnte Internetverkehr regelmäßig analysiert?	Nein (nie) Ja (täglich) Ja (wöchentlich) Ja (monatlich)
128. Sind alle Internetzugangspunkte durch entsprechend konfigurierte Firewalls gesichert (Büro und zu Hause)?	Ja Nein
129. Sind alle Internet-Zugangspunkte durch Firewalls der nächsten Generation (sogenannte NextGen-Firewalls) abgesichert?	Ja Nein
130. Haben Sie eine Network Access Control ("NAC")-Technologie für den Zugriff auf Ihre drahtlosen Unternehmensnetzwerke implementiert?	Ja Nein
131. Überwachen Sie Ihr Netzwerk und identifizieren Sie sicherheitsrelevante Ereignisse?	Ja Nein
132. Wird der eingehende Datenverkehr aus dem Internet von einem IDS gefiltert?	Nein Ja, ohne Monitoring Ja, mit Monitoring Ja, und blockiert
133. Beinhaltet Ihr Traffic-Analyse-Prozess Kompromissindikatoren (IOC), die von den nationalen Behörden veröffentlicht werden?	Ja Nein
134. Haben Sie spezielle Filterregeln definiert, um die von den nationalen Behörden geforderten regelmäßigen Schwachstellen-Scans zu ermöglichen?	Ja Nein
135. Haben Sie ein Security Operations Center (SOC), das alle Ereignisse rund um die Uhr (24-7) überwacht?	Ja Nein
136. Sind alle aus dem Internet erreichbaren Systeme (z. B. Web-, E-Mail-Server) von Ihrem vertrauenswürdigen Netzwerk getrennt (z. B. innerhalb einer entmilitarisierten Zone (DMZ) oder bei einem Drittanbieter)?	Ja Nein
137. Sind alle risikoreichen Netzwerksegmente (z. B. Point of Sales (PoS)-Systeme, sensible Datenverarbeitung, Produktionsnetzwerke für Büro- und Betriebstechnik (OT) etc.) voneinander getrennt?	Ja Nein
138. Verschlüsseln Sie vertrauliche Kommunikation (z. B. sichere E-Mails mit S/MIME (Secure Multipurpose Internet Mail Extensions) oder SMTP-over-TLS (Simple Mail Transfer Protocol Secure))?	Ja Nein
139. Setzen Sie eine Data Loss Prevention (DLP)-Lösung ein?	Ja Nein

140. Liegen Vereinbarungen mit SaaS-Dienstleistern über ein Sicherheitsniveau vor, das Ihrem eigenen Informationssicherheitsstandard entspricht?	Ja, aber nichts, was mit Sicherheit zu tun hat Kein SaaS im Einsatz Ja, sicherheitsbezogen
141. Liegen Vereinbarungen mit Ihren Cloud-Service-Anbietern über ein Sicherheitsniveau vor, das Ihrem eigenen Informationssicherheitsstandard entspricht?	Ja, aber nichts, was mit Sicherheit zu tun hat Keine Cloud im Einsatz Ja, sicherheits-bezogen
142. Wird die Digitale Krankenakte außerhalb Ihrer Organisation, oder mithilfe externer Partnern verwaltet?	Ja, aber nichts, was mit Sicherheit zu tun hat Nicht vernetzt Ja, auch Sicherheit abgedeckt
143. Betreiben Sie mit oder durch externe Partner, Telemedizin-Dienstleistungen?	Ja, aber nichts, was mit Sicherheit zu tun hat Nicht vernetzt Ja, auch Sicherheit abgedeckt
144. Sind Sie im Rahmen gemeinsamer medizinischer Tätigkeiten (Röntgen, Apotheke) mit Infrastrukturen Dritter vernetzt?	Ja, aber nichts, was mit Sicherheit zu tun hat Nicht vernetzt Ja, auch Sicherheit abgedeckt
145. Haben Sie alle Ihre wichtigen Lieferanten (auch Drittanbieter) identifiziert und dokumentiert?	Ja Nein
146. Haben Sie Maßnahmen zur Informationssicherheit identifiziert und im Rahmen einer Richtlinie eingeführt, um den Zugriff von Lieferanten oder Drittanbietern auf Ihre Informationen zu schützen?	Ja Nein
147. Liegen Vereinbarungen mit Drittanbietern über ein Sicherheitsniveau vor, das Ihrem eigenen Informationssicherheitsstandard entspricht?	Ja Nein
148. Überprüfen und aktualisieren Sie regelmäßig Verträge mit Ihren wichtigen Lieferanten (einschließlich Drittdienstleistern)?	Ja Nein
149. Legen Sie in Ihren vertraglichen Vereinbarungen die Berechtigung für die Durchführung externer Audits fest?	Ja Nein
150. Überwachen Sie die Aktivitäten von Drittanbietern auf sicherheitsrelevante Ereignisse, um das vereinbarte Informationssicherheitsniveau zu gewährleisten?	Ja Nein
151. Führen Sie Audits (Informationssicherheitsbewertungen) bei Lieferanten (einschließlich Drittdienstleistern) durch und verfolgen Sie die festgestellten Probleme?	Ja Nein

152. Enthalten Ihre schriftlichen und unterzeichneten Verträge mit Lieferanten (einschließlich Drittdienstleistern) eine Freistellungsvereinbarung oder einen Haftungsverzicht zu Ihren Ungunsten, falls diese Lieferanten Ihre sensiblen Daten nicht adäquat schützen?	Ja Nein
153. Haben Sie eine verantwortliche Person oder ein Team für die Reaktion auf Vorfälle ernannt?	Ja Nein
154. Haben Sie ein Team, das sich der Abwehr von Sicherheitsvorfällen widmet?	Nein Verfügbar außerhalb der Arbeitszeiten Verfügbar 24/7 Nur während der Arbeitszeit verfügbar
155. Kennen alle Ihre Mitarbeiter und Drittanbieter die Berichtslinie für Ereignisse in der Informationssicherheit?	Ja Nein
156. Sind sich alle Mitarbeiter und Auftragnehmer ihrer Verpflichtung zur Meldung von Ereignissen der Informationssicherheit bewusst?	Ja Nein
157. Sind Mitarbeiter und Auftragnehmer verpflichtet, identifizierte Schwachstellen der Informationssicherheit (noch kein Vorfall oder Ereignis) in Systemen oder Diensten zu melden?	Ja Nein
158. Wird das Pflegepersonal aufgefordert, unerwünschte Ereignisse zu melden, wenn diese durch technische Probleme mit der IT verursacht wurden?	Nein Ja, keine Verwendung Ja, verwendet
159. Bieten Sie ein Bug-Bounty-Programm an, um Fehler, Exploits oder Schwachstellen zu melden?	Ja Nein
160. Haben Sie einen Plan zur Reaktion auf Informationssicherheitsvorfälle (Incident Response Plan)?	Ja Nein
161. Testen Sie jährlich Ihren Reaktionsplan für Vorfälle?	Ja Nein
162. Dokumentieren Sie alle Ereignisse der Informationssicherheit in einem zentralen Security Information and Event Management (SIEM)-System?	Ja Nein
163. Haben Sie ein Eskalationsverfahren für Vorfälle der Informationssicherheit eingerichtet?	Ja Nein
164. Sammeln Sie Daten, die später für eine forensische Analyse verwendet werden können?	Ja Nein
165. Informieren Sie das Management regelmäßig über vergangene Vorfälle?	Ja Nein

166. Nutzen Sie die Erkenntnisse aus der Analyse und Aufklärung von Vorfällen der Informationssicherheit, um die Wahrscheinlichkeit oder das Ausmaß zukünftiger Vorfälle zu reduzieren?	Ja Nein
167. Quantifizieren und überwachen Sie Arten, Anzahl und Kosten von Vorfällen der Informationssicherheit?	Ja Nein
168. Haben Sie ein Verfahren zur Überprüfung und Analyse von "glass breakage"?	Nein Nicht zutreffend (N/A) Ja
169. Haben Sie mechanische oder physische Schutzmaßnahmen (Videoüberwachung, Zugangskontrolle) zum Schutz vor Diebstahl von Geräten für den gesamten Bestand (IT, OT, medizinische Geräte) ergriffen?	Nein Nur IT Ja für alle
170. Wurden Sie in den letzten drei Jahren mit einer Unterbrechung der Pflegeaktivitäten aufgrund eines IT-Problems (Ausfälle, Bugs, Langsamkeit) konfrontiert, das von den Benutzern gelöst werden konnte?	Jeden Tag Jeden Monat Jedes Jahr Niemals
171. Wurden Sie in den letzten drei Jahren mit einer Unterbrechung der Pflegeaktivitäten infolge eines IT-Problems (Ausfälle, Bugs, Verzögerungen) konfrontiert, die ein Eingreifen der IT-Abteilung erforderte?	Jeden Tag Jeden Monat Jedes Jahr Niemals
172. Haben Sie eine Business Impact Analyse (BIA) durchgeführt?	Ja Nein
173. Sind Recovery Time Objectives (RTO) und Recovery Point Objectives (RPO) für kritische Systeme und Prozesse definiert und dokumentiert?	Ja Nein
174. Haben Sie einen Plan für das betriebliche Kontinuitätsmanagement (Business Continuity Management, BCM), der sich speziell mit Vorfällen in der Informationssicherheit befasst?	Ja Nein
175. Haben Sie einen IT Disaster Recovery Plan (DRP)?	Ja Nein
176. Verfügen Sie über erweiterte Implementierungskontrollen für Disaster-Recovery-Funktionen (z. B. vollständige Redundanz oder automatische Failover-Mechanismen)?	Ja Nein
177. Testen Sie Ihre Pläne zur Kontinuität der Informationssicherheit (z. B. Business Continuity Management, Disaster Recovery) mindestens einmal jährlich?	Ja Nein
178. Überprüfen und aktualisieren Sie Ihre Pläne zur Kontinuität der Informationssicherheit (z. B. Business Continuity Management, Disaster Recovery) mindestens einmal jährlich?	Ja Nein

179. Werden die Ergebnisse der Kontinuitätstests überprüft, dokumentiert, an das Management berichtet und werden die Pläne auf der Grundlage der gewonnenen Erkenntnisse überarbeitet?	Ja Nein
180. Sind Ihre Einrichtungen zur Informationsverarbeitung (d. h. alle Systeme und Dienste, jede Infrastruktur oder physischer Standort, in dem sie untergebracht sind) redundant ausgeführt?	Ja Nein
181. Führen Sie regelmäßig - mindestens einmal jährlich - Redundanztests durch, um sicherzustellen, dass der Failover von einer Komponente zur anderen Komponente wie vorgesehen funktioniert?	Ja Nein
182. Haben Sie ein Verfahren zur dauerhaften Einhaltung aller datenschutzrelevanten gesetzlichen, regulatorischen und vertraglichen Anforderungen implementiert?	Ja Nein
183. Haben Sie einen Compliance Officer eingesetzt?	Ja Nein
184. Berichtet Ihr Compliance Officer regelmäßig an das Top-Management?	Ja Nein
185. Haben Sie eine Leitlinie zur Aufbewahrung, Lagerung, Handhabung und Entsorgung von Aufzeichnungen und Informationen erlassen?	Ja Nein
186. Haben Sie einen Aufbewahrungsplan, der für Aufzeichnungen, Dokumente oder sonstige Informationen einen Aufbewahrungszeitraum beschreibt?	Ja Nein
187. Haben Sie eine verantwortliche Person für die Beratung und Sensibilisierung zu den Grundsätzen des Datenschutzes ernannt (z. B. einen Datenschutzbeauftragten, Data Privacy Officer DPO)?	Ja Nein
188. Berichtet Ihr Datenschutzbeauftragter regelmäßig an das Top-Management?	Ja Nein
189. Haben Sie eine Richtlinie zum Schutz der Privatsphäre und zum Schutz personenbezogener Daten entwickelt und umgesetzt?	Ja Nein
190. Überprüfen Sie regelmäßig kritische Systeme (inkl. Penetrationstests oder Schwachstellenanalysen) - entweder selbst oder von Dritten unterstützt - insbesondere bei jeder Einführung neuer Systeme und nach Änderungen?	Ja Nein
191. Würden Sie auf Anfrage das "Verzeichnis der Verarbeitungstätigkeiten gemäß GDPR" zur Verfügung stellen?	Nein Ja

192.	**Erhalten Sie regelmäßig Informationen bezüglich Sicherheitsfragen Ihrer "OT" Technik und medizinischen Geräte?**	Nein Ja

Antragsteller erklärt darüber informiert zu sein, dass die in dem vorliegenden Dokument enthaltenen Informationen Angaben zur Risikobewertung darstellen, die für die Bewertung der Versicherungsleistungen und die Festsetzung des Beitrags verwendet werden; jede Verletzung der Anzeigepflicht, falsche Darstellung, Auslassung oder Ungenauigkeit kann daher versicherungsvertragliche Folgen nach dem Versicherungsvertragsgesetz bzw. den vereinbarten Bedingungen zur Folge haben.

Ich, (Name und Funktion) _____
bestätige die Richtigkeit der in dem vorliegenden Antrag enthaltenen Angaben.

_____ _____
Ort, Datum Unterschrift des Antragstellers

Datenschutzhinweise:

Allgemeines
Relyens nimmt den Schutz Ihrer personenbezogenen Daten sehr ernst und verpflichtet sich zur Wahrung Ihrer Privatsphäre. Relyens Mutual Insurance Niederlassung Deutschland, handelt als Verantwortliche i.S.d. Datenschutzgrundverordnung (DSGVO EU/2016/679 vom 27. April 2016) und beachtet bei der Verarbeitung Ihrer personenbezogenen Daten die datenschutzrechtlichen Bestimmungen.

Diese Hinweise dienen der umfassenden Information über die Verarbeitung Ihrer personenbezogenen Daten, die wir insbesondere im Rahmen der Erfüllung unserer vertraglichen Verpflichtungen benötigen.

Name und Kontaktdaten des Verantwortlichen
Relyens Mutual Insurance
Niederlassung Deutschland
Königswall 22
44137 Dortmund
Tel : +49 (0) 231 – 534013 0
E-Mail : kontakt@relyens.eu

Kontaktdaten des Datenschutzbeauftragten
Für etwaige datenschutzrechtliche Fragen oder zur Ausübung Ihrer Rechte bezüglich Ihrer personenbezogenen Daten steht der Datenschutzbeauftragte Ihnen unter Angabe Ihrer Identität zur Verfügung:
Relyens Mutual Insurance
Niederlassung Deutschland
Datenschutzbeauftragter
Königswall 22
44137 Dortmund
Email: privacy.de@relyens.eu

Für etwaige Fragen bezüglich Ihres Vertrages wenden Sie sich bitte an Ihren persönlichen Ansprechpartner oder an die allgemeine Kontaktadresse unter: kontakt@relyens.eu

Zweck und Rechtsgrundlage der Datenverarbeitung

Wir verarbeiten Ihre personenbezogenen Daten unter Beachtung der Bestimmungen der EU-Datenschutz-Grundverordnung (DSGVO), des Bundesdatenschutzgesetzes (BDSG) sowie aller weiteren maßgeblichen Gesetze (z.B. Versicherungsaufsichtsgesetz, etc.).

a) Wir verarbeiten Ihre personenbezogenen Daten:

aa) zur Erfüllung des Vertrages (Art. 6 Abs. 1 lit. b DSGVO).
Hiervon sind insbesondere die Risikoeinschätzung vor Abschluss eines Versicherungsvertrages, die Vertragsabschlüsse selbst, die Vertragsverwaltung und das Erbringen unserer Versicherungsleistungen, die Bearbeitung und Regulierung angemeldeter Ansprüche und Beschwerden, sowie die Abwicklung von Schadenfällen betroffen.

bb) zur Wahrung unserer berechtigten Interessen oder die eines Dritten (Art. 6 Abs. 1 lit. f DSGVO).
Dies kann insbesondere der Fall sein:

- zur Gewährleistung der IT-Sicherheit und des IT-Betriebs,
- zur Direktwerbung für Versicherungsprodukte und Dienstleistungen der Unternehmen der Relyens-Gruppe sowie für Markt- und Meinungsumfragen
- zur Verhinderung und Aufklärung von Straftaten (insbesondere Betrug und Versicherungsmissbrauch)
- zur Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche
- im Konzern zu Zwecken der Konzernsteuerung, der internen Kommunikation und sonstiger Verwaltungszwecke

- zur Erstellung von versicherungsspezifischen Statistiken (z.B. für die Entwicklung neuer Produkte und Tarife)
- zur (teilweisen) Weitergabe der versicherten Risiken an Rückversicherer

cc) zur Erfüllung einer rechtlichen Verpflichtung (Art. 6 Abs. 1 lit. c DSGVO).
Da wir als Versicherer diversen rechtlichen Pflichten, insbesondere im Bereich des Aufsichts-, Steuer-, Handels- und Geldwäscherechts unterliegen, müssen wir zur Erfüllung dieser gesetzlichen Pflichten Ihre personenbezogenen Daten verarbeiten.

Darüber hinaus sind wir aufgrund der europäischen Anti-Terrorverordnungen 2580/2001 und 881/2002 verpflichtet, Ihre Daten gegen die sog. „EU-Terrorlisten" abzugleichen, um sicherzustellen, dass keine Gelder oder sonstigen wirtschaftlichen Ressourcen für terroristische Zwecke bereitgestellt werden.

dd) für den Fall Ihrer ausdrücklichen Einwilligung (Art. 6 Abs. 1 lit.a DSGVO) für einen oder mehrere bestimmte Zwecke.

Ein bestimmter Zweck kann z. B. die Durchführung einer Marketingmaßnahme sein. Eine erteilte Einwilligung können Sie jederzeit widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird. Der Widerruf gilt also erst für die Zukunft; Verarbeitungen, die vor dem Widerruf erfolgt sind, sind davon nicht betroffen.

b) Besondere Kategorien personenbezogener Daten (z.B. Gesundheitsdaten) verarbeiten wir nur dann, wenn Sie uns hierzu Ihre ausdrückliche Einwilligung nach Art. 9 Abs. 2 lit. a DSGVO erteilt haben oder ein anderer gesetzlicher Erlaubnistatbestand nach Art. 9 Abs. 2 lit. b bis j DSGVO gegeben ist. Eine erteilte Einwilligung können Sie jederzeit widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird. Der Widerruf gilt also erst für die Zukunft; Verarbeitungen, die vor dem Widerruf erfolgt sind, sind davon nicht betroffen.

Empfänger Ihrer personenbezogenen Daten
Ihre erhobenen personenbezogenen Daten werden im Rahmen des oben beschriebenen Zweckes unseren Mitarbeitern mitgeteilt, die zur Verschwiegenheit und zur Einhaltung der Bestimmungen der Datenschutzgesetze verpflichtet sind. Eine Weitergabe Ihrer personenbezogenen Daten erfolgt an Dritte in folgenden Fällen:

a) Rückversicherer
Wir geben in bestimmten Fällen zum Teil der durch den Vertrag übernommenen Risiken an Rückversicherer weiter. Hier kann es notwendig sein, dem Rückversicherer entsprechende personenbezogene Daten und versicherungstechnische Angaben mitzuteilen, damit sich dieser ein eigenes Bild vom Risiko machen kann.

b) Versicherungsvermittler
Soweit Sie hinsichtlich Ihrer Versicherungsverträge von einem Vermittler betreut werden, verarbeitet ihr Vermittler die zum Abschluss und zur Durchführung des Vertrags benötigten Antrags-, Vertrags- und Schadendaten. Wir übermitteln Ihrem Sie betreuenden Vermittler diese Daten, soweit er diese zur Betreuung und Beratung in Ihren Versicherungsangelegenheiten benötigt.

c) Datenübermittlung an andere Versicherer
In bestimmten Fällen ist es notwendig, dass wir Ihre personenbezogenen Daten an andere Versicherer weitergeben. Dies ist insbesondere der Fall, wenn Sie Ihren Versicherungsvertrag zu einem anderen Versicherer (Nachversicherer) gewechselt haben und es im Rahmen eines Schadenfalls zu Unstimmigkeiten kommen sollte, welcher Versicherer ggf. eintrittspflichtig ist (wir als Vorversicherer oder der Nachversicherer).

d) Externe Dienstleister
Wir bedienen uns zur Erfüllung unserer vertraglichen und gesetzlichen Pflichten zum Teil externer Dienstleister. Der im Internet unter www.relyens.com/de hinterlegten Liste können Sie die einzelnen von uns beauftragten externen Dienstleister entnehmen, zu denen nicht nur vorübergehende Geschäftsbeziehungen bestehen.

e) Zentralisierte Datenverarbeitung innerhalb der Unternehmen der europäischen Relyens-Gruppe

Spezialisierte Unternehmen bzw. Bereiche unserer Unternehmensgruppe nehmen bestimmte Datenverarbeitungsaufgaben für die in der Gruppe verbundenen Unternehmen zentral wahr.
Innerhalb der Unternehmen der Relyens-Gruppe benutzen wir ein zentrales System, in dem Ihre Stammdaten wie Ihre Versicherungsnummer, die Art der Verträge aber auch Ihre allgemeine Antrags-, Vertrags-, und Leistungsdaten gespeichert werden. Die Daten werden aber von den betroffenen Stellen nur sicht- und benutzbar, wenn diese für die Erbringung der Leistungen erforderlich sind. Zum Beispiel verfügt die Gruppe über einzelne Dienstleister wie z. B. in den Bereichen IT und Zahlungssysteme etc., die technisch auf personenbezogene Daten zugreifen können. Eine Aufstellung der unternehmenszugehörigen Dienstleister können Sie auf der Internetseite www.relyens.com/de einsehen.

f) Weitere Empfänger
Darüber hinaus geben wir Ihre personenbezogenen Daten an weitere Empfänger außerhalb der Unternehmensgruppe weiter, soweit dies zur Erfüllung der vertraglichen und gesetzlichen Pflichten notwendig ist. Dies können Behörden (z.B. Finanzbehörden, Strafverfolgungsbehörden), Kreditinstitute zur Abwicklung des Zahlungsverkehrs oder weitere Stellen, für die Sie uns Ihre Einwilligung erteilt haben, sein.
Sofern es zur Vertragsdurchführung erforderlich ist, teilen wir dem Mitversicherten die Daten des Versicherungsnehmers mit.

Quelle und Kategorien personenbezogener Daten, die verarbeitet werden
Grundsätzlich erheben wir personenbezogene Daten direkt beim Betroffenen. In bestimmten Fällen kann es jedoch sein, dass wir personenbezogene Daten von Dritten (Sozialversicherungsträger, Vorversicherer, Hinweis- und Informationssystem des GDV (HIS) etc.) erheben. Zudem verarbeiten wir personenbezogene Daten, die wir aus öffentlich zugänglichen Quellen zulässigerweise gewonnen haben. Wir verarbeiten folgende Datenkategorien:

- Personenstammdaten (wie Vorname, Nachname, Namenszusätze, Geburtsdatum, Familienstand, Staatsangehörigkeit),
- Kontakt-/Kommunikationsdaten (etwa Anschriften, Telefonnummern, E-Mail-Adressen)
- Daten zur Einschätzung des zu versichernden Risikos
- Daten zur Feststellung und Bewertung der Schaden, insbesondere Gesundheitsdaten

Datenübermittlung in Drittstaaten außerhalb der EU
Keine personenbezogenen Daten werden außerhalb der Europäischen Union übermittelt. Soweit ausnahmsweise im Einzelfall eine Datenübermittlung in Drittstaaten erfolgen sollte, wird die Sicherheit und der Schutz der Daten auf der Basis der von der europäischen Kommission erstellten Vertragsklausel-Mustern gesichert.

Dauer der Speicherung
Soweit erforderlich, speichern wir Ihre personenbezogenen Daten für die Dauer unserer Geschäftsbeziehung, die Erfüllung unserer Versicherungsdienstleistungen und den damit verbundenen gesetzlichen Pflichten. Dazu gehören insbesondere die Aufbewahrungs- und Dokumentationspflichten nach dem Handelsgesetzbuch, der Abgabenordnung und dem Geldwäschegesetz (Speicherfristen bis 10 Jahre) sowie Ansprüche, die z. B. der gesetzlichen Verjährungsfrist nach dem Bürgerlichen Gesetzbuch (3 bis 30 Jahre) unterliegen.

Betroffenenrechte
Sie haben uns gegenüber das Recht auf Auskunft nach Art. 15 DSGVO, das Recht auf Berichtigung nach Art. 16 DSGVO, das Recht auf Löschung nach Art. 17 DSGVO, das Recht auf Einschränkung der Verarbeitung nach Art. 18 DSGVO sowie das Recht auf Datenübertragbarkeit (d.h. das Recht des Betroffenen auf Herausgabe der von ihm bereitgestellten personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format nach Art. 20 DSGVO). Beim Auskunftsrecht und beim Löschungsrecht gelten ferner die Einschränkungen nach §§ 34 und 35 BDSG.

Widerspruchsrecht nach Art. 21 DSGVO:
Verarbeiten wir Ihre personenbezogenen Daten zur Wahrung berechtigter Interesse nach Art. 6 Abs. 1 f) DSGVO können Sie dieser Verarbeitung aus Gründen, die sich aus Ihrer besonderen Situation ergeben, jederzeit widersprechen; dies gilt auch für ein auf diese Bestimmung gestütztes Profiling im Sinne von Art. 4 Nr. 4 DSGVO. Wir verarbeiten die personenbezogenen Daten dann nicht mehr, es sei denn, wir können zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die Ihre Interessen, Rechte

und Freiheiten überwiegen oder die Verarbeitung diente der Geltendmachung, Ausübung oder Verteidigung von Rechtsan-sprüchen.

Sofern wir in Einzelfällen Ihre personenbezogenen Daten verarbeiten, um Direktwerbung zu betreiben, haben Sie ebenfalls das Recht, jederzeit Widerspruch gegen die Verarbeitung Ihrer personenbezogenen Daten zum Zwecke derartiger Werbung einzulegen; dies gilt auch für das Profiling (Art. 4 Nr. 4 DSGVO), soweit es mit solcher Direktwerbung in Verbindung steht. Widersprechen Sie der Verarbeitung für Zwecke der Direktwerbung, so werden wir Ihre personenbezogenen Daten nicht mehr für diese Zwecke verarbeiten.

Beschwerderecht
Sofern Sie der Ansicht sind, dass die Verarbeitung Ihrer personenbezogenen Daten gegen geltendes Recht verstößt, bieten wir Ihnen an, sich im Vorfeld an den oben genannten Datenschutzbeauftragten zu wenden. Sie haben jedoch das Recht, sich nach Art. 77 DSGVO bei einer Aufsichtsbehörde zu beschweren.
Sie können die Beschwerde an die für uns zuständige Aufsichtsbehörde richten:

Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen
Kavalleriestr. 2-4
40213 Düsseldorf

Bereitstellung Ihrer personenbezogenen Daten
Die Begründung, Durchführung und Erfüllung des Versicherungsvertrages und die Erfüllung der entsprechenden Leistungen sind ohne die Bereitstellung Ihrer personenbezogenen Daten nicht möglich. Daher ist es erforderlich, dass Sie personenbezogene Daten preisgeben. Ansonsten kann daraus folgen, dass wir z. B. ein Angebot nicht prüfen oder einen Versicherungsvertrag nicht abschließen können oder unsere Leistungsverpflichtung im Rahmen der Schadenbearbeitung nicht nachkommen können.

Automatisierte Entscheidungsfindung (einschließlich Profiling)
Zur Begründung, Durchführung und Abwicklung des Versicherungsvertrages nutzen wir grundsätzlich keine automatisierte Entscheidungsfindung – einschließlich Profiling – gemäß Art. 22 DS-GVO. Sollten wir diese Verfahren in Einzelfällen einsetzen, werden wir Sie hierüber gesondert informieren, sofern dies gesetzlich vorgegeben ist.