DER OPTIMALE KOMPLETTSCHUTZ!

CYBER CRIME. VERSICHERUNG.
ANTRAGSMODELL.

ÖSTERREICH VERSION 09/2020

CYBER CRIME. VERSICHERUNG.
BE SAFE!

BE SAFE!

CYBER CRIME. VERSICHERUNGSSCHUTZ.

DIE HIGHLIGHTS UNSERES VERSICHERUNGSSCHUTZES

CYBER.

HAFTPFLICHTVERSICHERUNG

Versicherungsschutz besteht für Ansprüche Dritter im Zusammenhang mit:

- Dateninfizierungen, -missbrauch, -beschädigung
- Verletzung von Bestimmungen des Datenschutzes
- **Verstöße gegen Geheimhaltungspflichten**
- Rechtsverletzung durch Weitergabe/Veröffentlichung von Informationen oder Medieninhalten
- **Bußgeldern** von Datenschutzbehörden
- Schmerzensgeld aus Verletzungen der Informationssicherheit
- Unzulässigem Zugriff auf versicherte IT-Systeme
- E-Payment inkl. Vertragsstrafen
- Entschädigung mit Strafcharakter
- **Vertragsstrafen**
- **Straf- und Ordnungswidrigkeitsverfahren inkl. Kautionen sowie behördlichen Verfahren**

EIGENSCHADENVERSICHERUNG

Versicherungsschutz für eigene Schäden und Kosten:

- Verletzungen der Informationssicherheit
- Datenmissbrauch und -beschädigung
- fehlerhafte Bedienung und **unvorhergesehene Ausfälle des Computersystems**
- Anordnungen von Datenschutzbehörden
- **Vertragsstrafen**
- **Sachschäden an der Hardware**
- **Verzicht auf den Einwand der groben Fahrlässigkeit**
- **Beweislastumkehr**

Abhängig vom jeweiligen Vorfall werden unter anderem Kosten übernommen im Zusammenhang mit:

- dem Krisenmanagement
- Benachrichtigungspflichten bei Informationssicherheitsverletzungen
- **Kosten einer freiwilligen Anzeige**
- Internen Untersuchungen
- Computer-Forensik
- **Betriebsunterbrechung:** Ertragsausfall und entgangener Betriebsgewinn für bis zu 180 Tage
- der Wiederherstellung von Daten und des Computersystems
- Kreditüberwachungsdienstleistungen
- Sicherheitsanalysen und **Sicherheitsverbesserungen** inkl. Übernahme der **Kosten** für die **Durchführung** der empfohlenen Maßnahmen
- Public-Relation Maßnahmen

CRIME.

VERTRAUENSSCHADENVERSICHERUNG

Versicherungsschutz besteht für unmittelbare Schäden durch Dritte oder kriminelle Mitarbeiter aufgrund von vorsätzlichen unerlaubten Handlungen, die zum Schadenersatz verpflichten, insbesondere alle Vermögensdelikte wie:

- Diebstahl, Raub, Unterschlagung
- Betrug, Untreue
- **fake president fraud**
- **Verzicht auf den Einwand der groben Fahrlässigkeit**

In diesem Zusammenhang besteht auch Versicherungsschutz bei

- **Beschädigung oder Zerstörung von Bargeld oder Wertpapieren**
- **Geheimnisverrat inkl**. dem daraus resultierenden **entgangenem Gewinn**
- **Vertragsstrafen**
- **Mittelbare Schäden / Schäden bei Dritten**

BE SAFE!

Abhängig vom jeweiligen Vorfall leistet der Versicherer unter anderem:

- den Ersatz des Schadens
- Abwehrkosten
- Rechts- und Strafverfolgungskosten
- Anwalts-, Sachverständigen-, Zeugen- und Gerichtskosten
- Kosten bei Rufschädigung
- Kosten bei Verdacht auf Geheimnisverrat

CYBER CRIME. VERSICHERUNGSSCHUTZ.

SOFORTHILFE – SCHADENBEISPIELE

SOFORTHILFE.

ACCENTURE
Rufnummer Österreich: +43 800 909563
Weltweite Rufnummer: +44 1895519407

SOFORTHILFE IM NOTFALL

Unbegrenzter, direkter Zugang zum Krisendienstleister Accenture
Der Versicherer übernimmt im Rahmen der vereinbarten Versicherungsbedingungen die Kosten des Krisendienstleisters für eine erste telefonische Notfall- und Krisenunterstützung, **ohne Anrechnung eines Selbstbehaltes.**
Die vereinbarte Versicherungssumme bleibt ebenfalls unberührt.
Hierunter fällt bei Bestehen einer konkreten Risikolage (z. B. Hacker-Angriff, IT-Ausfall, Verschlüsselung von Daten, Datenmissbrauch) Krisenunterstützung in Form von:

- Experteneinschätzung zur geschilderten Lage,
- Empfehlungen für Sofortmaßnahmen zur Schadenbegrenzung,
- Empfehlungen für Sofortmaßnahmen zur Ursachenermittlung
- Bewertung der bisherigen Maßnahmen

SCHADENBEISPIELE.

FAKE PRESIDENT FRAUD: WENN DIE VORTÄUSCHUNG FALSCHER IDENTITÄTEN ZU ZAHLUNGEN AUF EXTERNE KONTEN FÜHRT

Erst ein imitiertes, vertrauliches Schreiben eines angeblich führenden Organs des versicherten Unternehmens, dann die Aufforderung, eine dringende Überweisung auszuführen – so der Trick der Hacker beim „Fake President Fraud", (dt.: „falscher Chef"). Eine Masche mit fatalen Folgen: Die Überweisung führt meist auf ausländische Konten, hauptsächlich in Asien und Osteuropa. Fliegt der Betrug auf, sind diese meist leergeräumt – eine Rückholung ist aufgrund der ausländischen Rechtssysteme erheblich erschwert.

DIGITALE ERPRESSUNG – RANSOMWARE

Hackern gelingt es, Zugriff auf die Patientendaten eines Allgemeinmediziners zu erlangen. Nachdem die Datenbank erfolgreich kopiert wurde, schreiben sie dem Praxisinhaber per Mail und drohen mit der Veröffentlichung der Anamnesen – inklusive Vermerk, woher die Daten stammen. Gegen Zahlung einer horrenden Geldsumme via Western Union könnte er die Veröffentlichung verhindern.

BE SAFE!

KONTAKTDATEN

AssPro managerline • E-Mail: cyber@apml.at • Website: www.cyberversicherung.eu

CYBER CRIME. VERSICHERUNGSANTRAG.

I. VERMITTLERANGABEN

Vermittlernummer:

Vermittlername:

II. WAS IST DIE HAUPTTÄTIGKEIT DES VERSICHERUNGSNEHMERS?

III. ANGABEN ZUM VERSICHERUNGSNEHMER

Name, Rechtsform

Straße, Nr.

PLZ, Ort

IV. BEGINN DES VERTRAGES

Beginn (Tag/Monat/Jahr):

Hauptfälligkeit entspricht Beginn, abweichende Hauptfälligkeit (Tag/Monat):

Der Beginn darf **maximal 14 Tage** in der Vergangenheit liegen. Versicherungsschutz besteht frei von bekannten Pflichtverletzungen und Versicherungsfällen.

CYBER CRIME. FRAGEBOGEN.

V. RISIKOFRAGEN

1. FINANZKENNZAHLEN	des letzten Geschäftsjahres	aktuell	
a. Umsatz	€	€	
b. Aktueller Umsatzanteil Europa			%
c. Aktueller Umsatzanteil USA/Kanada			%
d. Aktueller Umsatzanteil für ROW (Rest of World)			%
e. Aktueller Umsatzanteil bzgl. E-Commerce			%

2. IST IHR UNTERNEHMEN IN FOLGENDEN RISIKOBEREICHEN TÄTIG?

Airlines, Versorgungsunternehmen (Wasser/ Strom), Hotelketten mit US Präsenz, Banken, Versicherungen, Investmentgesellschaften, Unternehmen des Zahlungsverkehrs, Adult Industries, Glücksspiel, Franchise--unternehmen, Spitäler (ausgenommen Tageskliniken und Ambulatorien) und Behörden (Gemeinden)

○ **NEIN** ○ ja

3. RISIKO-INFORMATIONEN

Sie haben mindestens die folgenden IT-Risikovorkehrungen in Ihrem Unternehmen in Kraft:
Virenschutzprogramme | Firewalls | Regelmäßige Datensicherung

○ **JA** ○ nein

4. RISIKO USA / KANADA

Maximal 25 % Ihres Jahresumsatzes wird in USA / Kanada erzielt und
Sie haben keine Niederlassungen in USA / Kanada

○ **JA** ○ nein

5. KREDITKARTEN

SPEICHERN oder BEARBEITEN Sie über IHRE EIGENE EDV **im Jahr nicht mehr als** 50.000 Kreditkartendaten und bestätigen hiermit, dass Sie die Standards gemäß PCI DSS (Payment Card Industry Data Security Standard) einhalten (sofern Kreditkartendaten vorhanden sind).

○ **JA** ○ nein

6. LÖSEGELD

Wurde in Ihrem Unternehmen eine präventive Beratung anhand eines Sicherheitskonzeptes seitens eines Sicherheitsunternehmen durchgeführt?
(siehe beiliegendes Dokument "Empfehlungen zu IT-Sicherheit" von accenture)

○ **JA** ○ nein

CYBER CRIME. FRAGEBOGEN.

7. SOCIAL ENGINEERING

Voraussetzung für den Versicherungsschutz ist, dass die nachfolgend geforderten Sicherheitsvorkehrungen vor Abschluss dieses Antrages im Unternehmen eingeführt und kommuniziert wurden.

Gibt es für den Bereich Social Engineering Fraud (Betrügerische Nachrichten, Fake Mails) eine Risikomanagementstrategie im Unternehmen und wurden alle Mitarbeiter im Umgang mit betrügerischen Nachrichten (Fake Mails) informiert und sensibilisiert? (Falls nicht, werden diese in den nächsten sechs Monaten verbindlich umgesetzt?)	○ **JA**	○ nein
Werden ungewöhnliche Zahlungsanweisungen, die vorgeblich von Unternehmensleitern / Vorgesetzten erteilt wurden, unter Verwendung der üblichen bekannten Telefonnummern rückbestätigt und auf Authentizität überprüft?	○ **JA**	○ nein
Werden Anfragen zur Verifizierung von Bankdaten / zum Erhalt von Informationen über Bankkonten, die vorgeblich von Bankangestellten kommen, mit Unternehmensleitern / Vorgesetzten besprochen und wird die Authentizität solcher Anfragen unter Verwendung der bekannten Banktelefonnummer bestätigt?	○ **JA**	○ nein
Werden Anweisungen zur Änderung von Bankdaten, die vorgeblich von Lieferanten oder Anbietern erteilt wurden, unter Verwendung der bekannten Telefonnummern rückbestätigt und auf Authentizität überprüft und ist immer die Genehmigung eines Vorgesetzten erforderlich?	○ **JA**	○ nein
Wird das Vieraugenprinzip bei Prüfung der Kontoauszüge eingehalten?	○ **JA**	○ nein

8. SCHADENERFAHRUNG / UMSTANDSMELDUNGEN

Haben sich in der Vergangenheit behördliche Maßnahmen gegen Ihr Unternehmen gerichtet, die im Zusammenhang mit Ihren IT- bzw. Cyberrisiken stehen?	○ **NEIN**	○ ja
Wurde bzw. wird gegen Ihr Unternehmen wegen der Verletzung nationalen oder internationalen IT-Rechts (Dateninfizierungen, Verletzungen von Bestimmungen des Datenschutzes, Verstöße gegen Geheimhaltungspflichten, Rufschädigung, Verletzungen von Persönlichkeitsrechten, Markenrechten oder anderen Formen geistigen Eigentums oder Verstöße gegen Wettbewerbsrecht) behördlich oder strafrechtlich ermittelt?	○ **NEIN**	○ ja
Haben Sie Kenntnis von einem Tatbestand, einer Situation, einem Ereignis oder einer Transaktion, der/die möglicherweise zu einem Schaden im Sinne der beantragten Cyber Crime Versicherung führen könnte?	○ **NEIN**	○ ja
Wurde Ihr Unternehmen in der Vergangenheit Opfer unbefugten Eindringens in die IT, eines Versagens des Betriebes oder eines sonstigen Angriffs auf Ihre IT-Infrastruktur?	○ **NEIN**	○ ja
Sind in den letzten fünf Jahren in Ihrem Unternehmen Vertrauensschäden (Unterschlagung, Diebstahl, Betrug, Sabotage etc.) aufgedeckt worden?	○ **NEIN**	○ ja

CYBER CRIME. VERSICHERUNGSANTRAG.

VI. VERSICHERUNGSSUMMEN UND SELBSTBEHALTE

Die Versicherungssumme steht einmal im Jahr zur Verfügung. Prämie netto zzgl. 11% Versicherungssteuer

Versicherungssumme	500.000	1.000.000	2.000.000	3.000.000	5.000.000	10.000.000
Umsätze in Mio. €						
0 bis 1	1.407	2.010	3.375	4.050	5.263	7.368
1 bis 2,5	1.715	2.450	3.890	4.668	6.066	8.492
2,5 bis 5	2.097	2.996	4.056	4.902	6.372	8.921
5 bis 10	2.854	4.077	5.404	6.671	8.690	12.167
10 bis 25	3.828	4.620	6.740	8.546	11.220	17.160
25 bis 50	4.620	5.280	7.362	9.109	11.880	18.216
50 bis 75	4.700	6.797	8.920	11.011	14.569	20.392
75 bis 100	5.280	7.788	10.709	13.154	17.134	26.268
100 bis x	auf Anfrage	auf Anfrage	auf Anfrage	auf Anfrage	auf Anfrage	auf Anfrage

CYBER CRIME. Selbstbehalt

- € 10.000 je Versicherungsfall
- Bei einer Cyber-Betriebsunterbrechung gilt ein zeitlicher Selbstbehalt von 6 Stunden und eine Haftzeit von 180 Tagen.

Der Selbstbehalt findet **keine** Anwendung auf Abwehrkosten und bei Kosten im Zusammenhang oder aufgrund von Leistungen bei Soforthilfe im Notfall, Kosten für Wiederherstellung, Kosten für Computer-Forensik, Informationskosten, Kosten einer freiwilligen Anzeige, Kosten für Kreditüberwachungsdienstleistungen, vorbeugende Rettungsaufwendungen, Sicherheitsanalyse und Sicherheitsverbesserungen, Kosten für Krisenmanagement und PR-Maßnahmen und E-Discovery (Ziff. I. 2.2., 2.3. und 2.4. AVB)

CYBER CRIME. Sublimits

Als Gesamtleistungsobergrenze je Versicherungsfall und je Versicherungsjahr gilt die ausgewiesene Gesamtversicherungssumme. Je Versicherungsfall und Versicherungsjahr gelten folgende Leistungen bis zu den genannten Leistungsobergrenzen (Sublimits) als versichert:

Vertrauensschäden gemäß (Ziffer I.3. der AVB)	20% der Versicherungssumme
Sachschäden an Hardware (Ziffer I. 2.6. der AVB)	€ 1 Mio., max. in Höhe der Versicherungssumme

CYBER CRIME. VERSICHERUNGSANTRAG.

CYBER CRIME. Versicherungsprämie

Jahresnettoprämie	€	0,00
+ 11% Versicherungssteuer	+ €	0,00
Jahresbruttoprämie	**= €**	0,00

Zahlungsweise: ○ Zahlschein (jährlich) ○ SEPA (beil. Mandatsblatt)

VII. RISIKOTRÄGER

XL Insurance Company SE
Zweigniederlassung für Österreich
Tuchlauben 3, A - 1010 Wien

VIII. EXKLUSIVITÄT

Die vorliegende exklusive AssPro Cyber Crime Versicherung ist nicht übertragbar. Im Fall eines Betreuungswechsels von der Asspro managerline auf Dritte kann der Vertrag nicht über den Vertragsablauf hinaus fortgeführt werden. Der Vertrag wird in diesem Fall zum nächstmöglichen ordentlichen Kündigungstermin aufgehoben.

IX. SCHLUSSERKLÄRUNG

Diese ausgefüllte Erklärung sowie die beigefügten Anlagen werden bei Abschluss eines Vertrages Grundlage und Bestandteil des Versicherungsvertrages. Die Risikoangaben sind vorvertragliche Anzeigen. Hinsichtlich der Folgen bei der Verletzung vorvertraglicher Anzeigepflichten verweisen wir auf die beigefügte Belehrung. Mit Ihrer Unterschrift bestätigen Sie, dass die gemachten Angaben vollständig und richtig sind und dass Sie folgende Dokumente rechtzeitig vor Antragsstellung erhalten und zur Kenntnis genommen haben: AssPro Cyber Crime Bedingungen, Informationspflichten, Belehrung gemäß §§ 16 ff VersVG, Datenschutzhinweis.

Der Unterzeichner bestätigt, dass die in dem Fragebogen abgegebenen Erklärungen und Angaben nach bestem Wissen und Gewissen vollständig und richtig sind und nach Rücksprache mit dem Vorstands- oder Geschäftsführungsgremium oder einer vorhandenen Rechts- oder Versicherungsabteilung beantwortet wurden. Änderungen, die sich nachträglich vor dem Abschluss des Vertrages ergeben, sind dem Versicherer unverzüglich anzuzeigen. Der Unterzeichner weiß, dass seine Angaben Grundlage der Risikobeurteilung des Versicherers sind. Bei Zustandekommen des Vertrages gelten die Angaben als vorvertragliche Angaben im Sinne der §§ 16 ff. Versicherungsvertragsgesetz (VersVG). In Hinsicht auf den Kenntnisstand für die in dem Antrag abgegebenen Erklärungen und Angaben werden keine Angaben bzw. Wissen oder Handlungen, Unterlassungen oder Zusicherungen jeglicher versicherter Personen einer anderen versicherten Person zugerechnet.

Datum	Unterschrift eines Repräsentanten des Unternehmens	Stellung im Unternehmen

EINE VORLÄUFIGE DECKUNG BESTEHT ERST NACH RÜCKBESTÄTIGUNG DURCH ASSPRO!

DRUCKEN | ZURÜCKSETZEN

CYBER CRIME. SEPA-LASTSCHRIFTMANDAT FÜR WIEDERKEHRENDE ZAHLUNGEN.

AssPro managerline GmbH | Augustinusstraße 11c | 50226 Frechen
Gläubiger-Identifikations-Nummer **DE05ZZZ00000073987**

Ich ermächtige / wir ermächtigen die AssPro managerline GmbH, wiederkehrende Zahlungen von meinem / unserem Konto mittels Lastschrift einzuziehen.
Zugleich weise ich / weisen wir mein / unser Kreditinstitut an, die von der AssPro managerline GmbH von meinem / unserem Konto gezogenen Lastschriften einzulösen.

HINWEIS: Ich kann / wir können innerhalb von acht Wochen, beginnend mit dem Belastungsdatum, die Erstattung des belasteten Betrages verlangen. Es gelten dabei die mit meinem / unserem Kreditinstitut vereinbarten Bedingungen.

Versicherungsnehmer

Kontoinhaber – wenn abweichend zum Versicherungsnehmer

Straße, Hausnummer

PLZ, Ort

Bitte unbedingt ausfüllen:

BIC __ __ __ __ __ __ __ __ | __ __ __
8 oder 11 Stellen

IBAN __ __ __ __ | __ __ __ __ | __ __ __ __ | __ __ __ __ | __ __ __ __ | __ __

Zahlungsweise: ○ Jährliche Zahlung ○ Halbjährliche Zahlung (3% Zuschlag)

Jahresbruttoprämie bei jährlicher Zahlung	= €	0,00
Jahresbruttoprämie inklusive 3 % Zuschlag bei halbjährlicher Zahlung	= €	0,00

Im Falle einer Rücklastschrift, die mangels Deckung oder Angabe einer falschen Kontoverbindung erfolgt ist, darf der Zahlungsempfänger dem Zahlungspflichtigen die tatsächlichen Kosten für die Lastschriftrückbuchung im Sinne eines Schadenersatzes in Rechnung stellen.

Datum, Ort und Unterschrift / Firmenstempel des Kontoinhabers

Die Informationen zum Datenschutz gemäß Art. 13 und 14 DSGVO finden Sie unter
https://www.asspromanagerline.at/de/impressum-datenschutz/datenschutzerklaerung.pdf

XL Insurance Company SE

Informationsblatt zur CYBER – CRIME - VERSICHERUNG

ACHTUNG:
Hier finden Sie nur ausgewählte Informationen in vereinfachter Form, um Ihnen einen Überblick zu geben. Alle vorvertraglichen und vertraglichen Informationen über das Produkt finden Sie im Versicherungsantrag, in der Versicherungspolizze und in den Versicherungsbedingungen.

Um welche Versicherung handelt es sich: **CYBER – CRIME – Versicherung**

Was ist versichert?

Die Versicherung umfasst im Rahmen der vereinbarten Versicherungssumme(-n)

Cyberversicherung:

- ✓ Haftpflichtansprüche gegen Versicherte aus Datenschutz-, Vertraulichkeits-, Netzwerksicherheitsverletzungen, rechtswidriger Kommunikation oder aus Vertragsstrafen wegen Verletzung von Datensicherheitsstandards in Form der Prüfung der Haftung, der Erfüllung von gerechtfertigten Haftpflichtansprüchen oder der Übernahme der Kosten der Abwehr unberechtigter Ansprüche
- ✓ Eigenschäden des Versicherungsnehmers aus Betriebsunterbrechungsschäden und den notwendigen Wiederherstellungsaufwand
- ✓ den Ersatz von Kosten aus Datenschutzverfahren des Versicherungsnehmers
- ✓ den Ersatz von Kosten aus Krisenmanagement des Versicherungsnehmers
- ✓ den Ersatz von Kosten aus Datenerpressung sowie zu zahlende Lösegelder

Vertrauensschadenversicherung (Crime):

- ✓ Schäden durch vorsätzlich unerlaubte Handlungen von Mitarbeitern, auch wenn diese Dritten zugefügt wurden und Sie für den von Ihrem Mitarbeiter verursachten Schaden haften.
- ✓ Schäden, die Ihnen von Dritten durch vorsätzlich unerlaubte Handlungen unmittelbar zugefügt wurden, sofern diese Handlungen eine Täuschung beinhalten.
- ✓ Schäden durch Geheimnisverrat

Die Versicherungssummen vereinbaren wir mit Ihnen im Versicherungsvertrag.

Was ist nicht versichert?

Allgemeine Ausschlüsse

- x vorsätzlich und rechtswidrig herbeigeführte Schäden
- x Schäden aufgrund vertraglich übernommener Haftungen
- x Schäden wegen der Verletzung von Patentrechten sowie des Missbrauchs von Patenten, wegen der Verletzung von Betriebs- oder Geschäftsgeheimnissen sowie Vorschriften des Kartellrechts.
- x Schäden aufgrund von oder im Zusammenhang mit Krieg und hoheitlichen Eingriffen, mit Naturgefahren, mit Kernenergie oder radioaktiven Substanzen sowie mit Umweltschäden
- x Schäden aufgrund von oder im Zusammenhang mit jedweder Form von Finanztransaktionen, Lizenzen, Wertpapierrechtsverstößen
- x Schäden aufgrund oder im Zusammenhang mit Glückspiel
- x Schäden im Zusammenhang mit Personenschäden

Ausschlüsse für die Vertrauensschadenversicherung

- x Schäden die durch fahrlässige Handlungen verursacht werden
- x Mittelbare Schäden
- x Schäden die von Anteilseignern mit mehr als 30% Anteilsbesitz verursacht wurden

Gibt es Deckungsbeschränkungen?

Die Leistungen des Versicherers sind

- ! pro Versicherungsfall begrenzt mit der vereinbarten Versicherungssumme bzw. den vereinbarten Sublimits sowie mit dem vereinbarten Selbstbehalt.
- ! für alle innerhalb eines Versicherungsjahres eingetretenen Versicherungsfälle begrenzt mit der in der Versicherungspolizze vereinbarten Versicherungssumme.

Bei Verletzung der vertraglichen Verpflichtungen Entfällt der Versicherungsschutz ganz oder teilweise.

Darüber hinaus gelten beispielsweise folgende wichtige Deckungsbeschränkungen:

- ! In der Versicherungspolizze angeführte Nachmeldefristen
- ! Internationale Sanktionen und Embargos können die Deckung beschränken

Wo bin ich versichert?

✓ Der Versicherungsschutz besteht weltweit.

Welche Verpflichtungen habe ich?

- Der Versicherer ist vor Abschluss des Vertrages, aber auch während der Laufzeit über das versicherte Risiko vollständig und wahrheitsgemäß zu informieren.
- Die Versicherungsprämien sind fristgerecht zu zahlen.
- Das versicherte Risiko darf nach Abschluss des Versicherungsvertrages nicht erheblich vergrößert oder erweitert werden. Eine dennoch eingetretene Gefahrerhöhung ist dem Versicherer zu melden.
- Dem Versicherer sind Versicherungsfälle oder Schäden, die Geltendmachung von Ansprüchen und die Einleitung eines verwaltungsbehördlichen oder gerichtlichen Strafverfahrens unverzüglich in Textform zu melden. Bei der Feststellung und Erledigung oder Abwehr des Schadens ist mitzuwirken (z.B.: Erteilung von Auskünften und Überlassung von Originalbelegen).
- Es müssen alle Maßnahmen getroffen werden, um den Schaden und dessen Folgen so gering wie möglich zu halten.
- Geltend gemachte Ansprüche dürfen nicht anerkannt werden. Wenn Ansprüche gerichtlich geltend gemacht werden, müssen alle Weisungen des Versicherers befolgt und dem vom Versicherer beauftragten Anwalt Vollmacht erteilt werden.
- Wenn die Versicherungsprämie auf Basis des Umsatzes bemessen wird, ist der Versicherer wahrheitsgemäß zu informieren.

Wann und wie zahle ich?

Die Prämie ist jährlich während der Vertragsdauer und im Vorhinein zu bezahlen. Eine halbjährliche Zahlungsweise und die Zahlungsart (z.B.: Zahlungsanweisung per Zahlschein oder online, SEPA-Mandat) können vereinbart werden.

Wann beginnt und endet die Deckung?

- Der Beginn des Vertrages und der Deckung ist in der Versicherungspolizze angegeben. Voraussetzung ist, dass die Zahlung der ersten Versicherungsprämie rechtzeitig und vollständig erfolgt.
- Der Vertrag und die Deckung enden durch Kündigung durch den Versicherer oder den Kunden.
- Beträgt die vereinbarte Vertragsdauer weniger als 1 Jahr, endet der Vertrag ohne das es einer Kündigung bedarf.

Wie kann ich den Vertrag kündigen?

- Unternehmer können Verträge zum Ende der in der Versicherungspolizze angeführten Vertragslaufzeit mit einer Kündigungsfrist von drei Monaten kündigen.
- Darüber hinaus kann der Vertrag aus weiteren Gründen, z.B. nach Eintritt des Versicherungsfalls, vorzeitig gekündigt werden.

XL Insurance Company SE
Tuchlauben 3, 1010 Wien, Österreich

Telephone: +43 1 50602 102 Fax: +43 1 50602 111 axaxl.com

XL Insurance Company SE, Zweigniederlassung für Österreich
Handelsgericht Wien, FirmenbuchNr: FN 176093k, DVR: 0977659, Bank: Citibank, Swift Code: CITIATWX, IBAN: AT07 1814 0000 0194 3006, UID-#: AT U4626 7908
Hauptsitz der Gesellschaft: 8 St. Stephen´s Green, Dublin 2, Ireland
XL Insurance Company SE
A European public limited liability company registered in Ireland
Registered in Ireland No. 641686 | Regulated by the Central Bank of Ireland | Directors: P.R. Bradbook (UK), B.R.P. Joseph (UK), Y. Slattery, P. Wilson (UK),
D. Palici-Chehab (FR), J. O´Neill, H. Browne, P.H. Rastoul (FR)

accenture

Empfehlungen zu IT-Sicherheit (Mindest-) Standards

IT-Sicherheits-Strategie

Umsetzung und Dokumentation einer IT-Sicherheits-Strategie, um alle notwendigen IT-Sicherheits-Anforderungen konkret zu definieren und strategische Anforderungen zu beschreiben.

IT Governance und Organisation

Implementation einer IT-Sicherheitsorganisationsstruktur (Organigramm, RACI Matrix) mit Definition von notwendigen Aufgaben, Rollen und Verantwortlichkeiten (z.B. IT-Sicherheitsbeauftragter, IT Risk Manager, IT Compliance Manager, IT-Sicherheitsgremium) sowie Reporting-strukturen.

Training und Awareness

Ein Schulungskonzept zum Thema IT-Sicherheit sollte im Einklang mit den Sicherheitsrichtlinien erarbeitet und regelmäßig auf Basis von gewonnenen Erkenntnissen aus ua. Informationssicherheits-Vorfällen aktualisiert werden.

IT-Risikomanagement

Die Erstellung einer IT-Risikomanagement-struktur mit Risikomanagementlebenszyklus und -prozess sowie einem Behandlungsplan zur Überwachung und Reporting von IT-Risiken sollte durchgeführt werden.

Benutzer- und Berechtigungsmanagement

Erstellung der notwendigen Prozesse für Benutzer- und Berechtigungsmanagement unter Berücksichtigung von IT-Sicherheitsprinzipien, wie z.B. Aufgabentrennung (Segregation of Duties), geringsten Rechte (Principle of Least Privilege) und “Kenntnis nur bei Bedarf“ (Need to Know).

IT Betriebskontinuitäts-Management und Notfallplanung

Umsetzung angemessener Vorkehrungen, um die Kontinuität und Ordnungsmäßigkeit der IT-unterstützenden Tätigkeiten im Unternehmen zu gewährleisten.

Updates und Sicherheitspatches

Update und Sicherheitspatches sollten zeitnah eingespielt werden. Es wird empfohlen, das Patchmanagement und der dafür notwendige Prozess unter Einbezug jeglicher Software (inkl. Firmware) zu definieren.

Backup / Datensicherungen

Ein Datensicherungskonzept sollte vorhanden und umgesetzt sein. Eine mögliche Manipulation der Sicherungskopien sollte mittels technischer Maßnahmen (z.B. für den Fall einer Ransomeware-Attacke) verhindert werden.

Protokollierung und Überwachung

Festlegung von Prozessen für die regelmäßige Aufzeichnung von Ereignissen in den IT-Systemen (Benutzeraktivitäten, Fehler, Sicherheitsereignis, Administratoraktivitäten, ...) und für die sichere Aufbewahrung der Log- und Protokolldateien zum Schutz vor Manipulation und unerlaubtem Zugriff.

Kommunikationssicherheit

Mobile Datenträger (z.B. Mobilgeräte) sollten entsprechend gesichert, verschlüsselt und mithilfe von Passwörtern geschützt werden. Maßnahmen zum Umgang und zur Entsorgung von Datenträgern sollten definiert sein. Firmenserver sollten mit einer Firewall geschützt sein.

Weiterführende Informationen zum Thema IT-Sicherheit

- Finanzmarktaufsichtsbehörde (FMA) Leitfäden zum Thema IT-Sicherheit https://www.fma.gv.at/fma/fma-leitfaeden/
- Wirtschaftskammer Österreich (WKO) https://www.wko.at/service/innovation-technologie-digitalisierung/it-sicherheit-datensicherheit.html
- IKT-Sicherheitsportal Österreich https://www.onlinesicherheit.gv.at/
- Gesamtverband der Deutschen Versicherungswirtschaft e.V. (Der GDV) https://www.gdv.de/de/themen/schwerpunkte/cybersecurity
- Allianz für Cyber-Sicherheit https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Informationspool/ErsteSchritte/Erste_Schritte_node.html
- Bundesamt für Sicherheit in der Informationstechnik https://www.bsi.bund.de/DE/Home/home_node.html

Copyright © 2020 Accenture. All Rights Reserved.

Weitere Details - Empfehlungen zu IT-Sicherheit (Mindest-)Standards

IT-Sicherheits-Strategie

Diese sollte diverse strategische Sicherheits-Anforderungen beschreiben, wie zum Beispiel die Steuerung der IT-Sicherheit sowie Definitionen von Grundsatzstrategien zu den Themen der IT-Landschaft, IT-Notfallpläne und Lebenszyklusmanagement. Die IT Sicherheits-Strategie sollte unter Einbindung aller relevanten Stakeholder in regelmäßigen Abständen diskutiert und auf Aktualität sowie Erreichung überprüft werden.

IT Governance und Organisation

Erstellung und Implementierung einer IT-Sicherheitsorganisationsstruktur (Organigramm, RACI Matrix), Definition von notwendigen Aufgaben, Rollen und Verantwortlichkeiten (z.B. IT-Sicherheitsbeauftragter, IT Risk Manager, IT Compliance Manager, IT-Sicherheitsgremium) sowie Reportingstrukturen. Bei der Definition der Aufgaben, Rollen und Verantwortlichkeiten sollte auf Interessenskonflikte geachtet und nach dem Prinzip „Segregation of Duties“ gehandelt werden.

Training und Awareness

Ein Schulungskonzept zum Thema IT-Sicherheit sollte im Einklang mit den Sicherheitsrichtlinien erarbeitet und regelmäßig auf Basis von gewonnenen Erkenntnissen aus ua. Informationssicherheitsvorfällen aktualisiert werden. Hierbei können die Schulungen auf unterschiedlichen Kanälen wie Vorträge, Online Trainings, Selbststudium oder Kampagnen (z.B. Phishing-Nachrichten) durchgeführt werden. Schulungen sind nach dem Schulungskonzept in regelmäßigen Abständen durchzuführen. Empfohlen wird nicht nur die einführende Einschulung rasch nach dem Dienstantritt, sondern auch die regelmäßige Weiterbildung.

IT Risikomanagement

Die Erstellung einer IT-Risikomanagementstruktur mit Risikomanagementlebenszyklus und -prozess sowie einem Behandlungsplan zur Überwachung und Reporting von IT-Risiken sollte durchgeführt werden. IT-Risiken sollten entsprechend analysiert und behandelt werden, um mögliche negative Auswirkungen auf den IT-Betrieb und die operativen Kernprozesse des Unternehmens rechtzeitig zu erkennen und zu beheben. Weiters sollten IT-Risiken in den IT-abhängigen Kernprozessen im unternehmensweiten Risikomanagementprozess entsprechend berücksichtigt werden.

Benutzer- und Berechtigungsmanagement

Erstellung der notwendigen Prozesse für Benutzer- und Berechtigungsmanagement unter Berücksichtigung von IT-Sicherheitsprinzipien, wie z.B. Aufgabentrennung (Segregation of Duties), geringsten Rechte (Principle of Least Privilege) und “Kenntnis nur bei Bedarf“ (Need to Know).

Folgende Punkte sollten ua dabei berücksichtigt werden:

IT-Administrator einrichten, sparsam nutzen und für die tägliche Arbeit einen Zugang mit weit weniger Rechten nutzen

Individuelle Mitarbeiterzugänge einrichten und keine „Sammeluser“ verwenden (eigenen Benutzeraccount mit eigenem Passwort für jeden Mitarbeiter)

Komplexe Passwörter erzwingen (z.B. empfohlen min. 10 Zeichen, Sonderzeichen, Zahlen, Groß- und Kleinschreibung, …)

Die Authentifizierung von Benutzern muss auf sicheren Login Prozeduren basieren. Remote-Zugriffe sollten besonders abgesichert werden, wie zum Beispiel mittels Zwei-Faktor-Authentifizierung

IT Betriebskontinuitäts-Management und Notfallplanung

Umsetzung angemessener Vorkehrungen, um die Kontinuität und Ordnungsmäßigkeit der IT-unterstützenden Tätigkeiten im Unternehmen zu gewährleisten.

Folgende Punkte sollten ua dabei berücksichtigt werden:

- Erstellung eines unternehmensweiten Notfallplans, der alle relevanten Bedrohungsszenarien berücksichtigt und auf Basis einer Risikoanalyse ausgearbeitet wird
- Erarbeitung und Dokumentation der Reaktion auf diese Risiken; Festlegen von Maßnahmen, um den Risiken entgegenwirken zu können (siehe IT Risikomanagement)
- Entwicklung eines operativen Notfallplans unter Berücksichtigung der Szenarien aus der Risikoanalyse sowie Definition der Verantwortlichen für die jeweiligen Notfallszenarien
- Festlegung eines Prozesses zur Durchführung und Dokumentation von regelmäßigen Tests des Notfallplans
- Festlegung eines Prozesses für die laufende Weiterentwicklung des Notfallplans

Copyright © 2020 Accenture. All Rights Reserved.

Updates und Sicherheitspatches

Update und Sicherheitspatches sollten zeitnah eingespielt werden. Es wird empfohlen, das Patchmanagement und der dafür notwendige Prozess unter Einbezug jeglicher Software (inkl. Firmware) zu definieren.

Der Patchmanagement Prozess für IT-Systeme sollte ua beinhalten:

- Dokumentation (Test) von Updates und Patches
- Regelmäßige Überprüfung der Aktualität und Verteilung von Updates und Patches
- Programme (z.B. Antivirus) auf dem neuesten Stand halten
- Automatisierte Benachrichtigungen durch Hersteller einzurichten

Backup / Datensicherungen

Ein regelmäßiges (je öfter Daten gesichert werden, desto besser) Datensicherungskonzept sollte vorhanden und umgesetzt sein. Eine mögliche Manipulation der Sicherungskopien sollte mittels technischer Maßnahmen (z.B. für den Fall einer Ransomeware Attacke) verhindert werden. Sicherungskopien sollten in regelmäßigen Abständen getestet werden.

Protokollierung und Überwachung

Festlegung von Prozessen für die regelmäßige Aufzeichnung von Ereignissen in den IT-Systemen (Benutzeraktivitäten, Fehler, Sicherheitsereignis, Administratoraktivitäten, ...) und für die sichere Aufbewahrung der Log- und Protokolldateien zum Schutz vor Manipulation und unerlaubtem Zugriff.

Kommunikationssicherheit

Mobile Datenträger (z.B. Mobilgeräte) sollten entsprechend gesichert, verschlüsselt und mithilfe von Passwörtern geschützt werden. Maßnahmen zum Umgang und zur Entsorgung von Datenträgern sollten definiert sein. Darüber hinaus sollten die Daten auf Handys oder Laptops aus der Ferne gelöscht werden können. Firmenserver sollten mit einer Firewall geschützt sein. Um unberechtigten Zugriff und Sicherheitsvorfälle im Netzwerk erkennen zu können, sollte eine entsprechende Software und technische Maßnahmen zur Sicherheitsüberwachung (Monitoring, Angriffserkennung, Intrusion Detection, ...) definiert und umgesetzt werden.

Copyright © 2020 Accenture. All Rights Reserved.

Copyright © 2020 Accenture
All rights reserved.

Accenture, its logo, and
High Performance Delivered
are trademarks of Accenture.

Informationen zur Verarbeitung Ihrer Daten

Mit diesen Hinweisen informieren wir Sie über die Verarbeitung Ihrer personenbezogenen Daten durch AXA XL und die Ihnen nach dem Datenschutzrecht zustehenden Rechte.

Diese Informationen gelten auch für die versicherte Person. Wenn die versicherte Person nicht zugleich Versicherungsnehmer ist, wird der Versicherungsnehmer diese Informationen an die versicherte Person weitergeben.

Darüber hinaus gelten diese Informationen auch für beteiligte berechtige Dritte (z. B. gesetzliche Vertreter, Bevollmächtigte, etc.) an die der (potentielle) Kunde diese Informationen weitergeben wird.

Verantwortlicher für die Datenverarbeitung

XL Insurance Company SE
AXA XL – A Division of AXA

8 St Stephen's Green
Dublin 2
D02 VK30
Irland

Tel.: +353 1 607 5300
Fax: +353 1 607 5333

(Adresse der XL Insurance Company SE - Zweigniederlassung für Österreich: Tuchlauben 3, 1010 Wien)

Unseren **Datenschutzbeauftragten** erreichen Sie per Post unter den im Dokument angegebenen Adressen mit dem Zusatz „– DPO –“ oder per E-Mail unter: legalcompliance@axaxl.com

Zwecke und Rechtsgrundlagen der Datenverarbeitung

Wir verarbeiten Ihre personenbezogenen Daten unter Beachtung der EU-Datenschutz-Grundverordnung (DSGVO), des Datenschutzgesetzes (DSG), der datenschutzrechtlich relevanten Bestimmungen des Versicherungsvertragsgesetzes (VersVG), sowie aller weiteren maßgeblichen Gesetze.

Stellen Sie einen Antrag auf Versicherungsschutz, benötigen wir die von Ihnen hierbei gemachten Angaben für den Abschluss des Vertrages und zur Einschätzung des von uns zu übernehmenden Risikos. Kommt der Versicherungsvertrag zustande, verarbeiten wir diese Daten zur Durchführung des Vertragsverhältnisses, z.B. zur Policierung oder Rechnungsstellung.

Für den Fall, dass Sie einen Schaden melden oder Schadensersatzansprüche geltend machen, benötigen wir die angegebenen personenbezogenen

Fair Processing Notice

By means of this privacy notice, we inform you about the processing of your personal data by AXA XL and the rights that have been granted to you in accordance with the applicable data protection legislation.

This information is also applicable in relation to the insured person. Where the insured person is not also the policyholder, the policyholder shall forward this information to the insured person.

In addition, this information also applies to third parties (e.g. legal representatives, plenipotentiaries, etc.) which have been authorised by the customer and to which this information has been forwarded.

Data Controller responsible for the Processing of your Personal Data

XL Insurance Company SE
AXA XL – A Division of AXA

8 St Stephen's Green
Dublin 2
D02 VK30
Eire

Tel.: +353 1 607 5300
Fax: +353 1 607 5333

(Address of XL Insurance Company SE Austrian Branch: Tuchlauben 3, 1010 Vienna, Austria)

You may contact our **Data Protection Officer** by post at the addresses given in the document by adding "- DPO -" to the address or via e-mail at: legalcompliance@axaxl.com

Purpose and Legal Basis of the Data Processing

We process your personal data in compliance with the EU General Data Protection Regulation (GDPR), the Austrian Data Protection Act (DSG), the applicable provisions affecting or ensuring data privacy within the Insurance Act (VersVG), as well as all other applicable laws.

When applying for an insurance contract, we require your personal information to conclude the contract and to assess the risks that would be assumed by us. Once the contract has been concluded, the personal data is processed within the performance of the contractual relationship, e.g. for policing or invoicing.

In the event you report or assert a claim, we need the personal information provided to assess our

Daten, um unsere Eintrittspflicht zu überprüfen sowie die Höhe der zu zahlenden Entschädigung zu ermitteln.

Der Abschluss und die Durchführung des Versicherungsvertrages oder die Bearbeitung eines Schadenfalls ist ohne die Verarbeitung Ihrer personenbezogenen Daten nicht möglich. Ihre personenbezogenen Daten benötigen wir auch für die Erstellung eines Angebots.

Darüber hinaus benötigen wir Ihre personenbezogenen Daten zur Erstellung von versicherungsspezifischen Statistiken, z. B. für die Entwicklung neuer Tarife oder zur Erfüllung aufsichtsrechtlicher Vorgaben. Die Daten aller mit einer AXA-Gesellschaft bestehenden Verträge nutzen wir für eine Betrachtung der gesamten Kundenbeziehung, beispielsweise zur Beratung hinsichtlich einer Vertragsanpassung, -ergänzung, für Kulanzentscheidungen oder für umfassende Auskunftserteilungen.

Rechtsgrundlage für diese Verarbeitungen personenbezogener Daten für vorvertragliche und vertragliche Zwecke und die Schadenbearbeitung ist Art. 6 Abs. 1 b) DSGVO. Soweit dafür besondere Kategorien personenbezogener Daten erforderlich sind, holen wir Ihre Einwilligung nach Art. 9 Abs. 2 a) i. V. m. Art. 7 DSGVO ein. Erstellen wir Statistiken mit diesen Datenkategorien, erfolgt dies auf Grundlage von Art. 9 Abs. 2 j) DSGVO i. V. m. § 7 DSG.

Ihre Daten verarbeiten wir auch, um berechtigte Interessen von uns oder von Dritten zu wahren. Rechtsgrundlage dafür ist Art. 6 Abs. 1 f) DSGVO. Dies kann insbesondere erforderlich sein:

- zur Gewährleistung der IT-Sicherheit und des IT-Betriebs einschließlich Tests (sofern nicht bereits für die Vertragsdurchführung oder zur Erfüllung einer gesetzlichen Verpflichtung erforderlich),
- zur Werbung für unsere eigenen Versicherungsprodukte und für andere Produkte der AXA-Unternehmensgruppe und deren Kooperationspartner sowie für Markt- und Meinungsumfragen, soweit Sie der Nutzung Ihrer Daten dafür nicht widersprochen haben,
- zur Verhinderung und Aufklärung von Straftaten, soweit dies nicht bereits Gegenstand einer gesetzlichen Verpflichtung ist; hierbei nutzen wir insbesondere Datenanalysen und –recherchen (auch in öffentlich zugänglichen Quellen) zur Erkennung von Hinweisen, die auf Versicherungsmissbrauch hindeuten können,

obligation and to determine the amount of compensation to be paid.

The conclusion or the performance of the insurance contract, as well as the processing of a claim, are not possible without processing your personal data. This applies also to quotation purposes.

We also require your personal data to compile statistics that are specific to the insurance industry, for instance to develop new pricing models or to fulfil regulatory requirements. We use the data contained in all contracts entered into with an AXA company to review the entire customer relationship, for instance to advise on policy adjustments, additions, for goodwill decisions or to provide complete information

Legal basis for the processing of personal data for pre-contractual and contractual purposes and the handling of claims is Article 6 (1) (b) GDPR. Where special categories of personal data (e.g. your health data) are required for this purpose, we will obtain your consent in accordance with Article 9 (2) (a) in conjunction with Article 7 GDPR. Where we use these data categories to compile statistics, we do so in accordance with Article 9 (2) (j) GDPR in conjunction with Section 7 DSG

Moreover, we process your personal data to protect our legitimate interests or the legitimate interests of third parties. The legal basis thereof is Art. 6 paragraph 1 (f) GDPR. This may be particularly necessary in the following cases:

- to guarantee IT security and IT operations including testing (where not required for the performance of the contract already),
- for the marketing of our insurance products and other products by AXA Group companies and their cooperation partners, as well as for market surveys and opinion polls, unless you have objected to the use of your data for this purpose,
- for the prevention and prosecution of criminal offenses, unless this is already subject to a statutory obligation; in particular, we use data analysis and research (also in publicly accessible sources) to detect indications of insurance fraud,

- zur Risikosteuerung innerhalb der AXA XL sowie der AXA-Unternehmensgruppe insgesamt,
- zur Geschäftssteuerung und Weiterentwicklung von Prozessen, Dienstleistungen und Produkten.

Darüber hinaus verarbeiten wir Ihre personenbezogenen Daten zur Erfüllung gesetzlicher Verpflichtungen wie z. B. aufsichtsrechtlicher Vorgaben, handels- und steuerrechtlicher Aufbewahrungspflichten oder unserer Beratungspflicht. Als Rechtsgrundlage für die Verarbeitung dienen in diesem Fall die jeweiligen gesetzlichen Regelungen i. V. m. Art. 6 Abs. 1 c) DSGVO.

Sollten wir Ihre personenbezogenen Daten für einen oben nicht genannten Zweck verarbeiten wollen, werden wir Sie im Rahmen der gesetzlichen Bestimmungen darüber u.a. auf unserer Webseite https://axaxl.com/de-at/privacy-notice zuvor informieren.

Daten und Datenkategorien

Wir verarbeiten insbesondere folgende Daten und Datenkategorien:

- Stamm- und Vertragsdaten (z.B. Name, Adresse, Kontaktdaten, Familienstand, Beruf, Beginn- und Ablaufdaten, Angaben zum zu versichernden Risiko)
- Besondere personenbezogene Daten (z.B. Gesundheitsdaten)
- Informationen über persönliche Situationen (z.B. Sachwerte)
- Daten zu Ihren Schäden und andere Daten aus der Erfüllung unserer rechtlichen Verpflichtungen
- Daten zu Kontakten zu Ihnen und zur Vorgangsbearbeitung
- Rollen der Betroffenen (z.B. Versicherungsnehmer, versicherte Person, Geschädigter, Zeuge)
- Vollmachten
- Interessentendaten

Kategorien von Empfängern der personenbezogenen Daten

Rückversicherer:

Von uns übernommene Risiken versichern wir bei speziellen Versicherungsunternehmen (Rückversicherer). Dafür kann es erforderlich sein, Ihre Vertrags- und ggf. Leistungs-/ Schadendaten an einen Rückversicherer zu übermitteln, damit dieser

- for risk management within AXA XL and the AXA Group as a whole,
- for business management and the improvement of processes, services and products.

In addition, we process your personal data for the fulfilment of legal obligations such as regulatory requirements, storage periods required under commercial and fiscal law or for the fulfilment of our advisory duties. The basis for processing in this case are the applicable statutory provisions in conjunction with Article 6 (1) (c) GDPR.

Where we wish to process your personal data for a purpose not mentioned above, we will inform you in advance within the framework of our legal obligations, including on our website https://axaxl.com/de-at/privacy-notice.

Data and data categories

We process, particularly the following data and data categories:

- Master and contract data (e.g. name, address, contact details, marital status, occupation, start and expiry dates, details of the risk to be insured)
- Special categories of personal data (e.g. health data, personal data)
- Information about personal situations (e.g. creditworthiness data, material assets)
- Data on your claims and other data arising from the fulfilment of our legal obligations
- Data on contacts to you and on transaction processing
- Roles of the data subjects (e.g. policyholder, insured person, injured party, witness)
- Powers of attorney
- Data of prospects

Categories of recipient of the personal data

Reinsurers:

We insure the risks we accept with special insurance companies (reinsurers). It may be necessary to submit your contract and possibly your benefit/claim data as well to a reinsurer so that it may form its own opinion of the risk or the claim. We may also obtain

sich ein eigenes Bild über das Risiko oder den Versicherungsfall machen kann. Darüber hinaus ist es möglich, dass der Rückversicherer AXA XL aufgrund seiner besonderen Sachkunde bei der Risiko- oder Leistungsprüfung sowie bei der Bewertung von Verfahrensabläufen unterstützt. Wir übermitteln Ihre Daten an den Rückversicherer nur soweit dies für die Erfüllung unseres Versicherungsvertrages mit Ihnen erforderlich ist bzw. im zur Wahrung unserer berechtigten Interessen erforderlichen Umfang.

advice from the reinsurer AXA XL based on its particular expertise in risk or benefit assessment or in the evaluation of procedural matters. We only transmit your data to the reinsurer where it is necessary for the performance of our insurance contract with you, i.e. in the extent that is required to protect our legitimate interests.

Vermittler:

Soweit Sie hinsichtlich Ihrer Versicherungsverträge von einem Vermittler betreut werden, verarbeitet Ihr Vermittler die zum Abschluss und zur Durchführung des Vertrages benötigten Antrags-, Vertrags- und Schadendaten. Auch übermittelt AXA XL diese Daten an die Sie betreuenden Vermittler, soweit diese die Informationen zu Ihrer Betreuung und Beratung in ihren Versicherungs- und Finanzdienstleistungsangelegenheiten benötigen.

Intermediaries:

Where you receive assistance from an intermediary regarding your insurance contracts, your intermediary will process the application, contract and loss data required to conclude and perform the contract. AXA XL also transmits this data to the intermediaries who are responsible for you, insofar as they require the information for your support and advice in their insurance and financial services matters.

Datenverarbeitung innerhalb der AXA Unternehmens-gruppe:

Spezialisierte Unternehmen bzw. Bereiche unserer Unternehmensgruppe nehmen bestimmte Datenverarbeitungsaufgaben für die in der Gruppe verbundenen Unternehmen zentral wahr. Soweit ein Versicherungsvertrag zwischen Ihnen und einem oder mehreren Unternehmen unserer Gruppe besteht, können Ihre Daten etwa zur zentralen Verwaltung von Anschriftendaten, für den telefonischen Kundenservice, zur Vertrags- und Leistungs-/ Schadenbearbeitung, für In- und Exkasso oder zur gemeinsamen Postbearbeitung zentral durch ein Unternehmen der Gruppe verarbeitet werden. In unserer angehängten Dienstleisterliste finden Sie die AXA-Gesellschaften, die an einer zentralisierten Datenverarbeitung teilnehmen. Die jeweils aktuelle Version können Sie jederzeit unter www.axaxl.com abrufen.

Data processing within AXA Group:

Specialized companies or divisions within our group of companies are assigned central responsibility for certain data processing tasks for the group of affiliated companies. Where you have entered into an insurance contract with one or several companies in our group, your data may be processed centrally by a group company, for instance for the central management of address data, for telephone customer service, for the processing of contracts and benefits/claims, for collections/disbursements or for the central processing of mail. You will find the AXA companies participating in centralized data processing in the attached List of service providers. You can access the respective current version at any time at www.axaxl.com.

Externe Dienstleister:

Wir bedienen uns zur Erfüllung unserer vertraglichen und gesetzlichen Pflichten sowie zur Erfüllung unserer berechtigten Interessen zum Teil externer Dienstleister.

External service providers:

In some cases, we use external service providers in order to comply with our contractual and legal obligations as well as to pursue our legitimate interests.

In unserer angehängten Dienstleisterliste finden Sie die Kategorien der für uns tätigen Dienstleister, zu denen nicht nur vorübergehende Geschäftsbeziehungen bestehen. Die jeweils aktuelle Version können Sie jederzeit unter www.axaxl.com abrufen.

In our attached list of service providers, you will find the categories of service providers, with whom we entertain not only temporary business relationships. You can access the current version at any time at www.axaxl.com/de.

Weitere Empfänger:

Darüber hinaus können wir Ihre personenbezogenen Daten an weitere Empfänger übermitteln, wie etwa an

Other recipients:

In addition, we may transfer your personal data to other recipients, such as public authorities (e.g. due

Behörden, (z. B. wegen gesetzlichen Mitteilungspflichten an Sozialversicherungsträger, Finanzbehörden oder Strafverfolgungsbehörden), an Kreditinstitute (z.B. zur Abwicklung des Zahlungsverkehrs), an Ärzte oder Gutachter (z.B. zur Schadenabwicklung oder zur Beurteilung von Risiken und Leistungspflichten), an Auskunfteien (z.B. zur Bonitätsprüfung und Risikobeurteilung) oder an Rechtsanwälte (z.B. zur Abwehr und Durchsetzung von Rechtsansprüchen).

to statutory notification obligations to social insurance carriers, tax authorities or criminal prosecution authorities), credit institutions (e.g. to process payment transactions), physicians or experts (e.g. for claims handling or for the assessment of risks and obligations), credit agencies (e.g. to check creditworthiness and assess risks), or lawyers / solicitors (e.g. to defend against and enforce legal claims).

Dauer der Datenspeicherung

Wir löschen Ihre personenbezogenen Daten, sobald sie für die oben genannten Zwecke nicht mehr erforderlich sind. Dabei kann es vorkommen, dass personenbezogene Daten für die Zeit aufbewahrt werden, in der Ansprüche gegen AXA XL geltend gemacht werden können. Dabei liegen die gesetzlichen Verjährungsfristen zwischen drei bis dreißig Jahren.

Data Retention

We delete your personal data as soon as it is no longer required for the aforementioned purposes. It may occur that personal data is kept for the time in which claims against AXA XL can be made. In these cases, the statutory limitation periods are between three and thirty years.

Zudem speichern wir Ihre personenbezogenen Daten, soweit wir dazu gesetzlich verpflichtet sind. Entsprechende Nachweis- und Aufbewahrungspflichten ergeben sich unter anderem aus dem Unternehmensgesetzbuch, der Bundesabgabenordnung und dem Finanzmarkt-Geldwäschegesetz. Die Speicherfristen betragen danach bis zu zehn Jahre. Die Speicherfristen betragen danach bis zu zehn Jahre. Als Rechtsgrundlage für die Verarbeitung dienen in diesem Fall die jeweiligen gesetzlichen Regelungen i. V. m. Art. 6 Abs. 1 c) DSGVO.

We also store your personal data, in case of a legal obligation requiring us to do so. Among other, such legal requirements for evidence and retention are provided by means of the Corporate Code, the Federal Tax Code and the Financial Market Money Laundering Act. According to those, retention periods can be up to ten years. In this case, the respective legal regulations serve as the legal basis for processing as referred to in Art. 6 (1) (c) GDPR.

Bei Nichtzustandekommen eines Versicherungsvertrages werden wir Ihre Daten nach 3 Jahren zum Ende der gesetzlichen Verjährungsfrist löschen.

If an insurance contract is not concluded, we will delete your data at the end of the 3 year statutory limitation period.

Betroffenenrechte

Sie können uns gegenüber unter den oben genannten Adressen die folgenden Rechte geltend machen:

Data Subject Rights

You may exercise the following rights against us at one the aforementioned addresses:

- Bestätigung und Auskunft über die zu Ihrer Person gespeicherten Daten (Art. 15 DSGVO).
- Berichtigung oder Vervollständigung unrichtiger bzw. unvollständiger Daten (vgl. auch Art. 16 DSGVO);
- Unverzügliche Löschung der Sie betreffenden Daten (Art. 17 DSGVO), bzw. die Einschränkung der Verarbeitung nach Maßgabe von Art. 18 DSGVO, sollte eine Löschung aus den in Art. 17 Abs. 3 DSGVO genannten Gründen noch nicht in Betracht kommen;

- Confirmation and access to personal data stored about you (Art. 15 GDPR).
- Rectification or completion of inaccurate or incomplete data (see also Art. 16 GDPR);
- Immediate erasure of data concerning you (Art. 17 GDPR), or the restriction of the processing in accordance with Art. 18 GDPR, if a deletion should is not yet to be considered for reasons pursuant to Art. 17(3) GDPR;

- Herausgabe der Sie betreffenden und von Ihnen bereitgestellten Daten in einem strukturierten, gängigen und maschinenlesbaren Format sowie die Übermittlung dieser Daten an andere Anbieter/Verantwortliche (Art. 20 DSGVO);

- Reception of the data concerning you, and which have been provided by you, in a structured, common and machine-readable format as well as transmission of those data to other providers/controllers (Art. 20 GDPR);

- Beschwerde gegenüber den unten genannten Aufsichtsbehörden, sofern Sie der Ansicht sind, dass die Sie betreffenden Daten unter Verstoß gegen die datenschutzrechtlichen Bestimmungen verarbeitet werden (Art. 77 DSGVO).

- Lodge a complaint with one of the supervisory authorities listed below, if you are of the opinion that the processing of personal data relating to you infringes any of the data protection regulations (Art. 77 GDPR).

Widerspruchsrecht	**Right to object**
Sie haben ferner das Recht, einer Verarbeitung Ihrer personenbezogenen Daten zu Zwecken der Direktwerbung zu widersprechen.	**You have the right to object to the processing of your personal data for direct marketing purposes.**
Verarbeiten wir Ihre Daten zur Wahrung berechtigter Interessen, können Sie dieser Verarbeitung ebenfalls widersprechen, wenn sich aus Ihrer besonderen Situation Gründe ergeben, die gegen die Datenverarbeitung sprechen.	**Where we process your data to pursue our legitimate interests, you may object to this processing on grounds relating to your particular situation that contradict data processing.**

Datenschutzaufsichtsbehörden

Die für uns zuständigen Datenschutzaufsichtsbehörden sind:

Federführende Datenschutzaufsichtsbehörde im Sinne des Art. 56 Abs. 1 DSGVO:

Data Protection Commission
(An Coimisiún um Chosaint Sonraí)

21 Fitzwilliam Square South
Dublin 2
D02 RD28
Irland

Datenschutzbehörde zur Erfüllung der Aufgaben und Ausübung der Befugnisse im Hoheitsgebiet der Republik Österreich (Art. 55 DSGVO):

Österreichische Datenschutzbehörde (dsb)

Wickenburggasse 8
1080 Wien
Tel.: +43 (0) 1 52 152 0
E-Mail: dsb@dsb.gv.at

Data Protection Supervisory Authorities

The data protection supervisory authorities competent for us are:

Lead data protection supervisory authority within the meaning of Art. 56, 60 GDPR:

Data Protection Commission
(An Coimisiún um Chosaint Sonraí)

21 Fitzwilliam Square South
Dublin 2
D02 RD28
Eire

Data protection authority for the fulfilment of tasks and exercise of competences in the territory of the Republic of Austria (Art. 55, 60 GDPR):

Austrian Data Protection Authority (dsb)

Wickenburggasse 8
1080 Vienna
Tel.: +43 (0) 1 52 152 0
E-Mail: dsb@dsb.gv.at

Schriftliche Beschwerden können Sie grundsätzlich an beide Behörden richten, in deutscher Sprache jedoch ausschließlich an die österreichische Datenschutzbehörde.

Bonitätsauskünfte

Wir behalten uns vor, bei externen Dienstleistern (z.B. Creditreform, Schufa, Bürgel oder infoscore) Bonitätsauskünfte auf der Basis mathematisch-statistischer Verfahren einzuholen. Hierzu werden Ihre Daten, soweit sie erheblich sind (in der Regel Name und Anschrift) an den Dienstleister weiterleiten. Rechtsgrundlage für diese Verarbeitung ist unser berechtigtes Interesse an der Ausfallsicherheit unserer Forderungen sowie der Vorbeugung von Versicherungsbetrug gem. Art. 6 Abs.1 lit. f) DSGVO.

Datenaustausch mit Ihrem früheren Versicherer

Um Ihre Angaben bei Abschluss des Versicherungsvertrages bzw. Ihre Angaben bei Eintritt des Versicherungsfalls überprüfen und bei Bedarf ergänzen zu können, kann im dafür erforderlichen Umfang ein Austausch von personenbezogenen Daten, mit dem von Ihnen im Antrag benannten früheren Versicherer erfolgen.

Datenübermittlung in ein Drittland

Wenn wir personenbezogene Daten an AXA-Gesellschaften und Dienstleister außerhalb des Europäischen Wirtschaftsraums (EWR) übermitteln, erfolgt die Übermittlung nur, soweit dem Drittland durch die EU-Kommission ein angemessenes Datenschutzniveau bestätigt wurde oder Schutzmaßnahmen zur Gewährleistung der Sicherheit und Vertraulichkeit Ihrer personenbezogenen Daten umgesetzt worden sind, namentlich entweder (i) die von der Europäischen Kommission verabschiedeten Standardvertragsklausel oder (ii) verbindliche unternehmensinterne Datenschutzvorschriften (Binding Corporate Rules) wenn Ihrer personenbezogenen Daten an andere Einheiten der AXA-Gruppe übermittelt werden.

Stand: 06/2020

In general, you can address written complaints to both supervisory authorities. Complaints in German language, however, must be addressed exclusively to the Austrian Data Protection Authority.

Credit Information

We reserve the right to request credit information from external service providers (e.g. Creditreform, Schufa, Bürgel or infoscore) based on mathematical-statistical methods. For this purpose, your data will be forwarded to the service provider, provided it is relevant (usually name and address). The legal basis for this processing is our legitimate interest in the reliability of our claims and the prevention of insurance fraud in accordance with Art. 6 para. 1 lit. f) GDPR.

Exchanging data with your previous insurer

To be able to check and, if necessary, amend your details when the insurance contract is established or when the insured event occurs, personal data may be exchanged to the necessary extent with the previous insurer named by you in the application form.

Transfer to a Third Country

Where we transfer personal data to AXA companies and service providers outside the European Economic Area (EEA), the transfer will only take place if the level of data protection has been decided to be adequate in the respective third country by the EU Commission or by implementing other safeguards to ensure the security and the confidentiality of your personal data, by framing the transfer through either (i) the Standard Contractual Clauses adopted by the European Commission or (ii) through Binding Corporate Rules when your personal data is transferred to other entities of the AXA Group.

Status: 06/2020

Übersicht der Dienstleister der AXA XL

Gesellschaften, die an einer gemeinsamen Verarbeitung von Daten innerhalb der AXA Unternehmensgruppe teilnehmen oder bei denen die Datenverarbeitung Hauptgegenstand des Auftrages ist:

- AXA Versicherung AG, Köln
- AXA Versicherungen AG, Winterthur
- AXA Logistics and Service GmbH
- AXA Group Solutions SA
- AXE Services SAS
- AXA Technology Services Germany GmbH
- AXA Konzern AG
- AXA Business Services, India
- XL Catlin Services SE

Dienstleisterkategorien, bei denen Datenverarbeitung Hauptgegenstand des Auftrages ist:

Dienstleisterkategorie	Gegenstand / Zweck der Beauftragung	Gesundheitsdaten
Watchlist Management	Rechtliche Verpflichtung. Sanktionskontrolle und Verhinderung von Geldwäsche	nein
Claims Services	Unterstützung bei der Bearbeitung von Schadenfällen (externe Claims-Handler)	möglich
Rechtsanwaltskanzleien	Forderungseinzug, Vertretung in Rechtsstreitigkeiten	möglich
Marktforschungsunternehmen	Marktforschung, Kundenzufriedenheitsanalyse	nein
Marketingagenturen/-provider	Marketingaktionen	nein
Inkassounternehmen/Auskunfteien	Forderungsbearbeitung, Identitätsprüfung	nein
Rehabilitationsdienst	Rehabilitationsmanagement	ja
Karten- und Routenplaner (Software)	Ermittlung des Risikoortes und Schadenbearbeitung	nein
Telefonischer Kundendienst	Temporärer Kundendienst in besonderen Geschäftsprozessen, Kundenbetreuung	ja
Vermittler/Makler/Agenten	Antrags-/Leistungs- u. Schadenbearbeitung, Beratung	zum Teil
Gutachter/med. Experten/Berater	Antrags-/Leistungs-/Regressprüfung/Beratung	zum Teil

Dienstleisterkategorien, bei denen Datenverarbeitung kein Hauptgegenstand des Auftrages ist:

Dienstleisterkategorie	Gegenstand / Zweck der Beauftragung	Gesundheitsdaten
Assisteure	Assistanceleistungen	zum Teil
Lettershops/Druckereien	Postsendungen/Newsletter (E-Mail)	ja
Aktenlager	Lagerung von Akten	ja
IT-Dienstleister	Wartung/Betrieb/Entwicklung Systeme/Anwendungen/Online-Services	ja
Rückversicherungsunternehmen	Monitoring	ja
Entsorgungsunternehmen	Abfallbeseitigung und Aktenvernichtung (professionelle Aktenentsorger)	ja
Karten- und Routenplaner (Software)	Terminplanung	nein

List of AXA XL Service Provider

Companies participating in the joint processing of personal data within the AXA Group or for which the processing of such data is the main subject of their contract:

- AXA Versicherung AG, Köln
- AXA Versicherungen AG, Winterthur
- AXA Logistics and Service GmbH
- AXA Group Solutions SA
- AXE Services SAS
- AXA Technology Services Germany GmbH
- AXA Konzern AG
- AXA Business Services, India
- XL Catlin Services SE

Categories of service providers for whom the processing of personal data processing is the main subject of their contract:

Service Provider Category	Subject / Purpose of the Commissioning	Health Data
Watchlist Management	Legal obligation. Sanction control and prevention of money laundering.	no
Claims Services	Assistance in processing and handling claims (external loss-adjusters)	possible
Law firms	Debt collection, representation in litigation issues.	possible
Market research companies	Market research, customer satisfaction surveys / analysis	no
Marketing agencies / -provider	Marketing events	no
Debt collection agencies / credit bureaus	Debt collection and identity verification	no
Rehabilitation services	Rehabilitation management	yes
Maps and route planner (software)	Determination of the risk location and claims processing	no
Telephone customer service	Temporary customer service in special business processes, customer care	ja
Intermediaries / broker / agents	Processing of application, services and claims, consultation	partially
Experts / physicians / consultants	Reviews of applications, services, and recourse, consultation	partially

Categories of service providers for whom the processing of personal data is not the main subject of their contract:

Service Provider Category	Subject / Purpose of the Commissioning	Health Data
Assistance providers	Assistance services	partially
Letter shops / Printing houses	Mailings / Newsletter (email)	Yes
File archives	Storage of (paper) files	Yes
IT-Providers	Maintenance / operation / system development / applications / online services	Yes
Reinsurance companies	Monitoring	Yes
Waste disposal companies	Waste disposal and file destruction (professional file disposal companies)	Yes
Maps and route planner (software)	Scheduling	no

Vertragsinformationen für Geschäftskunden, XL Insurance Company SE

Mit diesen Vertragsinformationen stellen wir Ihnen vor Abschluss Ihres Versicherungsvertrags mit XL Insurance Company SE wichtige Informationen zur Verfügung.

Folgendes gilt im Falle des Führungs- oder Beteiligungsgeschäfts:

Die nachfolgenden Informationen, Belehrungen und Mitteilungen gelten grundsätzlich für den von AXA XL, a division of AXA, angebotenen Führungs- bzw. Mitversicherungsanteil. Je nach Ausgestaltung des Mitversicherungsverhältnisses durch entsprechende Führungsklauseln oder andere vertragliche Regelungen können die Regelungsgegenstände dieses Infopaketes von AXA XL oder vom führenden Versicherer teilweise auch im Namen der übrigen Beteiligungsversicherer mit Wirkung für deren jeweilige Mitversicherungsanteile erteilt werden. Näheres dazu entnehmen Sie bitte etwaigen Regelungen aus Ihren Vertragsunterlagen.

Inhaltsübersicht

1 Informationen über Ihren Versicherungsvertrag

2 Belehrung über Ihre Rücktrittsrechte

Informationen über Ihren Versicherungsvertrag

1 Informationen zum Versicherer

1.1 Versicherer des angebotenen Versicherungsvertrags wird

XL Insurance Company SE, Zweigniederlassung für Österreich
Tuchlauben 3
1010 Wien

Rechtsform: Europäische Aktiengesellschaft: Societas Europaea (SE)
(Gesellschaft mit beschränkter Haftung nach europäischem Recht)
Sitz: Wien
Handelsgericht Wien,
Firmenbuchnummer: 176093k

1.2 Sie vereinbaren den Versicherungsvertrag über den Versicherungsagenten

XL Catlin Services SE - Zweigniederlassung für Österreich (Wien)
Tuchlauben 3
1010 Wien.

1.3 XL Insurance Company SE, Zweigniederlassung für Österreich betreibt die Schaden- und Unfallversicherung.

1.4 XL Insurance Company SE (einschließlich ihrer Niederlassung in Österreich) wird durch die folgende irische Aufsichtsbehörde beaufsichtigt:

Central Bank of Ireland
New Wapping Street
North Wall Quay
Dublin D01F7X3
Ireland
https://www. Centralbank.ie/regulation

Im Hinblick auf die Versicherung von in Österreich belegenen Risiken übt auch die österreichische Aufsichtsbehörde

Finanzmarktaufsicht (FMA)
Otto-Wagner-Platz 5
1090 Wien

eine begrenzte Rechtsaufsicht aus.

2 Informationen zum Vertrag

2.1 Der Versicherungsvertrag kommt mit Zustellung des Versicherungsscheins oder einer gesonderten Annahmeerklärung zustande (§ 1a Absatz 2 VersVG). Vor diesem Zeitpunkt besteht kein Versicherungsschutz, außer dies wird gesondert mit XL Insurance Company SE, Zweigniederlassung für Österreich vereinbart.

2.2 Den Zeitpunkt des Beginns des Versicherungsschutzes entnehmen Sie bitte den Angebotsunterlagen.

2.3 Als Versicherungsnehmer haben Sie eine Reihe an Rücktrittsrechten. Eine genaue Übersicht entnehmen Sie bitte der Beilage "Belehrung über Ihre Rücktrittsrechte".

2.4 Die Laufzeit des angebotenen Vertrags sowie Ihre Kündigungsmöglichkeiten entnehmen Sie bitte den Angebotsunterlagen. Vor Ablauf der vereinbarten Vertragslaufzeit können Sie den Versicherungsvertrag nur aus den gesetzlichen Gründen nach § 8 VersVG und gegebenenfalls den in den Versicherungsbedingungen vorgesehenen Gründen gemäß kündigen.

2.5 Ist das Versicherungsverhältnis demnach auf unbestimmte Zeit eingegangen, so können Sie es nur für den Schluss der laufenden Versicherungsperiode kündigen.

2.6 Nähere Informationen zu den Modalitäten Ihrer Kündigung entnehmen Sie bitte den Angebotsunterlagen.

2.7 Für diesen Vertrag und die vorvertragliche Beziehung findet materielles österreichisches Recht unter Ausschluss der internationalen Verweisungsnormen und des UN-Kaufrechts oder das zwischen Ihnen und dem Versicherer wirksam vereinbarte ausländische Recht Anwendung.

2.8 Für Klagen aus dem Versicherungsvertrag gegen XL Insurance Company SE bestimmt sich die gerichtliche Zuständigkeit nach dem Hauptsitz der für den Versicherungsvertrag zuständigen Niederlassung.

2.9 Die Angebotsunterlagen und diese Vorabinformationen stellen wir Ihnen in deutscher Sprache zur Verfügung. Die Kommunikation zwischen Ihnen und dem Versicherer während der Laufzeit des Vertrages erfolgt ebenfalls in deutscher Sprache oder, mit Ihrem Einverständnis, in englischer Sprache.

3 Informationen zu außergerichtlichen Beschwerde- und Rechtsbehelfsverfahren

3.1 Im Falle von Anfragen und Reklamationen wenden Sie sich bitte zunächst an die XL Catlin Services SE - Zweigniederlassung für Österreich (s.o. Ziff. 1.2).

Ihr Anliegen können Sie entweder an Ihren regelmäßigen Ansprechpartner oder an die neutrale Beschwerdestelle xlcatlinautcomplaints@xlcatlin.com richten. Über diese E-Mail-Adresse angebrachte Beschwerden werden jeden Werktag während der Geschäftszeiten vom zuständigen Mitarbeiter abgerufen.

Ihre Beschwerde, die über Telefon, eine andere E-Mail-Adresse, über die Hauptniederlassung der XL Insurance Company SE, Dublin, einen externen Versicherungsvermittler oder auf andere Art und Weise angebracht werden, werden unverzüglich an den zuständigen Mitarbeiter weitergeleitet, der sodann Ihr Anliegen bearbeitet.

Bei Eingang einer Beschwerde, für die eine andere Stelle zuständig ist, wird Sie der zuständige Mitarbeiter entsprechend informieren und die Beschwerde an die zuständige Stelle weiterleiten, soweit diese feststellbar ist.

Jede Beschwerde wird auf faire und objektive Weise unter Einhaltung der anwendbaren Rechtsvorschriften, insbesondere des Versicherungsaufsichtsgesetzes, der Gewerbeordnung sowie der Datenschutzgrundverordnung (jeweils in der geltenden Fassung) bearbeitet.

Im Weiteren bestätigt Ihnen der zuständige Mitarbeiter unverzüglich das Einlangen der Beschwerde. In dieser Bestätigung werden Ihnen nochmals die Informationen in Bezug auf das weitere Verfahren der Beschwerdebearbeitung zur Verfügung gestellt.

Der zuständige Mitarbeiter informiert Sie in weiterer Folge über die laufende Bearbeitung Ihrer Beschwerde und fordert gegebenenfalls die für die Beschwerdebearbeitung relevanten Beweismittel und Informationen von Ihnen an. Unterlagen zu erhaltenen Beschwerden werden geordnet und in sicherer Weise für einen angemessenen Zeitraum aufbewahrt.

Ihre Beschwerde wird sodann binnen einer Frist von 15 Werktagen ab Beschwerdeeingang beantwortet. Sollte diese Frist nicht eingehalten werden können, so werden Ihnen innerhalb der Frist die Verzögerung, die Gründe der Verzögerung sowie der Zeitpunkt des voraussichtlichen Abschlusses der Prüfung mitgeteilt. Die Beschwerde soll spätestens innerhalb von 8 Wochen abschließend bearbeitet werden.

Sollten Ihren Forderungen nicht vollinhaltlich entsprochen werden, so wird Ihnen der Standpunkt von AXA XL dargelegt und über die weiteren Möglichkeiten zur Aufrechterhaltung der Beschwerde informiert.

Sollten Sie mit der Bearbeitung einer Reklamation nicht zufrieden sein, können Sie sich schriftlich an die für die Bearbeitung von Beschwerden zuständige Stelle unter der folgenden Adresse wenden:

The Financial Services and Pensions Ombudsman („FSPO")
Lincoln House
Lincoln Place
Dublin D02VH29
Ireland
Telephone: +353 1 567 7000
www.fspo.ie

3.2 Beschwerden können auch an die irische oder an die österreichische Aufsichtsbehörde unter den folgenden Adressen gerichtet werden:

Central Bank of Ireland
New Wapping Street
North Wall Quay
Dublin D01F7X3
Ireland
https://www. Centralbank.ie/regulation

Finanzmarktaufsicht (FMA)
Otto-Wagner-Platz 5

1090 Wien

Auch wenn Sie eine Beschwerde eingelegt haben, haben Sie die Möglichkeit, den Rechtsweg zu beschreiten.

4 Datenschutzhinweise

Der Schutz Ihrer persönlichen Daten ist uns ein besonderes Anliegen. Wir verarbeiten Ihre Daten daher ausschließlich auf Grundlage der gesetzlichen Bestimmungen (DSGVO, DSG). Weitere Informationen zum Thema Datenschutz finden Sie in der Beilage "Datenschutzhinweis" sowie auf der Website:

https://axaxl.com/de-at/privacy-and-cookies

Belehrung über Ihre Rücktrittsrechte

Im Folgenden informieren wir Sie über Ihr Recht, von Ihrer Vertragserklärung zurückzutreten. Bitte lesen Sie diese Information aufmerksam.

Die folgende Belehrung richtet sich nicht an Versicherungsnehmer, die einen Vertrag über Rück- oder Seeversicherung abschließen.

1 Rücktrittsrecht nach § 5c Versicherungsvertragsgesetz

Sie können von Ihrem Versicherungsvertrag innerhalb von 14 Tagen ohne Angabe von Gründen in geschriebener Form (z. B. Brief, Fax, E-Mail) zurücktreten.

Die Rücktrittsfrist beginnt mit der Verständigung vom Zustandekommen des Versicherungsvertrages (= Zusendung der Polizze bzw. Versicherungsschein), jedoch nicht, bevor Sie den Versicherungsschein und die Versicherungsbedingungen einschließlich der Bestimmungen über die Prämienfestsetzung oder -änderung und diese Belehrung über das Rücktrittsrecht erhalten haben.

Ihre Rücktrittserklärung richten Sie bitte an Ihren regelmäßigen Ansprechpartner oder:

XL Catlin Services SE - Zweigniederlassung für Österreich (Wien)
Tuchlauben 3
1010 Wien
Tel: +43 1 50 602 0
Fax: +43 1 50 602 111

Zur Wahrung der Rücktrittsfrist reicht es aus, dass Sie die Rücktrittserklärung vor Ablauf der Rücktrittsfrist absenden. Die Erklärung ist auch wirksam, wenn sie in den Machtbereich Ihres Versicherungsvertreters gelangt.

Mit dem Rücktritt enden ein allfällig bereits gewährter Versicherungsschutz und Ihre künftigen Verpflichtungen aus dem Versicherungsvertrag. Hat der Versicherer bereits Deckung gewährt, so gebührt ihm eine der Deckungsdauer entsprechende Prämie. Wenn Sie bereits Prämien an den Versicherer geleistet haben, die über diese Prämie hinausgehen, so hat sie Ihnen der Versicherer ohne Abzüge zurückzuzahlen.

Ihr Rücktrittsrecht erlischt spätestens einen Monat, nachdem Sie den Versicherungsschein einschließlich dieser Belehrung über das Rücktrittsrecht erhalten haben.

Dieses Rücktrittsrecht steht für Versicherungsverträge über Großrisiken gemäß § 5 Z 34 VAG 2016 nicht zu.

2 Rücktrittsfolgen

Im Falle eines wirksamen Rücktritts endet Ihr Versicherungsschutz, und wir erstatten Ihnen den auf die Zeit nach Zugang der Rücktrittserklärung entfallenden Teil der Prämien, wenn Sie zugestimmt haben, dass der Versicherungsschutz vor Ablauf der Rücktrittsfrist beginnt. Den Teil der Prämie, der auf die Zeit bis zum Zugang der Rücktrittserklärung entfällt, dürfen wir in diesem Fall einbehalten. Dabei handelt es sich um einen Betrag, der sich wie folgt berechnet:

Anzahl der Tage vom Beginn des Versicherungsschutzes bis zum Zugang der Rücktrittserklärung multipliziert mit der in Ihrem Versicherungsschein / Versicherungszertifikat angegebenen Versicherungsprämie und geteilt durch die Anzahl der Tage, für die die Versicherungsprämie zu entrichten ist. Ist eine Monatsprämie vereinbart, wird ein Monat mit 30 Tagen, und ist eine Jahresprämie vereinbart, wird ein Jahr mit 360 Tagen berücksichtigt.

Die Erstattung zurückzuzahlender Beträge erfolgt unverzüglich, spätestens 30 Tage nach Zugang der Rücktrittserklärung.

Beginnt der Versicherungsschutz nicht vor Ablauf der Rücktrittsfrist, hat der wirksame Rücktritt zur Folge, dass empfangene Leistungen zurück zu gewähren und gezogenen Nutzungen (z.B. Zinsen) herauszugeben sind.