HISCOX
WISSEN VERSICHERT.

Hiscox CyberClear Österreich

Gegenüberstellung der wesentlichen Neuerungen von Hiscox CyberClear 10/2020 zu Hiscox CyberClear 06/2022

Alle Änderungen können Sie bei Bedarf gerne im Detail mit Ihrem Underwriter besprechen.

CYBERCLEAR 10/2020 ÖSTERREICH		CYBER CLEAR 06/2022 ÖSTERREICH		Kommentar
I. Was ist versichert?				
I. Was ist versichert?	Der Versicherer gewährt den Versicherten im Rahmen der nachstehenden Bedingungen Versicherungsschutz für Vermögensschäden aufgrund folgender Ereignisse (Cyber-Schäden): • einer Netzwerksicherheitsverletzung; • eines Bedien- und Programmierfehlers; • einer Datenrechtsverletzung; • einer Cyber-Erpressung; • einer Rechtsverletzung durch Werbung und Marketing. Versicherungsschutz besteht für Eigenschäden in Form von Soforthilfe im Notfall gemäß Ziffer II.1.1., für Kosten und Schäden gemäß Ziffer II.2. als auch für Cyber-Betriebsunterbrechungsschäden gemäß Ziffer II.4. Zudem besteht Versicherungsschutz für Vermögensschäden eines Dritten gemäß Ziffer II.3., aufgrund derer ein Versicherter in Anspruch genommen wird (Cyber-Haftpflicht). Vermögensschäden sind Schäden, die weder Personenschäden (Tötung, Verletzung des Körpers oder Schädigung der Gesundheit von Menschen) noch Sachschäden (Beschädigung, Verderben, Vernichtung oder Abhandenkommen von Sachen, insbesondere von Geld und geldwerten Zeichen) sind noch sich aus solchen Schäden herleiten. Schäden infolge des Verlusts oder der Einschränkung der Verfügbarkeit, Integrität oder Vertraulichkeit elektronischer Daten werden als Vermögensschäden angesehen.	I. Was ist versichert?	Der Versicherer gewährt den Versicherten im Rahmen der nachstehenden Bedingungen Versicherungsschutz für Vermögensschäden aufgrund folgender Ereignisse (Cyber-Schäden): • einer Netzwerksicherheitsverletzung; • eines Bedien- und Programmierfehlers; • einer Datenrechtsverletzung; • einer Cyber-Erpressung. Versicherungsschutz besteht für Eigenschäden in Form von Soforthilfe im Notfall gemäß Ziffer II.1.1., für Kosten und Schäden gemäß Ziffer II.2. als auch für Cyber-Betriebsunterbrechungsschäden gemäß Ziffer II.4. Zudem besteht Versicherungsschutz für Vermögensschäden eines Dritten gemäß Ziffer II.3., aufgrund derer ein Versicherter in Anspruch genommen wird (Cyber-Haftpflicht). Vermögensschäden sind Schäden, die weder Personenschäden (Tötung, Verletzung des Körpers oder Schädigung der Gesundheit von Menschen) noch Sachschäden (Beschädigung, Verderben, Vernichtung oder Abhandenkommen von Sachen, insbesondere von Geld und geldwerten Zeichen) sind noch sich aus solchen Schäden herleiten. Schäden infolge des Verlusts oder der Einschränkung der Verfügbarkeit, Integrität oder Vertraulichkeit elektronischer Daten werden als Vermögensschäden angesehen.	Rechtsverletzung durch Werbung und Markting nur infolge eines Triggers gem. Zif. I.1 - I.4 versichert
I.5. Rechtsverletzung durch Werbung und Marketing	Eine Rechtsverletzung durch Werbung und Marketing liegt vor, wenn im Zusammenhang mit Veröffentlichungen zu Werbe- und Marketingzwecken für die Produkte oder die Dienstleistungen der Versicherten Rechte Dritter verletzt werden.	I.5. Rechtsverletzung durch Werbung und Marketing	gestrichen	Rechtsverletzung durch Werbung und Markting nur infolge eines Triggers gem. Zif. I.1 - I.4 versichert
II. Was leistet der Versicherer?				
	Der Versicherer gewährt den Versicherten Versicherungsschutz in Form der nachstehenden Leistungen.	II. Was leistet der Versicherer?	Der Versicherer gewährt den Versicherten Versicherungsschutz in Form der nachstehenden Leistungen. Leistungen nach den Ziffern II.2.7. (Cyber-Diebstahl), II.2.8. (Cyber-Betrug), II.2.13. (E-Discovery), II.4.1. (Cyber-Betriebsunterbrechung On-Premises), II.4.1.4. (Cyber-Betriebsunterbrechung On-Premises bei technischen Problemen) und II.4.2. (Cyber-Betriebsunterbrechung bei Cloud-Ausfall) werden nur gewährt, wenn und soweit dies im Versicherungsschein durch Aufnahme einer diesbezüglichen Entschädigungsgrenze vereinbart wird. Soweit der Versicherungsschein keine diesbezügliche Entschädigungsgrenze enthält, sind diese Leistungsarten nicht vom Versicherungsschutz umfasst.	Klarstellung, dass optionale Bausteine nur dann als versichert gelten, wenn im Versicherungsschein mit einer entsprechenden Entschädigungsgrenze explizit die Deckung ausgewiesen ist.

HISCOX
WISSEN VERSICHERT.

Hiscox CyberClear Österreich

Gegenüberstellung der wesentlichen Neuerungen von Hiscox CyberClear 10/2020 zu Hiscox CyberClear 06/2022

II.1. Assistance-Leistungen		II.1. Assistance-Leistungen		
II.1.1. Soforthilfe im Notfall	Bei Bestehen einer konkreten Risikolage für einen Versicherten übernimmt der Versicherer die Kosten des Krisendienstleisters für eine erste telefonische Notfallund Krisenunterstützung in Form von: • einer Experteneinschätzung zur geschilderten Lage, • Empfehlungen für Sofortmaßnahmen zur Schadenbegrenzung, • Empfehlungen für Sofortmaßnahmen zur Ursachenermittlung, • einer ersten Bewertung der bisherigen Maßnahmen und soweit erforderlich • einer Ermittlung, ob eine Netzwerksicherheitsverletzung vorliegt. Eine konkrete Risikolage liegt vor, wenn aus Sicht eines Versicherten oder einer mitversicherten natürlichen Person der tatsächliche oder der künftige Eintritt eines versicherten Ereignisses gemäß Ziffern I.1. bis I.4. aufgrund der objektiven Umstände zu vermuten ist. Darüber hinaus ersetzt der Versicherer im Rahmen der Soforthilfe im Notfall auch die notwendigen anfallenden Kosten, die zur Bestimmung der geltenden Melde- und Anzeigepflichten infolge einer Datenrechtsverletzung gemäß Ziffer I.3. und zur Erstellung entsprechender Anzeigen und Meldungen entstehen. Hinsichtlich der Kosten für die Soforthilfe im Notfall fällt weder ein Selbstbehalt an, noch werden diese Kosten auf die Versicherungssumme angerechnet.	II.1.1. Soforthilfe im Notfall	Bei Bestehen einer konkreten Risikolage für einen Versicherten übernimmt der Versicherer bei entsprechender Verfügbarkeit die Bereitstellung und Kosten des Krisendienstleisters für eine erste Notfall- und Krisenunterstützung in Form von: • einer Experteneinschätzung zur Risikolage, • Empfehlungen für Sofortmaßnahmen zur Schadenbegrenzung, • Empfehlungen für Sofortmaßnahmen zur Ursachenermittlung, • einer ersten Bewertung der bisherigen Maßnahmen und • soweit erforderlich einer Ermittlung, ob eine Netzwerksicherheitsverletzung vorliegt. Eine konkrete Risikolage liegt vor, wenn aus Sicht eines Versicherten oder einer mitversicherten natürlichen Person der tatsächliche oder der künftige Eintritt eines versicherten Ereignisses gemäß Ziffern I.1. bis I.4. aufgrund der objektiven Umstände zu vermuten ist. Darüber hinaus ersetzt der Versicherer im Rahmen der Soforthilfe im Notfall auch die notwendigen anfallenden Kosten, die zur Bestimmung der geltenden Melde- und Anzeigepflichten infolge einer Datenrechtsverletzung gemäß Ziffer I.3. und zur Erstellung entsprechender Anzeigen und Meldungen entstehen. Hinsichtlich der Kosten für die Soforthilfe im Notfall fällt weder ein Selbstbehalt an, noch werden diese Kosten auf die Versicherungssumme angerechnet.	Klarstellende Änderung. Es wird keine Änderung am Assistance Angebot oder Verhalten im Schadenfall auf Seiten der Hiscox oder des Krisendienstleisters geben. Im Fall eines Kumul-Schadenfalls soll an dieser Stelle jedoch transparent auf die Möglichkeiten eines Engapsses in der Kapazität hingewiesen werden. Hiscox begenet dieser Herausforderung bereits jetzt, indem Kapazitäten bei den Krisendienstleistern deutlich ausgeweitet wurden.
II.2.7. Cyber-Diebstahl	Der Versicherer ersetzt Vermögensschäden, die einem Versicherten dadurch entstehen, dass unmittelbar infolge einer Netzwerksicherheitsverletzung gemäß Ziffer I.1. Gelder (auch Kryptowährungen), Waren oder Wertpapiere abhandenkommen oder dass erhöhte Nutzungsentgelte anfallen, da Anwendungen, z. B. Voice-over-IP, in unzulässiger Weise genutzt werden. Im Rahmen des Cyber-Diebstahls besteht Versicherungsschutz auch für Vermögensschäden, die einem Versicherten dadurch entstehen, dass unmittelbar infolge einer Netzwerksicherheitsverletzung gemäß Ziffer I.1. erhöhte Nutzungsentgelte oder Versorgungsrechnungen (Strom, Gas oder Wasser) anfallen, weil das IT-System des Versicherten zur Schürfung von Kryptowährungen (Krypto-Mining) missbraucht wird. Nicht vom Versicherungsschutz umfasst sind somit lediglich mittelbar entstandene Schäden, insbesondere Schäden, die als Folge einer Täuschung hervorgerufen werden, wie beispielsweise bei Fake-President-Fällen. Für Cyber-Diebstahl gilt die im Versicherungsschein benannte Entschädigungsgrenze.	II.2.7. Cyber-Diebstahl (sofern im Versicherungsschein besonders vereinbart)	Der Versicherer ersetzt Vermögensschäden, die einem Versicherten dadurch entstehen, dass unmittelbar infolge einer Netzwerksicherheitsverletzung gemäß Ziffer I.1. Gelder (auch Kryptowährungen), Waren oder Wertpapiere abhandenkommen oder dass erhöhte Nutzungsentgelte anfallen, da Anwendungen, z. B. Voice-over-IP, in unzulässiger Weise genutzt werden. Im Rahmen des Cyber-Diebstahls besteht Versicherungsschutz auch für Vermögensschäden, die einem Versicherten dadurch entstehen, dass unmittelbar infolge einer Netzwerksicherheitsverletzung gemäß Ziffer I.1. erhöhte Nutzungsentgelte oder Versorgungsrechnungen (Strom, Gas oder Wasser) anfallen, weil das IT-System des Versicherten zur Schürfung von Kryptowährungen (Krypto-Mining) missbraucht wird. Nicht vom Versicherungsschutz umfasst sind somit lediglich mittelbar entstandene Schäden, insbesondere Schäden, die als Folge einer Täuschung hervorgerufen werden, wie beispielsweise bei Fake-President-Fällen. Für Cyber-Diebstahl gilt die im Versicherungsschein ausgewiesene Entschädigungsgrenze.	Cyber Diebstahl nur noch optionaler Baustein für mehr Flexibilität in der Deckung. Keine Änderung an der Deckung selbst.

HISCOX
WISSEN VERSICHERT.

Hiscox CyberClear Österreich

Gegenüberstellung der wesentlichen Neuerungen von Hiscox CyberClear 10/2020 zu Hiscox CyberClear 06/2022

II.3. Cyber-Haftpflicht	Der Versicherer gewährt den Versicherten Versicherungsschutz, wenn sie infolge eines versicherten Ereignisses gemäß Ziffern I.1. bis I.4. von einem Dritten aufgrund gesetzlicher Haftpflichtansprüche privatrechtlichen Inhalts für einen Vermögensschaden in Anspruch genommen werden. Versicherungsschutz in der Cyber-Haftpflicht besteht auch für immaterielle Schäden, die sich aus versicherten Vermögensschäden herleiten. Hierzu zählen immaterielle Schäden aufgrund einer Persönlichkeitsrechtsverletzung sowie psychischer Beeinträchtigungen (mental anguish oder emotional distress). Darüber hinaus gewährt der Versicherer den Versicherten auch Versicherungsschutz, wenn sie infolge von Werbung und Marketing für das eigene Unternehmen gemäß Ziffer I.5. von einem Dritten aufgrund gesetzlicher Haftpflichtansprüche privatrechtlichen Inhalts für einen Vermögensschaden in Anspruch genommen werden (Werbe-Haftpflicht)."	II.3. Cyber-Haftpflicht	Der Versicherer gewährt den Versicherten Versicherungsschutz, wenn sie infolge eines versicherten Ereignisses gemäß Ziffern I.1. bis I.4. von einem Dritten aufgrund gesetzlicher Haftpflichtansprüche privatrechtlichen Inhalts für einen Vermögensschaden in Anspruch genommen werden. Versicherungsschutz in der Cyber-Haftpflicht besteht auch für immaterielle Schäden, die sich aus versicherten Vermögensschäden herleiten. Hierzu zählen immaterielle Schäden aufgrund einer Persönlichkeitsrechtsverletzung sowie psychischer Beeinträchtigungen (mental anguish oder emotional distress). Insofern gewährt der Versicherer den Versicherten auch Versicherungsschutz, wenn sie im Zusammenhang mit einem versicherten Ereignis gemäß Ziffern I.1. bis I.4. infolge von Werbung und Marketing für das eigene Unternehmen von einem Dritten aufgrund gesetzlicher Haftpflichtansprüche privatrechtlichen Inhalts für einen Vermögensschaden in Anspruch genommen werden.	Haftpflichtansprüche aus Rechtsverletzungen durch Werbung und Markting nur infolge eines Triggers gem. Zif. I.1 - I.4 versichert
II.3.5.3. Vertragsstrafen wegen verzögerter Leistungser-bringung (sofern im Versicherungsschein besonders vereinbart)	Der Versicherer erstattet Vertragsstrafen, die ein Versicherter wegen verzögerter Leistungserbringung zahlen muss. Für Vertragsstrafen wegen verzögerter Leistungserbringung gilt die im Versicherungsschein benannte Entschädigungsgrenze.		gestrichen	Optional auf Anfrage weiterhin möglich.
II.4. Cyber-Betriebs-unterbrechung	Der Versicherer gewährt den Versicherten unter Berücksichtigung des im Versicherungsschein vereinbarten zeitlichen Selbstbehalts und der Haftzeit Versicherungsschutz, wenn unmittelbar und ausschließlich durch ein versichertes Ereignis im Sinne der Ziffern I.1. bis I.4. eine Cyber-Betriebsunterbrechung verursacht wird und hierdurch den Versicherten ein Ertragsausfallschaden entsteht. Versicherungsschutz im Rahmen der Cyber-Betriebsunterbrechung besteht nur, wenn die Daten und das IT-System der alleinigen Herrschaftsgewalt des Versicherten unterliegen oder er die vollständige Kontrolle darüber hat. Darüber hinaus besteht Versicherungsschutz im Rahmen der Cyber-Betriebsunterbrechung, wenn die Daten und das IT-System nicht der alleinigen Herrschaftsgewalt des Versicherten unterliegen und er nicht die vollständige Kontrolle darüber hat, sofern das versicherte Ereignis von dem Teil des IT-Systems des Versicherten ausgeht, der seiner alleinigen Herrschaftsgewalt unterliegt und über den er die vollständige Kontrolle hat. Außerdem besteht Versicherungsschutz im Rahmen der Cyber-Betriebsunterbrechung, wenn die Erreichbarkeit einer Webseite eines Versicherten ganz oder teilweise durch einen Denial-of-Service-Angriff unterbrochen wird, auch wenn die Webseite nicht der alleinigen Herrschaftsgewalt des Versicherten unterliegt oder er nicht die vollständige Kontrolle darüber hat.	II.4. Cyber-Betriebsunterbrechung (sofern im Versicherungsschein hierfür eine oder mehrere Entschädigungsgrenzen ausgewiesen sind)	Der Versicherer gewährt den Versicherten unter Berücksichtigung des im Versicherungsschein vereinbarten zeitlichen Selbstbehalts und der Haftzeit Versicherungsschutz, wenn unmittelbar und ausschließlich durch ein versichertes Ereignis im Sinne der Ziffern I.1. bis I.4. eine Cyber-Betriebsunterbrechung On-Premises (Ziffer II.4.1) oder eine Cyber-Betriebsunterbrechung bei Cloud-Ausfall (Ziffer II.4.2) verursacht wird und hierdurch den Versicherten ein Ertragsausfallschaden entsteht.	Cyber Betriebsunterbrechung insgesamt als optionaler Baustein. Eigenständige Bausteine entweder für IT-Systeme „On-Premises" oder in der Cloud möglich für individuellen Deckungsschutz je nachdem wo der Kunde seine IT-Systeme hat.
		4.1. Cyber-Betriebsunterbrechung On-Premises (sofern im Versicherungsschein hierfür eine Entschädigungsgrenze ausgewiesen ist)		Cyber BU für IT Systeme des Kunden vor Ort/ "On-Premises".

HISCOX
WISSEN VERSICHERT.

Hiscox CyberClear Österreich

Gegenüberstellung der wesentlichen Neuerungen von Hiscox CyberClear 10/2020 zu Hiscox CyberClear 06/2022

		II.4.1.1. Inhalt der Cyber-Betriebsunterbrechung On-Premises	Versicherungsschutz im Rahmen der Cyber-Betriebsunterbrechung On-Premises besteht nur, wenn die Daten und der Teil des IT-Systems, die von dem versicherten Ereignis betroffen sind, der alleinigen Herrschaftsgewalt des Versicherten unterliegen oder er die vollständige Kontrolle darüber hat. Darüber hinaus besteht Versicherungsschutz im Rahmen der Cyber-Betriebsunterbrechung On-Premises, soweit die Daten und das IT-System, die von dem versicherten Ereignis betroffen sind, nicht der alleinigen Herrschaftsgewalt des Versicherten unterliegen und er nicht die vollständige Kontrolle darüber hat, sofern das versicherte Ereignis von dem Teil des IT-Systems des Versicherten ausgeht, der seiner alleinigen Herrschaftsgewalt unterliegt oder über den er die vollständige Kontrolle hat.	Versicherungsschutz in der BU On-Premises besteht für das IT-System des Kunden vor Ort. Dies definiert sich über die Herrschaftsgewalt und Kontrolle. Weiterhin besteht Deckung auch für Daten und Systeme in der Cloud oder bei einem dritten Dienstleister, wenn die Netzwerksicherheitsverletzung oder ein anderes versichertes Ereignis von dem IT-System On-Premises ausgeht und auf die Daten und Systeme in der Cloud übergeht.
II.4.1. Begriff der Cyber-Betriebsunterbrechung	Eine versicherte Cyber-Betriebsunterbrechung liegt vor, wenn die Produktion eines Versicherten oder die Erbringung von Dienstleistungen durch einen Versicherten vollständig oder teilweise unterbrochen ist und wenn diese Unterbrechung unmittelbar und ausschließlich durch ein versichertes Ereignis gemäß Ziffern I.1. bis I.4. verursacht wird. Darüber hinaus besteht Versicherungsschutz für eine Betriebsunterbrechung, die durch eine Reparatur im Rahmen einer gemäß Ziffer II.2.5. versicherten Wiederherstellung verursacht wird. Außerdem besteht Versicherungsschutz für eine Betriebsunterbrechung, die durch eine geplante Abschaltung verursacht wird, um die Entstehung weiterer Schäden am IT-System oder den weiteren Verlust von Daten des Versicherten zu verhindern.	II.4.1.2. Begriff der Cyber-Betriebsunterbrechung On-Premises	Eine versicherte Cyber-Betriebsunterbrechung On-Premises liegt vor, wenn die Produktion eines Versicherten oder die Erbringung von Dienstleistungen durch einen Versicherten vollständig oder teilweise unterbrochen ist und wenn diese Unterbrechung unmittelbar und ausschließlich durch ein versichertes Ereignis gemäß Ziffern I.1. bis I.4. verursacht wird. Eine versicherte Cyber-Betriebsunterbrechung On-Premises liegt auch vor, wenn die Betriebsunterbrechung durch eine Reparatur im Rahmen einer gemäß Ziffer II.2.5. versicherten Wiederherstellung oder durch eine geplante Abschaltung verursacht wird, um die Entstehung weiterer Schäden am IT-System oder den weiteren Verlust von Daten des Versicherten zu verhindern.	Anpassung auf Systeme "On-Premises".
Alte Ziffer: II:4.7. Cyber-Betriebsunterbrechung durch Verfügung einer Datenschutzbehörde	Über die Cyber-Betriebsunterbrechung gemäß den vorstehenden Regelungen unter Ziffer II.4. hinaus besteht Versicherungsschutz auch für den einem Versicherten entstandenen Ertragsausfallschaden, der sich unmittelbar und ausschließlich aufgrund einer gegenüber einem Versicherten ergehenden Verfügung einer Datenschutzbehörde innerhalb des Europäischen Wirtschaftsraumes (EWR) oder des Vereinigten Königreichs Großbritannien und Nordirland (UK) infolge einer Datenrechtsverletzung gemäß Ziffer I.3. ergibt. Datenschutzbehörde in diesem Sinne ist jede Behörde, die nach dem Recht des jeweiligen Staates mit dem Vollzug datenschutzrechtlicher Normen beauftragt ist.	II.4.1.3. Cyber-Betriebsunterbrechung On-Premises durch Verfügung einer Datenschutzbehörde	Über die Cyber-Betriebsunterbrechung On-Premises gemäß den vorstehenden Regelungen unter Ziffer II.4.1.1. und II.4.1.2. hinaus besteht auch Versicherungsschutz für den einem Versicherten entstandenen Ertragsausfallschaden, der sich unmittelbar und ausschließlich aufgrund einer gegenüber einem Versicherten ergehenden Verfügung einer Datenschutzbehörde innerhalb des Europäischen Wirtschaftsraumes (EWR) oder des Vereinigten Königreichs Großbritannien und Nordirland (UK) infolge einer Datenrechtsverletzung gemäß Ziffer I.3. ergibt. Datenschutzbehörde in diesem Sinne ist jede Behörde, die nach dem Recht des jeweiligen Staates mit dem Vollzug datenschutzrechtlicher Normen beauftragt ist.	Nur sprachliche Anpassungen sowie neue Ziffer.

Hiscox CyberClear Österreich

Gegenüberstellung der wesentlichen Neuerungen von Hiscox CyberClear 10/2020 zu Hiscox CyberClear 06/2022

Alte Ziffer: II.4.9. Cyber-Betriebsunterbrechung bei Technischen Problemen (sofern im Versicherungsschein besonders vereinbart)	Über die Cyber-Betriebsunterbrechung gemäß den vorstehenden Regelungen unter Ziffer II.4. hinaus besteht auch Versicherungsschutz für den Ertragsausfallschaden eines Versicherten unmittelbar und ausschließlich aufgrund Technischer Probleme. Technische Probleme sind Fehlfunktionen des IT-Systems eines Versicherten, die nicht von einem versicherten Ereignis gemäß Ziffern I.1. bis I.4. verursacht werden, sondern unmittelbar und ausschließlich auf • einen Ausfall der Stromversorgung, • eine Über- und Unterspannung, • eine elektrostatische Aufladung und statische Elektrizität, • eine Überhitzung, • ein unterlassenes IT-Systemupgrade, • einen Softwarefehler, • einen internen Netzwerkfehler oder • einen IT-Hardwarefehler zurückzuführen sind. Die Fehlfunktion muss dabei unvorhergesehen und unbeabsichtigt gewesen sein. Darüber hinaus muss die Fehlfunktion von dem Teil des IT-Systems und der Stromversorgung ausgehen, welcher der alleinigen Herrschaftsgewalt eines Versicherten unterliegt oder über den der Versicherte die vollständige Kontrolle hat. Fehlfunktionen aufgrund allmählicher oder altersbedingter Reduzierung der Leistungsfähigkeit oder aufgrund von Überlastungen durch die fehlerhafte Planung der Auslastung des IT-Systems im gewöhnlichen Betrieb beziehungsweise der erhöhten Beanspruchung sind keine Technischen Probleme im Sinne dieser Bedingungen. Bei der Cyber-Betriebsunterbrechung bei Technischen Problemen kommen die Ziffern II.4.1. bis II.4.6. entsprechend zur Anwendung. Ergänzend gilt die im Versicherungsschein benannte Entschädigungsgrenze.	II.4.1.4. Cyber-Betriebsunterbrechung On-Premises bei technischen Problemen (sofern im Versicherungsschein hierfür eine Entschädigungsgrenze ausgewiesen ist)	Über die Cyber-Betriebsunterbrechung On-Premises gemäß den vorstehenden Regelungen unter Ziffer II.4.1.1. und II.4.1.2. hinaus besteht auch Versicherungsschutz für den Ertragsausfallschaden eines Versicherten unmittelbar und ausschließlich aufgrund technischer Probleme. Technische Probleme sind Fehlfunktionen des IT-Systems eines Versicherten, die nicht von einem versicherten Ereignis gemäß Ziffern I.1. bis I.4. verursacht werden, sondern unmittelbar und ausschließlich auf • einen Ausfall der Stromversorgung, • eine Über- und Unterspannung, • eine elektrostatische Aufladung und statische Elektrizität, • eine Überhitzung, • einen Softwarefehler, • einen internen Netzwerkfehler oder • einen IT-Hardwarefehler zurückzuführen sind. Die Fehlfunktion muss dabei unvorhergesehen und unbeabsichtigt gewesen sein. Darüber hinaus muss die Fehlfunktion von dem Teil des IT-Systems und der Stromversorgung ausgehen, welcher der alleinigen Herrschaftsgewalt eines Versicherten unterliegt oder über den der Versicherte die vollständige Kontrolle hat. Fehlfunktionen aufgrund allmählicher oder altersbedingter Reduzierung der Leistungsfähigkeit oder aufgrund von Überlastungen durch die fehlerhafte Planung der Auslastung des IT-Systems im gewöhnlichen Betrieb bzw. der erhöhten Beanspruchung sind keine technischen Probleme im Sinne dieser Bedingungen.	Nur sprachliche Anpassungen sowie neue Ziffer.
		II.4.2. Cyber-Betriebsunterbrechung bei Cloud-Ausfall (sofern im Versicherungsschein hierfür eine Entschädigungsgrenze ausgewiesen ist)		Cyber BU für IT Systeme des Kunden in der Cloud. Neu als eigenständiger Baustein auch einzeln abzuschließen.

HISCOX
WISSEN VERSICHERT.

Hiscox CyberClear Österreich

Gegenüberstellung der wesentlichen Neuerungen von Hiscox CyberClear 10/2020 zu Hiscox CyberClear 06/2022

Alte Ziffer: II.4.8. Cyber-Betriebsunterbrechung bei Cloud-Ausfall (sofern im Versicherungsschein besonders vereinbart)	Über die Cyber-Betriebsunterbrechung gemäß den vorstehenden Regelungen unter Ziffer II.4. hinaus besteht auch Versicherungsschutz für den Ertragsausfallschaden eines Versicherten unmittelbar und ausschließlich aufgrund eines versicherten Ereignisses gemäß Ziffern I.1. bis I.4., das von dem Teil des IT-Systems des Versicherten ausgeht, welches der Herrschaftsgewalt und Kontrolle eines dritten Dienstleisters (z. B. externes Rechenzentrum, Cloud-Anbieter) unterliegt, den ein Versicherter entgeltlich in Anspruch nimmt. Bei der Cyber-Betriebsunterbrechung bei Cloud-Ausfall kommen die Ziffern II.4.1. bis II.4.6. entsprechend zur Anwendung. Ergänzend gilt die im Versicherungsschein benannte Entschädigungsgrenze.	II.4.2.1 Inhalt der Cyber-Betribesunterbrechung bei Cloud-Ausfall	Versicherungsschutz im Rahmen der Cyber-Betriebsunterbrechung bei Cloud-Ausfall besteht nur, wenn die Daten und das IT-System, die von dem versicherten Ereignis betroffen sind, nicht der alleinigen Herrschaftsgewalt oder Kontrolle des Versicherten, sondern auch der Herrschaftsgewalt oder Kontrolle eines dritten Dienstleisters (z. B. externes Rechenzentrum, Cloud-Anbieter) unterliegen, den ein Versicherter entgeltlich in Anspruch nimmt. Darüber hinaus besteht Versicherungsschutz im Rahmen der Cyber-Betriebsunterbrechung bei Cloud-Ausfall, soweit die Daten und der Teil des IT-Systems, die von dem versicherten Ereignis betroffen sind, der alleinigen Herrschaftsgewalt oder Kontrolle des Versicherten unterliegen, sofern das versicherte Ereignis von dem Teil des IT-Systems des Versicherten ausgeht, der auch der Herrschaftsgewalt oder Kontrolle eines dritten Dienstleisters (z. B. externes Rechenzentrum, Cloud-Anbieter) unterliegt, den ein Versicherter entgeltlich in Anspruch nimmt. Eine versicherte Cyber-Betriebsunterbrechung bei Cloud-Ausfall im Sinne dieser Bedingungen setzt zudem voraus, dass der dritte Dienstleister mindestens ISO27001-zertifiziert oder in Tier Level 3 gemäß TIA-942 (Telecommunications Infrastructure Standard für Data Centers) eingestuft ist.	Deckung besteht auch bei versicherten Ereignissen, die Daten und Systeme des Kunden bei Cloud-Dienstleistern oder externen Rechenzentren betreffen (nicht in der Herrschaftsgewahlt und Kontrolle des VN). Weiterhin besteht Deckung auch für Daten und Systeme On-Premises, wenn die Netzwerksicherheitsverletzung oder ein anderes versichertes Ereignis von dem IT-System in der Cloud ausgeht und nur auf die Daten und Systeme On Premises übergeht. Deckungsvoraussetzung ist, dass der Dienstleister mind. ISO 27001 zertifiziert ist oder in Tier Level 3 eingestuft ist.
		II.4.2.2 Begriff der Cyber-Betriebsunterbrechung bei Cloud Ausfall	Eine versicherte Cyber-Betriebsunterbrechung bei Cloud-Ausfall liegt vor, wenn die Produktion eines Versicherten oder die Erbringung von Dienstleistungen durch einen Versicherten vollständig oder teilweise unterbrochen ist und wenn diese Unterbrechung unmittelbar und ausschließlich durch ein versichertes Ereignis gemäß Ziffern I.1. bis I.4. verursacht wird.	Neu für Cyber BU Cloud. Siehe Alte Ziffer II.4.1.
		II.4.3. Allgemeine Bestimmungen für die Cyber-Betriebsunterbrechung On-Premises oder bei Cloud-Ausfall		Neue Struktur, allgemeine Bestimmungen sowohl für BU On-Premises als auch für BU Cloud.
II.4.2. Begriff des Ertragsausfallschadens	Der Ertragsausfallschaden besteht aus den fortlaufenden Kosten und dem Betriebsgewinn, soweit ein Versicherter diese fortlaufenden Kosten und den Betriebsgewinn unmittelbar und ausschließlich infolge der durch die vollständige oder teilweise Nichtverfügbarkeit des IT-Systems bedingten Betriebsunterbrechung nicht – auch nicht zukünftig – erwirtschaften kann.	II.4.3.1 Begriff des Ertragsausfallschadens	Der Ertragsausfallschaden besteht aus den fortlaufenden Kosten und dem Betriebsgewinn, soweit ein Versicherter diese fortlaufenden Kosten und den Betriebsgewinn unmittelbar und ausschließlich infolge der durch die vollständige oder teilweise Nichtverfügbarkeit des IT-Systems bedingten und nach den Absätzen II.4.1. und II.4.2. versicherten Betriebsunterbrechung nicht – auch nicht zukünftig – erwirtschaften kann.	Nur Klarstellung.
II.4.3. Versicherter Zeitraum	Der versicherte Zeitraum beginnt ab dem Zeitpunkt, zu welchem der Versicherte dem Krisendienstleister oder dem Versicherer den Eintritt eines Versicherungsfalles angezeigt hat. Der versicherte Zeitraum endet zu dem Zeitpunkt, zu dem ein Ertragsausfallschaden nicht mehr entsteht, spätestens jedoch mit Ablauf der Haftzeit.	II.4.3.2 Versicherter Zeitraum	Der versicherte Zeitraum und die Haftzeit beginnen mit Eintritt der versicherten Cyber-Betriebsunterbrechung. Der versicherte Zeitraum endet zu dem Zeitpunkt, zu dem ein Ertragsausfallschaden nicht mehr entsteht, spätestens jedoch mit Ablauf der Haftzeit.	Beginn der Haftzeit mit Eintritt der Cyber-Betriebsunterbrechung nicht mehr mitAnzeige beim Dienstleister (jedoch weiterhin Obliegenheit zur unverzüglichen Anzeige des Schadens).

HISCOX
WISSEN VERSICHERT.

Hiscox CyberClear Österreich

Gegenüberstellung der wesentlichen Neuerungen von Hiscox CyberClear 10/2020 zu Hiscox CyberClear 06/2022

Alte Ziffer: IV.7.2. Zeitlicher Selbstbehalt (Wartezeit)	Die Laufzeit des zeitlichen Selbstbehalts beginnt mit Eintritt der versicherten Cyber-Betriebsunterbrechung und endet mit Ablauf der im Versicherungsschein bestimmten Zeit. Der zeitliche Selbstbehalt gilt als überschritten, wenn auch nach Ablauf des im Versicherungsschein vereinbarten zeitlichen Selbstbehalts das IT-System des Versicherten noch nicht wiederhergestellt ist und weiterhin ein Ertragsausfallschaden entsteht. Überschreitet der versicherte Zeitraum der Cyber-Betriebsunterbrechung die Laufzeit des zeitlichen Selbstbehalts, ersetzt der Versicherer den vollen Ertragsausfallschaden sowie etwaige Mehrkosten. Andernfalls wird ein Ertragsausfallschaden nicht ersetzt. Die Regelung zum monetären Selbstbehalt gemäß Ziffer IV.7.1.bleibt unberührt.	II.4.3.3. Zeitlicher Selbstbehalt	Die Laufzeit des im Versicherungsschein ausgewiesenen zeitlichen Selbstbehalts beginnt mit Eintritt der versicherten Cyber-Betriebsunterbrechung und endet mit Ablauf der im Versicherungsschein bestimmten Zeit. Der zeitliche Selbstbehalt gilt als überschritten, wenn auch nach Ablauf des im Versicherungsschein vereinbarten zeitlichen Selbstbehalts das IT-System des Versicherten noch nicht wiederhergestellt ist und weiterhin ein Ertragsausfallschaden entsteht. Die Regelung zum monetären Selbstbehalt gemäß Ziffer IV.7. bleibt unberührt.	Logisch in Ziffer II.4 integriert. NEU: Zeitlicher Selbstbehalt statt Wartezeit.
II.4.4. Wechselwirkungsschäden bei Cyber-Betriebsunterbrechung	Eine versicherte Betriebsunterbrechung liegt auch vor, wenn bei einem Versicherten ein Ertragsausfallschaden eintritt, der unmittelbar und ausschließlich aufgrund einer versicherten Cyber-Betriebsunterbrechung bei einem anderen Versicherten entsteht, sofern die Cyber-Betriebsunterbrechung bei diesem anderen Versicherten den zeitlichen Selbstbehalt gemäß Ziffer IV.7.2. überschreitet.	II.4.3.4. Wechselwirkungsschäden bei Cyber-Betriebsunterbrechung	Eine versicherte Betriebsunterbrechung liegt auch vor, wenn bei einem Versicherten ein Ertragsausfallschaden eintritt, der unmittelbar und ausschließlich aufgrund einer gemäß Ziffer II.4.1. oder Ziffer II.4.2. versicherten Cyber-Betriebsunterbrechung bei einem anderen Versicherten entsteht, sofern die Cyber-Betriebsunterbrechung bei diesem anderen Versicherten den zeitlichen Selbstbehalt gemäß Ziffer II.4.3.3. überschreitet.	Keine Änderung
II.4.5. Schadenunabhängige Umstände	Bei der Berechnung des Ertragsausfallschadens sind alle Umstände zu berücksichtigen, die das Geschäftsergebnis des Versicherten günstig oder ungünstig beeinflusst hätten, wenn die Cyber-Betriebsunterbrechung nicht eingetreten wäre. Die Entschädigung darf nicht zu einer Bereicherung eines Versicherten führen.	II.4.3.5. Schadenunabhängige Umstände	Bei der Berechnung des Ertragsausfallschadens sind alle Umstände zu berücksichtigen, die das Geschäftsergebnis des Versicherten günstig oder ungünstig beeinflusst hätten, wenn die Cyber-Betriebsunterbrechung nicht eingetreten wäre. Die Entschädigung darf nicht zu einer Bereicherung eines Versicherten führen.	Keine Änderung
II.4.6. Mehrkosten	Der Versicherer erstattet den Versicherten auch alle angemessenen und notwendigen Mehrkosten, die unmittelbar und ausschließlich infolge der durch die vollständige oder teilweise Nichtverfügbarkeit des IT-Systems bedingten Betriebsunterbrechung verursacht werden. Mehrkosten sind Kosten, die einem Versicherten unter normalen Umständen nicht entstehen und nach einer versicherten Cyber-Betriebsunterbrechung von einem Versicherten zur Fortführung des Betriebs aufgewendet werden müssen. Mehrkosten sind insbesondere Kosten für die Benutzung anderer Anlagen, die Anwendung anderer Arbeits- oder Fertigungsverfahren, die Inanspruchnahme von Lohndienstleistungen oder Lohn-Fertigungsleistungen, den Bezug von Halb- oder Fertigfabrikaten, einmalige Umprogrammierungskosten sowie Kosten, die durch die Ermittlung und Feststellung einer versicherten Cyber-Betriebsunterbrechung entstehen, soweit der Versicherte sie den Umständen nach für geboten halten durfte.	II.4.3.6. Mehrkosten	Der Versicherer erstattet den Versicherten auch alle angemessenen und notwendigen Mehrkosten, die unmittelbar und ausschließlich infolge der durch die vollständige oder teilweise Nichtverfügbarkeit des IT-Systems bedingten und gemäß Ziffer II.4.1. oder Ziffer II.4.2. versicherten Cyber-Betriebsunterbrechung verursacht werden. Mehrkosten sind Kosten, die einem Versicherten unter normalen Umständen nicht entstehen und nach einer versicherten Cyber-Betriebsunterbrechung von einem Versicherten zur Fortführung des Betriebs aufgewendet werden müssen. Mehrkosten sind insbesondere Kosten für die Benutzung anderer Anlagen, die Anwendung anderer Arbeits- oder Fertigungsverfahren, die Inanspruchnahme von Lohndienstleistungen oder Lohn-Fertigungsleistungen oder den Bezug von Halb- oder Fertigfabrikaten, einmalige Umprogrammierungskosten sowie Kosten, die durch die Ermittlung und Feststellung einer versicherten Cyber-Betriebsunterbrechung entstehen, soweit der Versicherte sie den Umständen nach für geboten halten durfte.	Keine Änderung
		4.3.7. Anwendbarkeit der Entschädigungsgrenzen	Für sämtliche Leistungen wegen einer Cyber-Betriebsunterbrechung gelten die im Versicherungsschein ausgewiesenen Entschädigungsgrenzen.	Klarstellung
II.4.10. Schadenminderungskosten	Der Versicherer ersetzt die Kosten eines Versicherten zur – auch erfolglosen – Abwendung oder Minderung eines Versicherungsfalles, soweit der Versicherte sie den Umständen nach für geboten halten durfte.		gestrichen	Logisch nur noch im Eigenschadenbaustein umfasst, da dort diese Kosten anfallen würden (vgl. Ziff. 2.17).

HISCOX
WISSEN VERSICHERT.

Hiscox CyberClear Österreich

Gegenüberstellung der wesentlichen Neuerungen von Hiscox CyberClear 10/2020 zu Hiscox CyberClear 06/2022

III. Was ist nicht versichert?				
III.2. Krieg und Cyber-Operationen	Kein Versicherungsschutz besteht wegen Schäden, die sich direkt oder indirekt im Zusammenhang mit einem der folgenden Ereignisse ergeben: 2.1. dem Einsatz physischer Gewalt eines Staates gegenüber einem anderen Staat (Krieg), unabhängig davon, ob eine Kriegserklärung vorliegt oder nicht, oder 2.2. dem unzulässigen Zugriff auf ein IT-System durch einen Staat im Territorium eines anderen Staates oder die unzulässige Nutzung eines IT-Systems durch einen Staat im Territorium eines anderen Staates (Cyber-Operation), wenn diese Cyber-Operation: • im Zuge eines Krieges ausgeführt wird und/oder • direkt oder indirekt zu einer Störung der Verfügbarkeit, Integrität oder Leistungsfähigkeit der kritischen Infrastruktur oder aber der Sicherheit oder Verteidigung des anderen Staates führt. Die vorstehende Ziffer III.2.2. findet keine Anwendung bei Schäden, die sich daraus ergeben, dass IT-Systeme eines Versicherten, die sich nicht auf dem Territorium eines von der Cyber-Operation betroffenen Staates befinden, von der Cyber-Operation betroffen sind. Als betroffener Staat gilt hierbei jeder Staat, dessen kritische Infrastruktur durch die Cyber-Operation eine Störung der Verfügbarkeit, Integrität oder Leistungsfähigkeit erleidet. Als kritische Infrastruktur im Sinne des vorliegenden Ausschlusses gelten alle in der jeweiligen Fassung des § 2 Nr. 10 BSIG einschließlich der dazugehörigen Verordnungen oder einer etwaigen Nachfolgeregelung sowie alle in entsprechenden ausländischen Rechtsnormen als kritische Infrastruktur oder wesentliche Dienste (essential services) definierten Einrichtungen.	III.2. Gewaltsame Auseinandersetzungen und Cyber-Operationen	Kein Versicherungsschutz besteht wegen Schäden, die sich direkt oder indirekt im Zusammenhang mit einem der folgenden Ereignisse ergeben: 2.1. dem Einsatz physischer Gewalt eines Staates gegenüber einem anderen Staat (Krieg), unabhängig davon, ob Krieg erklärt wurde oder nicht, 2.2. Invasion, Bürgerkrieg, Aufstand, Streik, Revolution, Aufruhr sowie militärischer oder anderer Formen der gewaltsamen Machtergreifung oder 2.3. dem unzulässigen Zugriff auf ein IT-System durch oder im Namen eines Staates im Territorium eines anderen Staates oder die unzulässige Nutzung eines IT-Systems durch oder im Namen eines Staates im Territorium eines anderen Staates (Cyber-Operation), wenn diese Cyber-Operation einem Staat zugeschrieben werden kann und: • im Zuge eines Krieges ausgeführt wird und/oder • direkt oder indirekt zu einer Störung der Verfügbarkeit, Integrität oder Leistungsfähigkeit der kritischen Infrastruktur oder aber der Sicherheit oder Verteidigung eines anderen Staates führt. Eine Cyber-Operation kann insbesondere dann einem Staat zugeschrieben werden, wenn die Regierung oder eine Sicherheitsbehörde (einschließlich Geheimdiensten und Verfassungsschutzbehörden) eines relevanten Staates dies öffentlich kommuniziert. Ein relevanter Staat ist jeder Staat, • dessen Verfügbarkeit, Integrität oder Leistungsfähigkeit der kritischen Infrastruktur oder aber der Sicherheit oder Verteidigung durch die Cyber-Operation gestört wurde (betroffener Staat) oder • der Mitglied der Europäischen Union oder • der Mitglied der NATO ist. Bei widersprüchlichen Zuschreibungen innerhalb eines relevanten Staates ist die von der Regierung des jeweiligen Staates im Rahmen der offiziellen Kommunikation vorgenommene Zuschreibung maßgeblich. Bei widersprüchlichen Zuschreibungen zwischen verschiedenen relevanten Staaten ist die Zuschreibung durch den betroffenen Staat maßgeblich. Hat der betroffene Staat keine Zuschreibung vorgenommen, genügt die Zuschreibung durch einen relevanten Staat, auch wenn ein oder mehrere andere relevante Staaten diese nicht teilen oder ihr widersprechen. Sofern keine Zuschreibung einer Cyber-Operation durch einen relevanten Staat erfolgt, kann eine Cyber-Operation auch dann einem Staat zugeschrieben werden, wenn der Versicherer dies durch geeignete Beweise nachweist. Als kritische Infrastruktur im Sinne des vorliegenden Ausschlusses gelten alle in der jeweiligen Fassung des § 2 Nr. 10 BSIG einschließlich der dazugehörigen Verordnungen oder einer etwaigen Nachfolgeregelung sowie alle in entsprechenden ausländischen Rechtsnormen als kritische Infrastruktur oder wesentliche Dienste (essential services) definierten Einrichtungen.	Noch transparentere Formulierung des Ausschlusses: Ziff. 2.1 Beschreibt den Aussschluss für Krieg durch Einsatz physischer Gewalt. Ziff. 2.2 beschreibt den Ausschluss für Schäden aufgrund von Invasionen, Bürgerkriegen sowie weitere gewaltsame Machtergreifungen. Ziff 2.3 beschreibt den Ausschluss für eine Cyber-Operation. Diese umfasst den unzulässigen Zugriff durch oder im Namen eines Staates auf die IT-Systeme eines anderen Staates, sofern diese Cyber-Operation einem Staat zugeschrieben werden kann. Klarstellend ist eine Cyber Operation nur dann ausgeschlossen, wenn Sie entweder im Zuge eines Krieges durchgeführt wird oder aber die kritische Infrastruktur, Sicherheit oder Verteidigung eines anderen Staates direkt oder indirekt beeinträchtigt (Störung der Verfügbarkeit, Integrität oder Leistungsfähigkeit). Eine Zuschreibung muss offiziell durch eine Regierung oder eine Sicherheitsbehörde kommuniziert werden und durch einen definierten relevanten Staaten vorgenommen worden sein. Auch ist eine Klarstellung bei widersprüchlichen Zuschreibung aufgenommen. Die Definition der kritischen Infrastruktur richtet sich nach dem BSIG bzw. vergleichbaren ausländischen Rechtsnormen.

HISCOX
WISSEN VERSICHERT.

Hiscox CyberClear Österreich

Gegenüberstellung der wesentlichen Neuerungen von Hiscox CyberClear 10/2020 zu Hiscox CyberClear 06/2022

III.3. Technische Infrastruktur	Kein Versicherungsschutz besteht wegen Schäden aufgrund einer Störung oder eines Ausfalls der öffentlichen oder privaten technischen Infrastruktur. Zur öffentlichen und privaten Infrastruktur gehören: • Strom- und Wasserversorgung, • Netzstrukturen, die der überregionalen Informationsvermittlung dienen, insbesondere Telefon-, Internet- oder Funknetze, sowie Leistungen von Internet- und Telekommunikationsanbietern bzw. -providern, • Domain Name Systems sowie • alle weiteren vergleichbaren privaten Einrichtungen oder Einrichtungen der Gebietskörperschaften. Vom Versicherungsschutz umfasst bleiben nur Störungen und Ausfälle des IT-Systems eines Versicherten, soweit dieses IT-System seinerseits Teil der vorher beschriebenen technischen Infrastruktur ist.	III.3. Technische Infrastruktur	Kein Versicherungsschutz besteht wegen Schäden aufgrund einer Störung oder eines Ausfalls der öffentlichen oder privaten technischen Infrastruktur, die nicht vom Versicherungsnehmer selbst betrieben wird. Zur öffentlichen und privaten Infrastruktur gehören: • Strom-, Gas-, Wasser- und Wasserstoffversorgung, • externe Netzstrukturen, die der überregionalen Informationsvermittlung dienen, insbesondere Telefon-, Internet-, Computer-, Daten- oder Funknetze, sowie Leistungen von Internet- und Telekommunikationsanbietern bzw. Providern, Satelliten, • Domain Name Systems (DNS), Internet Service Provider (ISP), Content Delivery Networks (CDN) oder Certificate Authorities (CA) sowie • alle weiteren vergleichbaren privaten Einrichtungen oder Einrichtungen der Gebietskörperschaften.	Zusätzlich Aufnahme der Gas- und Wasserstoffversorgung. Erweiterung der Netzstrukturen um Computer- und Datennnetze sowie Satelliten. Erweiterung um Internet Service Provider, Content Delivery. Networks und Certificate Authorities.
III.8. Rechtswidriges Erfassen von Daten	Kein Versicherungsschutz besteht, wenn ein Versicherter mit Kenntnis oder infolge grob fahrlässiger Unkenntnis eines Repräsentanten personenbezogene Daten im Sinne der Datenschutz-Grundverordnung (DSGVO) oder entsprechender ausländischer Rechtsnormen rechtswidrig erfasst.	III.8. Rechtswidriges Erfassen und Nutzen von Daten	Kein Versicherungsschutz besteht, wenn ein Versicherter mit Kenntnis oder infolge grob fahrlässiger Unkenntnis eines Repräsentanten personenbezogene Daten im Sinne der Datenschutz-Grundverordnung (DSGVO) oder entsprechender, auch ausländischer, Rechtsnormen rechtswidrig erfasst oder nutzt.	Erweiterung um rechtswidrige Nutzung von Daten.
III.10. Hoheitliche Eingriffe	Kein Versicherungsschutz besteht im Zusammenhang mit hoheitlichen Eingriffen, insbesondere Beschlagnahme, Verstaatlichung, Zerstörung oder anderweitigen Maßnahmen einer Behörde oder sonstigen staatlichen Einrichtung. Dies gilt nicht für Datenschutzbehörden im EWR oder UK.	III.10. Hoheitliche Eingriffe	Kein Versicherungsschutz besteht im Zusammenhang mit hoheitlichen Eingriffen, insbesondere Beschlagnahme, (teilweise) Betriebseinstellung, (teilweise) Betriebsschließung, Verstaatlichung, Zerstörung oder anderweitigen Maßnahmen einer Behörde oder sonstigen staatlichen Einrichtung. Dies gilt nicht für Datenschutzbehörden im EWR oder UK.	Aufnahme von Betriebseinstellungen bzw. Betriebsschließungen.
		III. 11. Naturkatastrophen	Kein Versicherungsschutz besteht wegen Schäden durch Erdbeben, Vulkanausbruch, Flutwelle, Flut, Feuer, Explosion, Wind, Blitzschlag, Frost, Sonneneruption, Asteroideneinschlag, Magnetfeldverschiebung oder andere Naturereignisse.	Neu!
		III. 12. Sachschäden	Kein Versicherungsschutz besteht für Sachschäden. Dies gilt nicht für Wiederherstellungskosten für IT-Hardware gemäß Ziffer II.2.5. oder sonstige, explizit im Versicherungsschein versicherte Sachschäden.	Neu!
		III. 13. Personenschäden	Kein Versicherungsschutz besteht für Personenschäden.	Neu!
		III. 14. Kernenergie, Radioaktivität, biologische und chemische Ursachen	Kein Versicherungsschutz besteht für Schäden durch Kernenergie oder Radioaktivität und Schäden aufgrund biologischer oder chemischer Ursachen, einschließlich mittelbarer und unmittelbarer Folgeschäden.	Neu!
IV. Allgemeine Regelungen				
IV.7. Monetärer und zeitlicher Selbstbehalt		IV.7. Monetärer und zeitlicher Selbstbehalt		

HISCOX
WISSEN VERSICHERT.

Hiscox CyberClear Österreich

Gegenüberstellung der wesentlichen Neuerungen von Hiscox CyberClear 10/2020 zu Hiscox CyberClear 06/2022

IV.7.1. Monetärer Selbstbehalt	Ein Versicherter beteiligt sich in jedem Versicherungsfall mit dem im Versicherungsschein vereinbarten Betrag an der Leistung des Versicherers (monetärer Selbstbehalt). Bei Versicherungsfällen, die ausschließlich auf einer Rechtsverletzung durch Werbung und Marketing gemäß Ziffer I.5. beruhen, gilt abweichend von dem im Versicherungsschein vereinbarten Betrag ein Selbstbehalt in Höhe von EUR 500,-. Der Versicherungsnehmer kann den im Versicherungsschein vereinbarten monetären Selbstbehalt um 25 % je Schadenfall reduzieren, wenn die im Versicherungsschein-Beiblatt und unter www.hiscox.de/cybercleargo näher beschriebenen Voraussetzungen zu dem Cyber-Training erfüllt werden.		Ein Versicherter beteiligt sich in jedem Versicherungsfall mit dem im Versicherungsschein vereinbarten Betrag an der Leistung des Versicherers (monetärer Selbstbehalt). Der Versicherungsnehmer kann den im Versicherungsschein vereinbarten monetären Selbstbehalt um 25 % je Schadenfall reduzieren, wenn die im Versicherungsschein-Beiblatt und unter www.hiscox.de/cybercleargo näher beschriebenen Voraussetzungen zu dem Cyber-Training erfüllt werden.	Selbstbehalt bei Rechtsverletzung durch Werbung und Markting infolge eines Triggers gem. Zif. I.1 - I.4 entspricht dem Policen Selbstbehalt.
IV.7.2. Zeitlicher Selbstbehalt (Wartezeit)	Die Laufzeit des zeitlichen Selbstbehalts beginnt mit Eintritt der versicherten Cyber-Betriebsunterbrechung und endet mit Ablauf der im Versicherungsschein bestimmten Zeit. Der zeitliche Selbstbehalt gilt als überschritten, wenn auch nach Ablauf des im Versicherungsschein vereinbarten zeitlichen Selbstbehalts das IT-System des Versicherten noch nicht wiederhergestellt ist und weiterhin ein Ertragsausfallschaden entsteht. Überschreitet der versicherte Zeitraum der Cyber-Betriebsunterbrechung die Laufzeit des zeitlichen Selbstbehalts, ersetzt der Versicherer den vollen Ertragsausfallschaden sowie etwaige Mehrkosten. Andernfalls wird ein Ertragsausfallschaden nicht ersetzt. Die Regelung zum monetären Selbstbehalt gemäß Ziffer IV.7.1.bleibt unberührt.		gestrichen (neue Ziffer: II.4.3.3.)	Unter Ziff. I.4 Betriebsunterbrechung logisch erfasst NEU: Zeitlicher SB statt Wartezeit

IV.10.2. Mitversicherte Unternehmen	Mitversicherte Unternehmen sind: • bei Versicherungsbeginn bereits als rechtlich selbstständig existierende Gesellschaften innerhalb des EWR und UK, auf die der Versicherungsnehmer unmittelbar oder mittelbar einen beherrschenden Einfluss ausüben kann; • neue Tochtergesellschaften. Wird eine Gesellschaft durch Gründung oder Erwerb während der Vertragslaufzeit zu einer Tochtergesellschaft, gilt sie ab dem Zeitpunkt der Gründung oder des Erwerbs automatisch als mitversichertes Unternehmen. Dies gilt nicht für Gesellschaften • mit im Vergleich zum Versicherungsnehmer insgesamt erheblich niedrigerem IT-Sicherheitsniveau, • außerhalb des EWR und UK, • oder für Kredit- oder Finanzdienstleistungsunternehmen sowie Pensionskassen. Gesellschaften mit im Vergleich zu dem Versicherungsnehmer insgesamt erheblich niedrigerem IT-Sicherheitsniveau gewährt der Versicherer Versicherungsschutz für die Dauer von maximal 60 Tagen ab dem Zeitpunkt der rechtswirksamen Gründung, des Erwerbs oder der Umwandlung, sofern eine Versicherung der Tochtergesellschaft beim Versicherer innerhalb der vorgenannten Frist angefragt wird. Die Deckung endet bereits vor Ablauf der 60 Tage, sobald der Versicherer den Versicherungsschutz für die Tochtergesellschaft ablehnt oder der Versicherungsvertrag insgesamt endet. Beläuft sich der Umsatz der neu gegründeten oder erworbenen Tochtergesellschaft zum Zeitpunkt der Wirksamkeit des Erwerbs auf mehr als 20 % der konsolidierten Umsatzsumme des Versicherungsnehmers, so gilt sie nur vorbehaltlich einer Einigung über eine Bedingungs- und Prämienanpassung als mitversichertes Unternehmen. Nicht vom Versicherungsschutz umfasst sind Versicherungsfälle, die auf Pflichtverletzungen neuer Tochtergesellschaften beruhen, für die aus einem anderen Versicherungsvertrag Versicherungsschutz besteht, oder die auf Pflichtverletzungen neuer Tochtergesellschaften beruhen, wenn jene einem Versicherten zum Zeitpunkt des Erwerbs oder der Gründung bekannt waren.	IV.10.2. Mitversicherte Unternehmen	Mitversicherte Unternehmen sind: • bei Versicherungsbeginn bereits als rechtlich selbstständig existierende Gesellschaften innerhalb des EWR und UK, auf die der Versicherungsnehmer unmittelbar oder mittelbar einen beherrschenden Einfluss ausüben kann, • neue Tochtergesellschaften. Wird eine Gesellschaft durch Gründung oder Erwerb während der Vertragslaufzeit zu einer Tochtergesellschaft, gilt sie ab dem Zeitpunkt der Gründung oder des Erwerbs automatisch als mitversichertes Unternehmen. Entsprechendes gilt für Gesellschaften, die während der Vertragslaufzeit mit dem Versicherungsnehmer oder einer Tochtergesellschaft verschmolzen werden, ab dem Zeitpunkt des Vollzugs der Verschmelzung. Dies gilt nicht für: • Gesellschaften mit im Vergleich zum Versicherungsnehmer insgesamt niedrigerem IT-Sicherheitsniveau, • Gesellschaften außerhalb des EWR und UK, • Gesellschaften, deren Gesellschaftszweck von dem des Versicherungsnehmers abweicht, • IT-Unternehmen mit Fernzugriffsrechten auf die IT-Systeme ihrer Kunden oder • Kredit- oder Finanzdienstleistungsunternehmen sowie Pensionskassen. Gesellschaften mit im Vergleich zu dem Versicherungsnehmer insgesamt niedrigerem IT-Sicherheitsniveau gewährt der Versicherer Versicherungsschutz für die Dauer von maximal 60 Tagen ab dem Zeitpunkt der rechtswirksamen Gründung, des Erwerbs, der Umwandlung oder der Verschmelzung, sofern eine Versicherung der Tochtergesellschaft beim Versicherer innerhalb der vorgenannten Frist angefragt wird. Die Deckung endet bereits vor Ablauf der 60 Tage, sobald der Versicherer den Versicherungsschutz für die Tochtergesellschaft ablehnt oder der Versicherungsvertrag insgesamt endet. Beläuft sich der Umsatz der neu gegründeten, erworbenen oder verschmolzenen (Tochter-)Gesellschaft zum Zeitpunkt der Wirksamkeit der Gründung, des Erwerbs, der Umwandlung oder der Verschmelzung auf mehr als 20 % der konsolidierten Umsatzsumme des Versicherungsnehmers, so gilt sie nur vorbehaltlich einer Einigung über eine Bedingungs- und Prämienanpassung als mitversichertes Unternehmen. Nicht vom Versicherungsschutz umfasst sind Versicherungsfälle, die auf Pflichtverletzungen neuer Tochtergesellschaften beruhen, für die aus einem anderen Versicherungsvertrag Versicherungsschutz besteht, oder die auf Pflichtverletzungen neuer Tochtergesellschaften beruhen, wenn jene einem Versicherten zum Zeitpunkt des Erwerbs oder der Gründung bekannt waren.	Klarstellung für die Verschmelzung von Unternehmen. Automatischer Einschluss neuer Tochtergesellschaften nur noch bei gleichem Sicherheitsniveau, in der gleichen Branche und ohne Fernzugriffsmöglichkeiten auf IT-Systeme von Kunden (managed service provider).
		IV. 15. Obliegenheiten vor Eintritt des Versicherungsfalles	Der Versicherte hat vor Eintritt des Versicherungsfalles die folgenden Obliegenheiten zu beachten und zu erfüllen.	NEU! Aufnahme der IT-Mindestanforderung als technische Obliegenheiten.
		IV. 15. 1 Datensicherung	Die Versicherten haben mindestens wöchentlich eine vollständige Datensicherung vorzunehmen. Für die Erstellung dieser Datensicherung ist eine Offline-Datensicherung mit dauerhafter physischer Trennung von den zu sichernden IT-Systemen oder eine unveränderbare Online-Datensicherung, auf die Administratoren nur mit einer Zwei-Faktor-Authentifizierung oder aus einer separaten Domain zugreifen können, zu nutzen. Diese Datensicherung ist für mindestens 30 Tage aufzubewahren.	Neu
		IV. 15. 2 Patchmanagement	Die Versicherten haben Sicherheitsupdates auf Servern und Clients (mobilen Geräten, Desktops und Terminals) sowie auf Netzwerkgeräten und Sicherheitssystemen (z. B. Firewalls, Virenschutz) innerhalb von 30 Tagen nach Veröffentlichung des Updates durch den Hersteller einzuspielen.	Neu

		IV. 15. 3 Betrieb von Altsystemen	Sofern die Versicherten Betriebssysteme nutzen, für die ihnen keine Sicherheitsupdates mehr bereitgestellt werden (Altsysteme), hat der Betrieb dieser Altsysteme ausschließlich in einer isolierten Netzwerkumgebung ohne direkten Internetzugang und mit durchgehender Kontrolle des Datenverkehrs zu erfolgen.	Neu
		IV. 15. 4 Folgen einer Obliegenheitsverletzung vor Eintritt des Versicherungsfalles	Verletzt ein Versicherter vorsätzlich oder grob fahrlässig eine Obliegenheit, die er vor Eintritt des Versicherungsfalles gegenüber dem Versicherer zu erfüllen hat, so kann der Versicherer innerhalb eines Monats, nachdem er von der Verletzung Kenntnis erlangt hat, den Vertrag fristlos kündigen. Der Versicherer hat kein Kündigungsrecht, wenn der Versicherte nachweist, dass er die Obliegenheit weder vorsätzlich noch grob fahrlässig verletzt hat. Verletzt der Versicherte eine vor Eintritt des Versicherungsfalls gegenüber dem Versicherer zu erfüllende Obliegenheit vorsätzlich, so ist der Versicherer von der Verpflichtung zur Leistung frei. Bei grob fahrlässiger Verletzung der Obliegenheit ist der Versicherer berechtigt, seine Leistung in dem Verhältnis zu kürzen, das der Schwere des Verschuldens des Versicherten entspricht. Verletzt ein Versicherter eine Obliegenheit, die die dem Versicherungsvertrag zugrundeliegende Äquivalenz zwischen Risiko und Prämie aufrechterhalten soll,ist der Versicherer von der Verpflichtung zur Leistung in dem Verhältnis, in dem die vereinbarte hinter der für das höhere Risiko tarifmäßig vorgesehenen Prämie zurückbleibt, frei. Bei der Verletzung von Obliegenheiten zu sonstigen bloßen Meldungen und Anzeigen, die keinen Einfluss auf die Beurteilung des Risikos durch den Versicherer haben, tritt Leistungsfreiheit nur ein, wenn die Obliegenheit vorsätzlich verletzt worden ist. Der Versicherer bleibt zur Leistung verpflichtet, wenn der Versicherte nachweist, dass er die Obliegenheit nicht grob fahrlässig verletzt hat. Dies gilt auch, wenn der Versicherte nachweist, dass die Verletzung der Obliegenheit weder für den Eintritt oder die Feststellung des Versicherungsfalles noch für die Feststellung oder den Umfang der dem Versicherer obliegenden Leistung ursächlich war. Das gilt nicht, wenn der Versicherte die Obliegenheit arglistig verletzt hat.	Neu

Hiscox
Arnulfstraße 31, 80636 München

Für Makler
T +49 89 54 58 01 100
E hiscox.info@hiscox.de
W **makler.hiscox.de**