Cyberport Datenrettung

Professioneller Support bei Datenverlust

SCHUTZBRIEF FÜR SMARTPHONES,
TABLETS, NOTEBOOKS UND MEHR

Datenwiederherstellung bei Geräteausfall

**Bei Datenverlust durch Viren, Software,
mechanische Beschädigung oder Bedienungsfehler**

Ein Schutzbrief für alle Geräte

Schneller und unkomplizierter Support
durch unseren professionellen Dienstleister

Laufzeit 12 oder 24 Monate

AB 9,90

cyberport

Ontrack®

Kooperationspartner

PRODUKTINFORMATIONSBLATT
„Cyberport Datenrettung"

Mit den nachfolgenden Informationen möchten wir Ihnen einen ersten Überblick über den von Ihnen gewünschten Schutzbrief geben. Diese Informationen sind jedoch nicht abschließend. Der vollständige Vertragsinhalt ergibt sich aus der Leistungsbeschreibung und den Allgemeinen Geschäftsbedingungen für Dienstleistungen unseres Datenrettungs-Partners Kroll Ontrack GmbH. Bitte lesen Sie daher die gesamten Vertragsbestimmungen sorgfältig.

1. Um welche Art von Schutzbrief handelt es sich?
Vertragsinhalt der „Cyberport Datenrettung" ist die Wiederherstellung von beschädigten digital gespeicherten Daten auf einem PC, Notebook, Tablet oder Mobiltelefon, sowie Festplatten und SSDs.

Die Analyse und Datenrettung erfolgt durch unseren Partner Kroll Ontrack – ein auf Datenrettung spezialisierter, professioneller IT-Dienstleister. Nach der kostenlosen Abholung Ihres beschädigten Datenträgers führen Experten innerhalb weniger Stunden eine Freeval-Analyse durch, bei der der Umfang des Datenverlustes geprüft und eine Prognose erstellt wird, wie hoch die Wahrscheinlichkeit einer erfolgreichen Datenrettung ist.

Kroll Ontrack wird versuchen, die Daten vom beschädigten Gerät oder Datenträger zu retten und Ihnen bei erfolgreicher Wiederherstellung die Daten auf einem geeigneten Datenträger zur Verfügung stellen. Die Datenrettung erfolgt mit über 120 selbstentwickelten Tools und Werkzeugen, mit denen Dateistrukturen repariert und rekonstruiert und die Daten in Feinarbeit wiederhergestellt werden. Dass eine Datenrettung in jedem Fall erfolgreich ist, kann Ihnen jedoch nicht garantiert werden.

Die Leistung dieses Schutzbriefes ist begrenzt auf einen Versicherungsfall und eine Gesamtleistungssumme von 1.000,- € je Versicherungsjahr. Maßnahmen, die diese Grenze übersteigen, können im Bedarfsfall von Ihnen selbst übernommen werden. Alternativ können Sie auch auf die Datenrettung verzichten, wenn sich bei der Analyse herausstellt, dass eine Zuzahlung erforderlich wäre.

2. Welche Risiken sind abgedeckt?
- Schäden durch einen technischen Defekt des Speichermediums (zum Beispiel Beschädigung des Lesekopfs)
- Schäden durch eine sonstige physische Beschädigung des Speichermediums (zum Beispiel Herunterfallen des Laptops)
- Schäden durch Softwarefehler
- Schäden durch Viren bzw. Schadsoftware
- Schäden am Speichermedium durch Bedienungsfehler (nicht jedoch das unbeabsichtigte Löschen von Daten)

Voraussetzung ist, dass diese Schäden während der Laufzeit des Vertrags entstanden sind und auch die Wiederherstellung der Daten während der Laufzeit dieses Vertrags beauftragt wird. Art und Umfang der Datenbeschädigung sind stark abhängig vom einzelnen Schadensfall. Geschuldet ist daher lediglich das Bemühen durch unseren Datenrettungs-Dienstleister. Eine Erfolgsgarantie können wir Ihnen nicht geben.

3. Wann kann der Schutzbrief nicht helfen?

- Bei bereits geöffneten Festplatten
- Bei Schäden durch vorsätzliche Zerstörung
- Wenn Daten gelöscht wurden
- Bei gebraucht erworbenen Geräten
- Bei Schäden, die durch einen unsachgemäßen Reparaturversuch oder durch Veränderung des Gerätes entgegen den Herstellervorgaben entstanden sind.
- Reparatur des defekten Gerätes
- Datenrettung von verschlüsselten Datenträgern

Bitte beachten Sie, dass Sie bei einem Datenverlust keine eigenen Versuche unternehmen die Daten selbst wiederherzustellen, da dies die Erfolgschancen für eine erfolgreiche Wiederherstellung erheblich mindern kann.

4. Wie hoch ist der Beitrag und wann müssen Sie ihn bezahlen?
Für die Gesamtdauer der Laufzeit wird ein Beitrag erhoben, dessen Höhe sich nach dem von Ihnen gewählten Tarif richtet.

Beitrag „Cyberport Datenrettung" für 12 Monate/24 Monate:

Warenwert/€	12 Monate		24 Monate	
alle	GE38-001	9,90 €	GE38-002	16,90 €

Einmalprämie inklusive gesetzlicher Mehrwertsteuer

Die Beitragszahlung erfolgt einmalig gegenüber der Cyberport GmbH. Der Beitrag ist unverzüglich nach Abschluss des Vertrages zu zahlen.

5. Wann beginnt und endet der Vertrag?
Die Schutzleistung beginnt mit der Registrierung der „Cyberport Datenrettung" durch Cyberport. Die Laufzeit des Vertrages beträgt mindestens 12 und maximal 24 Monate. Die Laufzeit richtet sich nach dem gewählten Paket bei Abschluss. Ein Wechsel des Paketes während der Vertragslaufzeit ist nicht möglich. Der Vertrag endet stillschweigend zum Ende der Vertragslaufzeit. Eine automatische Verlängerung erfolgt nicht.

VERHALTEN IM SCHADENSFALL

› Rufen Sie die kostenfreie Kunden-Hotline an und Sie erhalten umgehend alle Informationen zur weiteren Abwicklung
› Informieren Sie sich direkt unter folgender Servicenummer:

HOTLINE:	+49 800/102 30 85	Deutschland
	+43 800/022 556	Österreich
	+49 2381 969 219 283	International (Festnetztarif)
Mo – Fr 8 – 20 Uhr | Sa 8 – 18 Uhr		

Bitte beachten Sie: Bei Inlands-Telefonaten ersetzen Sie bitte die Ländervorwahl (+49 bzw. +43) durch eine 0.

› E-Mail: cyberport@extrapolice24.de

Halten Sie bitte Ihre Kundennummer bereit und schildern Sie genau welcher Schaden vorliegt und wie der Schaden entstanden ist. Wir werden dann die weiteren Schritte mit Ihnen besprechen. Nach Aufnahme des Schadenfalls erhalten Sie zeitnah einen Anruf von unserem Datenrettungs-Partner Kroll Ontrack, der die weitere Vorgehensweise mit Ihnen bespricht und die kostenlose Abholung bzw. Versendung Ihres beschädigten Datenträgers beauftragt.

Bitte beachten Sie, dass es bei einzelnen Geräten mit fest verbautem Datenträger nicht möglich ist, den Datenträger zu entfernen ohne das Gerät dabei zu zerstören.
Eine Reparatur des beschädigten Gerätes oder des Datenträgers selbst ist nicht Bestandteil der Cyberport-Datenrettung und somit ausgeschlossen. Sollten Sie zusätzlich zur Datenrettung noch einen Schutzbrief für das Gerät abgeschlossen haben, weisen Sie den Kundenberater bitte im Rahmen der Meldung darauf hin.

Stand: Mai 2019

VERTRAGSINFORMATIONEN „Cyberport Datenrettung“

1. Allgemeine Bestimmungen?
Der Vertrag zum Cyberport-Schutzbrief Datenrettung wird zwischen Ihnen und der Extrapolice24 GmbH (Geschäftsführer: Wilhelm Einhaus, Sitz der Gesellschaft in Hamm – Handelsregister HRB 6240) geschlossen.

Im Schadenfall und allen anderen Fragen, wenden Sie sich bitte an die Extrapolice24 Verwaltungs- und Vertriebsgesellschaft mbH

Hotline für Kunden aus Deutschland: 0800/102 30 85
Hotline für Kunden aus Österreich: 0800/022 556
International erreichbare Hotline: +49 2381 969 219 283 (Festnetztarif)
E-Mail: cyberport@extrapolice24.de
(Montag – Freitag 8 – 20 Uhr | Samstag 8 – 18 Uhr)
*Sie erreichen uns kostenfrei aus dem nationalen Fest- oder Mobilfunknetz

Postanschrift: Postfach 4327, D-59039 Hamm
Hausanschrift: Römerstr. 104, D-59075 Hamm

2. Leistungsbeschreibung Freeval Analyse für Cyberport

§1 Freeval Analyse
1. Vertragsinhalt eines Freeval Analyseauftrags an die Kroll Ontrack GmbH ist die Dienstleistung, eine möglichst genaue Vorhersage über die Wahrscheinlichkeit zu machen, die auf einem beschädigten Datenträger enthaltenen Daten zu retten bzw. durch entsprechende Maßnahmen wieder lesbar zu machen sowie herauszufinden, welche Datenrettungsmaßnahmen voraussichtlich erfolgversprechend sein werden.

2. Die Vorhersage über den Anteil der wiederherstellungsfähigen Daten beruht auf einem vorläufigen Check der Daten sowie umfangreichen Erfahrungswerten über die Chancen der Wiederherstellung bei verschiedenen Schadensbildern und -ursachen.

3. Die zur Freeval Analyse notwendigen Bearbeitungsvorgänge beinhalten trotz höchster Sicherheits- und Bearbeitungsstandards nach dem Stand der Technik das Risiko des teilweisen oder völligen Untergangs noch verbliebener Daten und/oder der nur teilweisen Wiederherstellbarkeit von Daten. Dem Kunden ist bekannt, dass auch bei sachgemäßer Vorgehensweise bei der Freeval Analyse ein Risiko verbleibt, dass einmal vorhandene Daten nicht mehr gerettet werden können, zusätzliche Daten verloren gehen, wiederhergestellte Daten vom Kunden nicht genutzt werden können, und/oder der in den Datenträgern verkörperte Informationsgehalt

ganz oder teilweise zerstört wird, sowie die zur Verfügung gestellten Datenträger, Software und andere überlassenen Sachen beschädigt, unbrauchbar oder zerstört werden. Abhängig von der Art des Mediums kann es bereits während der Analyse zur Übertragung der Daten auf ein anderes Medium und zur Zerstörung des Originalmediums kommen.

4. Eine Beauftragung erfolgt ausschließlich auf der Basis der Allgemeinen Geschäftsbedingungen der Firma Ontrack GmbH.

§2 Freeval Analyse Ergebnis

1.Der Kunde bekommt durch die kostenfreie Freeval Analyse eine qualifizierte Begutachtung des Datenträgers durch die Datenrettungsexperten der Ontrack GmbH. Die Freeval Analyse besteht aus Ermittlungen über Art und Umfang des Datenschadens sowie den Ermittlungen der Möglichkeiten der Datenwiederherstellung an dem vom Auftraggeber überlassenen Datenträger. Hierbei wird festgestellt, ob die Beschädigung logisch und/oder physikalisch ist und ob der Datenträger zur Bearbeitung in das Reinraumlabor gegeben werden muss. Zudem wird eine Einschätzung des zu erwartenden Datenrettungsergebnisses gegeben.

2. Ontrack wird den Kunden nach der Freeval Analyse darüber informieren, ob eine Datenrettung durchgeführt werden kann, oder ob der Datenträger so beschädigt ist, dass keine sinnvolle Datenrettung möglich ist.

§3 Durchführung der Datenrettung für den Kunden

1. Ontrack wird für den Kunden nach der Freeval Analyse die Datenrettung für alle noch lesbaren und wiederherstellbaren Daten durchführen.

2. Die geretteten Daten werden auf einem verschlüsselten Backup-Medium gesichert und werden dem Kunden zugesandt. Der defekte Datenträger wird zurückgesandt.

3. Die Datenrettung ist für den Kunden bis zu einem Betrag von 1.000,- € netto durch den Service-Vertrag abgedeckt. Der Betrag für eine Datenrettung ist pro Vertragsjahr auf 1.000,- € begrenzt.

4. Sollte der Kunde innerhalb eines Vertragsjahres einen weiteren Fall für Datenrettung haben, der die festgelegte Grenze von 1.000,- € überschreitet, ist dieser nicht durch den Service-Vertrag abgedeckt. Der Kunde kann in diesem Fall den dann kostenpflichtigen Datenrettungs-Service von Ontrack in Anspruch nehmen.

5. Sollte eine Datenrettung technisch nicht möglich sein, wird der Datenträger zurückgesandt.

§4 Daten- und Geheimnisschutz, Haftung

1. Ontrack wird im Rahmen der Freeval Analyse nur die Qualität und Lesbarkeit der Daten beurteilen und keine personenbezogenen Daten gezielt auslesen.

2. Da dennoch eine Zugriffsmöglichkeit auf personenbezogene Daten auch im Rahmen der Freeval Analyse theoretisch möglich ist, ist es dennoch rechtlich notwendig, die beigefügte Anlage zur Auftragsdatenverarbeitung in den Vertrag einzubeziehen.

3. Ontrack haftet im Rahmen dieses Vertrags nur für durch Vorsatz oder grobe Fahrlässigkeit verursachte Schäden, wobei die Haftung im Falle von leichter Fahrlässigkeit auf die üblicherweise vorhersehbare Schadenshöhe begrenzt ist. Für den Verlust von Daten und/oder Programmen haftet Ontrack insoweit nicht, als der Schaden darauf beruht, dass es der Kunde unterlassen hat, Datensicherungen durchzuführen und dadurch sicherzustellen, dass verlorengegangene Daten mit vertretbarem Aufwand wiederhergestellt werden können.

4. Die vorstehenden Regelungen gelten auch zugunsten der Erfüllungsgehilfen des Auftragnehmers.

5. Im Übrigen ist jegliche Haftung von Ontrack für die Zahlung von Schadensersatz oder Aufwendungsersatz, gleich aus welchem Rechtsgrund, ausgeschlossen.

6. Die vorstehenden Haftungsbeschränkungen gelten nicht in den Fällen zwingender gesetzlicher Haftung, insbesondere der Haftung nach dem Produkthaftungsgesetz, bei Übernahme einer Garantie oder bei Verletzungen des Lebens, des Körpers oder der Gesundheit.

Stand: Mai 2019

3. Allgemeine Geschäftsbedingungen für Dienstleistungen der Kroll Ontrack GmbH

1. Auftragsgegenstand, Geltung der allgemeinen Geschäftsbedingungen

1.1 Der Umfang der von Kroll Ontrack für den Kunden zu erbringenden Leistung richtet sich nach dem konkreten schriftlichen mit dem Kunden vereinbarten Auftrag.

1.2 Sofern ein Rahmenvertrag abgeschlossen wurde, richtet sich der Vertrag nach dem Rahmenvertrag in Verbindung mit den jeweiligen Leistungsscheinen.

1.3 Ergänzend geltend die nachfolgenden allgemeinen Geschäftsbedingungen. Allgemeine Geschäftsbedingungen des Kunden finden keine Anwendung.

2. Art des Vertrages, Vertragsabschluss

2.1 Beim Löschen von Daten gewährleistet Kroll Ontrack das fachgerechte Entfernen der Daten vom Datenträger im Sinne eines Werkvertrages.

2.2 Ontrack erbringt alle übrigen Leistungen in der Form eines Dienstvertrages, daher schuldet Kroll Ontrack keinen Erfolg der Leistung, wie z.B. bei der Wiederherstellung von defekten Datenträgern oder der Suche nach bestimmten Informationen.

2.3 Unsere Angebote sind stets freibleibend und unverbindlich.

2.4 Technische und gestalterische Abweichungen von Beschreibungen und Angaben in Prospekten, Katalogen und schriftlichen Unterlagen sowie Änderungen im Zuge des technischen Fortschritts bleiben vorbehalten, ohne dass hieraus Rechte gegen uns hergeleitet werden können.

3. Verfügungsbefugnis des Kunden/Datensicherheit und Datenschutz

Der Kunde erklärt mit der Erteilung des Auftrags, dass er zur Verfügung über den übergebenen Datenträger und die dort gespeicherten Daten berechtigt ist. Der Kunde ist damit einverstanden, dass Kroll Ontrack die ihr zur Verfügung gestellten gegebenenfalls auch personenbezogenen Daten im Rahmen einer Auftragsdatenverarbeitung speichert und bearbeitet. Kroll Ontrack hält alle kundenbezogenen Daten gegenüber nicht mit der Kroll Ontrack GmbH im Sinne des §15 des deutschen Aktiengesetzes verbundenen Unternehmen geheim. Kroll Ontrack beachtet die Vorschriften des Bundesdatenschutzgesetzes für nichtöffentliche Stellen.

4. Vergütung/Fälligkeit

4.1 Die Vergütung einschließlich der Kosten für neue Datenträger, Fracht und Transportversicherung ist vor Rücksendung der wiederhergestellten oder untersuchten Daten und Datenträger zur Zahlung fällig.

4.2 Gleiches gilt entsprechend für Datenträger, von denen Dateien gelöscht wurden.

4.3 Sollten auf Wunsch des Kunden reservierte Arbeitstage weniger als 5 Tage vor deren Beginn durch den Kunden storniert oder verschoben werden, berechnen wir eine Ausfallgebühr i.H.v. 50% der Dienstleistungssumme. Bei einer Stornierung kleiner als 2 Tage berechnen wir 100% der Dienstleistungssumme. Dem Kunden bleibt vorbehalten, nachzuweisen, dass der Ausfall zu keinem oder zu einem wesentlich niedrigeren Schaden geführt hat, als diese Pauschale.

4.4 Teilleistungen und deren gesonderte Fakturierung sind zulässig, soweit dies dem Kunden zumutbar ist.

5. Leistungszeit

5.1 Die von uns genannten Termine und Fristen sind unverbindlich, sofern nicht ausdrücklich etwas anderes vereinbart wurde.

5.2 Leistungsverzögerungen aufgrund von höherer Gewalt und/oder aufgrund von Ereignissen, die uns die Leistung wesentlich erschweren oder unmöglich machen, z. B. Betriebsstörungen, Streik, Materialbeschaffungsschwierigkeiten, behördliche Anordnungen etc. berechtigen uns, die Lieferung um die Dauer der Behinderung zuzüglich einer angemessenen Anlaufzeit hinauszuschieben oder wegen des noch nicht erfüllten Teiles ganz oder teilweise vom Vertrag zurückzutreten.

5.3 Der Kunde hat während des Auftrags für die ganze Zeit einen kompetenten Ansprechpartner zur Verfügung zu stellen, der ermächtigt ist, die erforderlichen Entscheidungen über Eingriffe auf Rechner des Kunden im Namen des Kunden zu treffen. Für die Dauer der Nichterfüllung dieser Bedingung kommen wir nicht in Verzug mit unseren Leistungen.

5.4 Im Übrigen kommen wir erst dann in Verzug, wenn uns der Kunde schriftlich eine Nachfrist von mindestens 1 Monat gesetzt hat. Im Falle des Verzuges hat der Kunde Anspruch auf eine Verzugsentschädigung in Höhe von 0,5% für jede vollendete Woche des Verzuges, insgesamt jedoch bis zu 5% des Rechnungswertes der vom Verzug betroffenen Leistungen. Darüber hinaus sind Ansprüche aus Verzug, insbesondere Schadensersatzansprüche jedweder Art, ausgeschlossen.

6. Gefahrtragung

Die Gefahr des Verlustes von Daten und Datenträgern durch den Transport trägt der Kunde. Auf Wunsch des Kunden kann auf dessen Kosten eine gesonderte Transportversicherung abgeschlossen werden.

7. Gewährleistung

7.1 Die Gewährleistung beträgt gegenüber Verbrauchern 24 Monate, gegenüber Unternehmern 12 Monate.

7.2 Der Kunde wird offensichtliche Mängel schriftlich unverzüglich mitteilen.

7.3 Tritt ein Mangel auf, so ist der Kunde verpflichtet, diesen binnen zwei Wochen schriftlich zu melden. Im Rahmen der schriftlichen Mängelrüge sind der Mangel und seine Erscheinungsform so genau zu beschreiben, dass eine Überprüfung des Mangels möglich ist.

7.4 Erweist sich die Mängelrüge als berechtigt, setzt der Kunde der Firma eine angemessene Frist zur Nacherfüllung. Der Kunde teilt uns mit, welche Art der Nacherfüllung – Verbesserung der bisherigen oder Lieferung/Erbringung einer neuen, mangelfreien Ware bzw. Dienstleistung – er wünscht. Wir sind jedoch berechtigt, die gewählte Nacherfüllung zu verweigern, wenn diese nur mit unverhältnismäßigen Kosten durchgeführt werden kann und wenn die andere Art der Nacherfüllung keine erheblichen Nachteile für den Kunden mit sich bringen würde. Wir können außerdem die Nacherfüllung insgesamt verweigern, wenn sie nur mit unverhältnismäßigen Kosten durchführbar ist. Zur Durchführung der Nacherfüllung für denselben oder in direktem

Zusammenhang stehenden Mangel stehen uns zwei Versuche innerhalb der gesetzten Frist zu. Nach dem zweiten fehlgeschlagenen Nacherfüllungsversuch kann der Kunde vom Vertrag zurücktreten oder die Vergütung mindern. Das Rücktritts- bzw. Minderungsrecht kann bereits nach dem ersten erfolglosen Nacherfüllungsversuch ausgeübt werden, wenn weitere Versuche innerhalb der gesetzten Frist dem Kunden nicht zuzumuten sind. Der Rücktritt wegen eines unerheblichen Mangels ist ausgeschlossen.

8. Haftung

8.1 Kroll Ontrack haftet im Rahmen dieses Vertrags nur für durch Vorsatz oder grobe Fahrlässigkeit verursachte Schäden oder Aufwendungen und durch den Verstoß gegen sogenannte wesentliche Vertragspflichten verursachte Schäden oder Aufwendungen. Wesentliche Vertragspflichten sind solche grundlegenden Pflichten, die für den Abschluss des Vertrags wesentlich waren und deren Erfüllung die ordnungsgemäße Durchführung des Vertrags überhaupt erst ermöglichen und auf deren Einhaltung der Kunde regelmäßig vertrauen darf, wobei die Haftung im Falle von leichter Fahrlässigkeit auf die üblicherweise vorhersehbare Schadenshöhe begrenzt ist; diese Haftung ist jedoch beschränkt auf maximal die Höhe des Auftragswertes pro Schadensfall und insgesamt maximal auf das Vierfache dieses Auftragswertes.

8.2 Für den Verlust von Daten und/oder Programmen haftet Kroll Ontrack insoweit nicht, als der Schaden darauf beruht, dass es der Kunde unterlassen hat, Datensicherungen durchzuführen und dadurch sicherzustellen, dass verlorengegangene Daten mit vertretbarem Aufwand wiederhergestellt werden können.

8.3 Die vorstehenden Regelungen gelten auch zugunsten der Erfüllungsgehilfen des Auftragnehmers.

8.4 Im Übrigen ist jegliche Haftung von Kroll Ontrack für die Zahlung von Schadensersatz oder Aufwendungsersatz, gleich aus welchem Rechtsgrund, ausgeschlossen.

8.5 Die vorstehenden Haftungsbeschränkungen gelten nicht in den Fällen zwingender gesetzlicher Haftung, insbesondere der Haftung nach dem Produkthaftungsgesetz, bei Übernahme einer Garantie oder bei Verletzungen des Lebens, des Körpers oder der Gesundheit.

8.6 Sämtliche Ansprüche, die sich gegen uns richten, sind ohne unsere schriftliche Zustimmung nicht abtretbar und können ausschließlich vom Kunden selbst geltend gemacht werden, soweit §354a HGB nicht entgegensteht.

9. Gerichtsstand/Anzuwendendes Recht

Gerichtstand gegenüber Kaufleuten, juristischen Personen des öffentlichen Rechts oder öffentlichrechtlichen Sondervermögen ist Böblingen. Es gilt das Recht der Bundesrepublik Deutschland. Die Anwendung des UN-Kaufrechts (CISG) ist ausgeschlossen.

10. Wiederherstellung von Daten

10.1 Sofern im konkreten Auftrag nicht anders vereinbart, teilt Kroll Ontrack dem Kunden zunächst das Diagnoseergebnis mit. Der Kunde entscheidet dann über die Erteilung des Auftrags zur Datenwiederherstellung.

10.2 Die Diagnosetätigkeit sowie das Bemühen um die Datenwiederherstellung beinhalten das Risiko des Unterganges noch vorhandener Daten sowie der Beschädigung von Datenträger und Systemen. Dieses Risiko trägt der Kunde, es sei denn, der Verlust wurde von Ontrack vorsätzlich oder grob fahrlässig verursacht. Der Wiederherstellungsprozess kann zu einer Veränderung der Datenstruktur führen.

10.3 Sofern im konkreten Auftrag nicht anders vereinbart, bewahrt Kroll Ontrack die Kundendaten 14 Tage lang unentgeltlich auf und vernichtet diese anschließend unwiederbringlich.

11. Löschen von Daten

11.1 Bei einem ausschließlich auf die Löschung von Daten gerichteten Auftrag überprüft Kroll Ontrack nicht den Inhalt des Datenträgers.

11.2 Weist Kroll Ontrack nach, dass sämtliche Daten nach dem Standard BS-GS oder BS-GSE gelöscht wurden, wird das Löschen der Daten als dem Stand der Technik entsprechend anerkannt.

Stand: Mai 2019

ANLAGE ZUR AUFTRAGSDATENVERARBEITUNG KROLL ONTRACK GMBH

Präambel

Die Vertragsparteien sind mit der Leistungsvereinbarung ein Auftragsdatenverarbeitungsverhältnis gemäß §11 Bundesdatenschutzgesetz (BDSG) eingegangen. Um die Rechte und Pflichten aus dem Auftragsdatenverarbeitungsverhältnis gemäß der gesetzlichen Verpflichtung zu konkretisieren, vereinbaren die Vertragsparteien ergänzend die nachfolgenden Regelungen:

§1 Anwendungsbereich

Die Vereinbarung findet Anwendung auf alle Tätigkeiten, die Gegenstand der Leistungsvereinbarung sind und bei deren Verrichtung Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer nach Maßgabe dieser Vereinbarung beauftragte Dritte mit personenbezogenen Daten in Berührung kommen, für die der Auftraggeber die gemäß §3 Abs. 7 BDSG verantwortliche Stelle ist.

§2 Begriffsbestimmung
Diese Vereinbarung bezieht sich nur auf die Durchführung der technischen Erhebung, Verarbeitung und Nutzung personenbezogener Daten nach einem vom Auftraggeber vorgegebenen Algorithmus (Auftragsdatenverarbeitung). Eine inhaltliche Aufgabenübertragung wird mit dieser Vereinbarung nicht getroffen.

§3 Konkretisierung des Auftragsinhalts
(1) Der Gegenstand und die Dauer der Auftragsdatenverarbeitung (§11 Abs. 2 S. 2 Nr. 1 BDSG) sowie Umfang, Art und Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten (§11 Abs. 2 S. 2 Nr. 2 BDSG) sind in der Leistungsvereinbarung niedergelegt.
(2) Die Art der verwendeten personenbezogenen Daten.
Gegenstand der Erhebung, Verarbeitung und/oder Nutzung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien)

- Personenstammdaten
- Kommunikationsdaten (z.B. Telefon, E-Mail)
- Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- Kundenhistorie
- Vertragsabrechnungs- und Zahlungsdaten
- Planungs- und Steuerungsdaten
- Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)
- weitere Daten

(3) Der Kreis der durch den Umgang mit ihren personenbezogenen Daten Betroffenen umfasst (Aufzählung/Beschreibung der betroffenen Personenkategorien):

- Kunden
- Interessenten
- Abonnenten
- Beschäftigte i. S. d. §3 Abs. 11 BDSG
- Lieferanten
- Handelsvertreter
- Ansprechpartner
- weitere Personen

§4 Verantwortlichkeit und Weisungsbefugnis
1) Der Auftraggeber ist für die Einhaltung der datenschutzrechtlichen Bestimmungen, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung verantwortlich (§3 Abs. 7 BDSG). Er kann jederzeit die Herausgabe, Berichtigung, Löschung und Sperrung der Daten verlangen (§11 Abs. 2 S. 2 Nr. 4 und 10 BDSG). Soweit ein Betroffener sich zwecks Löschung oder Berichtigung seiner Daten unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen
(2) Der Auftragnehmer darf Daten ausschließlich im Rahmen der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen. Eine Weisung ist die auf einen bestimmten Umgang des Auftragnehmers mit personenbezogenen Daten gerichtete schriftliche Anordnung des Auftraggebers. Die Weisungen werden zunächst durch die Leistungsvereinbarung definiert und können von dem Auftraggeber danach in schriftlicher Form durch eine einzelne Weisung geändert, ergänzt oder ersetzt werden (§11 Abs. 2 S. 2 Nr. 9 BDSG).
(3) Der Auftragnehmer hat den Auftraggeber unverzüglich entsprechend §11 Abs. 3 Satz 2 BDSG zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.
(4) Änderungen des Verarbeitungsgegenstandes mit Verfahrensänderungen sind gemeinsam abzustimmen und dokumentieren Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen. Der Auftragnehmer verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien und Duplikate werden ohne Wissen des Auftraggebers nicht erstellt.
(5) Der Auftraggeber führt das Verfahrensverzeichnis gem. §4g Abs. 2 Satz 2 BDSG. Der Auftragnehmer stellt dem Auftraggeber auf dessen Wunsch Informationen zur Aufnahme in das Verfahrensverzeichnis zur Verfügung.
(6) Die Daten werden ausschließlich im Gebiet der Bundesrepublik Deutschland gespeichert. Eine Verlagerung in einen Staat außerhalb der Bundesrepublik Deutschland bedarf der vorherigen Zustimmung des Auftraggebers. Die Verarbeitung und Nutzung der Daten im Auftrag des Auftraggebers findet ausschließlich durch Mitarbeiter der Kroll Ontrack GmbH oder mit ihr direkt oder indirekt i. S.d.

§15 AktG verbundenen Unternehmen (Kroll Konzern) innerhalb des europäischen Wirtschaftsraums (EWR) statt. Ein Zugriff auf die Daten von Mitarbeitern des Kroll Konzerns außerhalb des EWR ist nur zulässig, sofern eine konzernweite Datenschutzrichtlinie nach den europäischen Datenschutzstandards oder eine Selbstverpflichtungserklärung des jeweiligen Konzernunternehmens vorliegt. Die besonderen Voraussetzungen der §§4b, 4c BDSG bleiben unberührt.

§5 Beachtung zwingender gesetzlicher Pflichten durch den Auftragnehmer
(1) Neben den vertraglichen Regelungen dieser Vereinbarung und der Leistungsvereinbarung treffen den Auftragnehmer gemäß §11 Abs. 4 BDSG die nachfolgenden gesetzlichen Pflichten.
(2) Der Auftragnehmer stellt sicher, dass die mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter gemäß §5 BDSG (Datengeheimnis) verpflichtet und in die Schutzbestimmungen des Bundesdatenschutzgesetzes eingewiesen worden sind. Dies umfasst auch die Belehrung über die in diesem Auftragsdatenverarbeitungsverhältnis bestehende Weisungs- und Zweckbindung.

(3) Der Auftragnehmer hat nach Maßgabe des §4f BDSG einen Datenschutzbeauftragten bestellt, der seine Tätigkeit gemäß §§4f und 4g BDSG ausübt. Die Kontaktdaten des Datenschutzbeauftragten sind dem Auftraggeber zum Zwecke der direkten Kontaktaufnahme mitzuteilen.
(4) Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollen und Maßnahmen durch die Aufsichtsbehörden nach §38 BDSG oder falls eine Aufsichtsbehörde nach §§ 43, 44 BDSG bei dem Auftragnehmer ermittelt.

§6 Technisch-organisatorische Maßnahmen und deren Kontrolle
(1) Die Vertragsparteien vereinbaren die in dem Anhang „Technisch-organisatorische Maßnahmen" zu dieser Vereinbarung niedergelegten konkreten technischen und organisatorischen Sicherheitsmaßnahmen gemäß §11 Abs. 2 S. 2 Nr. 3 BDSG in Verbindung mit §9 BDSG. Er ist Gegenstand dieser Vereinbarung.
(2) Technische und organisatorische Maßnahmen unterliegen dem technischen Fortschritt. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der in dem Anhang „Technischorganisatorische Maßnahmen" festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.
(3) Der Auftragnehmer wird dem Auftraggeber auf Anforderung die zur Wahrung seiner Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte geben und die entsprechenden Nachweise verfügbar machen. Aufgrund der Kontrollverpflichtung des Auftraggebers gemäß §11 Abs. 2 Satz 4 BDSG vor Beginn der Datenverarbeitung und während der Laufzeit des Auftrags stellt der Auftragnehmer sicher, dass sich der Auftraggeber von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen überzeugen kann. Hierzu weist der Auftragnehmer dem Auftraggeber auf Anfrage die Umsetzung der technischen und organisatorischen Maßnahmen gemäß §9 BDSG nach. Der Nachweis der Umsetzung solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann dabei auch durch Vorlage eines aktuellen Testats, von Berichten unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz) erbracht werden.
(4) Der Auftraggeber kann sich jederzeit zu Prüfzwecken in den Betriebsstätten des Auftragnehmers zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs von der Angemessenheit der Maßnahmen zur Einhaltung der technischen und organisatorischen Erfordernisse der für die Auftragsdatenverarbeitung einschlägigen Datenschutzgesetze überzeugen (§11 Abs. 2 S. 2 Nr. 7 BDSG).

§7 Mitteilung bei Verstößen durch den Auftragnehmer
(1) Der Auftragnehmer unterrichtet den Auftraggeber umgehend bei schwerwiegenden Störungen seines Betriebsablaufes, bei Verdacht auf Verstöße gegen vertragliche oder gesetzliche Datenschutzbestimmungen, bei Verstößen gegen solche Bestimmungen oder anderen Unregelmäßigkeiten bei der Verarbeitung der Daten des Auftraggebers (§11 Abs. 2 S. 2 Nr. 8 BDSG).
(2) Der Auftragnehmer hat im Benehmen mit dem Auftraggeber angemessene Maßnahmen zur Sicherung der Daten sowie zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen.

§8 Löschung und Rückgabe von Daten
(1) Überlassene Datenträger und Datensätze verbleiben im Eigentum des Auftraggebers.
(2) Nach Abschluss der vertraglich vereinbarten Leistungen oder früher nach Aufforderung durch des Auftraggebers, jedoch spätestens mit Beendigung der Leistungsvereinbarung hat der Auftragnehmer sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs-und Nutzungsergebnisse sowie Datenbestände (wie auch hiervon gefertigten Kopien oder Reproduktionen), die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung des Auftraggebers datenschutzgerecht zu vernichten (§11 Abs. 2 S. 2 Nr. 10 BDSG). Gleiches gilt für Test- und Ausschussmaterial. Ein Löschungsprotokoll ist dem Auftraggeber auf Anforderung vorzulegen.
(3) Der Auftragnehmer kann Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufbewahren. Alternativ kann er sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

§9 Subunternehmer
(1) Aufträge an Subunternehmer durch den Auftragnehmer dürfen nur mit vorheriger ausdrücklicher schriftlicher Genehmigung des Auftraggebers vergeben werden (§11 Abs. 2 S. 2 Nr. 6 BDSG). Nicht als Leistungen von Subunternehmen im Sinne dieser Regelung gelten Dienstleistungen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung der Auftragsdurchführung in Anspruch nimmt, beispielsweise Telekommunikationsdienstleistungen und Wartungen. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.
(2) Wenn Subunternehmer durch den Auftragnehmer eingeschaltet werden, hat der Auftragnehmer sicherzustellen, dass seine vertraglichen Vereinbarungen mit dem Subunternehmer so gestaltet sind, dass das Datenschutzniveau mindestens der Vereinbarung zwischen dem Auftraggeber und dem Auftragnehmer entspricht und alle gesetzlichen und vertraglichen Pflichten beachtet werden.
(3) Dem Auftraggeber sind in der vertraglichen Vereinbarung mit dem Subunternehmer Kontroll-und Überprüfungsrechte entsprechend dieser Vereinbarung einzuräumen. Ebenso ist der Auftraggeber berechtigt, auf schriftliche Anforderung vom Auftragnehmer Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen des Unterauftragnehmers zu erhalten.

§10 Nebenleistungen
Die §§1 bis 8 gelten entsprechend, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch andere Stellen im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann (§11 Abs. 5 BDSG).

§11 Datenschutzkontrolle
Der Auftragnehmer verpflichtet sich, dem/der betrieblichen Datenschutzbeauftragten des Auftraggebers zur Erfüllung seiner jeweiligen gesetzlichen Aufgaben im Zusammenhang mit diesem Auftrag jederzeit Zugang zu den üblichen Geschäftszeiten zu gewähren.

§12 Schlussbestimmungen
(1) Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.
(2) Der Anhang „Technisch-organisatorische Maßnahmen" ist Bestandteil dieser Vereinbarung.

ANHANG „TECHNISCH-ORGANISATORISCHE MASSNAHMEN" NACH §9 BDSG

§1 Technische und organisatorische Sicherheitsmaßnahmen
Gemäß §11 Abs. 2 S. 2 Nr. 3 BDSG in Verbindung mit §9 BDSG sind die Vertragspartner verpflichtet, die technischen und organisatorischen Sicherheitsmaßnahmen festzulegen.
§2 Innerbehördliche oder innerbetriebliche Organisation des Auftragnehmers
Der Auftragnehmer wird seine innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schätzenden personenbezogenen Daten oder Datenkategorien geeignet sind.
§3 Konkretisierung der Einzelmaßnahmen
Im Einzelnen werden folgende Maßnahmen bestimmt:

Nr.	Maßnahme	Umsetzung der Maßnahme
1	**Zutrittskontrolle** Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.	• Festlegung befugter Personen • (Betriebsangehörige und Betriebsfremde) • Access-Chip Regelung • Regelung für Firmenfremde • Sicherung auch außerhalb der Arbeitszeit durch Alarmanlage • Türsicherung (elektrischer Türschließer, Ausweisleser) • Entsprechende Ausgestaltung der Maßnahmen zur Objektsicherung (z. B. Einbruchmeldesystem, Geländebewachung)
2	**Zugangskontrolle** Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.	• Teilweise Verschlüsselung • Vergabe und Sicherung von Identifizierungsschlüsseln (User ID) • Regelung der Benutzerberechtigung • Verpflichtung auf das Datengeheimnis nach §5 BDSG • Differenzierte Zugriffsregelung (z. B. durch Segmentzugriffsperren) • Protokollierung und Auswertung der Dateibenutzung
3	**Zugriffskontrolle** Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung entsprechenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.	• Verschlüsselung • Regelung der Zugriffsberechtigung • Auswertung von Protokollen • Teilzugriffsmöglichkeiten auf Datenbestände und Funktionen
4	**Weitergabekontrolle** Es ist zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.	• Verschlüsselung • Feststellung befugter Personen • Gesicherter RZ Eingang für An- und Ablieferung • Ausgabe von Datenträgern nur an autorisierte Personen (z. B. Auftragsquittung, Begleitpapier) • Datenträger Verwaltung Bestandskontrolle • Gesonderter Verschluss vertraulicher Datenträger • Sicherheitsschränke • Kontrollierte Vernichtung von Datenträgern (z. B. Fehldrucke) • Regelung der Anfertigung von Kopien • Dokumentation der Abruf und • Übermittlungsprogramme • Bestimmte autorisierte Benutzer • Verpackungs- und Versandvorschriften (Versandart z. B. in verschlossenen Behältnissen) • Direktabholung, Kurierdienst, Transportbegleitung • Löschung von Datenresten vor Datenträgeraustausch

Nr.	Maßnahme	Umsetzung der Maßnahme
5	**Eingabekontrolle** Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind	• Nachweis der organisatorisch festgelegten Zuständigkeiten für die Eingabe • Protokollierung von Eingaben • Protokollierung der Dateibenutzung • Verfahrens-, Programm- und Arbeitsablauforganisation • Verpflichtung auf das Datengeheimnis
6	**Auftragskontrolle** Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.	• Erfüllung von Datenverarbeitungsverträgen • Sicherer Daten- und Datenträgertransport (idR. DHL) • Sichere Datenverarbeitung • Sichere Datenlöschung nach erfülltem Auftrag • Interne Prozesse zur Auftragserfüllung und Überwachung der Prozesse • Standard Change Management Prozess (nach ITIL)
7	**Verfügbarkeitskontrolle** Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind	• Maßnahmen zur Datensicherung (physikalisch/logisch) • Backups • Sicherungsverfahren und Archivierung • Wiederherstellung der Infrastruktur (Desaster Recovery) • Schutz gegen „malicious code"
8	**Trennungskontrolle** Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können	• Maßnahmen zur getrennten Verarbeitung (Speicherung, Veränderung, Löschung, Übermittlung) von Daten mit unterschiedlichen Zwecken • Mandantentrennung • Funktionstrennungen • Trennung von Test- und Produktivsystemen

Ihre Notizen:

HERZLICHEN GLÜCKWUNSCH ZUM KAUF IHRER:

Cyberport Datenrettung

Professioneller Support bei Datenverlust

So funktioniert's:

Sie erhalten in den nächsten Tagen eine Bestätigung von Extrapolice24 mit weiteren Informationen an die von Ihnen angegebene Email-Adresse.

Sollten Sie innerhalb von 14 Tagen keine E-Mail erhalten, wenden Sie sich bitte an Extrapolice24:

Hotline für Kunden aus Deutschland: 0800 / 102 30 85
Hotline für Kunden aus Österreich: 0800 / 022 556
International erreichbare Hotline: 02381 / 969 219 283 (Festnetztarif)
(Montag – Freitag 8 – 20 Uhr | Samstag 8 – 18 Uhr)