

Cyber-Versicherung für die Visa, Mastercard und Diners Club Karten der Cornèr Bank AG

Versicherungsbedingungen – Allianz – Ausgabe 06.2026

Zur besseren Lesbarkeit sind die unten verwendeten männlichen Formen von Personal- und Possessivpronomen dahingehend zu verstehen, dass diese auch die entsprechenden weiblichen Formen einschliessen. Bitte bewahren Sie diese Allgemeinen Versicherungsbedingungen mit Ihren anderen Versicherungsunterlagen an einem sicheren Ort auf.

I Gemeinsame Bestimmungen für alle Versicherungskomponenten

Alle Versicherungskomponenten sind Schadenversicherungen.

1. Maximale Versicherungssummen

	Einzeldeckung	Familiendeckung
A. Rechtsschutz		
Rechtsschutz bei <i>Computer- und Internetdelikten</i> , Persönlichkeitsverletzungen und Urheberrechtsverletzungen im Internet	CHF 20'000 pro Ereignis	CHF 20'000 pro Ereignis
Streitigkeiten im Zusammenhang mit Verträgen, die über das Internet (online) für den persönlichen Gebrauch oder Bedarf abgeschlossen wurden	CHF 350'000 pro Ereignis	CHF 350'000 pro Ereignis
B. e-Reputation Unterstützung		
Beauftragung eines Spezialisten mit dem Entfernen diffamierender Inhalte	Unbegrenzt pro Ereignis, bis zu 2 Ereignisse pro Versicherungsschutz pro Jahr	Unbegrenzt pro Ereignis, bis zu 2 Ereignisse pro Versicherungsschutz pro Jahr
Vermittlung psychologischer Unterstützung.	CHF 3'000 pro Ereignis	CHF 3'000 pro Ereignis
C. Banking-Schutz		
<i>Nicht autorisierte missbräuchliche Zahlungsvorgänge mit Zahlungsmitteln</i> (finanzielle Verluste aufgrund des Missbrauchs eines Mobilgeräts, gesetzliche oder vertragliche Bestimmungen, <i>Selbstbehalte</i> und Eigenbeteiligung, die nicht vom <i>Finanzinstitut/Bankkartenherausgeber</i> übernommen werden): <ul style="list-style-type: none"> ▪ Erstattung <i>nicht autorisierter missbräuchlicher Zahlungsvorgänge</i> und/oder Erbringung von Informationsdienstleistungen ▪ Erstattung der damit verbundenen Verwaltungskosten und/oder Auslagen im Zusammenhang mit dem Anspruch im Schadenfall 	CHF 20'000 pro Versicherungsschutz pro Jahr CHF 300 pro Versicherungsschutz pro Jahr	CHF 20'000 pro Versicherungsschutz pro Jahr CHF 300 pro Versicherungsschutz pro Jahr
<i>Diebstahl, Beschädigung, Verlust oder Zerstörung der physischen Zahlungsmittel der versicherten Person:</i> <ul style="list-style-type: none"> ▪ Erstattung der damit verbundenen Verwaltungskosten und/oder Auslagen im Zusammenhang mit dem Anspruch im Schadenfall und/oder Erbringung von Informationsdienstleistungen 	CHF 300 pro Versicherungsschutz pro Jahr	CHF 300 pro Versicherungsschutz pro Jahr
<i>Autorisierter missbräuchlicher Zahlungsvorgang</i> aufgrund von <i>Phishing</i> und <i>Smishing</i> : <ul style="list-style-type: none"> ▪ Erstattung des <i>autorisierten missbräuchlichen Zahlungsvorgangs</i> ▪ Erstattung der damit verbundenen Verwaltungskosten und/oder Auslagen im Zusammenhang mit dem Anspruch im Schadenfall und/oder Erbringung von Informationsdienstleistungen 	CHF 1'000 pro Versicherungsschutz pro Jahr	CHF 1'000 pro Versicherungsschutz pro Jahr

D. Allyz Security App		
Beinhaltet digitale Sicherheitstools wie VPN, Viren- und Malware-Schutz, ID-Überwachung und Passwort-Manager	3 Geräte	5 Geräte
E. Datenwiederherstellung		
Wiederherstellung digitaler Daten	Unbegrenzt pro Ereignis, bis zu 2 Ereignisse pro <i>Versicherungsschutz</i> pro Jahr	Unbegrenzt pro Ereignis, bis zu 2 Ereignisse pro <i>Versicherungsschutz</i> pro Jahr

2. Wer ist der Versicherer?

**AWP P&C S.A., Saint-Ouen (Paris),
Zweigniederlassung Wallisellen (Schweiz)**

Richtiplatz 1
8304 Wallisellen
Schweiz

(nachstehend «Allianz» genannt)

Für Informationen, Anfragen oder Beschwerden:

Tel.: +41 44 283 31 12

E-Mail: allyzcyber@allianz.com

Risikoträger und Anbieter des Rechtsschutzes:

CAP Rechtsschutz-Versicherungsgesellschaft AG

Neue Winterthurerstrasse 88
8304 Wallisellen
Schweiz

(nachstehend «CAP» genannt)

Für Informationen, Anfragen oder Beschwerden:

Tel.: +41 58 358 09 09

E-Mail: capoffice@cap.ch

Im Rahmen der Erbringung seiner Leistungen überträgt *Allianz* unter Umständen Aufgaben an externe Anbieter.

3. Wer ist versichert?

Auf der Grundlage des Kollektivversicherungsvertrags zwischen Cornèr Banca SA (nachstehend «*Cornèr*» genannt) in Lugano und AWP P&C S.A., Saint-Ouen (Paris), Zweigniederlassung Wallisellen (Schweiz) gewährt die *Allianz/CAP* im Rahmen der folgenden *Allgemeinen Versicherungsbedingungen Versicherungsschutz* für folgende Personen:

Karteninhaber einer gültigen, nicht gekündigten und von *Cornèr* herausgegebenen Kreditkarte, mit Wohnsitz in der Schweiz und die die Cyber-Versicherung abgeschlossen haben (nachfolgend «*versicherte Person*» genannt). Aus dem *Bestätigungsschreiben* geht hervor, ob *Einzel- oder Familiendeckung* besteht.

Einzeldeckung: Versichert ist die im *Bestätigungsschreiben* genannte Person.

Familiendeckung: Versichert sind die im *Bestätigungsschreiben* genannte Person und ihre *Familienmitglieder*.

4. Geografischer Geltungsbereich

Der *Versicherungsschutz* gilt weltweit, es sei denn, im Abschnitt «II Besondere Bestimmungen für die einzelnen Versicherungskomponenten» ist für die einzelnen Komponenten ein anderer geografischer Geltungsbereich vorgesehen.

5. Beginn und Ende des Versicherungsschutzes

5.1. Beginn des Versicherungsschutzes

Der *Versicherungsschutz* beginnt an dem im *Bestätigungsschreiben* von *Cornèr* angegebenen Datum und besteht für ein Jahr. Sofern die *versicherte Person* oder *Cornèr* nicht zwei Monate vor Ablauf schriftlich kündigt, verlängert sich die *Einzel-/Familiendeckung* automatisch jeweils um ein Jahr.

5.2. Ende des Versicherungsschutzes

In jedem Fall endet der *Versicherungsschutz* mit Beendigung des Vertragsverhältnisses gemäss den Allgemeinen Geschäftsbedingungen von *Cornèr* oder mit Ablauf des Kollektivversicherungsvertrags zwischen der *Allianz* und *Cornèr*.

Kündigung durch die *Allianz*:

Die *Allianz* kann die Kündigung des *Versicherungsschutzes* für die *Einzel-/Familiendeckung* verlangen, wenn die *versicherte Person*:

- Bei der Beantragung des *Versicherungsschutzes* im Rahmen des Kollektivversicherungsvertrags unehrlich gehandelt oder unvollständige Angaben gemacht hat;
- Bei der Geltendmachung eines Anspruchs im Schadenfall vorsätzlich falsche Angaben gemacht oder Tatsachen verschwiegen hat;
- Betrug begangen oder zu begehen versucht hat.

Sollte die *Allianz* die Kündigung des *Versicherungsschutzes* für die *Einzel-/Familiendeckung* beantragen, wird die *versicherte Person* schriftlich benachrichtigt und der *Versicherungsschutz* durch den *Versicherungsnehmer* gekündigt.

6. Änderung der Allgemeinen Versicherungsbedingungen

Im Falle von Änderungen der *Allgemeinen Versicherungsbedingungen* wird die *versicherte Person* mindestens einen Monat im Voraus über die vom *Versicherungsnehmer* vorgeschlagenen Änderungen informiert, es sei denn, diese Änderungen müssen aufgrund gesetzlicher oder behördlicher Vorschriften früher vorgenommen werden. Ist die *versicherte Person* mit den Änderungen nicht einverstanden, kann sie ihren *Versicherungsschutz* für die *Einzel-/Familiendeckung* innerhalb von 30 Tagen nach Benachrichtigung über die Änderungen kündigen.

7. Pflichten der versicherten Person

Die *versicherte Person* muss angemessene Sorgfalt walten lassen, um ihre *personenbezogenen Daten* und persönlichen Gegenstände, darunter vertrauliche Informationen und Geräte, zu schützen, um mögliche Ansprüche im Schadenfall zu minimieren, andernfalls fallen diese möglicherweise nicht unter den *Versicherungsschutz* für die *Einzel-/Familiendeckung*.

Die *Allianz/CAP* ist berechtigt, die Kündigung des *Versicherungsschutzes* für die *Einzel-/Familiendeckung* zu verlangen, und lehnt jede Haftung für damit verbundene Ansprüche im Schadenfall ab oder reduziert die zu zahlenden Leistungen entsprechend der Schwere des Verschuldens der *versicherten Person*, wenn folgende Pflichten verletzt werden:

- Einhaltung aller Bestimmungen der *Allgemeinen Versicherungsbedingungen*.
- Unverzügliche Mitteilung aller Änderungen an die *Allianz/CAP*, die sich auf den *Versicherungsschutz* auswirken könnten.
- Bereitstellung vollständiger und korrekter Angaben an die *Allianz/CAP* bei Abschluss eines *Versicherungsschutzes* für die *Einzel-/Familiendeckung* und bei der Geltendmachung von Ansprüchen im Schadenfall.

Sollten aufgrund falscher oder unrichtiger Angaben Kosten entstehen, die bei korrekter Angabe nicht entstanden wären, behält sich die *Allianz/CAP* das Recht vor, diese Kosten in Rechnung zu stellen.

Kann der Versicherungsschutz für die Einzel-/Familiendeckung auf jemand anderen übertragen werden?

Der *Versicherungsschutz* kann nicht auf eine andere Person übertragen werden.

8. Internationale Sanktionen

Dieser *Versicherungsschutz* gewährt keine Deckung oder Leistungen, wenn diese gegen geltende Sanktionen, Gesetze oder Vorschriften des *Wohnsitzlandes* der *versicherten Person*, der Vereinten Nationen, der Europäischen Union, der Vereinigten Staaten von Amerika oder andere geltende Wirtschafts- oder Handelssanktionen, Gesetze oder Vorschriften verstossen würden. Die *Allianz/CAP* lehnt Ansprüche im Schadenfall von Personen, Unternehmen, Regierungen und anderen Parteien ab, für die eine Leistungserbringung nach nationaler oder internationaler Vereinbarungen oder Sanktionen untersagt ist.

9. Anwendbares Recht und Gerichtsstand

Es gilt schweizerisches Recht. Sämtliche Streitigkeiten, die sich aus oder im Zusammenhang mit dem *Versicherungsschutz* ergeben, sind vor den zuständigen Gerichten am Wohnsitz der *versicherten Person* oder am Sitz der *Allianz/CAP* in der Schweiz zu klären.

Gerichtsstand für Klagen von *Allianz/CAP* ist der Wohnsitz der *versicherten Person*.

10. Allgemeine Ausschlüsse

Vom *Versicherungsschutz* ausgeschlossen sind neben den in den Modulen im Abschnitt «II Besondere Bestimmungen für die einzelnen Versicherungskomponenten» aufgeführten Ereignissen auch die folgenden:

10.1. Ausserhalb des *Versicherungszeitraums*: alle Vorfälle, die vor dem im *Bestätigungsschreiben* angegebenen Beginn oder nach dem Ende des *Versicherungsschutzes* der *versicherten Person* eingetreten sind.

- 10.2. Grobe Fahrlässigkeit, die zu einem Schadenfall führt.
- 10.3. Wenn Gesetze oder Vorschriften die *Allianz/CAP* daran hindern, Leistungen an die *versicherte Person* oder deren *Familienmitglieder* zu erbringen, wird keine andere Entschädigung gewährt.
- 10.4. Jeder Verlust oder Schaden, der durch die Anordnung einer staatlichen Behörde verursacht wird.
- 10.5. Jegliche Ansprüche im Schadenfall, die sich aus unehrlichen, betrügerischen, kriminellen, böswilligen oder vorsätzlichen Handlungen, Fehlern oder Unterlassungen der *versicherten Person* oder aus rechtswidrigen Handlungen oder Verstössen gegen geltende Gesetze, staatliche Verbote oder Vorschriften oder aus der rechtswidrigen Nutzung des versicherten Gegenstands ergeben.
- 10.6. Jegliche Ansprüche im Schadenfall, die sich aus den geschäftlichen Aktivitäten der *versicherten Person* (einschliesslich, aber nicht beschränkt auf E-Commerce und Blogging, für die die *versicherte Person* eine Vergütung oder Vorteile in irgendeiner Form erhält), ihrem Beruf oder geschäftlichen politischen Verbindungen ergeben.
- 10.7. Jegliche Ansprüche im Schadenfall, die sich aus Aktivitäten ergeben, die auf die Erzielung eines Vorteils oder finanziellen Gewinns ausgerichtet sind, auf den die *versicherte Person* keinen gesetzlichen Anspruch hat.
- 10.8. Jegliche entgangenen Gewinne, Zinsverluste, Folgeverluste oder -schäden.
- 10.9. Schäden durch äussere Ereignisse wie Stürme, Feuer, Überschwemmungen, Blitzschlag und Explosionen; Naturgewalten; Kernenergie; Bodensenkungen, Insektenbefall; elektromagnetische Impulse, unabhängig davon, ob sie künstlich oder natürlich entstanden sind, Versickerung, Verschmutzung oder Kontamination; ionisierende Strahlung oder Kontamination durch Radioaktivität aus Kernbrennstoffen oder aus nuklearen Abfällen aus der Verbrennung von Kernbrennstoffen oder durch radioaktive, toxische, explosive oder andere gefährliche Eigenschaften von explosiven Kernmaschinen oder Teilen davon; Druckwellen von Flugzeugen und anderen Flugobjekten, die sich mit Schallgeschwindigkeit oder schneller bewegen.
- 10.10. Folgen von infektiösen Risikosituationen im Rahmen einer Epidemie oder Pandemie.
- 10.11. Schäden, die unmittelbar oder mittelbar durch oder im Zusammenhang mit Krieg, Invasion, Revolution, Verstaatlichung, Beschlagnahme, Enteignung, Entziehung, Requisition oder einem terroristischen Akt verursacht werden, unabhängig von anderen Ursachen oder Ereignissen, die gleichzeitig oder in anderer Reihenfolge zum Schaden beitragen. Als Terrorakt im Sinne dieses Ausschlusses gilt die Anwendung oder angedrohte Anwendung biologischer, chemischer und/oder nuklearer Gewalt durch eine Person oder eine Gruppe von Personen, die allein oder im Namen oder in Verbindung mit einer oder mehreren Organisationen oder einer oder mehreren Regierungen zu politischen, religiösen, ideologischen oder ähnlichen Zwecken handelt, einschliesslich der Absicht, eine Regierung zu beeinflussen und/oder die Öffentlichkeit oder einen Teil der Öffentlichkeit in Angst und Schrecken zu versetzen, und/oder jede Handlung, die von der Regierung des *Wohnsitzlandes* als Terrorakt angesehen wird.
- 10.12. Versicherte Ereignisse im Zusammenhang mit Rechtsfällen, die bei Beginn des *Versicherungsschutzes* hängig oder abgeschlossen sind.
- 10.13. Hat die *versicherte Person* Ansprüche im Schadenfall aus einem anderen Versicherungsvertrag (freiwillige oder obligatorische private oder soziale Versicherung), beschränkt sich die durch die *Allianz/CAP* gewährte Deckung auf den Teil der Versicherungsleistungen, der über diejenigen aus dem anderen Versicherungsvertrag hinausgeht. Kosten werden nur einmal erstattet.
- 10.14. Zahlt die *Allianz/CAP* Leistungen, die eine *versicherte Person* auch gegenüber Dritten hätte geltend machen können, treten die Anspruchsberechtigten diese Ansprüche im Schadenfall an *Allianz/CAP* ab.

11. Kontakt im Schadenfall

Allianz Partners

Schadenabteilung

Richtiplatz 1

8304 Wallisellen

Schweiz

Telefon: +41 44 283 31 12

E-Mail: allyzcyber@allianz.com

CAP Rechtsschutz-Versicherungsgesellschaft AG

Grosskundenbetreuung

Neue Winterthurerstrasse 88

8304 Wallisellen

Schweiz

Telefon: +41 58 358 09 09

E-Mail: capoffice@cap.ch

Die *versicherte Person* muss einen Anspruch im Schadenfall unverzüglich der *Allianz/CAP* melden und alle erforderlichen Informationen vorlegen, darunter unter anderem:

- Nachweis, dass die *versicherte Person* bei der *Allianz/CAP* versichert ist.
- Beschreibung des versicherten Ereignisses.
- Konkrete Informationen zu jeder Komponente, die im Abschnitt «II Besondere Bestimmungen für die einzelnen Versicherungskomponenten» aufgeführt ist.

Was passiert, wenn die *versicherte Person* oder eine in ihrem Namen handelnde Person falsche oder unvollständige Angaben macht?

Wenn die *versicherte Person* oder eine in ihrem Namen handelnde Person gegenüber der *Allianz/CAP* falsche oder unvollständige Angaben macht, kann die *Allianz/CAP* den *Versicherungsschutz* verweigern.

Wenn die *versicherte Person* oder eine in ihrem Namen handelnde Person einen Anspruch im Schadenfall geltend macht, der in irgendeiner Weise unwahr, übertrieben oder betrügerisch ist, oder einen Anspruch im Schadenfall mit unwahren, übertriebenen oder betrügerischen Angaben in Bezug auf das Versicherungsrisiko oder Dokumente stützt, verliert die *versicherte Person* sämtliche Leistungen. Die *Allianz/CAP* behält sich das Recht vor, auch die Kosten für bereits unter diesem *Versicherungsschutz* ausgezahlte Ansprüche im Schadenfall zurückfordern, die sich im Nachhinein als betrügerisch herausstellen. Die *Allianz/CAP* kann dies in Datenbanken zur Betrugsbekämpfung erfassen und auch andere Organisationen benachrichtigen.

Was passiert, wenn Ansprüche im Schadenfall aus anderen Versicherungen bestehen?

Wenn die *versicherte Person* Anspruch auf Leistungen aus anderen Versicherungen hat, ist der *Versicherungsschutz* nur subsidiär. Im Rahmen dieses *Versicherungsschutzes* wird jedoch ein Vorschuss für diese Leistungen gewährt. Die *versicherte Person* ist verpflichtet, diese Ansprüche im Schadenfall bis zur Höhe des gewährten Vorschusses an die *Allianz/CAP* abzutreten.

Was passiert, wenn Ansprüche im Schadenfall gegen Dritte bestehen?

Wenn die *Allianz/CAP* Leistungen zahlt, für die die *versicherte Person* auch Ansprüche im Schadenfall gegen Dritte hätte geltend machen können, ist die *versicherte Person* verpflichtet, diese Ansprüche im Schadenfall an die *Allianz/CAP* abzutreten.

12. Datenschutzhinweis

Für die *Allianz* hat der Schutz der Privatsphäre der *versicherten Person* oberste Priorität. Im Datenschutzhinweis wird erläutert, welche Arten personenbezogener Daten wie und zu welchem Zweck erfasst und an wen sie weitergegeben bzw. offengelegt werden.

Bitte lesen Sie diesen Hinweis unter dem folgenden Link sorgfältig durch: www.allianz-partners.com/datenschutz-partner

13. Definitionen

Die allgemeinen Definitionen der in den *Allgemeinen Versicherungsbedingungen* verwendeten Begriffe oder Ausdrücke werden im Folgenden erläutert und haben überall dieselbe Bedeutung. Die Begriffe sind im Text dieses Dokuments durch Kursivschrift gekennzeichnet.

Allgemeine Versicherungsbedingungen: detaillierte Beschreibung der allgemeinen Vertragsbedingungen; Auflistung der allgemeinen Ausschlüsse und allgemeinen Bedingungen, die für den *Versicherungsschutz* gelten. Wir weisen darauf hin, dass für den *Versicherungsschutz* ausschliesslich die in diesem Dokument aufgeführten *Allgemeinen Versicherungsbedingungen* gelten.

Allyz Security App: eine von der *Allianz* über ihren *Anbieter* bereitgestellte spezielle Technologielösung.

Anbieter: Anbieter der *Allyz Security App*, die der *versicherten Person* zur Verfügung gestellt wird. Der Name lautet F-Secure Corporation, Unternehmens-Identifikationsnummer 0705579-2, eingetragene Adresse Tammasaarenkatu 7, P.O. Box 24, 00181 Helsinki, Finnland.

Autorisierter missbräuchlicher Zahlungsvorgang: eine von der *versicherten Person* in der mit dem *Finanzinstitut/Bankkartenherausgeber* vereinbarten Form autorisierte Geldtransaktion, die jedoch von einer dritten Partei aus der Ferne durchgeführt wird und direkt und ausschliesslich zu einem finanziellen Verlust führt.

Beschädigung oder Zerstörung physischer Zahlungsmittel: Schäden oder Zerstörungen, die durch ein unerwartetes und unbeabsichtigtes Ereignis verursacht werden, das zu einem bestimmaren Zeitpunkt und an einem bestimmaren Ort eintritt und die Funktionalität oder sichere Nutzung der *physischen Zahlungsmittel* der *versicherten Person* beeinträchtigt.

Bestätigungsschreiben: Dokument, in dem das Beginn- und Enddatum des *Versicherungsschutzes* sowie die *versicherte Person* aufgeführt sind.

Computer- und Internetdelikt: Straftaten im Sinne des schweizerischen Strafgesetzbuches, die mithilfe des Internets begangen werden (z. B. Datendiebstahl, Datenverfälschung, Datenbetrug im Internet).

Datenpunkt: ein Element personenbezogener digitaler Daten laut Definition in lokalen Vorschriften der Datenschutz-Grundverordnung (DSGVO) oder anderen geltenden Gesetzen oder Vorschriften (beispielsweise ist eine E-Mail-Adresse ein *Datenpunkt*).

Solche Daten können in den Unterlagen des *Anbieters* der *Allianz* als personenbezogene Daten (PII – Personally Identifiable Information) bezeichnet werden.

Diebstahl durch illegales Eindringen: Diebstahl der *physischen Zahlungsmittel* der *versicherten Person*, während diese sich in ihrer Wohnung befinden, die von ihr bewohnt wird, durch das Eindringen eines Dritten, der in ihrer Gegenwart und ohne ihr Wissen oder das Wissen eines *Familienmitglieds* handelt.

Diebstahl im Vorbeigehen: Diebstahl der *physischen Zahlungsmittel* der *versicherten Person*, während diese sich in Reichweite und unter Aufsicht der *versicherten Person* in einem Umkreis von maximal einem Meter befinden, ohne physische oder moralische Gewaltanwendung.

Diebstahl von physischen Zahlungsmitteln:

Einbruchdiebstahl – gewaltsames Eindringen in Fahrzeuge

Einbruchdiebstahl – gewaltsames Eindringen in Räumlichkeiten, Raub, Taschendiebstahl, *Diebstahl im Vorbeigehen* und *Diebstahl durch illegales Eindringen*.

Einbruchdiebstahl – gewaltsames Eindringen in Fahrzeuge: zu einem bestimmbaren Zeitpunkt und an einem bestimmbaren Ort werden die *physischen Zahlungsmittel* der *versicherten Person* aus einem verschlossenen Fahrzeug gestohlen, wobei alle verfügbaren Schutzvorrichtungen eingesetzt wurden und die *physischen Zahlungsmittel* nicht sichtbar waren, sodass physische Gewalt und gewaltsames Eindringen in das Fahrzeug erforderlich waren.

Einbruchdiebstahl – gewaltsames Eindringen in Räumlichkeiten: zu einem bestimmbaren Zeitpunkt und an einem bestimmbaren Ort werden die *physischen Zahlungsmittel* der *versicherten Person* aus verschlossenen Räumlichkeiten gestohlen, wobei alle verfügbaren Schutzvorrichtungen eingesetzt wurden, sodass physische Gewalt und gewaltsames Eindringen in die Räumlichkeiten erforderlich waren.

Familienmitglieder: die mit der *versicherten Person* im selben Haushalt lebenden Personen sowie deren minderjährige Kinder, die nicht im selben Haushalt leben (gilt nur bei der *Familiendeckung*).

Finanzinstitut/Bankkartenherausgeber: Finanzunternehmen oder Bankkartenherausgeber, die von der Eidgenössischen Finanzmarktaufsicht (FINMA) zugelassen sind und beaufsichtigt werden.

Geräte: interne Laufwerke, die als Bestandteil eines Computers vorgesehen sind, und externe Laufwerke, die in erster Linie zur Speicherung digitaler Daten für den persönlichen Gebrauch dienen, die sich im Besitz der *versicherten Person* befinden und für die digitale Datenwiederherstellung gemäss der Liste der berechtigten *Geräte* im Abschnitt «Datenwiederherstellung» unter Absatz E.7 «Besondere Bedingungen und Anspruchsberechtigung» infrage kommen.

Influencer: ein Content-Ersteller mit kommerzieller Absicht, der (hauptsächlich auf Social-Media-Plattformen) auf Vertrauen und Authentizität basierende Beziehungen zu seinem Publikum aufbaut und zu Monetarisierungszwecken über verschiedene Geschäftsmodelle online mit gewerblichen Akteuren interagiert.

Kaufbeleg: ein *Kaufbeleg* (z. B. Rechnung) ist das Dokument, das nachweist, dass der versicherte Gegenstand der *versicherten Person* am Kaufdatum von der *versicherten Person* selbst oder einem *Familienmitglied* erworben wurde. Das Dokument muss bestimmte Angaben zur Identifizierung des versicherten Gegenstands enthalten, darunter Hersteller, Typ/Modell, Seriennummer und/oder IMEI-Nummer, ebenso wie Angaben zum *Verkäufer*, wie Name und Mehrwertsteuer-Identifikationsnummer oder Unternehmens-Identifikationsnummer.

Kaufdatum: das Datum, an dem der versicherte Gegenstand vom *Verkäufer* erworben wurde.

Maximale Versicherungssummen: die *maximale Versicherungssumme* für die *Einzel-/Familiendeckung* (Entschädigung), in Bezug auf den gewährten *Versicherungsschutz*.

Nicht autorisierter missbräuchlicher Zahlungsvorgang: eine Geldtransaktion, die von einem Dritten ohne Zustimmung der *versicherten Person* aus der Ferne veranlasst und autorisiert wurde und die unmittelbar und ausschliesslich zu einem finanziellen Verlust führt.

Personenbezogene Daten: jegliche Informationen, die sich auf die *versicherte Person* oder diese und ihre *Familienmitglieder* beziehen. Dazu gehören auch einzelne Informationen, die in ihrer Gesamtheit zu einer Identifizierung führen können.

Beispiele für personenbezogene Daten sind:

- Vor- und Nachname,
- Wohnadresse,
- E-Mail-Adresse wie vorname.nachname@firma.ch,
- Identitätskartennummer,
- Standortdaten (z. B. die Standortdatenfunktion eines Mobiltelefons),
- eine Internetprotokolladresse (IP-Adresse),
- eine Cookie-ID,
- die Werbe-ID des Telefons der *versicherten Person*,
- von einem Spital oder Arzt gespeicherte Daten, die ein eindeutiges Identifikationsmerkmal einer Person darstellen könnten.

Phishing: betrügerische Versuche per E-Mail, die *versicherte Person* dazu zu verleiten, eine Transaktion zu tätigen oder persönliche Daten preiszugeben, die dazu verwendet werden könnten, Geld über die *Zahlungsmittel* der *versicherten Person* abzuheben.

Physische Zahlungsmittel: Debit- und Kreditkarten, sowohl physische als auch virtuelle auf den mobilen Geräten der *versicherten Person*, die sich im Besitz der *versicherten Person* befinden und von einem *Finanzinstitut/Bankkartenherausgeber* in der Schweiz auf deren Namen ausgestellt wurden und mit deren *Zahlungskonto* bei diesem *Finanzinstitut/Bankkartenherausgeber* verbunden sind.

Raub: die unbefugte Entwendung der *physischen Zahlungsmittel* der *versicherten Person* durch physische Gewalt, Drohungen oder Einschüchterung der *versicherten Person* durch eine oder mehrere andere Personen.

Selbstbehalt: ein fester Betrag oder Prozentsatz eines finanziellen Verlusts, für den die *versicherte Person* selbst aufkommen muss und den das *Finanzinstitut/ Bankkartenherausgeber* gemäss seinen gesetzlichen oder vertraglichen Bestimmungen einbehält und nicht erstattet.

Smishing: betrügerische SMS-Nachrichten, die darauf abzielen, die *versicherte Person* zu einer Transaktion oder zur Preisgabe personenbezogener Daten zu verleiten, welche dazu verwendet werden können, Gelder von den *Zahlungsmitteln* der *versicherten Person* abzubuchen.

Taschendiebstahl: Diebstahl der *physischen Zahlungsmittel* der *versicherten Person* aus deren Kleidung oder Handtaschen, insbesondere in einer Menschenmenge.

Verkäufer: eine juristische Person, die in Übereinstimmung mit dem Land ihres Hauptgeschäftssitzes ordnungsgemäss gegründet, lizenziert und registriert ist und den Verkauf von Gegenständen online und/oder in einem physischen Geschäft betreibt.

Verletzung der Datensicherheit: eine Verletzung, bei der *Datenpunkte* von unbefugten Personen kopiert, übertragen, eingesehen, gestohlen, verändert oder verwendet werden.

Verletzung von Persönlichkeitsrechten: gemäss Art. 28 ff. des Schweizerischen Zivilgesetzbuches (ZGB) für *versicherte Personen*, die Opfer von Verleumdung, übler Nachrede oder Beleidigung geworden sind, die für Dritte offensichtlich sind und über elektronische Medien auf Websites oder in Foren, Blogs oder sozialen Netzwerken begangen wurden (z. B. Cybermobbing oder Identitätsdiebstahl).

Verlust von physischen Zahlungsmitteln: die *versicherte Person* ist infolge eines unbeabsichtigten Ereignisses, das nicht durch *Diebstahl physischer Zahlungsmittel* verursacht wurde, nicht im Besitz ihrer *physischen Zahlungsmittel* oder kann diese nicht wiedererlangen.

Versehentliche Beschädigung: Schaden, der durch ein unerwartetes und nicht vorsätzliches Ereignis verursacht wird, das zu einem bestimmbaren Zeitpunkt und an einem bestimmbaren Ort eintritt und die Funktionsfähigkeit oder den sicheren Gebrauch des versicherten Gegenstands durch Herunterfallen, Sturz, Aufprall oder Flüssigkeit beeinträchtigt.

Versicherte Person: die Person(en), die im Abschnitt «**Wer ist versichert?**» aufgeführt ist/sind.

Versicherungsnehmer: Cornèr Banca SA, Via Canova 16, 6900 Lugano.

Versicherungsschutz: der Versicherungsvertrag zwischen der *versicherten Person* und dem *Versicherungsnehmer* umfasst die *Allgemeinen Versicherungsbedingungen* und das *Bestätigungsschreiben*. Zusammen bilden diese Dokumente den *Versicherungsschutz*. Im Falle von Widersprüchen gelten die *Allgemeinen Versicherungsbedingungen*.

Versicherungszeitraum: die Dauer des *Versicherungsschutzes*, die im *Bestätigungsschreiben* angegeben ist.

Wohnsitzland: Schweiz.

Zahlungsmittel: *physische Zahlungsmittel* und Online-Zahlungskonten, die von einem *Finanzinstitut/Bankkartenherausgeber* bereitgestellt werden.

II Besondere Bestimmungen für die einzelnen Versicherungskomponenten

A. Rechtsschutz

1. Einführung

Gemäss diesen *Allgemeinen Versicherungsbedingungen* und in Bezug auf versicherte Ereignisse im Zusammenhang mit *Computer- und Internetdelikten*, *Verletzungen von Persönlichkeitsrechten* und Urheberrechtsverletzungen sowie Vertragsstreitigkeiten im Internet leistet die CAP Rechtsschutz.

2. Zeitlicher Geltungsbereich

Die CAP gewährt Rechtsschutz, wenn der Bedarf an rechtlicher Unterstützung nach Inkrafttreten des *Versicherungsschutzes* aufgetreten oder ersichtlich ist. Die CAP gewährt keinen Rechtsschutz, wenn der Bedarf an rechtlicher Unterstützung nach Ende des *Versicherungsschutzes* angemeldet wird.

3. Versicherte Ereignisse

- 3.1. Einfordern von Schadenersatz, wenn die *versicherte Person* Opfer eines *Computer- und Internetdelikts* wird. *Versicherungsschutz* besteht auch für das Durchsetzen dieser Ansprüche im Strafverfahren.
- 3.2. Einfordern von Schadenersatz, wenn die *versicherte Person* Opfer einer Urheberrechtsverletzung im Internet im Zusammenhang mit persönlichen Internetseiten und sozialen Netzwerken wird.
- 3.3. Geltend machen des Rechts auf Gegendarstellung und / oder Entfernung bei Darstellungen (Bild, Ton oder Text) im Internet, wenn die Persönlichkeit der versicherten Person infolge eines Computer- oder Internetdelikts unmittelbar betroffen ist.
- 3.4. Streitigkeiten im Zusammenhang mit Verträgen, welche die *versicherte Person* für ihren persönlichen Gebrauch oder Bedarf über das Internet abgeschlossen hat.

4. Versicherungsleistungen

- 4.1. Leistungen des Rechtsdienstes der CAP:
- 4.2. Geldleistungen bis zur *maximalen Versicherungssumme* pro Schadenfall für:
 - Kosten von Expertisen und Analysen;
 - Gerichts-, Schiedsgerichts- und Mediationskosten;
 - Reisekosten zu Gerichtsverhandlungen und gerichtlich angeordneten Augenscheinen, wenn die Anwesenheit der *versicherten Person* zwingend erforderlich ist;
 - Parteientschädigungen;
 - Anwaltskosten.
- 4.3. Die CAP kann sich durch die Bezahlung eines Teils oder des ganzen Streitwertes von ihrer Leistungspflicht befreien.

5. Versicherte Ereignisse, versicherte Leistungen und maximale Versicherungssummen

Versicherte Ereignisse	Versicherte Leistungen	Maximale Versicherungssummen
Einfordern von Schadenersatz, wenn die <i>versicherte Person</i> Opfer eines Computer- oder Internetdelikts wird. <i>Versicherungsschutz</i> besteht auch für das Durchsetzen dieser Ansprüche im Strafverfahren	Leistungen des Rechtsdienstes der CAP und weitere Kosten gemäss Abschnitt II A 4	CHF 20'000 pro Ereignis
Einfordern von Schadenersatz, wenn die <i>versicherte Person</i> Opfer einer Urheberrechtsverletzung im Internet im Zusammenhang mit persönlichen Internetseiten und sozialen Netzwerken wird	Leistungen des Rechtsdienstes der CAP und weitere Kosten gemäss Abschnitt II A 4	CHF 20'000 pro Ereignis
Geltend machen des Rechts auf Gegendarstellung und/oder Entfernung bei Darstellungen (Bild, Ton oder Text) im Internet, wenn die Persönlichkeit der versicherten Person infolge eines Computer- oder Internetdelikts unmittelbar betroffen ist	Leistungen des Rechtsdienstes der CAP und weitere Kosten gemäss Abschnitt II A 4	CHF 20'000 pro Ereignis
Streitigkeiten im Zusammenhang mit Verträgen, die die <i>versicherte Person</i> für ihren persönlichen Gebrauch oder Bedarf über das Internet abgeschlossen hat	Leistungen des Rechtsdienstes der CAP und weitere Kosten gemäss Abschnitt II A 4	CHF 350'000 pro Ereignis

6. Ausschlüsse und Einschränkungen

Zusätzlich zu Abschnitt I 10 «Allgemeine Ausschlüsse» besteht kein *Versicherungsschutz* für folgende Ereignisse oder Risiken:

- 6.1. Fälle, bei denen die *versicherte Person* gegen die *Allianz* oder die *CAP* und deren Mitarbeiter im Rahmen ihrer beruflichen Tätigkeit vorgehen will. Wenn die *versicherte Person* gegen Personen, die in einem durch die CAP versicherten Rechtsfall Dienstleistungen erbringen oder erbracht haben, vorgehen will.
- 6.2. Schadenersatz und Kosten, zu deren Übernahme ein haftpflichtiger Dritter oder eine Haftpflichtversicherung verpflichtet ist.

- 6.3. Rechtsschutz im Zusammenhang mit dem Inkasso unbestrittener Forderungen.
- 6.4. Rechtsstreitigkeiten und Verfahren im Zusammenhang mit Steuern, Gebühren, Abgaben und Zollangelegenheiten.
- 6.5. Streitigkeiten im Zusammenhang mit der Anlage und Verwaltung von Vermögenswerten, Kunstgegenständen, Wertpapieren und spekulativen Rechtsgeschäften.

7. Pflichten der versicherten Person

Zusätzlich zu Abschnitt I 7 «Pflichten der versicherten Person» und I 11 «Kontakt im Schadenfall» hat die versicherte Person folgende Pflichten:

- 7.1. Um die Leistungen beanspruchen zu können, muss die versicherte Person im Versicherungsfall unverzüglich die CAP kontaktieren.
- 7.2. Die versicherte Person unterstützt bei der Abklärung des Sachverhalts. Sie überlässt die Fallführung exklusiv der CAP. Ohne vorherige Zustimmung der CAP erteilt die versicherte Person keine Aufträge an Anwälte, Sachverständige, etc., leitet keine Verfahren ein, ergreift keine Rechtsmittel und schliesst keine Vergleiche ab. Die versicherte Person schliesst keine Honorarvereinbarung mit dem beauftragten Anwalt ab. Kommt die versicherte Person diesen Verpflichtungen nicht nach, kann die CAP ihre Leistungen kürzen oder verweigern, wenn die versicherte Person nicht beweist, dass sie nach den Umständen an der Verletzung dieser Obliegenheiten kein Verschulden trifft oder die Verletzung keinen Einfluss auf den Umfang der von der CAP geschuldeten Leistungen hatte.
- 7.3. Sofern der Beizug eines unabhängigen Anwalts für die Interessenwahrung der versicherten Person notwendig ist, hat die versicherte Person das Recht im Einvernehmen mit der CAP einen Anwalt seiner freien Wahl zu verlangen. Der von der versicherten Person vorgeschlagene Rechtsvertreter darf erst nach erfolgter Zustimmung der CAP beauftragt werden. Akzeptiert die CAP den vorgeschlagenen Rechtsvertreter nicht, hat die versicherte Person das Recht, drei andere Rechtsvertreter aus verschiedenen Kanzleien vorzuschlagen, von welchen einer von der CAP angenommen werden muss.
- 7.4. Treten zwischen der versicherten Person und der CAP Meinungsverschiedenheiten hinsichtlich der zu ergreifenden Massnahme zur Schadenerledigung auf oder erachtet die CAP eine Massnahme als aussichtslos, so teilt sie der versicherten Person ihre Ablehnung schriftlich und begründet mit und weist sie auf die Möglichkeit eines Schiedsverfahrens hin.
Die versicherte Person kann innert 30 Tagen verlangen, dass die Angelegenheit zur Beurteilung einem Schiedsrichter unterbreitet wird, der daraufhin durch die versicherte Person und die CAP gemeinsam bestimmt wird.
Der Schiedsrichter kann einen Vorschuss für die mutmasslichen Verfahrenskosten verlangen und die Durchführung des Verfahrens von dessen Leistung abhängig machen. Er bestimmt die Höhe des Vorschusses jeder Partei. Die Verfahrenskosten und die Parteientschädigung werden in der Regel der unterliegenden Partei auferlegt.
Die versicherte Person kann trotz Verneinung der Leistungspflicht auf eigene Kosten einen Prozess einleiten. Wird dabei ein günstigeres Urteil erwirkt als die von der CAP schriftlich begründete Lösung, übernimmt die CAP die durch dieses Vorgehen entstandenen Kosten bis zum Höchstbetrag der Versicherungssumme.

B. e-Reputation Unterstützung

1. Einführung

Gemäss diesen *Allgemeinen Versicherungsbedingungen* wird die Allianz:

- einen Anbieter beauftragen, der die versicherte Person dabei unterstützt, Folgendes zu versuchen:
 - die ohne Zustimmung der versicherten Person online veröffentlichten persönlichen Daten zu entfernen;
 - einen Diebstahl der digitalen Identität zu beheben;
- der versicherten Person Kontakte zu Anwälten vermitteln, die auf Probleme mit der unbefugten Verwendung *personenbezogener Daten* im Internet spezialisiert sind;
- der versicherten Person psychologische Hilfe und Umzugskosten zur Verfügung stellen.

2. Versicherte Ereignisse

Verletzung von Persönlichkeitsrechten im Zusammenhang mit Online-Ereignissen:

- 2.1. Unbefugte und nicht einvernehmliche Veröffentlichungen auf persönlichen Websites, Blogs und Social-Media-Konten.
- 2.2. Unbefugte und nicht einvernehmliche Offenlegung oder Veröffentlichung *personenbezogener Daten* im Internet.
- 2.3. Unbefugte und nicht einvernehmliche Anmeldung bei Webdiensten (z. B. Spam, Dating-Websites und Newsletter).

- 2.4. Unbefugtes und nicht einvernehmliches Abrufen oder Schliessen persönlicher Webkonten (z. B. soziale Medien und E-Mail).
- 2.5. Veraltete *personenbezogene Daten* in Suchmaschinen (z. B. weiterhin angezeigte Inhalte trotz erfolgter Löschung, mit negativen Ergebnissen verbundene Namensgleichheiten und falsche oder ungenaue *personenbezogene Daten*).
- 2.6. Online-Beleidigungen, Verleumdung, üble Nachrede, Aufstachelung zum Hass.
- 2.7. Unbefugte Nutzung der im öffentlichen Internet verfügbaren *personenbezogenen Daten* der *versicherten Person* durch unbefugte Dritte, die sich als die *versicherte Person* ausgeben.
- 2.8. Weitergabe der *personenbezogenen Daten* der *versicherten Person* im Darknet.

3. Versicherungsleistungen

- 3.1. Informationsdienstleistungen zu Veröffentlichungen im Internet.
Die *Allianz* unterstützt die *versicherte Person* mit Informationen, um ihre *personenbezogenen Daten* und Informationen vor weiterem Missbrauch zu schützen.
- 3.2. Informationsdienstleistungen zum Diebstahl digitaler Identitäten.
Die *Allianz* unterstützt die *versicherte Person* mit Informationen, um ihre *personenbezogenen Daten* und Informationen vor weiterem Missbrauch zu schützen, die online von Dritten verwendet wurden, um sich als die *versicherte Person* auszugeben, oder die im Darknet veröffentlicht wurden.
- 3.3. Entfernungsversuch.
Die *Allianz* beauftragt einen Anbieter, der gegebenenfalls versucht, das *versicherte Ereignis* zu beheben.
- 3.4. Zugang zu einem Netzwerk von Rechtsanwälten.
Die *Allianz* stellt der *versicherten Person* die Kontaktdaten von Rechtsanwälten zur Verfügung, die auf die Bearbeitung der versicherten Ereignisse spezialisiert sind.
- 3.5. Psychologische Hilfe und Umzug.
Die *Allianz* organisiert und bezahlt eine erste Beurteilung durch einen klinischen Psychologen, wobei diese mittels Telefoninterviews erfolgt. Erfordert die Situation der *versicherten Person* oder ihrer *Familienmitglieder* eine Behandlung, überweist der Psychologe die *versicherte Person* oder ihre *Familienmitglieder* zu persönlichen Beratungsgesprächen mit einem Psychologen in der Nähe des Wohn- oder Arbeitsortes der *versicherten Person*. Hält der Psychologe einen Umzug für notwendig, übernimmt die *Allianz* die Umzugskosten für die *versicherte Person* oder ihre *Familienmitglieder*.

4. Versicherte Ereignisse mit geltenden Leistungen und Obergrenzen

Die folgende Tabelle enthält eine Liste der Ereignisse (in Zeilen) mit einer Liste der Leistungen (in Spalten), die für diese Ereignisse gelten, sowie die kumulierte Obergrenze (in der letzten Zeile) jeder Leistung über alle versicherten Ereignisse hinweg.

Leistung \ Ereignis	Information sdienstleistungen zu Veröffentlichungen im Internet	Information sdienstleistungen zum Diebstahl digitaler Identitäten	Entfernungsversuch	Zugang zu einem Netzwerk von Rechtsanwälten	Psychologische Hilfe und Umzug
Unbefugte und nicht einvernehmliche Veröffentlichungen auf persönlichen Websites, Blogs und Social-Media-Konten	✓	✗	✓	✓	✓
Unbefugte und nicht einvernehmliche Offenlegung oder Veröffentlichung <i>personenbezogener Daten</i> im Internet	✓	✗	✓	✓	✓
Unbefugte und nicht einvernehmliche Anmeldung bei Webdiensten (z. B. Spam, Dating-Websites und Newsletter)	✓	✗	✓	✓	✓

Unbefugtes und nicht einvernehmliches Abrufen oder Schliessen persönlicher Webkonten (z. B. soziale Medien und E-Mail)	✓	x	✓	✓	✓
Veraltete <i>personenbezogene Daten</i> in Suchmaschinen	✓	x	✓	✓	✓
Online-Beleidigungen, Verleumdung, üble Nachrede, Aufstachelung zum Hass	✓	x	✓	✓	✓
Unbefugte Nutzung der im öffentlichen Internet verfügbaren <i>personenbezogenen Daten</i> der <i>versicherten Person</i> durch unbefugte Dritte, die sich als <i>versicherte Person</i> ausgeben	x	✓	x	✓	✓
Weitergabe der <i>personenbezogenen Daten</i> der <i>versicherten Person</i> im Darknet	x	✓	x	✓	✓
Kumulierte Obergrenzen	unbegrenzt	unbegrenzt	2 Ereignisse pro <i>Versicherungsschutz</i> pro Jahr	unbegrenzt	2 Ereignisse pro <i>Versicherungsschutz</i> pro Jahr CHF 3'000 pro Ereignis

5. Leistungsobergrenzen

Die *Allianz* garantiert zwar, dass die vereinbarten Massnahmen ergriffen werden, kann jedoch weder garantieren noch davon ausgehen, dass alle Fälle gelöst werden können.

Die Dienstleistung im Rahmen der e-Reputation Unterstützung wird erbracht, jedoch kann kein positives Ergebnis garantiert werden:

Tritt der Schaden oder das Ereignis in einer privaten Gruppe oder auf einer Webseite auf, deren Zugriff durch ein Passwort beschränkt ist (Chats, Instant-Messaging-Apps, E-Mails und geschlossene Social-Media-Gruppen), erhält die *versicherte Person* technische Beratung und bewährte Vorgehensweisen in Bezug auf den Fall.

Psychologische Betreuung:

- ist verfügbar von Montag bis Freitag, ausser an Feiertagen, von 9:00 bis 18:00 Uhr;
- deckt keine **vorbestehenden psychischen Erkrankungen ab, die vor dem Datum des Inkrafttretens des *Versicherungsschutzes* diagnostiziert wurden oder behandelt werden.**

6. Ausschlüsse und Einschränkungen

Zusätzlich zu Abschnitt I 10 «Allgemeine Ausschlüsse» besteht kein *Versicherungsschutz* für die folgenden Ereignisse oder Risiken:

6.1. Ereignisse im Zusammenhang mit nicht digitalen Medien (Printmedien, Radio, Fernsehen).

- 6.2. Ereignisse, die Gegenstand eines Verfahrens vor den zuständigen Gerichten sind oder Gegenstand gerichtlicher Entscheidungen waren.
- 6.3. Ereignisse im Zusammenhang mit der Tätigkeit der *versicherten Person* als *Influencer*.
- 6.4. *Verletzung von Persönlichkeitsrechten* und persönliche Beleidigungen durch ehemalige Ehegatten, im gleichen Haushalt lebende Ehegatten oder Partner, Lebenspartner.
- 6.5. Versicherte Ereignisse im Zusammenhang mit Journalisten oder journalistischen Tätigkeiten und/oder Veröffentlichungen.

C. Banking-Schutz

1. Einführung

Gemäss den *Allgemeinen Versicherungsbedingungen* und im Zusammenhang mit versicherten Ereignissen, welche die *versicherte Person* oder die *Zahlungsmittel* der *versicherten Person* und ihrer *Familienmitglieder* betreffen, leistet die *Allianz* Folgendes:

- Gibt der *versicherten Person* Auskunft, wie sie diese versicherten Ereignisse mit ihrem *Finanzinstitut/Bankkartenherausgeber* abwickeln kann.
- Übernimmt die notwendigen Verwaltungskosten.
- Übernimmt Auslagen.
- Erstattet der *versicherten Person* bei *nicht autorisierten missbräuchlichen Zahlungsvorgängen* bis zur Höhe der in der *Einzel-/Familiendeckung* angegebenen *maximalen Versicherungssumme* entweder ihre finanziellen Verluste, die durch den Missbrauch eines mobilen Geräts entstanden sind, oder gesetzliche oder vertragliche Bestimmungen und *Selbstbehalte*, die nicht durch die Erstattung ihrer Verluste durch das *Finanzinstitut/den Bankkartenherausgeber* auf subsidiärer Basis gedeckt sind.

Darüber hinaus deckt die *Allianz* die *versicherte Person* gemäss diesen *Allgemeinen Versicherungsbedingungen* bis zur *maximalen Versicherungssumme* der *Allianz* gegen *autorisierte missbräuchliche Zahlungsvorgänge* aufgrund der folgenden Betrugsmaschen ab:

- *Phishing*
- *Smishing*

2. Versicherte Ereignisse

- 2.1. *Nicht autorisierter missbräuchlicher Zahlungsvorgang*
- 2.2. *Diebstahl physischer Zahlungsmittel*
- 2.3. *Verlust physischer Zahlungsmittel*
- 2.4. *Beschädigung oder Zerstörung physischer Zahlungsmittel*
- 2.5. *Autorisierter missbräuchlicher Zahlungsvorgang* aufgrund von *Phishing*
- 2.6. *Autorisierter missbräuchlicher Zahlungsvorgang* aufgrund von *Smishing*

3. Versicherungsleistungen

Die von der *Allianz* angebotenen Leistungen sind nachfolgend aufgeführt:

3.1. Informationsdienstleistungen

Bereitstellung relevanter Informationen für die *versicherte Person* zu den folgenden Schritten:

- Meldung von Betrugsfällen an das *Finanzinstitut/den Bankkartenherausgeber*
- Rückforderung *nicht autorisierter missbräuchlicher Zahlungsvorgänge* direkt vom *Finanzinstitut/Bankkartenherausgeber*
- Einreichung einer Anzeige bei der Polizei
- Geltendmachung eines Anspruchs im Schadenfall gegenüber dem *Finanzinstitut/Bankkartenherausgeber*
- *Zahlungsmittel* erneuern
- Sperrung des *Zahlungsmittels*

3.2. Erstattung der damit verbundenen Verwaltungskosten

Die *Allianz* erstattet die notwendigen mit dem *versicherten Ereignis* verbundenen Verwaltungskosten, einschliesslich Briefmarken, Bearbeitungsgebühren, Steuern und Kosten für Auslandsgespräche.

3.3. Erstattung der Auslagen im Zusammenhang mit dem Anspruch im Schadenfall

Die *Allianz* erstattet notwendige Transport- und Unterbringungskosten im Zusammenhang mit dem *versicherten Ereignis*, einschliesslich Taxikosten für die Fahrt zum Polizeiposten oder zum *Finanzinstitut/Bankkartenherausgeber* sowie Hotelkosten, die erforderlich sind, um das Ereignis während einer Reise der Polizei zu melden.

3.4. Erstattung *nicht autorisierter missbräuchlicher Zahlungsvorgänge*

Die *Allianz* erstattet der *versicherten Person* im Rahmen der *maximalen Versicherungssumme* der *Allianz* *nicht autorisierte missbräuchliche Zahlungsvorgänge*, die über ihre *Zahlungsmittel* (einschliesslich des

Missbrauchs mobiler Geräte) getätigt wurden, sofern das *Finanzinstitut/der Bankkartenherausgeber* für diesen Vorfall keinerlei Erstattung leistet und die *versicherte Person* ihre im nachfolgenden Abschnitt dieses Dokuments aufgeführten Pflichten erfüllt hat.

Alternativ erstattet die *Allianz* der *versicherten Person* bis zur Höhe der *maximalen Versicherungssumme* der *Allianz* den *Selbstbehalt*, falls das *Finanzinstitut/der Bankkartenherausgeber* gesetzliche oder vertragliche Bestimmungen und *Selbstbehalte* für diesen Fall anwendet.

3.5. Erstattung *autorisierter missbräuchlicher Zahlungsvorgänge*

Die *Allianz* erstattet der *versicherten Person* bis zur Höhe der *maximalen Versicherungssumme* der *Allianz* *autorisierte missbräuchliche Zahlungsvorgänge*, die direkt verursacht wurden durch:

- *Phishing*
- *Smishing*

Falls das *Finanzinstitut/der Bankkartenherausgeber* für diesen Fall keinerlei Erstattung leistet und die *versicherte Person* ihre im folgenden Abschnitt dieses Dokuments aufgeführten Pflichten erfüllt hat.

Alternativ erstattet die *Allianz* der *versicherten Person* bis zur Höhe der *maximalen Versicherungssumme* der *Allianz* den *Selbstbehalt*, falls das *Finanzinstitut/der Bankkartenherausgeber* gesetzliche oder vertragliche Bestimmungen und *Selbstbehalte* für diesen Fall anwendet.

4. Versicherte Ereignisse, versicherte Leistungen und *maximale Versicherungssummen*

Versicherte Ereignisse	Versicherte Leistungen	Maximale Versicherungssummen
<i>Nicht autorisierte missbräuchliche Zahlungsvorgänge mit Zahlungsmitteln</i> (finanzielle Verluste aufgrund des Missbrauchs eines mobilen Geräts, gesetzliche oder vertragliche Bestimmungen und <i>Selbstbehalte</i> , die nicht vom <i>Finanzinstitut/Bankkartenherausgeber</i> übernommen werden)	<ul style="list-style-type: none"> ▪ Erstattung <i>nicht autorisierter missbräuchlicher Zahlungsvorgänge</i> ▪ Informationsdienstleistungen 	CHF 20'000 pro <i>Versicherungsschutz</i> pro Jahr
	<ul style="list-style-type: none"> ▪ Erstattung der damit verbundenen Verwaltungskosten ▪ Erstattung der Auslagen im Zusammenhang mit dem Anspruch im Schadenfall 	CHF 300 pro <i>Versicherungsschutz</i> pro Jahr
<i>Diebstahl, Beschädigung, Verlust oder Zerstörung der physischen Zahlungsmittel der versicherten Person</i>	<ul style="list-style-type: none"> ▪ Erstattung der damit verbundenen Verwaltungskosten ▪ Erstattung der Auslagen im Zusammenhang mit dem Anspruch im Schadenfall ▪ Informationsdienstleistungen 	CHF 300 pro <i>Versicherungsschutz</i> pro Jahr
<i>Autorisierter missbräuchlicher Zahlungsvorgang</i> aufgrund von <i>Phishing</i> und <i>Smishing</i>	<ul style="list-style-type: none"> ▪ Erstattung des <i>autorisierten missbräuchlichen Zahlungsvorgangs</i> ▪ Erstattung der damit verbundenen Verwaltungskosten ▪ Erstattung der Auslagen im Zusammenhang mit dem Anspruch im Schadenfall ▪ Informationsdienstleistungen 	CHF 1'000 pro <i>Versicherungsschutz</i> pro Jahr

Die *Allianz* nimmt keine direkte Kommunikation/Kontaktaufnahme mit Bonitätsauskunftsdienssten, Kartennetzwerken und/oder *Finanzinstituten/Bankkartenherausgebern* im Namen der *versicherten Person* vor. Die *Einzel-/Familiendeckung* bietet keinen *Versicherungsschutz* für *Zahlungsmittel*, die der *versicherten Person* nicht von *Finanzinstituten/Bankkartenherausgebern* zur Verfügung gestellt werden.

5. Pflichten der versicherten Person

Die *versicherte Person* muss die folgenden gesetzlichen Pflichten einhalten, um im Falle von versicherten Ereignissen Anspruch auf diesen *Versicherungsschutz* zu haben.

Stellt die *Allianz* Unstimmigkeiten zwischen der Erklärung und den vorgelegten Nachweisen fest, kann sie den *Versicherungsschutz* verweigern.

Frist für die Meldung von Ansprüchen im Schadenfall:

Zusätzlich zum Recht der *versicherten Person*, eine Transaktion innerhalb von 30 Tagen nach dem Datum der monatlichen Abrechnung durch das *Finanzinstitut/den Bankkartenherausgeber* gemäss den für dieses Bank- oder Zahlungskartenprodukt geltenden Allgemeinen Geschäftsbedingungen abzulehnen, muss die *versicherte Person* alles in ihrer Macht Stehende tun, um den Schaden zu vermeiden oder zu mindern. Dazu gehört auch die regelmässige und zeitnahe Überprüfung der Liste der ausgeführten Transaktionen, die der *versicherten Person* vom *Finanzinstitut/Bankkartenherausgeber* zur Verfügung gestellt wird. Unterlässt die *versicherte Person* dies, kann sie ihren Anspruch auf Entschädigung verlieren. Im Falle einer schuldhaften Unterlassung dieser Pflicht ist die *Allianz* berechtigt, die Entschädigung entsprechend dem Verschuldensgrad zu kürzen. Versichert sind nur rechtzeitig gemeldete Ansprüche im Schadenfall. Aus diesem Grund sind Ansprüche im Schadenfall, die von *versicherten Personen* geltend gemacht werden, innerhalb der folgenden Fristen zu melden.

In Fällen von *autorisierten missbräuchlichen Zahlungsvorgängen* muss die *versicherte Person* dies der *Allianz* innerhalb von 3 Tagen, nachdem sie davon Kenntnis erlangt hat, und spätestens 30 Tage nach dem Datum des oben genannten Monatsauszugs melden, indem sie einen Anspruch im Schadenfall geltend macht.

Im Falle eines *Diebstahls der physischen Zahlungsmittel* der *versicherten Person* darf die Zeitspanne zwischen dem Erkennen des *Diebstahls der physischen Zahlungsmittel* der *versicherten Person* und der Beantragung der Sperrung der gestohlenen *physischen Zahlungsmittel* bei dem *Finanzinstitut/Bankkartenherausgeber* maximal 24 Stunden betragen.

Vor Eintritt von versicherten Ereignissen:

5.1. Wirksames Sicherheitssystem

Die Pflicht, ein aktives und auf dem neuesten Stand befindliches Sicherheitssystem auf den Geräten zu installieren, die die *versicherte Person* und ihre *Familienmitglieder* für ihre Online-Aktivitäten und Zahlungen nutzen, das einen präventiven Mindestschutz gegen Folgendes bietet:

- Viren und Malware,
- *Phishing* und *Smishing* (betrügerische Weblinks und Websites),
- unsichere Verbindungen beim Aufrufen von Banking- und Zahlungswebsites.

Die *versicherte Person* ist berechtigt, ein Sicherheitssystem ihrer Wahl zu verwenden, sofern dieses das oben beschriebene Mindestmass an Schutz bietet.

Die *Allianz* kann der *versicherten Person* auch die *Allyz Security App* zur Verfügung stellen, die ein wirksames Sicherheitssystem eines externen *Anbieters* enthält.

Wir weisen darauf hin, dass in dem von der *Allyz Security App* der *Allianz* bereitgestellten Sicherheitssystem der Schutz möglicherweise nicht in allen Browsern aktiviert ist oder nicht von allen Browsern unterstützt wird gegen:

- *Phishing* und *Smishing* (betrügerische Weblinks und Websites) und
- unsichere Verbindungen beim Aufrufen von Banking- und Zahlungswebsites.

Wird ein Browser nicht unterstützt, muss die *versicherte Person* den in der *Allyz Security App* der *Allianz* enthaltenen Browser verwenden, um geschützt zu sein.

Das Sicherheitssystem der *Allyz Security App* gilt bei Ansprüchen im Schadenfall als nicht aktiv, wenn einer der obligatorischen Schutzmechanismen nicht aktiviert ist, selbst wenn das Sicherheitssystem auf dem neuesten Stand ist. In diesem Fall verliert die *versicherte Person* möglicherweise ihr Recht auf Entschädigung für solche Ansprüche im Schadenfall.

Sofern die *versicherte Person* ihre Pflichten erfüllt hat, hat sie Anspruch auf die Versicherungsleistungen.

Pflichten bei Ansprüchen im Schadenfall nach Feststellung des Eintritts eines versicherten Ereignisses:

5.2. Benachrichtigung des *Finanzinstituts/Bankkartenherausgebers*

Pflicht, das für die Verwaltung der *Zahlungsmittel* der *versicherten Person* zuständige *Finanzinstitut/den* zuständigen *Bankkartenherausgeber* so schnell wie möglich schriftlich über den Eintritt des versicherten Ereignisses und den entstandenen Schaden zu informieren.

5.3. Kontosperrung

Pflicht zur Sperrung der Konten der *versicherten Person* und zur Geltendmachung ihrer Ansprüche im Schadenfall gegenüber dem *Finanzinstitut/Bankkartenherausgeber*, das/der ihre *Zahlungsmittel* verwaltet.

- Die *versicherte Person* ist verpflichtet, das/den für die Verwaltung ihrer *Zahlungsmittel* zuständige *Finanzinstitut/Bankkartenherausgeber* unverzüglich mit der Sperrung dieser *Zahlungsmittel* zu beauftragen.

5.4. Polizeibericht

Pflicht, den Vorfall unverzüglich beim nächsten Polizeiposten zu melden und der *Allianz* eine Bestätigung der Polizei zuzusenden, dass die *versicherte Person* eine Anzeige im Zusammenhang mit dem Anspruch im Schadenfall erstattet hat.

- 5.5. Bestätigung des Versicherungsschutzes durch das *Finanzinstitut/den Bankkartenherausgeber*
Wenn das/der für die Verwaltung der *Zahlungsmittel* der *versicherten Person* zuständige *Finanzinstitut/Bankkartenherausgeber* den Schaden der *versicherten Person* nicht oder nicht vollständig übernimmt oder einen *Selbstbehalt* verlangt, muss die *versicherte Person* der *Allianz* eine entsprechende Bestätigung des *Finanzinstituts/Bankkartenherausgebers* vorlegen.
- 5.6. Betrügerisch bezahlte Partei
Pflicht, der *Allianz* die Angaben des *Finanzinstituts/Bankkartenherausgebers* der betrügerisch bezahlten Partei (z. B. Bankkontonummer, Name des Empfängers und *Wohnsitzland*) vorzulegen oder Massnahmen zu ergreifen, um diese zu beschaffen.
- 5.7. Zusätzliche Unterlagen
Pflicht, der *Allianz* die unten aufgeführten Unterlagen vorzulegen oder Schritte einzuleiten, um diese ausstellen zu lassen:
- Kopie der schriftlichen Mitteilung, durch die der Anspruch im Schadenfall entstanden ist (E-Mail oder SMS mit bösartigem Link oder Anweisungen zu einer Transaktion)
 - Kopie der Benachrichtigung darüber, wie und wann der Betrug und der *autorisierte missbräuchliche Zahlungsvorgang* stattgefunden haben (Widerspruchsformular), welche von der *versicherten Person* an das *Finanzinstitut/den Bankkartenherausgeber* gesendet wurde
 - Betrugsbericht des *Finanzinstituts/Bankkartenherausgebers* mit Identifizierung oder Schlussfolgerung zu:
 - *autorisiertem missbräuchlichem Zahlungsvorgang*
 - Grundursache des Betrugs sowohl aus Sicht des *Finanzinstituts/Bankkartenherausgebers* als auch aus Sicht der *versicherten Person*
 - Grad der Fahrlässigkeit der *versicherten Person*
 - Bestätigung des *Finanzinstituts/Bankkartenherausgebers* über Folgendes:
 - Dass eine Rückerstattung beim empfangenden *Finanzinstitut/Bankkartenherausgeber* des *autorisierten missbräuchlichen Zahlungsvorgangs* beantragt wurde
 - Die Daten der einzelnen Rückerstattungsanträge und die entsprechenden Antworten (falls vorhanden)
 - Ob das empfangende Institut den Rückerstattungsantrag abgelehnt hat und, falls ja, den Grund für die Ablehnung
- 5.8. Informationen zum Sicherheitssystem
Pflicht der *versicherten Person*, zu bestätigen, dass entweder ein gültiges Sicherheitssystem ihrer Wahl oder das in der *Allyz Security App* von *Allianz* enthaltene Sicherheitssystem auf den Geräten und in den von der *versicherten Person* verwendeten Browsern installiert, aktiv und auf dem neuesten Stand war, während die *versicherte Person* die *Phishing*-E-Mail oder *Smishing*-SMS gelesen und den *autorisierten missbräuchlichen Zahlungsvorgang* aufgrund von *Phishing* oder *Smishing* ausgelöst, ausgeführt und autorisiert hat.
Hat sich die *versicherte Person* für ein anderes wirksames Sicherheitssystem ihrer Wahl entschieden, benötigt die *Allianz* ausserdem die folgenden Informationen darüber:
- Name und Version
 - *Kaufbeleg* (falls nicht kostenlose Version)
 - Endbenutzer-Lizenzvertrag
 - Software-Dokumentation mit Beschreibung des bereitgestellten Schutzes
- 5.9. Status des Sicherheitssystems
Pflicht zur Bereitstellung aller Protokolle oder Aktivitätsverläufe des Geräts (Betriebssystem oder andere Quellen), die nachweisen, dass das Sicherheitssystem installiert, aktiv und auf dem neuesten Stand war, als die *Phishing*- oder *Smishing*-Nachricht gelesen und der *autorisierte missbräuchliche Zahlungsvorgang* ausgeführt wurde.

Nachstehend sind die Ereignisse und die jeweils geltenden Pflichten für die *versicherte Person* aufgeführt.

Pflicht Ereignis	Benachrichtigung des Finanzinstituts/Bankkartenherausgebers	Kontospeicherung	Polizeibericht	Bestätigung des Versicherungsschutzes durch das/den Finanzinstitut/Bankkartenherausgeber	Betrügerisch bezahlte Partei	Zusätzliche Unterlagen	Informationen zum Sicherheitssystem	Status des Sicherheitssystems
Nicht autorisierter missbräuchlicher Zahlungsvorgang	✓	✗	✓	✓	✓	✗	✓	✓
Diebstahl der physischen Zahlungsmittel der versicherten Person	✓	✓	✓	✓	✗	✗	✗	✗
Verlust der physischen Zahlungsmittel	✓	✓	✓	✓	✗	✗	✗	✗
Beschädigung oder Zerstörung der physischen Zahlungsmittel der versicherten Person	✓	✗	✗	✗	✗	✗	✗	✗
Autorisierter missbräuchlicher Zahlungsvorgang aufgrund von Phishing oder Smishing	✓	✗	✓	✓	✓	✓	✓	✓

Alle von der *versicherten Person* zurückerhaltenen Beträge, die über den finanziellen Verlust abzüglich der von der *Allianz* geleisteten Zahlungen aus Ansprüchen im Schadenfall hinausgehen, müssen von der *versicherten Person* bis zur Höhe des erstatteten Betrags an die *Allianz* zurückgezahlt werden.

6. Ausschlüsse und Einschränkungen

Zusätzlich zu Abschnitt I 10 «Allgemeine Ausschlüsse» besteht kein *Versicherungsschutz* für folgende Ereignisse oder Risiken:

6.1 Ansprüche im Schadenfall, die sich aus der Verbreitung vertraulicher Informationen, der Speicherung oder Weitergabe von Passwörtern, Zugangscodes und ähnlich vertraulichen Informationen (PIN, TAN, Kartennummern, CVV, andere Identifikations- oder Legitimationsdaten, digitale Signaturen oder echte Inhabertitel oder Ausweispapiere usw.) in der Öffentlichkeit und/oder durch mangelnde Sorgfalt ergeben.

6.2 Jegliche autorisierte missbräuchliche Zahlungsvorgänge:

- die nicht auf *Phishing* oder *Smishing* zurückzuführen sind;
- die nicht von der *versicherten Person* oder einem *Familienmitglied* in der mit dem *Finanzinstitut/Bankkartenherausgeber* vereinbarten Form autorisiert wurden;
- die aufgrund von *Phishing* oder *Smishing* erfolgten, während das Sicherheitssystem auf den Geräten, die die *versicherte Person* zum Lesen der *Phishing*-E-Mail oder *Smishing*-SMS und zum Auslösen, Ausführen und Autorisieren des *autorisierten missbräuchlichen Zahlungsvorgangs* aufgrund von *Phishing* oder *Smishing* verwendet hat, nicht installiert, nicht aktiv oder nicht auf dem neuesten Stand war;
- die auf *Phishing* und *Smishing* zurückzuführen sind, das aus E-Mails und SMS stammt, in denen dieselben Szenarien dargestellt werden, mit denen die *versicherte Person* bereits in der Vergangenheit dazu verleitet wurde, Schritte für einen Zahlungsvorgang zu unternehmen oder persönliche Daten preiszugeben, die dazu verwendet werden, Geld von den *Zahlungsmitteln* der *versicherten Person* abzuheben, wie beispielsweise ungewöhnliche Anfragen um Unterstützung oder Geld von:
 - *Familienmitgliedern* in Schwierigkeiten,
 - möglichen romantischen Partnern,
 - Technikern von Versorgungs-, Telekommunikations- oder IT-Unternehmen,
 - Bankangestellten oder Bankinstituten,
 - Kollegen oder Vorgesetzten am Arbeitsplatz oder
 - Headhuntern oder Arbeitgebern;
- die auf *Phishing*- oder *Smishing*-Korrespondenz zurückzuführen sind, die von anderen Personen als der *versicherten Person* und ihren *Familienmitgliedern*, einschliesslich, aber nicht beschränkt auf Mitinhaber ihrer *Zahlungsmittel*, empfangen oder bearbeitet wurde.

6.3 Jeglicher Zahlungsvorgang:

- der in der Erwartung getätigt wurde, Kryptowährungen, NFTs, Finanzinstrumente, Beratungsdienstleistungen, Gold und andere Edelmetalle, Gas- oder Stromlieferungen, Spielgegenstände, Konzert- oder Veranstaltungstickets zu erhalten – zum Zwecke der Gewinnerzielung;
- bei dem die von *Finanzinstituten/Bankkartenherausgebern* implementierten Massnahmen zur Betrugsbekämpfung von der *versicherten Person* deaktiviert wurden (z. B. Tageslimit/Einrichtung eines neuen Profils für die *versicherte Person*/Zwei-Faktor-Authentifizierung);
- der von einer anderen Person als der *versicherten Person* getätigt wurde, unabhängig davon, ob diese in ihrem Namen handelt oder nicht, einschliesslich, aber nicht beschränkt auf *Familienmitglieder* und Mitinhaber ihrer *Zahlungsmittel*, unabhängig davon, ob diese allein oder in Absprache mit anderen handeln;
- der zugunsten von Personen getätigt wurde, die die *versicherte Person* kennt oder mit denen die *versicherte Person* in irgendeiner Beziehung oder Bekanntschaft steht, zum Beispiel:
 - die Eltern, Kinder, Tanten, Onkel, Cousins, Enkelkinder der *versicherten Person* oder ihres Ehepartners,
 - Personen, mit denen die *versicherte Person* persönliche Beziehungen unterhält oder unterhalten hat, die durch Freundschaft, Vertrauen und regelmässigen Kontakt gekennzeichnet sind,
 - Personen, mit denen die *versicherte Person* geschäftliche oder berufliche Beziehungen unterhält oder unterhalten hat;
- unter Verwendung von Bargeld, Schecks, Bankenvollmachten;
- der von der *versicherten Person* als Reaktion auf eine Lösegeldforderung oder eine andere illegale Forderung oder Drohung geleistet wurde. Dazu gehören unter anderem: Daten-Kidnapping; Drohungen, Daten oder andere Vermögenswerte der *versicherten Person* zu löschen, zu ändern, zu verbreiten oder den Zugriff darauf zu ändern;
- bei dem ein Teil oder der gesamte finanzielle Verlust durch eine andere Partei oder eine andere Versicherung gedeckt ist;
- im Zusammenhang mit Lotterien, unerwarteten Erbschaften oder ähnlichen unaufgeforderten Versprechungen oder unehrlichen Anreizen;
- der erfolgt, wenn die Sicherheitslösung installiert und auf dem neuesten Stand, aber nicht aktiv ist, insbesondere auf Geräten, Betriebssystemen oder Browsern, die von der gültigen Sicherheitslösung nicht unterstützt werden oder bei denen nicht alle Mindestschutzmassnahmen aktiviert sind;
- der nicht mit *Zahlungsmitteln* erfolgt, insbesondere solchen, die nicht von einem *Finanzinstitut/Bankkartenherausgeber* bereitgestellt werden.

6.4 Jegliche finanziellen Verluste:

- die aus der unbefugten Verwendung von *Zahlungsmitteln* oder PIN, TAN, CVV, anderen Identifikations- oder Legitimationsdaten, einer digitalen Signatur oder echten Inhabertiteln oder Ausweispapieren resultieren, die sich im Besitz anderer befanden oder in den Besitz anderer gelangt sind oder von denen

- andere vor Beginn des *Versicherungsschutzes* Kenntnis erlangt oder die sie gestohlen haben;
- die von einer anderen Partei oder einem anderen Unternehmen stammen, die bzw. das die personenbezogenen Daten der *versicherten Person* absichtlich, unabsichtlich oder infolge einer *Verletzung der Datensicherheit* oder eines Cyberangriffs offengelegt hat;
- die gemäss geltenden Gesetzen, Vorschriften oder Richtlinien einer zuständigen Behörde, eines Gerichts oder einer Regierung, sowohl auf lokaler als auch auf regionaler Ebene, versichert sind;
- für die ein *Finanzinstitut/Bankkartenherausgeber* haftet und seine Haftung nicht schriftlich ausgeschlossen hat;
- die entstanden sind, weil die *versicherte Person*, die für die Sperrung ihrer *Zahlungsmittel* zuständigen Institutionen nicht kontaktieren konnte;
- die auf Fehler in legitimem elektronischem Code oder Schäden durch Code zurückzuführen sind, der während des Herstellungsprozesses, des Upgrade-Prozesses oder der normalen Wartung auf den elektronischen Geräten der *versicherten Person* installiert wurde;
- die sich aus den Online-Aktivitäten der *versicherten Person* auf Geräten mit Browsern oder Betriebssystemen ergeben, die von der Sicherheitslösung nicht unterstützt werden.

6.5 Jegliche Ansprüche im Schadenfall, die sich aus der Verwendung nicht persönlicher *Zahlungsmittel* ergeben.

D. Allyz Security App

1. Einführung

Die folgenden Dienste werden über die *Allyz Security App* und ihre Komponenten als integraler Bestandteil der Produktkomponente Banking-Schutz angeboten.

Die *Allyz Security App* soll die *versicherte Person* und ihre *Familienmitglieder* im Rahmen der *Familiendeckung* bei ihren digitalen Aktivitäten schützen und bietet Schutz für die *versicherte Person* oder ihre *Familienmitglieder* in Bezug auf:

- Geräte und Surfen im Internet,
- online vorhandene *personenbezogene Daten*,
- digitale Passwörter,
- Datenschutz

vor digitalen Bedrohungen.

Die *Allianz* stellt der *versicherten Person* oder der *versicherten Person* und ihren *Familienmitgliedern* über einen externen *Anbieter der Allianz* eine spezielle Technologielösung zur Verfügung.

Komponente	Leistungsbeschreibung	Grenzen
Endpunktsicherheit	<p>Es handelt sich um eine Komponente der <i>Allyz Security App</i>, die der <i>versicherten Person</i> eine umfassende Reihe von Funktionen und Features bietet:</p> <ul style="list-style-type: none"> ▪ Schutz vor Malware ▪ Schutz beim Surfen <p>Sie bietet grundlegende Internetsicherheitsfunktionen zum Schutz vor:</p> <ul style="list-style-type: none"> ▪ allen gängigen Bedrohungen wie Viren, Trojanern und Ransomware, indem alle Dateien und Anwendungen gescannt werden ▪ unsicheren Websites wie <i>Phishing</i>-Seiten und Websites, die Malware verbreiten, indem diese als sicher oder unsicher eingestuft werden. 	<p><i>Versicherungsschutz</i> für <i>Einzeldeckung</i>: 3 Geräte*</p> <p><i>Versicherungsschutz</i> für <i>Familiendeckung</i>: 5 Geräte*</p>
Betrugsschutz	<p>Es handelt sich um eine Komponente der <i>Allyz Security App</i>, die bösartige Nachrichten und bösartige Shopping-Websites markieren soll.</p> <p>Darüber hinaus markiert sie auch unsichere WLAN-Netzwerke und blockiert viele Werbe-Pop-ups und Cookie-Zustimmungsaufforderungen.</p>	<p><i>Versicherungsschutz</i> für <i>Einzeldeckung</i>: 3 Geräte*</p> <p><i>Versicherungsschutz</i> für <i>Familiendeckung</i>: 5 Geräte*</p>

Familienregeln	Dies ist eine Komponente der <i>Allyz Security App</i> , die Eltern umfassende Funktionen zur Verfügung stellt, um gesunde Grenzen für Kinder im Internet festzulegen, wie z. B. Zeitlimits oder Inhaltsfilter.	<i>Versicherungsschutz für Einzeldeckung:</i> 3 Geräte* <i>Versicherungsschutz für Familiendeckung:</i> 5 Geräte*
ID-Überwachung	<p>Dies ist eine Komponente der <i>Allyz Security App</i>, die der <i>versicherten Person</i> Sicherheitsfunktionen für ihre Online-<i>Datenpunkte</i> bietet.</p> <p>Die ID-Überwachung überwacht das Internet einschliesslich des Darknets auf durchgesickerte oder gehackte <i>Datenpunkte</i>. Kontinuierliche Überwachung und umsetzbare Anweisungen im Falle einer Sicherheitsverletzung unterstützen die <i>versicherte Person</i> dabei, auf das Risiko eines Identitätsdiebstahls angemessen zu reagieren.</p> <p>In der Regel werden <i>Datenpunkte</i> im Rahmen einer grösseren Datenverletzung ins Internet geleakt. Falls die personenbezogenen Daten der <i>versicherten Person</i> unter den geleakten Daten gefunden werden, wird die <i>versicherte Person</i> per E-Mail und/oder anderen Kommunikationsmethoden, z. B. über die Anwendung, über die Datenverletzung informiert. In der Benachrichtigung wird hervorgehoben, welche personenbezogenen Daten von der Datenverletzung betroffen sind, um die Schwere der Verletzung besser zu verdeutlichen.</p>	<i>Versicherungsschutz für Einzeldeckung:</i> 3 Geräte* <i>Versicherungsschutz für Familiendeckung:</i> 5 Geräte*
Passwortverwaltung	<p>Es handelt sich um eine Komponente der <i>Allyz Security App</i>, die der <i>versicherten Person</i> eine Passwortverwaltungsfunktion bietet.</p> <p>Sie dient als vorbeugende Massnahme gegen viele Online-Bedrohungen wie Kontoübernahmen und Identitätsdiebstahl. Sie unterstützt die <i>versicherte Person</i> dabei, das Risiko einer Kontoübernahme und eines Identitätsdiebstahls zu verringern, indem sie der <i>versicherten Person</i> hilft, alle Konten und Passwörter unter Kontrolle zu behalten.</p> <p>Sie speichert Passwörter, PIN-Codes, Sozialversicherungsnummern und andere kleine Informationsangaben sicher. Auf den eigenen Geräten der <i>versicherten Person</i> wird ein sicherer Passwortspeicher eingerichtet. Dieser Speicher ist durch ein vom Benutzer festgelegtes Hauptpasswort geschützt, und die <i>versicherte Person</i> kann mühelos sichere und einzigartige Passwörter erstellen und speichern.</p> <p>Die Passwortanalysefunktion weist auf minderwertige, wiederverwendete und häufig verwendete Passwörter hin, die die <i>versicherte Person</i> im Passwortspeicher abgelegt hat. Durch die Passwortsynchronisierung werden die Passwörter der <i>versicherten Person</i> auf allen Geräten, auf denen die <i>Allyz Security App</i> installiert ist, auf dem neuesten Stand gehalten.</p>	<i>Versicherungsschutz für eine Einzeldeckung:</i> 3 Geräte* <i>Versicherungsschutz für Familiendeckung:</i> 5 Geräte*
Privatsphärenschutz (Virtual Private Network)	<p>Dies ist eine Komponente der <i>Allyz Security App</i>, die der <i>versicherten Person</i> eine auf VPN-Technologie (Virtual Private Network) basierende Funktion bietet.</p> <p>Sie fügt eine weitere Schutzebene für den gesamten Online-Datenverkehr hinzu und ermöglicht der <i>versicherten Person</i> eine sicherere Verbindung zum Internet.</p> <p>Ausserdem verbessert sie den allgemeinen Schutz für mobile Geräte und den Schutz für Kinder mit der Endpunktsicherheits-Komponente.</p> <p>Die Einrichtung von Komponenten kann je nach Plattform unterschiedlich sein.</p>	<i>Versicherungsschutz für Einzeldeckung:</i> 3 Geräte* <i>Versicherungsschutz für Familiendeckung:</i> 5 Geräte*

Technischer Support	Technischer Fernsupport, der der <i>versicherten Person</i> Informationen zur Nutzung der <i>Allyz Security App</i> und zur Behebung von damit zusammenhängenden Problemen bereitstellt: <ul style="list-style-type: none"> ▪ Online-Dokumentation ▪ Hotline Die <i>versicherte Person</i> kann die Hotline der <i>Allianz</i> unter +41 44 283 31 12 kontaktieren.	Montag bis Freitag: 8:00–17:00 Uhr ausser an Feiertagen
----------------------------	---	---

* Nur auf Geräten verfügbar, die die Systemanforderungen erfüllen; wird möglicherweise auf älteren Geräten nicht unterstützt.

2. Service-Spezifikationen

Die *Allianz* und der externe *Anbieter* der *Allianz* können Folgendes nicht garantieren:

- einen vollständigen und absoluten Schutz vor Computerviren und anderen Netzwerkbedrohungen und Betrugsversuchen;
- die Vollständigkeit der Suche;
- die Erkennung aller *Verletzungen der Datensicherheit* im Internet;
- die Löschung oder Blockierung aller gefundenen *Verletzungen der Datensicherheit*.

Die Komponenten der *Allyz Security App* sind nur auf Geräten verfügbar, auf denen die *Allyz Security App* installiert, auf dem neuesten Stand, aktiv und funktionsfähig ist. Die *Einzeldeckung* gilt nur für Geräte, die sich im Besitz der *versicherten Person* befinden.

3. Pflichten der versicherten Person

Zur Nutzung der *Allyz Security App* muss die *versicherte Person*:

- über ein aktives *Allyz-Konto* verfügen – die *versicherte Person* wird bei Vertragsabschluss aufgefordert, ein solches Konto auf der *Allyz-Website* mit einem persönlichen Benutzernamen und Passwort anzulegen;
- die *Allyz Security App* herunterladen – bei Abschluss des Vertrags wird eine Aktivierungs-E-Mail mit einem Zugriffslink an die *versicherte Person* gesendet;
- sich mit ihren *Allyz-Anmeldedaten* (Benutzername und Passwort) bei der *Allyz Security App* anmelden.

Vor dem Herunterladen und der Nutzung der *Allyz Security App* muss die *versicherte Person* die Endbenutzer-Lizenzvereinbarung des *Anbieters* sorgfältig lesen und akzeptieren.

Wenn die *versicherte Person* mit den Bedingungen nicht einverstanden ist, kann die *versicherte Person* den Dienst nicht nutzen.

Damit die *Allyz Security App* bei den Browsing-Aktivitäten der *versicherten Person* auf ihren Geräten aktiv ist, muss sie Browser verwenden, die alle zwingenden Schutzmassnahmen der *Allyz Security App* unterstützen und diese aktivieren. Verfügt die *versicherte Person* nicht über solche Browser, kann sie für ihre Browsing-Aktivitäten den in der *Allyz Security App* integrierten Browser verwenden.

4. Ausschlüsse in Bezug auf die *Allyz Security App*

Alle Einschränkungen hinsichtlich der Nutzung und des Umfangs sowie alle Haftungsbeschränkungen im Rahmen des angebotenen Dienstes müssen auch in der Endbenutzer-Lizenzvereinbarung des *Anbieters* überprüft werden, die die Zustimmung der *versicherten Person* vor der Nutzung des angebotenen Dienstes erfordert.

E. Datenwiederherstellung

1. Einführung

Gemäss diesen *Allgemeinen Versicherungsbedingungen* wird dieser *Versicherungsschutz* für die Wiederherstellung digitaler Daten gewährt, die auf dem *Gerät* der *versicherten Person* gespeichert sind, wenn ein versichertes Ereignis eintritt.

2. Versicherte Ereignisse

2.1. Datenverlust aufgrund einer *versehentlichen Beschädigung* des *Geräts* durch:

- Flüssigkeit,
- Herunterfallen,
- Sturz,
- Aufprall,
- sonstige Sachschäden.

- 2.2. Datenverlust aufgrund einer internen Fehlfunktion des *Geräts*
- 2.3. Datenverlust aufgrund von Malware
- 2.4. Datenverlust aufgrund eines Virus
- 2.5. Datenverlust aufgrund eines Softwarefehlers
- 2.6. Datenverlust aufgrund von Stromausfall
- 2.7. Datenverlust aufgrund von Bedienungsfehlern
- 2.8. Datenverlust aufgrund versehentlicher Löschung von Dateien
- 2.9. Datenverlust aufgrund eines Softwareausfalls

3. Versicherungsleistungen

- 3.1. Vermittlung eines Spezialanbieters für den Versuch der Wiederherstellung der digitalen Daten der *versicherten Person* oder ihrer *Familienmitglieder*

Die *Allianz* unternimmt den Versuch, die digitalen Daten der *versicherten Person* oder ihrer *Familienmitglieder* in einem Reparaturzentrum wiederherzustellen, einschliesslich einer erforderlichen ersten Schadensanalyse. Gelingt die Wiederherstellung der digitalen Daten, stellt die *Allianz* der *versicherten Person* oder ihren *Familienmitgliedern* die wiederhergestellten digitalen Daten auf einem externen Laufwerk zur Verfügung.

- 3.2. Versand- und Entsorgungskosten

Die *Allianz* unternimmt den Versuch, die digitalen Daten der *versicherten Person* oder ihrer *Familienmitglieder* in einem Reparaturzentrum wiederherzustellen, und gibt das *Gerät* der *versicherten Person* oder ihren *Familienmitgliedern* zurück oder entsorgt es auf Wunsch der *versicherten Person* oder ihrer *Familienmitglieder*, wenn es beschädigt ist – dies gilt nur im *Wohnsitzland* der *versicherten Person* oder ihrer *Familienmitglieder*.

4. Versicherte Ereignisse mit geltenden Leistungen und Obergrenzen

Die folgende Tabelle enthält eine Liste der Ereignisse (in Zeilen) mit einer Liste der Leistungen (in Spalten), die für diese Ereignisse gelten, sowie die kumulierte Obergrenze (in der letzten Zeile) jeder Leistung über alle versicherten Ereignisse hinweg.

Leistung \ Ereignis	Vermittlung eines Spezialanbieters für den Versuch der Wiederherstellung der digitalen Daten der <i>versicherten Person</i>	Versand- und Entsorgungskosten
Datenverlust aufgrund einer <i>versehentlichen Beschädigung</i> des <i>Geräts</i> durch: <ul style="list-style-type: none"> ▪ Flüssigkeit, ▪ Herunterfallen, ▪ Sturz, ▪ Aufprall, ▪ sonstige Sachschäden. 	✓	✓
Datenverlust aufgrund eines internen Defekts des <i>Geräts</i>	✓	✓
Datenverlust aufgrund von Malware	✓	✓
Datenverlust aufgrund eines Virus	✓	✓
Datenverlust aufgrund eines Softwarefehlers	✓	✓
Datenverlust aufgrund von Stromausfall	✓	✓
Datenverlust aufgrund von Bedienungsfehlern	✓	✓
Datenverlust aufgrund versehentlicher Löschung von Dateien	✓	✓
Datenverlust aufgrund eines Softwareausfalls	✓	✓
Kumulierte Leistungen	2 Ereignisse pro <i>Versicherungsschutz</i> pro Jahr	2 Ereignisse pro <i>Versicherungsschutz</i> pro Jahr

5. Leistungsobergrenzen

- Die *Allianz* kann nicht garantieren, dass verlorene digitale Daten erfolgreich wiederhergestellt werden können.
- Die *Allianz* kann digitale Daten der *versicherten Person* oder ihrer *Familienmitglieder* bis zu einer Grösse von 8 TB wiederherstellen.
- Während der Wiederherstellung digitaler Daten wird das *Gerät* der *versicherten Person* oder ihrer *Familienmitglieder* möglicherweise beschädigt (z. B. durch das Aufbrechen von Siegeln oder Gehäusen), sodass es nicht mehr repariert oder wiederhergestellt werden kann. Dies führt möglicherweise zum Verlust der Herstellergarantien.

6. Pflichten der versicherten Person

6.1. Informationen:

Die *versicherte Person* oder die *versicherte Person* und ihre *Familienmitglieder* müssen der *Allianz* oder dem Anbieter der *Allianz* Informationen über das Datenverlustproblem und die Details des *Geräts* und des Betriebssystems zur Verfügung stellen.

6.2. Wirksames Sicherheitssystem im Falle eines Datenverlusts aufgrund von Malware und Viren:

Pflicht zur Installation eines aktiven und aktuellen Sicherheitssystems auf *Geräten*, die die *versicherte Person* zur Speicherung ihrer Daten verwendet, das mindestens einen vorbeugenden Schutz vor Viren und Malware bietet.

Die *versicherte Person* ist berechtigt, ein Sicherheitssystem ihrer Wahl zu verwenden, sofern dieses das oben beschriebene Mindestmass an Schutz bietet.

Die *Allianz* kann der *versicherten Person* oder der *versicherten Person* und ihren *Familienmitgliedern* auch die *Allyz Security App* der *Allianz* zur Verfügung stellen, die ein wirksames Sicherheitssystem eines externen *Anbieters* der *Allianz* enthält.

Darüber hinaus müssen die *versicherte Person* oder die *versicherte Person* und ihre *Familienmitglieder* bestätigen, dass zum Zeitpunkt des Datenverlusts entweder ein wirksames Sicherheitssystem ihrer Wahl oder das in der *Allyz Security App* der *Allianz* enthaltene Sicherheitssystem auf ihrem *Gerät* installiert, aktiv und auf dem neuesten Stand war.

Hat sich die *versicherte Person* für ein anderes wirksames Sicherheitssystem ihrer Wahl entschieden, benötigt die *Allianz* ausserdem die folgenden Informationen darüber:

- Name und Version
- *Kaufbeleg* (falls nicht kostenlose Version)
- Endbenutzer-Lizenzvertrag
- Software-Dokumentation mit Beschreibung des bereitgestellten Schutzes

Weitere Informationen zur *Allyz Security App* der *Allianz* finden Sie in den entsprechenden Abschnitten dieser *Allgemeinen Geschäftsbedingungen*: «*Allyz Security App*», und «Ausschlüsse in Bezug auf die *Allyz Security App*».

Die Ereignisse (in Zeilen) und die Pflichten (in Spalten), die jeweils gelten, sind unten aufgeführt.

	Pflicht	Informationen	Wirksames Sicherheitssystem
Ereignis			
Datenverlust aufgrund einer <i>versehentlichen Beschädigung</i> des <i>Geräts</i> durch: <ul style="list-style-type: none"> ▪ Flüssigkeit, ▪ Herunterfallen, ▪ Sturz, ▪ Aufprall, ▪ sonstige Sachschäden. 		✓	✗
Datenverlust aufgrund eines internen Defekts des <i>Geräts</i>		✓	✗
Datenverlust aufgrund von Malware		✓	✓
Datenverlust aufgrund eines Virus		✓	✓
Datenverlust aufgrund eines Softwarefehlers		✓	✗
Datenverlust aufgrund von Stromausfall		✓	✗

Datenverlust aufgrund von Bedienungsfehlern	✓	✗
Datenverlust aufgrund versehentlicher Löschung von Dateien	✓	✗
Datenverlust aufgrund eines Softwareausfalls	✓	✗

7. Besondere Bedingungen und Anspruchsberechtigung

Die Datensicherung umfasst nur Versuche zur Datenwiederherstellung von folgenden *Geräten*:

- HDD und SSD von Laptops und Computern.
- Externe HDD und SSD (USB-Laufwerke).
- Handys und Smartphones.
- Tablets.
- Netbooks.
- Speicherkarten (z. B. SD-Karte, CF-Karte).
- USB-Sticks.

Voraussetzungen sind, dass das *Gerät*:

- bei der *Einzeldeckung* im Besitz der *versicherten Person* und bei der *Familiendeckung* im Besitz der *versicherten Person* und ihrer *Familienmitglieder* ist;
- bei der *Einzeldeckung* von der *versicherten Person* und bei *Familiendeckung* nur von der *versicherten Person* und ihren *Familienmitgliedern* genutzt wird;
- nur für den persönlichen Gebrauch genutzt wird.

8. Ausschlüsse und Einschränkungen

Zusätzlich zu Abschnitt I 10 «Allgemeine Ausschlüsse» besteht kein *Versicherungsschutz* für folgende Gegenstände, Ereignisse oder Risiken:

8.1. Folgende Gegenstände sind nicht abgedeckt:

- Spielkonsolen,
- Disketten, CDs, DVDs, Blu-Ray,
- VHS-Kassetten,
- mehrere Laufwerke in einer RAID-Konfiguration.

8.2. Ausfall eines *Geräts*, das von der *versicherten Person* geöffnet wurde.

8.3. Neukonfiguration oder Neuinstallation des *Geräts* oder seines Betriebssystems und Kosten für den Ersatz digitaler Daten und Anwendungen.

8.4. Kosten für den Erwerb neuer Lizenzen.

8.5. Versandkosten, wenn sich das *Gerät* der *versicherten Person* nicht in ihrem *Wohnsitzland* befindet.

8.6. Wiederherstellung von Daten, die noch vollständig als Sicherungskopie auf einem anderen Speichermedium vorhanden sind.

8.7. Schäden, für die der Hersteller haftet.

8.8. Serienfehler, die zu einem Rückruf durch den Hersteller führen.

8.9. Kosten, die durch Daten mit rechtswidrigen Inhalten und/oder Daten entstehen, zu deren Nutzung keine Berechtigung besteht.