Allgemeine Geschäftsbedingungen für ONTRACK Datenrettungs-Dienstleistungen

Bitte lesen Sie diese AGB sorgfältig durch, bevor Sie Ihre Bestellung an uns senden. Diese AGB sagen Ihnen, wer wir sind, wie wir Ihnen die Dienstleistungen zur Verfügung stellen, wie Sie und wir den Vertrag ändern oder beenden können, was zu tun ist, wenn es ein Problem gibt und andere wichtige Informationen.

1 DIESE AGB

1.1 Diese Allgemeinen Geschäftsbedingungen **(„AGB“)** regeln die Erbringung von Datenrettungs-Dienstleistungen der KLDiscovery Ontrack GmbH, nachfolgend als „Ontrack“ bezeichnet, mit Sitz in der Hanns-Klemm-Straße 5, 71034 Böblingen, eingetragen im Handelsregister Stuttgart unter HRB 244142.

1.2 Unsere Leistungsbeschreibung für Datenrettungsdienstleistungen sowie der Auftragsverarbeitungsvertrag (AVV), welcher die Verarbeitung personenbezogener Daten im Rahmen der Erbringung unserer Dienstleistung regelt, ist Bestandteil dieser AGB. Für weitere Informationen zu den Funktionen und Einschränkungen unseres Datenwiederherstellungsdienstes lesen Sie bitte unsere Leistungsbeschreibung. Der Auftragsverarbeitungsvertrag regelt die Verarbeitung von personenbezogenen Daten, die Ontrack vom Kunden zur Datenwiederherstellung zur Verfügung gestellt werden.

1.3 Informationen darüber, wie wir als Verantwortlicher personenbezogene Daten erheben, verarbeiten und speichern, entnehmen Sie bitte unserer Datenschutzerklärung.

1.4 Allgemeine Geschäftsbedingungen des Kunden oder Dritter werden explizit ausgeschlossen und finden keine Anwendung. Diese AGB, Leistungsbeschreibung und AVV gelten auch für alle künftigen Geschäftsbeziehungen, auch wenn sie nicht nochmals ausdrücklich vereinbart werden.

1.5 Die Dienstleistungen werden überwiegend in unserem Labor in Deutschland erbracht. Ontrack verfügt über technische Einrichtungen und Standorte in Europa und den USA. Falls erforderlich, können andere Ontrack-Einrichtungen in Europa, einschließlich des Vereinigten Königreichs, oder in den USA, Zugang zu Daten auf Speichergeräten erlangen, um die Erbringung der Dienstleistungen zu ermöglichen. Bitte beachten Sie hierzu die Ziffer 6.4.

2 ANSPRECHPARTNER

2.1 **Wie Sie uns erreichen können.** Sie können uns erreichen, indem Sie unser Kundendienstteam unter +49 7031 644 0 anrufen, uns an unserem Firmensitz anschreiben oder uns eine E-Mail an info@ontrack.com senden.

3 AUSLEGUNG

3.1 Für diese AGB gelten folgende Begriffsbestimmungen:

(a) **„Geschäftskunde“** ist eine natürliche oder juristische Person oder eine rechtsfähige Personengesellschaft, die bei Abschluss eines Rechtsgeschäfts in Ausübung ihrer gewerblichen oder selbständigen beruflichen Tätigkeit handelt (§ 14 BGB).

(b) **„Vertrauliche Informationen“** sind alle Informationen, die von einer Partei der jeweils anderen Partei im Rahmen der Geschäftsbeziehung offenbart oder mitgeteilt werden und bei denen die empfangende Partei aufgrund einer Kennzeichnung der betreffenden Informationen als vertraulich oder nach Treu und Glauben aufgrund der Art der Informationen davon ausgehen musste, dass die übermittelnde Partei ein besonderes schützenswertes Interesse daran hat, die betreffenden Informationen geheim zu halten.

(c) **„Verbraucher“** ist jede natürliche Person, die ein Rechtsgeschäft zu Zwecken abschließt, die überwiegend weder ihrer gewerblichen noch ihrer selbständigen beruflichen Tätigkeit zugerechnet werden können (§ 13 BGB).

(d) **„Vertrag“** ist in Ziffer 4.4 definiert.

(e) **„Kunde“** bezeichnet sowohl einen Geschäftskunden als auch einen Verbraucher.

(f) **„Daten“** sind Daten in elektronischer Form jeder Art, einschließlich personenbezogener Daten im Sinne der Datenschutz-Grundverordnung EU 2016/679.

(g) **„Geräte“** bezeichnen Ihre Speichermedien und ggf. Ihr Mobiltelefon oder Tablet.

(h) **„Gebühr“** bezeichnet die von Ihnen für die Dienstleistungen zu zahlende Gebühr, die im jeweiligen Angebot angegeben ist.

(i) **„Speichermedien“** sind Medien wie Festplatten, USB-Laufwerke, SSD, Speicherchips, Tapes oder andere Datenträger.

(j) **„Angebot“** und „Annahme“ sind in Ziffern 4.3 und 4.4 definiert.

(k) **„Leistungsbeschreibung“** bezeichnet die spezifischen Prozesse, die von Ontrack verwendet werden und unter folgendem Link beschrieben werden: https://www.ontrack.com/de-de/legal/agb, worin unter anderem Leistungsumfang und -einschränkungen der von uns erbrachten Datenrettungsdienstleistungen festlegt sind.

(l) **„Datenrettungsdienstleistungen“** (oder kurz „Dienstleistungen“) bezeichnet die von uns für Sie zu erbringenden Dienstleistungen, die in den Ziffern 4 (Bestellvorgang) und 6 (Unsere Datenrettungs-Dienstleistungen) dieser AGB sowie in der Leistungsbeschreibung beschrieben sind.

(m) **„Website“** bezeichnet unsere Website unter www.ontrack.com

(n) **„Backup-Medium“** bezeichnet einen Datenträger von Ontrack, auf dem die wiederhergestellten Daten verschlüsselt gespeichert werden. In der Regel ist dies eine USB-Festplatte.

4 BESTELLVORGANG (Angebot und Annahme)

4.1 Nach einer ersten telefonischen Beratung, dem Absenden eines Online-Formulars über unsere Website oder einer E-Mail-Korrespondenz stellen Sie uns Ihre Geräte zur Verfügung. Bei einer Standard-Datenwiederherstellung erfolgt zunächst eine **Evaluierung**, die in der Leistungsbeschreibung definiert ist. Abhängig vom Gerät sowie der Art des Schadens am Gerät erfolgt die Evaluierung kostenlos (ausgenommen sind hiervon Mobiltelefone, Tablets und Flashmendien, geöffnete Festplatten, gelöschte oder formatierte Medien sowie Wasser- und Brandschäden), sofern während des Bestellvorgangs nicht etwas anderes vereinbart wird. Danach erbringen wir die Evaluierung (sowie ggf. weitere Datenrettungsdienstleistungen) gemäß der Leistungsbeschreibung. Bei Mobiltelefonen, Tablets, geöffneten Festplatten und Flashmedien, sowie bei einigen Schadensarten oder wenn die Evaluierung keine Aussage über eine mögliche Datenrettung gibt, führen wir eine kostenpflichtige **Diagnose** durch. In diesem Fall erhalten Sie von uns einen Link zu einem Diagnose-Angebot, welches Sie im Falle unserer Beauftragung elektronisch autorisieren müssen.

4.2 Nach der Evaluierung oder der kostenpflichtigen Diagnose erhalten Sie eine Einschätzung, inwieweit eine Datenrettung unter Umständen erfolgreich wäre. Bei einer Diagnose erhalten Sie Angaben zu den voraussichtlich wiederherstellbaren Dateien. Für die Erklärung der Kategorien zur Einschätzung sowie den genauen Ablauf entnehmen Sie unserer Leistungsbeschreibung. Auf der Einschätzung basierend erhalten Sie von uns zeitgleich ein Festpreis-Angebot zur Datenrettung (**Datenrettungs-Angebot**). Sie können im Datenrettungs-Angebot für gewöhnlich zwischen verschiedenen Service-Leveln wählen, welche in unserer Leistungsbeschreibung näher beschrieben sind.

4.3 Nach Erhalt unseres Datenrettungs-Angebots haben Sie folgende Optionen: (i) das Angebot elektronisch zu autorisieren (**„Angebot“**); (ii) uns dazu aufzufordern, Ihre Geräte kostenpflichtig zurückzusenden; oder (iii) uns dazu aufzufordern, Ihre Daten unwiederbringlich zu löschen und/oder Ihre Geräte zu vernichten; in letzterem Fall sind wir zur unverzüglichen Ausführung der Löschung/Vernichtung verpflichtet und berechtigt. Wenn wir innerhalb von 14 (vierzehn) Kalendertagen nach dem Datum des Angebots keine Bestellung, Löschungsanweisung oder Aufforderung zur Rückgabe Ihrer Geräte erhalten, senden wir Ihnen eine Erinnerung per E-Mail und bitten Sie uns mitzuteilen, wie wir entsprechend den o.g. Optionen verfahren sollen. Wenn Sie auf diese Erinnerung nicht antworten, senden wir Ihnen im Abstand von 2 (zwei) Wochen 2 (zwei) weitere Erinnerungen. Wenn Sie auf diese Erinnerungen erneut nicht antworten und uns nicht instruieren, wie wir mit Ihren Geräten verfahren sollen, werden wir Ihre Geräte (inklusive Ihrer Daten) in Übereinstimmung mit dem jeweils geltenden Recht entsorgen.

4.4 Wir nehmen Ihre Bestellung (d.h. Ihr Angebot gemäß Ziffer 4.3) an, indem wir Ihnen per E-Mail eine Auftragsbestätigung senden (**„Annahme“**), wodurch ein rechtsverbindlicher Vertrag zwischen Ihnen und uns zustande kommt (**„Vertrag“**), der alle Regelungen gemäß dem Angebot, der Leistungsbeschreibung, dem AVV sowie diesen AGB enthält. Wir weisen Ihrer Bestellung eine Bestellnummer zu. Es wird uns helfen, wenn Sie uns die Bestellnummer mitteilen können, wenn Sie uns kontaktieren.

5 ÜBERMITTLUNG DER BESCHÄDIGTEN Speichermedien und Geräte und Rücksendung von Speichermedien und Geräten und Backup-Medien

5.1 Sie haben folgende Möglichkeiten, uns Ihre Geräte zur Verfügung zu stellen: (i) Sie können Ihre Speichermedien persönlich in unseren Geschäftsräumen während der Öffnungszeiten abgeben (vorherige Anmeldung erforderlich); (ii) Sie können auf eigene Kosten einen Kurierdienst Ihrer Wahl beauftragen oder (ii) Sie können Ihre Datenträger an einer unserer Abgabestellen abgeben (eine Liste der Abgabestellen finden Sie im Internet unter https://www.ontrack.com/de-de/kontakt - Lokale Abgabestellen in Deutschland) und, falls diese Option gewählt wird, erhalten von Ontrack Verpackungsanweisungen für Ihre Geräte. Alternativ bietet Ontrack einen Abholservice durch einen Drittanbieter an, indem Sie während des Bestellvorgangs die Option “Abholung und Zustellung” auswählen. Ontrack sendet Ihnen einen Versandaufkleber für Ihr Paket zusammen mit Verpackungsanweisungen zu und informiert Sie über den Ort, an dem Sie Ihre Datenträger zur Abholung durch den Drittanbieter-Kurierdienst abgeben können.

5.2 Wir akzeptieren nur Ihre Datenträger und - mit Ausnahme der oben definierten Geräte - keine komplette Hardware (z.B. Laptops und Desktops). Bitte entfernen Sie Ihre Datenträger (Festplatte, SSD, etc.) aus Ihrer Hardware. Handys oder Tablets sind hiervon ausgenommen.

5.3 Alle Speichermedien sollten gemäß den Anweisungen unter www.ontrack.com/de-de/datenrettung/shipping verpackt werden, da Ontrack keine Haftung für Schäden an Ihren Geräten während des Transports übernimmt, wenn die Pakete falsch verpackt sind.

5.4 Im Anschluss an die Diagnose oder Wiederherstellung (siehe Punkt 4) senden wir Ihnen Ihre Backup-Medien mittels eines anerkannten Kurierdienstes an Ihre Adresse. Die Zusendung Ihres Sicherungsmediums ist für Sie in der Regel kostenlos, sofern vertraglich nichts anderes vereinbart ist. Bitte setzen Sie sich vor Abschluss des Auftrags mit Ontrack in Verbindung, wenn Sie nicht möchten, dass Ontrack Ihre Backup-Medien per Kurierdienst zurückschickt. Sie können auch auf eigene Kosten z.B. einen Kurierdienst Ihrer Wahl beauftragen oder die Backup-Medien persönlich in unseren Geschäftsräumen während der Öffnungszeiten (nach vorheriger Anmeldung) persönlich abholen.

5.5 Die Kosten für die Rücksendung Ihrer Geräte richten sich nach den Angaben im jeweiligen Angebot. Die genauen Kosten werden Ihnen im Rahmen des Bestellvorgangs mitgeteilt. Alternativ zur Aufforderung zur Rücksendung Ihrer Geräte können sie uns auch aufzufordern, Ihre Daten auf den Originalkundengeräten unwiederbringlich zu löschen und/oder Ihre Geräte zu vernichten. In diesem Fall sind wir zur unverzüglichen Ausführung der Löschung/Vernichtung verpflichtet und berechtigt. Wenn Sie uns keine Anweisung zum Verfahren mit Ihren Originalgeräten geben, senden wir Ihnen eine Erinnerung per E-Mail und bitten Sie uns mitzuteilen, wie wir entsprechend den o.g. Optionen verfahren sollen. Wenn Sie auf diese Erinnerung nicht antworten, senden wir Ihnen im Abstand von 2 (zwei) Wochen 2 (zwei) weitere Erinnerungen. Wenn Sie auf diese Erinnerungen erneut nicht antworten und uns nicht instruieren, wie wir mit Ihren Geräten verfahren sollen, werden wir Ihre Geräte (inklusive Ihrer Daten) in Übereinstimmung mit dem jeweils geltenden Recht entsorgen.

6 UNSERE DATENRETTUNGS-DIENSTLEISTUNGEN

6.1 Als Gegenleistung für Ihre Zahlung der Gebühr erbringen wir die Dienstleistungen mit der erforderlichen Sorgfalt und Sachkenntnis. Unsere Datenrettungsdienstleitungen umfassen in der Regel die folgenden Dienstleistungen: Evaluierung oder/und Diagnose sowie – sofern möglich – Datenrettung.

Eine genaue Beschreibung dieser Dienstleistungen entnehmen Sie bitte unserer Leistungsbeschreibung. Die Leistungsbeschreibung ist Teil dieser AGB.

6.2 Wir werden angemessene Vorkehrungen treffen, um bei der Untersuchung der Geräte folgendes festzustellen: (i) welche Daten auf den Geräten zugänglich und wiederherstellbar sind; (ii) welche Schäden an den Geräten und/oder an den Datenstrukturen festgestellt werden können; (iii) wie viele Daten (falls vorhanden) auf den Geräten wahrscheinlich wiederhergestellt werden können; und (iv) Ihnen die zu erwartenden Ergebnisse einer Wiederherstellung der Daten von den Geräten mitzuteilen. Unsere Datenwiederherstellungsdienstleistungen können die Datenwiederherstellung von Daten im Labor, durch die Bereitstellung von Softwarelösungen und - für Geschäftskunden - mittels Remote Datenrettung umfassen.

6.3 Wir werden angemessene Anstrengungen unternehmen, um: (i) Ihre Daten wiederherzustellen und Ihnen die wiederhergestellten Daten auf einem verschlüsselten Backup-Medium zur Verfügung zu stellen; oder (ii) alle anderen Dienstleistungen auszuführen, deren Erbringung wir mit Ihnen schriftlich vereinbart haben, wie z.B. das Löschen der Daten auf den Speichermedien.

6.4 Wir erbringen unsere Dienstleistungen größtenteils in den Geschäftsräumen der KLDiscovery Ontrack GmbH in 71034 Böblingen, Deutschland. Wir dürfen ihr Gerät aber auch an eine Schwestergesellschaft senden, die sich im Europäischen Wirtschaftsraum

befindet. Die Datenrettung von Mobiltelefonen und Tablets wird in einem Ontrack Expertenlabor für Mobiltelefone durchgeführt. Gemäß Klausel 1.5 können wir auch einen Fernzugriff auf Ihre Daten von außerhalb des Europäischen Wirtschaftsraums durchführen, um die Dienstleistungen auszuführen.

6.5 Zum Zeitpunkt des Vertragsschlusses können wir den Zeitpunkt, zu dem Ihre Datenrettung voraussichtlich abgeschlossen ist, nur schätzen. Die Art der Dienstleistungen beinhaltet, dass uns die Erbringung der Datenrettungsdienstleitungen zu bestimmten Terminen nicht möglich ist. Sie werden während der Erbringung der Dienstleistung aber über das voraussichtliche Fertigstellungsdatum informiert. Wenn Sie Ihr Backup-Medium mit Ihren wiederhergestellten Daten von Ontrack erhalten, bitten wir Sie, das Backup-Medium (USB-Festplatte oder sonstiges Speichermedium) umgehend auf technische Funktionalität zu überprüfen. Ontrack kann Ihre wiederhergestellten Daten im Falle eines Ausfalls des Backup-Mediums nur innerhalb unserer Datenaufbewahrungsfrist für Ihre wiederhergestellten personenbezogenen Daten gemäß der Datenverarbeitungsvereinbarung von Ontrack reproduzieren.

6.6 Bitte beachten Sie, dass wir nicht alle Apple-Produkte für eine Datenrettung annehmen. Unsere Datenrettungsdienstleistungen beinhalten üblicherweise keine Datenrettung von Apple iMac Geräten, oder iPhones/iPads nach einem Factory-Reset. Bitte kontaktieren Sie unseren Kundendienst, bevor Sie Apple-Produkte einsenden.

6.7 Für einige Dienstleistungen benötigen wir möglicherweise bestimmte Informationen von Ihnen, wie Benutzernamen, Passwörter bzw. Zugangscodes. Wenn Sie diese Informationen nicht innerhalb einer angemessenen Frist nach unserer Anfrage zur Verfügung stellen oder wenn Sie unvollständige oder falsche Informationen angeben, können wir eine zusätzliche Gebühr in Höhe eines angemessenen Betrags erheben, um uns für die dadurch anfallende Mehrarbeit zu entschädigen. Wir sind nicht dafür verantwortlich, wenn die Dienstleistungen verspätet oder teilweise gar nicht erbracht werden, sofern dies darauf zurückzuführen ist, dass Sie uns nicht die erforderlichen Informationen zur Verfügung stellen.

6.8 Möglicherweise müssen wir die Bereitstellung von Dienstleistungen aussetzen, um (i) technische Probleme zu lösen oder technische Änderungen vorzunehmen oder (ii) die Dienstleistungen zu aktualisieren, um Änderungen der relevanten Gesetze und behördlichen Anforderungen zu berücksichtigen. Wir können nach entsprechender Vorankündigung auch die Bereitstellung der Dienstleistungen aussetzen, wenn Sie nicht bezahlen.

6.9 Im Rahmen unserer Leistungserbringung ist ein Erfolg nicht geschuldet. Insbesondere stehen wir nicht dafür ein, dass Ihre Daten ganz oder teilweise wiederherstellbar oder nutzbar sind, dass das Mobiltelefon oder Tablet, falls einschlägig, gemäß der ursprünglichen Bestimmung verwendet werden kann oder dass wir ein anderes bestimmtes Ergebnis erzielen werden.

6.10 Die folgende Regelung gilt nur für Kunden, bei denen es sich um Geschäftskunden handelt:

Remote Datenrettung. Bei der Remote Datenrettung (RDR), stellen wir eine Verbindung zum internen Netzwerk des Kunden her. Es werden keine Geräte bei uns eingereicht. Bei einer RDR erhalten Sie von uns einen Link zu einem Diagnose-Angebot, welches Sie im Falle unserer Beauftragung elektronisch autorisieren müssen. Nach der Diagnose erhalten Sie Angaben zu den voraussichtlich wiederherstellbaren Dateien. Darauf basierend erhalten Sie von uns ein Festpreis-Angebot zur Datenrettung (Datenrettungs-Angebot). Sie können im Datenrettungs-Angebot für gewöhnlich zwischen verschiedenen Service-Leveln wählen, welche in unserer Leistungsbeschreibung näher beschrieben sind.

Für eine Remote Datenrettung müssen Sie die Ontrack RDR-Client-Software über den von Ontrack bereitgestellten Link herunterladen und installieren. Nach der Installation ermöglicht der RDR-Client dem Benutzer, sich über eine verschlüsselte Internetverbindung mit Ontrack zu verbinden. Die RDR-Verbindung wird von Ontrack ausschließlich dazu verwendet, die Ontrack Recovery-Tools direkt auf dem Computer des Kunden auszuführen. Ontrack nutzt die RDR-Verbindung um die Ontrack Recovery Tools auf dem Computer des Kunden in einem geschützten Ordner zur speichern. Ihre Daten werden während diesem Vorgang nicht an Ontrack übermittelt. Nach Beenden der RDR werden die Ontrack Recovery Tools auf dem Computer des Kunden wieder gelöscht.

Ontrack versichert, dass die RDR-Client-Software, (a) frei ist von Programmcodes oder Programminstruktionen, welche vorsätzlich entwickelt wurden, um Computerprogramme, Dateien oder Arbeitsvorgänge zu unterbrechen, zu deaktivieren, zu beschädigen, zu behindern oder anderweitig nachteilig zu beeinflussen; und (b) keine anderen bösartigen oder schädlichen Codes enthält, welche typischerweise als Viren bezeichnet oder mit ähnlichen Begriffen einschließlich Trojanisches Pferd, Wurm oder Hintertür beschrieben werden.

7 RECHTE AM GEISTIGEN EIGENTUM

7.1 Ihre Geräte und Daten verbleiben jederzeit in Ihrem Eigentum, und wir haben keine Eigentums-, Nutzungs- und sonstigen Rechte daran, mit Ausnahme des Rechts auf Besitz und Nutzung Ihrer Geräte und Daten zur Erbringung der Dienstleistungen. Sie behalten alle geistigen Eigentumsrechte, die Sie an Ihren Daten haben.

7.2 Alle geistigen Eigentumsrechte, die im Zusammenhang mit der Bereitstellung der Dienstleistungen stehen, verbleiben bei Ontrack, einschließlich der Entwicklung, Erstellung und Bereitstellung der Dienste, Erfindungen, urheberrechtlich geschützte Werke, Methoden, Prozesse und des Know-hows, die zur Entwicklung der Dienstleistungen verwendet werden oder diese umfassen, zusammen mit jeglicher Hardware, Firmware, Plattformen, Software und allen Änderungen, Verbesserungen, neuen Merkmale oder Funktionen, die von Ontrack als Teil der Dienste erstellt oder verwendet werden („KLD-IP“).

8 WIDERRUFSRECHT

8.1. Diese Ziffer gilt nur für Verbraucher im Sinne von § 13 BGB.

8.2. Sie haben das Recht, binnen vierzehn Tagen ohne Angabe von Gründen diesen Vertrag zu widerrufen. Die Widerrufsfrist beträgt vierzehn Tage ab dem Tag des Vertragsschlusses. Während der Evaluierung können Sie jederzeit kündigen.

8.3. Um Ihr Widerrufsrecht auszuüben, müssen Sie Ontrack mittels einer eindeutigen Erklärung (z.B. durch einen mit der Post versandten Brief, ein Telefax, eine E-Mail oder telefonisch) über Ihrend Entschluss, diesen Vertrag zu widerrufen, informieren:

Per E-Mail: info@ontrack.com;

Per Telefon: +49 7031 644 0;

Per Post:

KLDiscovery Ontrack GmbH

Hanns-Klemm-Str. 5

71034 Böblingen

8.4. Sie können dafür auch das Muster-Widerrufsformular am Ende dieser AGB verwenden. Die Wirksamkeit Ihres Widerrufs ist nicht davon abhängig, dass Sie dieses Muster-Widerrufsformular verwenden. Wir werden Ihnen unverzüglich (z.B. per E-Mail) eine Bestätigung über den Eingang Ihres Widerrufs übersenden.

8.5. Zur Wahrung der Widerrufsfrist reicht es aus, dass Sie die Mitteilung über die Ausübung des Widerrufsrechts vor Ablauf der Widerrufsfrist absenden.

8.6. Wenn Sie diesen Vertrag widerrufen, hat Ontrack Ihnen alle Zahlungen, die Ontrack von Ihnen erhalten haben unverzüglich und spätestens binnen vierzehn Tagen ab dem Tag zurückzuzahlen, an dem die Mitteilung über Ihren Widerruf dieses Vertrags bei Ontrack eingegangen ist. Mit der elektronischen Autorisierung unserer Aufforderung zur Abgabe des Angebots (Ziffer 4.3), ermächtigen Sie uns ausdrücklich, die Dienstleistungen unverzüglich zu beginnen. Im Falle eines Widerrufs nach Beginn der Dienstleistung haben Sie für die bis dahin erbrachten Dienstleistungen Wertersatz zu leisten. Sobald wir die Dienstleistungen vollständig erbracht haben, können Sie den Vertrag nicht mehr widerrufen, auch wenn die Widerrufsfrist noch nicht verstrichen ist.

8.7. Für die Rückzahlung verwenden wir dasselbe Zahlungsmittel, das Sie bei der ursprünglichen Transaktion eingesetzt haben, es sei denn, mit Ihnen wurde ausdrücklich etwas anderes vereinbart. In keinem Fall werden Ihnen wegen der Rückzahlung Entgelte berechnet.

9 KEIN WIDERRUFSRECHT FÜR GESCHÄFTSKUNDEN

9.1 Die Regelung in Ziffer 8 gilt nicht für Geschäftskunden.

10 KÜNDIGUNGSRECHTE

10.1 Unbeschadet anderer Rechte kann das Dienstleistungsverhältnis von jedem Vertragsteil aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist gekündigt werden, wenn Tatsachen vorliegen, auf Grund derer dem Kündigenden unter Berücksichtigung aller Umstände des Einzelfalles und unter Abwägung der Interessen beider Vertragsteile die Fortsetzung des Vertragsverhältnisses bis zu der vereinbarten Beendigung des Vertragsverhältnis nicht zugemutet werden kann, insbesondere wenn:

a) eine Partei (i) auf nicht behebbare Weise einer Vertragsklausel wesentlich zuwiderhandelt; oder (ii) wenn eine solche Zuwiderhandlung behebbar ist, diese Zuwiderhandlung nicht innerhalb einer Frist von 7 (sieben) Tagen, nachdem die Partei schriftlich zu deren Behebung aufgefordert wurde, behebt; oder (iii) wiederholt gegen den Vertrag (einschließlich dieser AGB) verstößt; oder

b) (Kündigungsrecht von Ontrack): der Kunde die Vergütung für die Datenrettungs-Dienstleistungen bei Fälligkeit nicht zahlt und/oder

c) eine Partei ihre Geschäftstätigkeit ganz oder teilweise einstellt (oder einzustellen droht), für sie oder für einen Teil ihres Unternehmens oder ihrer Vermögenswerte ein Liquidator, Insolvenz- oder Zwangsverwalter bestellt wird oder ihre Auflösung beschließt (außer, wenn dies zwecks einer geplanten solventen Verschmelzung oder Neustrukturierung erfolgt, bei der das entstehende Unternehmen alle Verbindlichkeiten übernimmt), oder ein zuständiges Gericht einen Insolvenz-, Liquidations- oder einen ähnlichen Beschluss erlässt, oder die Partei einen Vergleich mit ihren Gläubigern schließt, sie nicht in der Lage ist, ihre Schulden bei Fälligkeit zu begleichen oder, wenn eine natürliche Person insolvent wird.

10.2 Wir (Ontrack) können den Vertrag kündigen, wenn wir durch die Erfüllung des Vertrages gegen geltende Ausfuhr- und Sanktionsgesetze im Zusammenhang mit Geschäften mit bestimmten Unternehmen und Personen verstoßen würden, die von der Europäischen Kommission oder anderen nationalen Behörden, einschließlich der Vereinigten Staaten, festgelegt wurden. Sie stimmen zu, auf unsere Aufforderung Identitätsnachweise zum Zwecke der Prüfung der Anwendbarkeit geltender Ausfuhr- und Sanktionsvorschriften zu erbringen.

10.3 Erfolgt die Kündigung aus einem Grund, der von Ontrack nicht zu vertreten ist, so ist der Kunde verpflichtet, die vereinbarte Vergütung für alle bis zum Wirksamwerden der Kündigung von Ontrack erbrachten Datenrettungs-Dienstleistungen zu leisten.

11 ZUSICHERUNGEN UND ANERKENNTNIS DES KUNDEN

11.1 Sie sichern uns zu, dass (i) Sie rechtlich in der Lage sind, verbindliche Verträge abzuschließen; (ii) Sie vollständig bevollmächtigt, ermächtigt und befugt sind, diesen AGB zuzustimmen, und wenn Sie ein Geschäftskunde sind, die entsprechende rechtliche Befugnis besitzen, den Vertrag abzuschließen; (iii) alle Informationen, die Sie uns im Zusammenhang mit Ihrer Bestellung zur Verfügung stellen, wahr, genau, vollständig und nicht irreführend sind; (iv) Sie der Eigentümer der Geräte sind bzw. die Erlaubnis des Eigentümers der Geräte haben, dass wir die Dienstleistungen erbringen dürfen; (v) es nicht gegen Verpflichtungen oder Rechte Dritter verstößt, dass Sie Ihre Geräte bzw. Daten an uns aushändigen; (vi) es nicht gegen geltendes Recht verstößt, dass Sie Ihre Geräte bzw. Daten an uns aushändigen; (vii) Sie gesetzlich berechtigt sind, Zugang zu den Daten zu gewähren; (viii) Ihre Geräte kein Material (wie beispielsweise Daten) enthalten, das die geistigen Eigentumsrechte Dritter verletzen könnte; und (ix) Ihre Geräte kein Material (z.B. Daten) enthalten, das geltendes Recht verletzt.

11.2 Wir behalten uns das Recht vor (und Sie erkennen hiermit an, dass wir dazu berechtigt sind), dokumentarische Nachweise über Ihr Eigentum, Ihre Erlaubnis oder Ihr gesetzliches Recht, die Dienstleistungen in Auftrag zu geben, anzufordern und die Dienstleistungen auszusetzen oder nicht zu starten, solange diese Nachweise fehlen. Sie erklären sich bereit, uns auf Anforderung Identitätsnachweise zukommen zu lassen, damit wir gemäß der Ziffer 10.2. die Anwendbarkeit geltender Ausfuhr- und Sanktionsvorschriften prüfen können.

11.3 Sie erkennen hiermit an und akzeptieren als vertragsgemäß, dass Ihre Geräte bzw. Daten bereits beschädigt sein können, bevor wir sie erhalten und dass unsere Bemühungen, die Dienstleistungen abzuschließen, zur Zerstörung oder weiteren Beschädigung Ihrer Geräte bzw. Daten führen können. Wir werden bei der Ausführung der Dienstleistungen mit angemessener Sorgfalt vorgehen, tragen aber keine Verantwortung für bestehende oder zusätzliche Schäden, die während der Ausführung der Dienstleistungen an Ihren Geräten bzw. Daten entstehen können. Die Regelung in Ziffer 13 wird hiervon nicht berührt.

12 PREIS UND ZAHLUNG

12.1 Der Preis der Dienstleistungen ist die im jeweiligen Angebot angegebene Gebühr (einschließlich Mehrwertsteuer, soweit einschlägig). Die Zahlung kann per Barzahlung, SEPA-Lastschrift, Banküberweisung oder Kreditkarte, bzw. für Geschäftskunden auch per Auftrag auf Rechnung (Bestellnummer), erfolgen.

12.2 Bei Cash-Zahlungen, Vorabüberweisung, Sepa-Lastschriftmandat oder Kreditkartenzahlung ist die Gebühr grundsätzlich vor Beginn der Dienstleistungen zu zahlen (Vorkasse), oder, falls zutreffend, zu dem in der mit Ontrack separat getroffenen Zahlungsvereinbarung angegebenem Zeitpunkt. Wenn Sie einen gemäß dem Vertrag fälligen Betrag nicht an uns zahlen, können wir

die Geräte und Daten bis zur vollständigen Zahlung zurückbehalten. Im Falle einer widerrufenden, zu spät erfolgten oder nicht geleisteten Zahlung erhalten Sie nach Fälligkeit der Zahlung eine erste Mahnung (Textform). Bei fehlendem Zahlungseingang nach der ersten Mahnung erhalten Sie noch eine weitere Mahnung, bevor wir uns vorbehalten, die Forderung an unser Inkassobüro zu übergeben. Wir behalten uns ferner vor, Verzugszinsen oder weitere Ansprüche geltend zu machen.

12.3 Im Falle der Kreditkartenzahlung sendet Ontrack Ihnen einen Zahlungslink zu einer sicheren Zahlungsplattform eines Drittanbieters zu, um die Zahlung zu autorisieren und den Zahlungsvorgang nach Abschluss der Arbeiten, aber vor Zusendung des Backup-Mediums, abzuschließen.

12.4 Geschäftskunden erhalten eine Rechnung. Wenn Sie die Rechnung nicht innerhalb der vereinbarten Zahlungsfrist vollständig begleichen, senden wir Ihnen eine Mahnung (Textform) zu. Bei fehlendem Zahlungseingang nach der ersten Mahnung erhalten Sie noch eine weitere Mahnung, bevor wir die Forderung an unser Inkassobüro übergeben. Wir können im Falle des Zahlungsverzugs Verzugszinsen in gesetzlich zulässiger Höhe erheben. Weitere Ansprüche (z.B. auf Verzugsschaden) bleiben vorbehalten.

13 HAFTUNGSBEGRENZUNG

13.1 Ansprüche des Kunden auf Schadensersatz sind ausgeschlossen. Hiervon ausgenommen sind Schadensersatzansprüche des Kunden aus der Verletzung des Lebens, des Körpers, der Gesundheit oder aus der Verletzung wesentlicher Vertragspflichten (Kardinalpflichten) sowie die Haftung für sonstige Schäden, die auf einer vorsätzlichen oder grob fahrlässigen Pflichtverletzung von Ontrack oder der gesetzlichen Vertreter oder Erfüllungsgehilfen von Ontrack beruhen. Wesentliche Vertragspflichten sind solche, deren Erfüllung zur Erreichung des Ziels des Vertrags notwendig ist.

13.2 Bei der Verletzung wesentlicher Vertragspflichten haftet Ontrack nur auf den vertragstypischen, vorhersehbaren Schaden, wenn dieser lediglich einfach fahrlässig (d.h. nicht grob fahrlässig oder vorsätzlich) verursacht wurde, es sei denn, es handelt sich um Schadensersatzansprüche des Kunden aus einer Verletzung des Lebens, des Körpers oder der Gesundheit. Gegenüber Geschäftskunden haftet Ontrack, sofern der Schaden nicht vorsätzlich oder grob fahrlässig verursacht wurde oder eine Haftung für die Verletzung des Lebens, des Körpers oder der Gesundheit besteht, in jedem Fall nur bis zu einer Höchstsumme von 20.000,- Euro. Sie (der Geschäftskunde) erkennen an und vereinbaren mit uns (Ontrack), dass die vorgenannte Haftungshöchstsumme den vertragstypischen, vorhersehbaren Schaden übersteigt.

13.3 Unbeschadet der vorstehenden Regelung in Ziffer 13.1 übernehmen wir keine Verantwortung für die physische oder sonstige Beschädigung oder Zerstörung Ihrer Geräte und Ihrer Daten oder den Verfall von Garantien in Bezug auf Ihre Geräte im Rahmen der Bereitstellung unserer Dienstleistungen, wenn diese Schäden, Zerstörungen, Beschädigungen oder ein Verfall aufgrund der vertragsgemäßen Durchführung der Dienstleistungen gemäß diesem Vertrag entstehen. Hiervon ausgenommen sind Schäden, die auf einer vorsätzlichen oder grob fahrlässigen Pflichtverletzung von Ontrack oder unserer gesetzlichen Vertreter oder Erfüllungsgehilfen beruhen.

13.4 Obgleich wir angemessene Anstrengungen unternehmen, sorgfältig mit Ihren Geräten oder Daten umzugehen, während sie in unserem Besitz sind, sind wir Ihnen gegenüber nicht verantwortlich, wenn Ihre Geräte oder Daten ohne unser Verschulden verloren gehen, zerstört, beschädigt oder anderweitig durch normalen Verschleiß oder aufgrund der Natur der Dienstleistungen beschädigt werden.

13.5 Keine der Parteien haftet gegenüber der anderen Partei, sei es aus Vertrag, unerlaubter Handlung (einschließlich Fahrlässigkeit), aus Verletzung gesetzlicher Pflichten oder anderweitig, die sich aus oder im Zusammenhang mit diesen AGB oder einem Vertrag ergeben, für indirekte oder Folgeschäden, Gewinn-, Umsatz- oder Geschäftsausfälle.

13.6 **Einsatz von Kurieren.** In Überreinstimmung mit den Bestimmungen der Ziffer 5 haftet Ontrack im Falle des Versands der Originaldatenträger durch einen von Ontrack beauftragten Drittkurier nur in Höhe der von dem Drittkurier angebotenen Entschädigung. Die Bedingungen des Drittkuriers lauten https://www.dhl.de/de/geschaeftskunden/express/infos-knowhow/downloads.html#agb oder https://www.dhl.de/de/geschaeftskunden/paket/rund-um-den-versand/agb.html.

14 FREISTELLUNG

14.1 Sie stellen Ontrack frei von Ansprüchen Dritter, die aufgrund Ihres rechtswidrigen Verhaltens gegen uns erhoben werden. Die Freistellung gilt insbesondere für Ansprüche wegen Verstoßes gegen datenschutz-, wettbewerbs- oder urheberrechtliche Bestimmungen.

14.2 Für den Fall, dass Ihre Zusicherung nach Ziffer 11.1 ganz oder teilweise nicht zutreffend sind, stellen Sie Ontrack frei von sämtlichen Ansprüchen Dritter, die nicht bestehen würden, wenn Ihre Zusicherungen zutreffend gewesen wären.

14.2 Sie stellen Ontrack frei von Ansprüchen Dritter, die darauf beruhen, dass Sie nicht der (alleinige) Eigentümer der Geräte und Daten auf den betreffenden Geräten sind, ihre Verfügungsmacht über die Geräte und Daten anderweitig eingeschränkt ist oder die Daten unter Verletzung von Rechten Dritter oder sonst in rechtswidriger Weise erhoben, erstellt, gespeichert oder anderweitig ver- bzw. bearbeitet wurden.

14.3 Die Haftungsfreistellung gemäß dieser Ziffer 14 umfasst neben Schadensersatzleistungen auch Bußgelder sowie nachgewiesene angemessene Verfahrenskosten (einschließlich Kosten der Rechtsverfolgung und -verteidigng).

15 DATENSCHUTZ

15.1 Informationen zum Datenschutz können Sie unter folgendem Link auf unserer Webseite einsehen: https://www.ontrack.com/de-de/datenschutzrichtlinie.

16 WIE WIR PERSONENBEZOGENE DATEN VERARBEITEN (WIEDERHERGESTELLTE DATEN)

16.1 Soweit Ontrack personenbezogene Daten im Rahmen der Datenrettung für Sie als Kunden verarbeitet, gilt unsere Auftragsdatenverarbeitungsvereinbarung, die unter https://www.ontrack.com/de-de/legal/agb#auftragsverarbeitungsvertrag abrufbar ist.

17 VERTRAULICHE INFORMATIONEN

17.1 Die übergebende Partei hat an den der empfangenden Partei bekannt gewordenen Vertraulichen Informationen ein Geheimhaltungsinteresse. Die empfangende Partei verpflichtet sich daher, die ihr übermittelten oder sonst zugänglich gemachten Vertraulichen Informationen streng vertraulich zu behandeln und weder ganz noch teilweise Dritten zugänglich zu machen, sofern nicht die übergebende Partei einer Offenbarung an Dritte vorher schriftlich zugestimmt hat und der Dritte sich in einer dieser AGB entsprechenden Weise zur Geheimhaltung verpflichtet hat.

17.2 Die Geheimhaltungsverpflichtungen erstreckt sich nicht auf vertrauliche Informationen, für die die empfangende Partei nachweisen kann, dass (a) sie der empfangenden Partei vor der Mitteilung bereits bekannt waren oder (b) sie zum Zeitpunkt der Mitteilung an die empfangende Partei bereits offenkundig, öffentlich bekannt und frei zugänglich waren, oder danach geworden sind oder (c) sie nach der Übermittlung ohne Verschulden der empfangenden Partei ohne Verletzung dieser AGB offenkundig wurden oder (d) sie im Wesentlichen Informationen entsprechen, die der empfangenden Partei zu irgendeinem Zeitpunkt von einem dazu berechtigten Dritten offenbart oder zugänglich gemacht wurden oder (e) sie von der empfangenden Partei unabhängig von den vertraulichen Informationen entwickelt wurden oder (f) sie von der übergebenden Partei zur Bekanntmachung vorher ausdrücklich schriftlich freigegeben wurden oder (g) deren Innehabung, Besitz oder Kenntnis gegen geltende Strafgesetze verstoßen oder (h) sie aufgrund einer bindenden behördlichen oder richterlichen Anordnung oder zwingender rechtlicher Vorschriften zu offenbaren sind.

18 WEITERE WICHTIGE BESTIMMUNGEN

18.1 Dieser Vertrag kommt zwischen Ihnen und uns zustande. Keine andere Person hat das Recht, seine Bestimmungen durchzusetzen. Jede Klausel dieser AGB wirkt getrennt. Wenn ein Gericht oder eine zuständige Behörde entscheidet, dass eine dieser Klauseln rechtswidrig bzw. nicht durchsetzbar ist, bleiben die übrigen Klauseln in vollem Umfang wirksam und in Kraft. Wenn wir in Bezug auf Ihre Vertragsverletzung nicht sofort Maßnahmen gegen Sie einleiten, hindert uns dies nicht daran, dies zu einem späteren Zeitpunkt zu tun, soweit dies dem jeweils geltenden Recht entspricht.

18.2 Wir können die Dienstleistungen anpassen, um Änderungen der relevanten Gesetze und regulatorischen Anforderungen zu berücksichtigen und kleinere technische Anpassungen und Verbesserungen vorzunehmen, z.B. um eine Sicherheitsbedrohung abzuwenden. Diese Änderungen haben keinen Einfluss auf Ihre Nutzung der Dienstleistungen. Darüber hinaus können wir weitere wesentliche Änderungen an diesen AGB oder den Dienstleistungen vornehmen, aber wenn dies geschieht, informieren wir Sie vorab darüber und Sie können dann den Vertrag vor Inkrafttreten der Änderungen beenden und eine Rückerstattung für alle bezahlten, aber nicht erhaltenen Dienstleistungen erhalten.

18.3 Wenn Sie in der Europäischen Union ansässig sind, können Sie möglicherweise Beschwerden über die Online-Streitbeilegungsplattform der Europäischen Union (die „Plattform“) einreichen, die es ermöglicht, Streitigkeiten online beizulegen. Weitere Informationen erhalten Sie auf der Plattform unter https://webgate.ec.europa.eu/odr/. Ontrack beabsichtigt nicht, die Plattform zur Beilegung von Streitigkeiten zu nutzen, und Sie akzeptieren, dass Ontrack nicht verpflichtet ist, die Plattform zur Beilegung von Streitigkeiten zu nutzen.

18.4 Die AGB und alle Angelegenheiten, die sich im Zusammenhang mit unserer Erbringung der Dienstleistungen ergeben, unterliegen deutschem Recht. Im Streitfall sind die ordentlichen Gerichte in Deutschland zuständig.

Gültigkeit ab 1. Mai 2023

ANLAGE

Muster-Widerrufsformular

(Wenn Sie den Vertrag widerrufen wollen, dann füllen Sie bitte dieses Formular aus und senden es zurück.)

An

KLDiscovery Ontrack GmbH,

Hanns-Klemm-Straße 5

71034 Böblingen

Tel. +49 7031 644 0,

E-Mail info@ontrack.de

Betreff: Widerruf des Dienstleistungsvertrages

Hiermit erkläre(n) ich/wir (*), dass ich/wir (*) von meinem/unserem (*) Vertrag über die Erbringung der folgenden Dienstleistung (*) zurücktrete(n),

Bestellt am (*)/erhalten am (*),

Name des/der Verbraucher(s),

Adresse des/der Verbraucher(s),

Ontrack Kundennummer,

Unterschrift des/der Verbraucher(s) (nur wenn dieses Formular in Papierform übermittelt wird),

Datum

_____

(*) Unzutreffendes streichen.

Leistungsbeschreibung für Ontrack Datenrettungsdienstleistungen

1. Der Datenrettungsprozess, Ontracks Dienstleistung und Grenzen

a) Datenrettungsdienstleistungen erfolgen in mehreren Schritten:

- Die Evaluation - siehe Abschnitt 2 unten -; **oder/und**
- Die Diagnose - siehe Abschnitt 3 unten -; **und**
- Die Datenrettung nach der Evaluation oder Diagnose - siehe Abschnitt 4 unten –, bzw. RDR Remote Datenrettungsdienst für Geschäftskunden – siehe Abschnitt 5 unten.

b) Ontrack wird so viele Daten wie möglich von einem oder mehreren beschädigten Datenträgern wiederherstellen. Ontrack testet keine Verwendbarkeit oder Kompatibilität auf Anwendungssoftware.

c) Es ist möglich, gelöschte und/oder beschädigte Daten auch bei Verwendung der Tools und Technologien von Ontrack nicht zu lesen. Daher kann Ontrack nicht garantieren, dass Daten auf beschädigten Datenträgern wiederhergestellt, repariert oder gelesen werden können.

d) Ontrack wird Datenträger dahingehend untersuchen, um festzustellen, welche Beschädigungen überwunden werden müssen, um Daten und Datenstrukturen soweit wiederherstellen zu können, dass sie in ihrer jeweiligen Anwendung voraussichtlich wieder gelesen und verwendet werden können. Dazu wendet Ontrack höchste technische Standards und eigenentwickelte Prozesse, sowie Software- und Hardware-Werkzeuge an. Aufgrund der Natur der Sache, dass Ontrack mit beschädigten Daten oder Datenträgern arbeitet, besteht ein allgemeines Risiko, dass verbleibende Daten teilweise oder vollständig auf den beschädigten Datenträgern untergehen oder zerstört werden können.

e) Der Kunde erkennt an, dass die Gefahr besteht, dass:

- sobald bestehende Daten nicht mehr wiederhergestellt werden können, auch zusätzliche Daten verloren gehen können;
- wiederhergestellte Daten vom Kunden nicht mehr verwendet werden können;
- der in den Datenträgern enthaltene Informationsgehalt ganz oder teilweise zerstört wird; und
- die bereitgestellten Datenträger, Software und andere Gegenstände beschädigt werden, unbrauchbar oder zerstört werden können.

2. Evaluation

a) Die Evaluation ist eine erste Begutachtung durch einen erfahrenen Datenrettungsingenieur, die ermittelt, welche Beschädigungen auf dem Datenträger zu erkennen sind, um eine Einschätzung der zu erwartenden Datenmenge, die wiederhergestellt werden kann, zu geben. Die Evaluation findet bei HDDs, SDDs, und RAID/NAS-Systemen Anwendung. Von der Evaluation ausgenommen sind unter anderem Mobiltelefone, Tablets und Flashmedien, sowie Medien mit gelöschten Daten, Wasser- und Feuerschäden, und bereits geöffnete Speichermedien. Bei der Evaluation werden die Datenträger des Kunden an eigene Spezialsysteme angeschlossen und ggf. geöffnet. In der Evaluation werden keine Daten kopiert/gesichert (Image) oder weitergehend analysiert. Es wird keine Auflistung wiederherstellbarer Datensätze oder eine Angabe, welche Dateien gerettet werden können, erstellt. Ontrack stellt keinen eigenständigen Schadensbericht zur Verfügung.

b) Ontrack wird den Kunden nach der Evaluation darüber informieren, ob (i) eine Datenrettung in Betracht kommt, (ii) die Durchführung einer weiteren kostenpflichtigen Diagnose notwendig ist, um die Möglichkeiten der Datenrettung samt der voraussichtlich wiederherstellbaren Datenmenge zu bestimmen (siehe Abschnitt 3); (iii) oder eine Datenrettung in dem vorliegenden Fall von Ontrack nicht durchgeführt werden kann.

c) Eine Einschätzung, inwieweit eine Datenrettung nach der Evaluation erfolgsversprechend ist, erfolgt anhand nachfolgender Klassifizierung:

- **Ausgezeichnet** - Wir erwarten, dass 95-100 % Ihrer Daten erfolgreich wiederhergestellt werden können.
- **Gut.** Wir erwarten, dass 75-100 % Ihrer Daten erfolgreich wiederhergestellt werden können
- **Teilweise wiederherstellbar** - Wir gehen davon aus, dass ein kleiner Teil Ihrer Rohdaten im Bereich von bis zu 50% wiederhergestellt werden kann
- **Komplex** Aufgrund der Komplexität des Fehlerbildes, können wir noch keine genaue Prozentzahl für die Wiederherstellbarkeit Ihrer Daten angeben. Deshalb empfehlen wir in diesem Fall eine erweiterte Diagnose.
- **Nicht wiederherstellbar** - Wir können auf die Daten Ihres Datenträgers nicht zugreifen.

d) Die Einschätzung der Erfolgsaussichten einer Datenrettung anhand der o.g. Klassifizierung ist keine Garantie, dass die in Abschnitt 2 Buchstabe c) aufgeführten Prozentsätze eingehalten werden, da bei einer Evaluation weder physikalische noch datenstrukturelle Schäden behoben werden.

e) Auf Wunsch des Kunden kann Ontrack nach der Evaluation eine erweiterte, kostenpflichtige Diagnose mit der Erstellung einer Verifile Dateiliste durchführen, in der die zu erwartende Datenmenge genauer bestimmt werden kann (siehe Abschnitt 3 unten). Bitte beachten Sie, dass es nicht in allen Fällen möglich ist, eine Dateiliste zu erstellen.

f) Erteilt der Kunde auf der Grundlage der Ergebnisse der Evaluation den Auftrag zur Datenrettung (siehe Abschnitt 4 unten), wird Ontrack die Datenrettung durchführen.

g) Der Kunde kann beschließen, die Datenrettung nach der Evaluation nicht durchzuführen. Auf Wunsch des Kunden wird der Datenträger gegen die im Angebotsformular angegebene Gebühr an den Kunden zurückgeschickt. Andernfalls werden die Medien fachgerecht entsorgt.

h) Bitte beachten Sie, dass durch die Bearbeitung während der Evaluation die Kundengeräte beschädigt werden können.

3. Diagnose

a) Für eine Widerherstellung von Daten auf Smartphones, Tablets oder Flashmedien oder bei bestimmten Datenschäden bietet Ontrack eine kostenpflichtige Diagnose (und keine Evaluation) an. Eine Diagnose kann von Ontrack aber auch nach der Durchführung der Evaluation, speziell bei komplexen Schadensbildern, empfohlen werden.

b) Bei der Diagnose werden Art und Umfang des Datenschadens, die genaue Bestimmung der Möglichkeiten der Datenrettung auf den vom Kunden zur Verfügung gestellten Datenträgern und die Menge der voraussichtlich wiederherstellbaren Dateien/Daten bestimmt. Ontrack gewährt dem Kunden Zugriff auf eine Firmeneigene Plattform, die ihm den Status nachverfolgen lässt sowie dem Kunden abschließend eine Dateiliste (Verifile) übermittelt, wenn eine Datenwiederherstellung möglich ist. In Ausnahmefällen kann es vorkommen, dass Ontrack keinen Zugriff auf die Daten bekommt und damit eine Dateiliste (Verifile) nicht zur Verfügung stellen kann.

c) Die Dateiliste (Verifile) enthält einen Hinweis auf die Qualität der Daten in Bezug auf ihre Verwendbarkeit im Ampelsystem:

- **Grün** - die Daten werden höchstwahrscheinlich in der jeweiligen Anwendung funktionieren, bzw. öffnen.
- **Gelb** - die Daten oder Dateien sind teilweise beschädigt - dies kann dazu führen, dass die Dateien in der jeweiligen Anwendung nicht geöffnet und bearbeitet werden können. Es ist möglich, dass die beschädigten Dateien repariert werden können. Eine solche Dienstleistung wird jedoch nicht von Ontrack angeboten.
- **Rot** - die Daten oder Dateien sind beschädigt - dies führt wahrscheinlich dazu, dass die Dateien in der jeweiligen Anwendung nicht geöffnet und bearbeitet werden können.

d) Prognosen über die Lesbarkeit von Daten aufgrund anderer Schadensursachen werden nicht vorgenommen. Es ist Ontrack daher nicht möglich, die Verwendbarkeit der Daten im Zusammenhang mit dem jeweiligen Anwendungsprogramm im Rahmen der Diagnose zu überprüfen. Deswegen kann Ontrack keine Garantie übernehmen, dass die geretteten Daten mit dem jeweiligen Anwenderprogramm lesbar sind. Dies gilt im speziellen Fall für Datenbankdateien aller Art. Das Einspielen der Datensätze, der Aufwand für das Bereinigen der Datensätze nach Stand der Technik der jeweiligen Datenbanksoftware und Applikation und die Konsultation weiterer Experten liegt allein in der Verantwortung des Auftraggebers. Ontrack unterstützt den Auftraggeber und beauftragte Auftragnehmer soweit möglich.

e) Es gibt spezielle Datenverlustszenarien, in denen die farbigen Aussagen in der Dateiliste (Verifile) keine Aussagekraft haben. Bei solch schwerwiegenden strukturellen Beschädigungen gibt Ontrack keine Garantie auf die Funktionalität der Dateien. Liegt ein solcher Fall vor, wird darauf im Diagnoseergebnis hingewiesen.

f) Die Diagnose wird im Labor von Ontrack durchgeführt. Mobiltelefone und Tablets senden wir üblicherweise in unser Schwesterlabor nach Polen.

g) Abhängig von der Art des Mediums kann die Diagnose zur Übertragung der Daten auf ein anderes Speichermedium und zur Zerstörung des Original-Kundengeräts führen.

h) Erteilt der Kunde auf der Grundlage der Ergebnisse der Diagnose den Auftrag zur Datenrettung (siehe Abschnitt 4 unten), wird Ontrack die Datenrettung durchführen.

g) Der Kunde kann beschließen, die Datenrettung nach der Diagnose nicht durchzuführen. Auf Wunsch des Kunden wird der Datenträger des Kunden gegen die im Angebotsformular angegebene Gebühr dann an diesen zurückgeschickt. Andernfalls werden die Medien fachgerecht entsorgt.

4.) Datenrettung nach Diagnose oder Evaluation

a) Angebot zur Datenrettung nach erfolgter Evaluation

Das Ergebnis der Evaluation wird zusammen mit einem Angebot zur Datenrettung übermittelt. Übermittelt wird nur die erwartete Erfolgseinschätzung sehr gut/gut/teilweise gut.

Das Angebot zur Datenrettung enthält den Datenrettungspreis in Bezug auf die Service Level (siehe Absatz c.), die die Bearbeitungszeit für den jeweiligen Datenrettungsprozess ausweisen und wird dem Kunden wie in unseren AGB beschreiben übermittelt.

b.) Angebot zur Datenrettung nach Diagnose

Nach der Diagnose übermittelt Ontrack dem Kunden die Verifile Liste, sofern diese erstellt werden konnte, und informiert den Kunden darüber, wie lange der Datenrettungsprozess dauert und welche Kosten für die Datenrettung anfallen werden. Der Kunde erhält ein Angebot zur Datenrettung, wie in unseren AGB beschrieben, welches den Datenrettungspreis in Bezug auf die Service Level (siehe Absatz c.), die die Bearbeitungszeit für den jeweiligen Datenrettungsprozess ausweisen, enthält.

c.) Service Levels

Für die Datenrettungsbeauftragung kann der Kunde je nach Dringlichkeit zwischen den folgenden Servicestufen wählen:

- Notfall-Service
  Die Bearbeitung erfolgt unmittelbar nach Auftragseingang rund um die Uhr.
- Express-Service
  Die Bearbeitung erfolgt unmittelbar nach Auftragseingang von Montag bis Freitag von 8.00 bis 18.00 Uhr. Die Dauer des Datenrettungsprozesses beträgt in der Regel 3-5 Werktage.
- Standard-Service
  Der Datenträger wird nach Auftragseingang von Montag bis Freitag zwischen 9.00 und 17.00 Uhr bearbeitet. Die Dauer des Datenrettungsprozesses beträgt in der Regel 7-10 Werktage.
- Economy-Service
  Die Bearbeitung des Datenträgers erfolgt nach Auftragseingang von Montag bis Freitag zwischen 9.00 und 17.00 Uhr. Die Dauer des Datenrettungsprozesses beträgt in der Regel 20 Werktage.

d.) Annahme der Datenrettung

Der Kunde nimmt das Datenrettungsangebot wie in unseren AGB beschreiben an.

Wenn der Kunde beschließt, die Datenrettung nicht auf der Grundlage der Evaluationsergebnisse oder Dateiliste (Verifile) durchzuführen, gilt die Bestellung als abgebrochen. Auf Wunsch des Kunden wird der Datenträger gegen die im Angebotsformular angegebene Gebühr an den Kunden zurückgeschickt. Andernfalls werden die Medien fachgerecht entsorgt.

e) Durchführung der Datenrettung

Wenn der Kunde einen Auftrag zur Datenrettung auf der Grundlage des Datenrettungsangebots nach Prüfung der Ergebnisse der Evaluation oder/und Diagnoseergebnisse erteilt, führt Ontrack die Datenrettung durch.

Der Kunde erhält die Daten, die von Ontrack wiederherstellbar waren. Nach einer Diagnose sind das üblicherweise die in der Dateiliste (Verifile) dargestellten Daten.

Die von Ontrack widerhergestellten Daten werden auf einem portablem Speichermedium gespeichert und an den Kunden gesandt. Zusätzlich zu dem separaten Datenträger mit den wiederhergestellten Daten kann Ontrack den beschädigten Datenträger zurücksenden, wenn der Kunde dies bei Erteilung des Auftrags zur Datenrettung, unter Entrichtung der dort genannten Rücksendegebühr, verlangt.

Auf Wunsch des Kunden kann Ontrack die Daten auf dem Datenträger gemäß den geltenden Vorschriften kostenlos löschen und/oder den Datenträger entsorgen.

f) Abweichungen im Datenrettungsergebnis

Sollte es vorkommen, dass die Menge der wiederhergestellten Daten erheblich geringer ist als die in der Evaluation geschätzte Menge an wiederherstellbaren Daten, wird dem Kunden ohne zusätzliche Kosten eine Dateiliste (verifile) zur Verfügung gestellt, um ihn bei der Entscheidung zu unterstützen, mit der Wiederherstellungsphase fortzufahren. Wurde bereits eine Dateiliste zur Verfügung gestellt und ist die Menge der wiederhergestellten Daten erheblich geringer als geschätzt, setzt sich ein Kundenbetreuer mit dem Kunden in Verbindung, um die Ergebnisse und die Optionen des Kunden für die Datenwiederherstellung zu besprechen.

5. RDR Remote Datenrettungsdienst

a) RDR® steht für Remote Data Recovery™ (“RDR”). RDR ist eine patentierte Technologie, die es den Ingenieuren von Ontrack ermöglicht, eine Datenwiederherstellung in Laborqualität direkt auf dem Server, Desktop oder Laptop des Kunden über eine Internetverbindung durchzuführen. Die einzige Voraussetzung ist, dass der Datenträger betriebsbereit ist. Die RDR von Ontrack besteht aus drei Hauptkomponenten:

Kommunikationsklient: Der Kunde initiiert eine Verbindung zu einem Ontrack RDR Server mit Hilfe der speziell entwickelten RDR Client Software. Der RDR-Client arbeitet mit gängigen Betriebssystemen. Die wiederherzustellenden Laufwerke müssen nicht von einem bestimmten Betriebssystem stammen.

RDR-Server: Ontrack hat mehrere Server-Standorte auf der ganzen Welt.

RDR-Arbeitsplatz: Er wird von Ontrack-Ingenieuren verwendet, um die Tools auf der Maschine des Kunden fernzusteuern und Daten des Kunden wiederherzustellen.

b) Zunächst lädt der Kunde die entsprechende RDR-Client-Version herunter und installiert sie auf dem Server, Desktop oder Laptop, der für die Wiederherstellung verwendet wird. Anschließend verbindet sich die Ontrack Client-Software als ausgehende TCP/IP-Verbindung vom Standort des Kunden zum Ontrack-Server und erstellt einen Tunnel oder eine Punkt-zu-Punkt Verbindung über das Internet. Da die Verbindung wahrscheinlich eine Webverbindung verwendet, kann sie die meisten Firewalls ohne zusätzliche Konfigurationsanforderungen passieren. Die Sicherheit der Daten ist aufgrund des proprietären Kommunikationsprotokolls von Ontrack, der verschlüsselten Pakete und der sicheren Ontrack-Einrichtungen von höchster Bedeutung.

RDR schützt Kundendaten über eine RDR-Verbindung auf vier Arten:

1 Direkte Verbindung zum RDR-Server: Die Client-Software verwendet eine direkte TCP-Verbindung vom Computer des Kunden zum Ontrack RDR-Server. RDR verwendet kein Hosting-Produkt von Drittanbietern.

2 Verschlüsselung: Die Kommunikationsverbindung verwendet 256 Bit Verschlüsselung auf allen Paketen.

3 Proprietäres Protokoll: Die RDR-Kommunikation verwendet ein proprietäres Protokoll, nicht jedoch HTTP oder ein anderes gängiges Protokoll, das andere verstehen würden.

4 Es werden keine Kundendaten über die Verbindung übertragen: Die RDR-Verbindung wird nur vom Ontrack-Ingenieur verwendet, um die Ontrack-Dienstprogramme direkt auf der Maschine des Kunden fernzusteuern. Bildschirmaktualisierungen und Tastaturpakete werden über die Verbindung gesendet, nicht aber tatsächliche Kundendatendateien. Stattdessen steuert der Ontrack-Ingenieur Werkzeuge zur Reparatur von Dateisystemstrukturen, um die Daten dem Kunden zugänglich zu machen.

c) Sobald die Verbindung hergestellt ist, beginnt entweder die Diagnose oder es beginnt der Wiederherstellungsprozess, wenn ein Datenrettungsauftrag erteilt wird.

Stand: Juni 2023

Auftragsverarbeitungsvertrag

Dieser Auftragsverarbeitungsvertrag ist eine Ergänzung zu den Allgemeinen Geschäftsbedingungen für Ontrack-Datenrettungsdienste („AGB“) und gilt für: (i) KLDiscovery Ontrack GmbH, im Folgenden „Ontrack“ genannt, mit Sitz in der Hanns-Klemm-Straße 5, 71034 Böblingen, eingetragen beim Handelsregister Stuttgart unter der Nummer HRB 244142; und (ii) der jeweilige Kunde, der Datenrettungsdienste gemäß den AGB bestellt.

Die Parteien haben vereinbart, dass die Bedingungen dieses Auftragsverarbeitungsvertrages für die Verarbeitung personenbezogener Daten (die nachstehend definiert sind) gelten, die erforderlich ist, damit Ontrack die Datenrettungsdienste für den jeweiligen Kunden leisten kann.

Begriffsbestimmungen

für diesen Auftragsverarbeitungsvertrag:

Verantwortlicher	hat die Bedeutung, die diesem Begriff im Datenschutzrecht zugewiesen ist;
Auftragsverarbeiter	hat die Bedeutung, die diesem Begriff im Datenschutzrecht zugewiesen ist;
Datenschutzrecht	bezeichnet das gesamte anwendbare Datenschutzrecht, das für den Kunden, Ontrack und/oder in Bezug auf die Datenrettungsdienste gilt, einschließlich: (i) die DSGVO und/oder entsprechende oder gleichwertige nationale Gesetze oder Verordnungen; und (ii) in den Mitgliedstaaten der Europäischen Union alle relevanten Gesetze oder Verordnungen, die die DSGVO wirksam machen oder ihr entsprechen.
Betroffene Person	hat die dem Begriff im Datenschutzrecht zugewiesene Bedeutung;
Anfrage der betroffenen Person	ist eine Anfrage einer betroffenen Person zur Ausübung der Rechte der betroffenen Personen nach Datenschutzrecht;
DSGVO	bezeichnet die Datenschutz-Grundverordnung (EU) 2016/679;
Personenbezogene Daten	hat die dem Begriff im Datenschutzrecht zugewiesene Bedeutung und umfasst alle personenbezogenen Daten, die Ontrack vom Kunden zur Verfügung gestellt werden;
Verletzungen des Schutzes personenbezogener Daten	bezeichnet einen Verstoß gegen die Sicherheit der zur unbeabsichtigten oder rechtswidrigen Vernichtung, zum Verlust, zur Veränderung, zur unbefugten Weitergabe oder zum unbefugten Zugriff auf personenbezogene Daten führt;
Personal	bezeichnet jeden derzeitigen, ehemaligen oder zukünftigen Mitarbeiter, Berater, Leiharbeiter, Zeitarbeiter, Praktikanten, sonstigen nicht ständigen Mitarbeiter, Auftragnehmer, Entsandten oder sonstige Arbeitskräfte;
Verarbeitung	hat die Bedeutung, die diesem Begriff im Datenschutzrecht zugewiesen wird (und verwandte Begriffe wie verarbeiten haben entsprechende Bedeutungen);
Unterauftragsverarbeiter	bezeichnet einen anderen Auftragsverarbeiter, der von Ontrack im Auftrag des Kunden mit der Durchführung von Verarbeitungstätigkeiten in Bezug auf die geschützten Daten, eingesetzt wird. Hiervon ausgenommen sind Nebenleistungen, wie z.B. Telekommunikationsdienste, Post-/ Transportdienste, Wartungs- oder Benutzersupportdienstleistungen oder die Entsorgung von Datenträgern und Papierdokumenten sowie sonstige Soft- oder Hardwarebasierte Maßnahmen; und

Aufsichtsbehörde	bezeichnet lokale, nationale oder multinationale Agenturen, Einrichtungen, Behörden, Parlamente, öffentliche oder juristische Personen oder eine Regierung oder Innung, Regulierungs- oder Aufsichtsbehörde, Kommission oder andere Stelle, die für die Verwaltung des Datenschutzrechts zuständig ist.

Bestimmungen zur Datenverarbeitung

1 Auftragsverarbeiter und Verantwortlicher

1.1 Die Parteien vereinbaren, dass in Bezug auf die geschützten Kundendaten der Kunde der Verantwortliche und Ontrack der Auftragsverarbeiter ist. Es wird anerkannt, dass der Kunde die alleinige Verantwortung für die Richtigkeit, Qualität, Integrität und Zuverlässigkeit aller geschützten Daten und der Mittel, mit denen er diese geschützten Daten erworben hat, trägt.

1.2 Der Kunde garantiert und sorgt dafür, dass: (i) alle geschützten Daten, die in Verbindung mit den Datenrettungsdiensten gemäß den Bedingungen verwendet werden, in jeder Hinsicht das Datenschutzrecht erfüllen; (ii) alle Anweisungen, die Ontrack in Bezug auf geschützte Daten erteilt werden, jederzeit das Datenschutzrecht erfüllen; (iii) er alle erforderlichen Einwilligungen von jedem Betroffenen eingeholt hat, dessen personenbezogene Daten in die geschützten Daten aufgenommen wurden oder anderweitig die entsprechende rechtliche Erlaubnis zur Bereitstellung der personenbezogenen Daten an Ontrack besitzt und (iv) er die Bedingungen dieses Auftragsverarbeitungsvertrags einhalten wird.

1.3 Ontrack garantiert und sorgt dafür, dass es: (i) die geschützten Daten nur in dem Umfang verarbeitet, der im Zusammenhang mit den AGB erforderlich ist; und (ii) die geschützten Daten nach den dokumentierten Anweisungen des Kunden und den Anforderungen der Datenschutzgesetze verarbeitet; (iii) den Kunden unverzüglich informiert, wenn Ontrack der Ansicht ist, dass die Anweisungen des Kunden gegen das Datenschutzrecht verstoßen, oder wenn Ontrack nicht in der Lage ist, die Anweisungen des Kunden bezüglich der Verarbeitung von geschützten Daten zu befolgen (sei es aufgrund einer Gesetzesänderung oder einer Änderung der Anweisungen des Kunden); und (iv) die Bedingungen dieses Auftragsverarbeitungsvertrags einhält.

1.4 Im Rahmen der Auftragsverarbeitung werden alle vom Kunden übergebenen Daten verarbeitet. Die Kategorien personenbezogener Daten und die Kategorien der Betroffenen sind dem Kunden bekannt und werden für den Auftragsverarbeiter spezifiziert, sofern das im Rahmen des Auftrags erforderlich ist. Bei einer Datenrettung ist die Kenntnis über den Inhalt der Kundendaten für den Auftragsverarbeiter in der Regel nicht relevant.

2 Anweisungen und Angaben zur Verarbeitung

2.1 Die von Ontrack im Rahmen dieses Auftragsverarbeitungsvertrages durchzuführende Verarbeitung von geschützten Daten umfasst die Verarbeitung, die Ontrack zur Erbringung der Datenrettungsdienste benötigt.

3 Technische und organisatorische Maßnahmen

3.1 Ontrack führt auf eigene Kosten und Aufwand geeignete technische und organisatorische Maßnahmen im Zusammenhang mit der Verarbeitung und Sicherheit von geschützten Daten gemäß Datenschutzrecht, insbesondere den Artikeln 32-34 der DSGVO, durch und hält diese aufrecht. Ontrack stellt sicher, dass diese technischen und organisatorischen Maßnahmen den besonderen Risiken, die sich aus der Verarbeitung ergeben, angemessen sind, insbesondere um Kundendaten vor versehentlicher oder unrechtmäßiger Zerstörung, Verlust, Veränderung, unbefugter Offenlegung oder Zugriff zu schützen.

4 Einsatz von Personal und Unterauftragsverarbeitern

4.1 Mit Ausnahme der in Ziffer 4.2 genannten Fälle beauftragt Ontrack ohne vorherige schriftliche Zustimmung des Kunden keinen Unterauftragsverarbeiter mit der Durchführung von Verarbeitungstätigkeiten in Bezug auf die geschützten Daten. Wird eine Zustimmung erteilt, sorgt Ontrack vor der Offenlegung an einen zugelassenen Unterauftragsverarbeiter für eine schriftliche Vereinbarung mit dem Unterauftragsverarbeiter, die gleichwertig zu den in diesem Vertrag festgelegten sind. Es wird anerkannt und akzeptiert, dass Ontrack, ungeachtet anders lautender Bestimmungen in dieser Vereinbarung, dem Kunden gegenüber in vollem Umfang für die Erfüllung der Verpflichtungen jedes Unterauftragsverarbeiters haftet. Ontrack informiert den Kunden über beabsichtigte Änderungen, die sich auf Hinzufügen oder Ersetzen solcher Unterauftragsverarbeiter beziehen und gibt dem Kunden ausreichend Gelegenheit, diesen Änderungen oder Ersetzungen aus wichtigen Gründen zu widersprechen.

4.2 Die zum Zeitpunkt dieses Auftragsverarbeitungsvertrages zugelassenen Unterauftragsverarbeiter sind in Anlage 1 aufgeführt.

4.3 Ontrack sorgt für die Zuverlässigkeit seiner Mitarbeiter, die Zugang zu personenbezogenen Daten haben, und stellt sicher, dass sie diese nur dann verarbeiten, wenn dies für die Datenwiederherstellungsdienste unbedingt erforderlich ist, stellt sicher, dass sie über die zu ergreifenden Maßnahmen und die bei der Verarbeitung der geschützten Daten unter Beachtung des Datenschutzrechts zu ergreifenden Maßnahmen informiert sind, und stellt sicher, dass sie sich verpflichtet haben, die Vertraulichkeit der geschützten Daten zu schützen, einschließlich einer angemessenen Geheimhaltungsverpflichtung (sei es durch schriftlichen Vertrag oder anderweitig) in Bezug auf die geschützten Daten.

5 Unterstützung bei der Einhaltung der Compliance- und Betroffenenrechte des Kunden

5.1 Ontrack leitet alle bei ihr eingehenden Anfragen von Betroffenen unverzüglich an den Kunden weiter. Ontrack leistet dem Kunden die angemessene Unterstützung, die der Kunde (unter Berücksichtigung der Art der Verarbeitung und der Ontrack zur Verfügung stehenden Informationen) vernünftigerweise verlangt, um die Einhaltung der datenschutzrechtlichen Verpflichtungen des Kunden in Bezug auf: (i) die Sicherheit der Verarbeitung; (ii) Datenschutzfolgenabschätzungen (nach der Definition des Begriffs im Datenschutzrecht); (iii) vorherige Konsultation mit einer Aufsichtsbehörde bezüglich der Verarbeitung mit hohem Risiko; (iv) Benachrichtigungen an die Aufsichtsbehörde und/oder Mitteilungen an betroffene Personen durch den Kunden als Reaktion auf eine Verletzung des Schutzes personenbezogener Daten; und (v) Bearbeitung der Anfragen von Betroffenen, wobei jedoch der Kunde, falls diese Unterstützung in Bezug auf Zeit und Ressourcen unverhältnismäßig umfangreich ist, die bei Ontrack für die Bereitstellung dieser Unterstützung angefallenen Gebühren zahlt.

6 Internationale Datenübertragungen

6.1 Der Kunde erkennt an, dass Ontrack zum Zeitpunkt dieser Datenverarbeitungsvereinbarung personenbezogene Daten in Europa, einschließlich des Vereinigten Königreichs, und in den Vereinigten Staaten von Amerika während der Laufzeit dieser Vereinbarung verarbeiten darf.

6.2 Der Kunde nimmt zur Kenntnis, dass das Vereinigte Königreich einen Angemessenheitsbeschluss der Europäischen Kommission vom 28. Juni 2021 gemäß Artikel 45 Absatz 3 der Datenschutz-Grundverordnung erhalten hat, in dem bestätigt wird, dass Übermittlungen ohne Einholung einer weiteren Genehmigung erfolgen können (“Angemessenheitsbeschluss”). Darüber hinaus ist es Ontrack in Bezug auf personenbezogene Daten, die dem Data Protection Act 2018 (UK) unterliegen, gestattet, alle oder einen Teil der personenbezogenen Daten im Europäischen Wirtschaftsraum (“EWR”) gemäß Sch.21 Absatz 5(1)(a) des Data Protection Act 2018 zu verarbeiten. Für den Fall, dass der Angemessenheitsbeschluss ausläuft oder anderweitig für ungültig erklärt wird, treten die Parteien in die zum jeweiligen Zeitpunkt geltenden Standardvertragsklauseln zwischen dem für die Verarbeitung Verantwortlichen und dem Auftragsverarbeiter in der EU ein, um eine konforme Verarbeitung personenbezogener Daten durch Ontrack im Vereinigten Königreich zu gewährleisten.

6.3 Im Hinblick auf Datenübertragungen von persönlichen Daten in die USA vereinbaren die Parteien die von der Europäischen Kommission genehmigten Standardvertragsklauseln (Modul 2) zwischen Verantwortlichen und Auftragsverarbeitern aus dem Jahr 2021 mit den geltenden Änderungen gemäß S119A(1) des Data Protection Act 2018, und gemäß den Vorgaben des schweizerischen Bundesgesetzes über den Datenschutz vom 19. Juni 1992 (“DSG”) und, nach Inkrafttreten, gemäß Art. 16 Absatz 2 Buchstabe d des künftigen revidierten Bundesgesetzes über den Datenschutz vom 25. September 2020 (“revDSG”), die unter folgendem Link einzusehen sind (“Standardvertragsklauseln”), und durch Verweis in diese Datenverarbeitungsvereinbarung einbezogen werden. Die Parteien vereinbaren ebenfalls, dass alle Übertragungen den Bestimmungen der Standardvertragsklauseln unterliegen. Für den Fall, dass die Standardvertragsklauseln von der Europäischen Kommission oder aufgrund geltender Datenschutzgesetze geändert, aufgehoben oder ersetzt werden, arbeiten die Parteien nach Treu und Glauben zusammen, um eine aktualisierte Version des Datenübertragungsmechanismus zu vereinbaren oder eine alternative Lösung auszuhandeln, die eine konforme Übermittlung von personenbezogenen Daten in die Vereinigten Staaten von Amerika ermöglicht.

6.4 Mit den in dieser Klausel 6 “Internationale Datenübertragungen“ genannten Bedingungen genehmigt der Kunde die Übermittlung von personenbezogenen Daten in die Vereinigten Staaten von Amerika für die Dauer der Vereinbarung. Die Zustimmung des Kunden zur Übermittlung personenbezogener Daten in die Vereinigten Staaten von Amerika kann jederzeit widerrufen werden, aber in einem solchen Fall erkennt der Kunde an, dass Ontrack möglicherweise nicht in der Lage ist, den Auftrag auszuführen, wenn der Kunde seine Zustimmung zur Datenübermittlung widerruft.

7 Aufzeichnungen, Informationen und Audits

7.1 Ontrack (i) erstellt, (ii) aktualisiert und (ii) führt vollständige und genaue Aufzeichnungen über die gesamte Verarbeitung von geschützten Daten.

7.2 Ontrack räumt dem Kunden das Recht ein, während der normalen Geschäftszeiten und vorbehaltlich angemessener Vertraulichkeitsverpflichtungen mit einer Frist von mindestens 30 (dreißig) Tagen schriftlich das Recht auf Zugang und Kopie solcher Aufzeichnungen über die Verarbeitung von geschützten Daten zu erhalten, und leistet dem Kunden jede angemessene Unterstützung bei der Ausübung seiner Prüfungsrechte. Dieses Prüfungsrecht erstreckt sich nicht auf Rechenzentren von Drittanbietern oder andere Einrichtungen von Drittanbietern, in denen sich Serveranlagen befinden, die nur eine visuelle und begleitende Einsichtnahme zulassen.

7.3 Ontrack stellt dem Kunden auf Wunsch und Kosten des Kunden unverzüglich alle notwendigen Informationen zur Verfügung, damit der Kunde die Erfüllung seiner Verpflichtungen aus der DSGVO nachweisen kann, soweit Ontrack in der Lage ist, diese Informationen zur Verfügung zu stellen.

8 Verletzungsmeldung

8.1 Falls der Schutz personenbezogener Daten verletzt wird und davon geschützte Daten betroffen sind, die ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen darstellen könnten, wird Ontrack unverzüglich: (i) den Kunden über die Verletzung des Schutzes personenbezogener Daten informieren; und (ii) dem Kunden Einzelheiten über die Verletzung des Schutzes personenbezogener Daten mitteilen.

9 Löschung oder Rückgabe von personenbezogenen Daten und Kopien

9.1 Nach schriftlicher Aufforderung durch den Kunden oder mit Zeitablauf interner Aufbewahrungsfristen löscht Ontrack entweder alle geschützten Daten oder sendet sie an den Kunden in jener Form zurück, die der Kunde vernünftigerweise verlangt, und zwar innerhalb einer angemessenen Frist nach dem früher eintretenden Ereignis: (i) dem Ende der Erbringung der entsprechenden Datenrettungsdienste gemäß den AGB bezogen auf die Verarbeitung; oder (ii) sobald die Verarbeitung von geschützten Daten durch Ontrack nicht mehr erforderlich ist, um die Erfüllung der Verpflichtungen von Ontrack aus diesem Auftragsverarbeitungsvertrag zu gewährleisten, und löscht bestehende Kopien (es sei denn, die Speicherung von geschützten Daten ist nach geltendem Recht erforderlich und wenn dem so ist, informiert Ontrack den Kunden über eine solche Notwendigkeit). Ontrack stellt sicher, dass seine Unterauftragsverarbeiter die gleichen Maßnahmen in Bezug auf geschützten Daten ergreifen.

9.2 Ontrack löscht diese geschützten Daten, falls geschützte Daten ohne aktive Anweisungen des Kunden länger als 12 (zwölf) Monate im Besitz oder unter der Kontrolle von Ontrack bleiben.

10 Freistellung

10.1 Jede Partei (die „entschädigende Partei“) hat die andere Partei (die „entschädigte Partei“) in Bezug auf alle Ansprüche, Forderungen, Klagen, Vergleiche, Zinsen, Gebühren, Verfahren, Ausgaben, Verluste und Schäden, die der entschädigten Partei durch Urteil, Vergleich oder anderweitig aus oder im Zusammenhang damit angefallen oder entstanden sind, dass die entschädigende Partei gegen diesen Auftragsverarbeitungsvertrag und/oder das Datenschutzrecht verstoßen hat.

11 Haftung

11.1 Die Gesamthaftung einer der Parteien aus diesem Auftragsverarbeitungsvertrag darf in keinem Fall die in den AGB festgelegten und vereinbarten vertraglichen Grenzen überschreiten.

12 Laufzeit und Kündigung

12.1 Sofern die Parteien ihn nicht einvernehmlich kündigen, beginnt dieser Auftragsverarbeitungsvertrag mit dem Datum, an dem eine Bestellung für Datenrettungsdienste gemäß den Bedingungen erteilt wird, und gilt so lange, wie Ontrack weiterhin geschützte Daten verarbeitet.

13 Anzuwendendes Recht

13.1 Dieser Auftragsverarbeitungsvertrag unterliegt den in den AGB festgelegten Bedingungen der Rechtswahl.

Datum: 1 Mai 2021

Anhang 1 - Unterauftragsverarbeiter und Übertragungen

Ontrack Produkt- oder Business-System	Name und Standort des Auftragsverarbeiters
Anrufe außerhalb der Öffnungszeiten	ebuero AG | Hauptstraße 8 | 10827 Berlin
Mobilgerät-Entsperrdienst	Cellebrite GmbH Herzog-Heinrich-Strasse 20 80336, München, Deutschland
Data Recovery (Group companies)	KLDiscovery Ontrack Limited Nexus, 25 Farringdon Street, London, EC4A 4AB, Vereinigtes Königreich KLDiscovery Limited 25-28 North Wall Quay, Dublin 1, DO1 H104, Irland Ibas Ontrack ApS C/O Regus Center Christians Brygge 28, 1559 København V, Dänemark Ibas Ontrack Oy Mannerheimintie 12 B, 00100 Helsinki, Finland KLDiscovery Ontrack B.V. De Brand 22, 3823 LJ Amersfoort, Niederlande Ibas Ontrack AB Box 1005, 751 40 Uppsala, Schweden Ibas Ontrack AS Fjellgata 2, 2212 Kongsvinger, Norwegen KLDiscovery Ontrack GmbH Hanns-Klemm-Str. 5, 71034 Böblingen, Deutschland KLDiscovery Ontrack Srl Gallarte (VA) Via Marsala 34/A CAP 21013, Italien KLDiscovery Ontrack Sp. z o.o Katowice (40-082), ul. Jana III Sobieskiego 11, Polen KLDiscovery Ontrack SL Paseo de la Castellana, Num 81, Planta 11, 28046, Madrid, Spanien KLDiscovery Ontrack Sarl 2, impasse de la Noisette, 91371 Verriéres-le-Buisson Cedex 413, Frankreich KLDiscovery Ontrack (Switzerland) GmbH Hertistrasse 25, 8304 Wallisellen KLDiscovery Ontrack, LLC 9023 Columbine Road, Eden Prairie, MN 55347, USA

Ontrack by KLDiscovery

Data Recovery

Anhang 2: Technisch-organisatorische Massnahmen / Technical-organisational Measures

KLDIscovery Ontrack GmbH

Hinweis zum Dokument: ***Beschrieben werden hier die allgemeinen technisch-organisatorischen Maßnahmen von KLDiscovery Ontrack GmbH. Dabei werden die vorhandenen Maßnahmen in diesem Dokument generisch aufgeführt. Diese Maßnahmen werden immer wo erforderlich und möglich umgesetzt.***	***Note on the document:*** ***The general technical and organizational measures of KLDiscovery Ontrack GmbH are described here. The existing measures are listed generically in this document. These measures are implemented wherever necessary and possible.***
1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO) **Kein unbefugter Zutritt zu Datenverarbeitungsanlagen;** √ Werkschutz im Gebäude √ Beauftragtes Schließdienst-Personal √ Besetzter Empfang während der Arbeitszeiten √ Magnetkarten für Zufahrt √ Access-Chip für Räume (Dokumentation im System) √ Verschiedener Sicherheitszonen mit verschiedenen Zutrittsberechtigungen √ Türsicherung (elektrischer Türschließer, Chip-Lesegerät) √ Generalschlüssel √ Schlüssel-/Chipregelung √ Regelung für Umgang mit Besuchern und firmenfremdem Personal √ Besucherliste √ Besucher dürfen sich in Serverräumen nur in Begleitung aufhalten √ Nur das für Computer-Forensik √ zuständige Personal hat Zugang zum Computer-Forensik-Labor √ Alarmanlage / Einbruchmeldesystem √ Videoanlage (Serverraum)	1. Confidentiality (Art. 32 para. 1 b GDPR) **Access Control** *No unauthorised access to data processing equipment;* √ Building security via Nexus Security on site (24/7) √ Manned reception during working hours √ Access fob for rooms √ Different security zones with different access authorizations √ Door security (Magnetic door closer, Key Fob) √ Master key √ Key/Chip regulation √ Rules for dealing with visitors and external personnel √ Visitors list √ Visitors may only be in server rooms when accompanied √ Only personnel responsible for computer forensics have access to the clean room and engineering lab √ Video system monitored by the US
Zugangskontrolle *Keine unbefugte Systemzugänge/Systembenutzung;* √ Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte √ zentrale Benutzerverwaltung √ sichere Kennwortverfahren / Passwort-Policy √ verschlüsselte Benutzerauthentifizierung √ automatische Sperrmechanismen nach fehlerhaften Zugangsversuchen √ Zwei-Faktor-Authentifizierung √ Verschlüsselung für Dateien und Datenträgern √ Einsatz von Firewalls und Virenschutz √ Einsatz von Virtual Private Network (VPN) √ Protokollierung von Zugängen und Zugangsversuchen (Raum-Zugänge, VPN, etc.)	**System Access Control** *No unauthorized access to data processing systems;* √ authorization concepts and needs-based access rights √ central user administration √ secure password procedures / password policy √ encrypted user authentication √ automatic blocking mechanisms after unsuccessful access attempts √ Two-Factor Authentication √ Encryption for files and data carriers √ Use of firewalls and virus protection √ Use of Virtual Private Network (VPN) √ Logging of accesses and access attempts (room access, VPN, etc)

Zugriffskontrolle *Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems;* √ Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte für Programme und Daten √ zentrale Benutzerverwaltung √ Automatisches Ausloggen im Falle von Inaktivität nach einer bestimmten Zeitspanne √ Anwendung von rotierenden Archivierungssystemen und kontrolliertem Zugriff auf Backup-Bänder √ Verschlüsselung für Dateien und Datenträgern √ Protokollierung von Zugriffen und fehlerhaften Zugriffsversuchen	**Data Access Control** *No unauthorized reading, copying, modification or removal within the system;* √ authorization concepts and needs-based access rights for programs and data √ central user administration √ Automatic logout in case of inactivity after a certain period of time √ Use of rotating archiving systems and controlled access to backup tapes √ Encryption for files and data carriers √ Logging of accesses and incorrect access attempts
Trennungskontrolle *Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden;* √ Mandantenfähigkeit √ Trennung nach unterschiedlichem Zweck wird durch unterschiedliche Systeme/Datenbanken gewährleistet √ Funktionstrennung für Produktion / Test √ Unterschiedliche Verschlüsselung von Datensätzen, um eine Trennung zu verschiedenen Zwecken der Verarbeitung sicher zu stellen √ Implementierung von definierten Funktionen in den Informationssystemen: Administrator, Revisor, Nutzer. √ Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte für Programme und Daten √ Nutzung sicherer Prozesse z. B. von „Challenge Response Procedures“, um eine authorised application sicherzustellen	**Separation Control** *Separate processing of data collected for different purposes;* √ Multi-client capability √ Separation according to different purposes is ensured by different systems/databases √ Separation of functions for production / test √ Different encryption of data records to ensure separation for different processing purposes √ implementation of defined functions in the information systems: Administrator, auditor, user. √ authorization concepts and needs-based access rights for programs and data √ Use of secure processes such as Challenge Response Procedures to ensure an authorised application
Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO) *Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen;* Eine Pseudonymisierung wird zwischen den Parteien im jeweiligen Auftrag abgestimmt.	**Pseudonymisation (Art. 32 para. 1 a GDPR; Art. 25 para. 1 GDPR)** *The processing of personal data in such a way that the data can no longer be attributed to a specific data subject without additional information, provided that this additional information is kept separately and is subject to appropriate technical and organisational measures;* Any pseudonymisation is agreed between the parties in the respective order or contract.

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

Weitergabekontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport;

√ Verschlüsselungskonzepte (Verschlüsselung von Datenträgern, Verschlüsselung von Dateien, Verschlüsselung von E-Mails)
√ Verwendung digitaler Signaturen
√ Virtual Private Networks (VPN)
√ Vereinbarungen zur Auftragsverarbeitung mit Auftragnehmern
√ Datenträgerverwaltung und Bestandskontrolle
√ Reglementierter Gebrauch externer Datenträger wie z. B. USB-Sticks, externe Festplatten, SD-Speicherkarten etc.
√ Ausgabe von Datenträgern nur an autorisierte Empfänger (z.B. Auftragsquittung, Begleitpapier)
√ Festlegung der autorisierten Benutzer für Datenträgerzugriff
√ Verpackungs- und Versandvorschriften (Versandart z.B. in verschlossenen Behältnissen)
√ Direktabholung, Kurierdienst, Transportbegleitung
√ Gesonderter Verschluss von vertraulichen Datenträgern
√ Regelung zur Anfertigung von Daten-Kopien
√ Dokumentation der Abruf- und Übermittlungsprogramme
√ sichere Dokumentenvernichtung und Datenlöschung
√ sichere Löschung von Daten vor Datenträgeraustausch und Neuverwendung
√ Datenträgerentsorgung nach DIN66399
√ Gesicherter Rechenzentrums-Eingang für An- und Auslieferung

2. Integrity (Art. 32 para. 1 b GDPR)

Transfer Control

No unauthorized reading, copying, modification or removal during electronic transmission or transport;

√ Encryption concepts (encryption of data carriers, encryption of files).
√ Use of digital signatures
√ Virtual Private Networks (VPN)
√ Agreements on order processing with contractors
√ Disk management and inventory control via Business System
√ Regulated use of external data carriers such as USB sticks, external hard drives.
√ Issue of data carriers only to authorized recipients (e.g. order receipt, accompanying document)
√ Definition of authorized users for media access
√ Packaging and shipping instructions (type of shipping e.g. in closed containers)
√ Direct collection, courier service, transport escort
√ Separate sealing of confidential data carriers
√ Arrangement for making copies of data
√ Documentation of the retrieval and transmission programs
√ Secure document destruction and data deletion
√ Secure deletion of data before data medium exchange and reuse
√ Data carrier disposal via degaussing according to CESG Claims Tested Mark then sent to Stone Group Ltd for recycling.
√ Secured building access entry for delivery and return

Eingabekontrolle

Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind;

√ Organisatorisch festgelegter Zuständigkeiten für Dateneingaben
√ rollenbasiertes Berechtigungskonzept
√ Protokollierung von Eingaben (Veränderte Daten, Nutzer, die die Daten verändert haben)
√ Sicherung der Protokolle gegen unbefugten Zugriff
√ Bearbeitung von Computer Forensik Medien erfolgt nur an Arbeitskopien, Originalmedien werden in einer Beweistasche (Evidence Bag) aufbewahrt
√ Protokollauswertesysteme
√ Vier-Augen-Prinzip für besonders sensible Daten

Input Control

Determining whether and by whom personal data have been entered, modified or removed in data processing systems;

√ Organizational defined responsibilities for data entries
√ Role-based authorization concept
√ Logging of inputs (Changed data, users who changed data) in Business System.
√ Securing the protocols against unauthorized access
√ Processing of Computer Forensics media only takes place on working copies, original media are stored in an evidence bag
√ Protocol evaluation systems
√ Dual control principle for particularly sensitive data (Standard process and Chain of Custody)

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO) **Verfügbarkeitskontrolle** *Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust;* √ Feuer- und Rauchmeldeanlagen √ Feuerlöscher für Serverraum √ Klimatisierung des Serverraums √ Serverraum-Temperaturüberwachung √ Einsatz von RAID-Systemen √ Backup-Konzepte & Recovery-Konzepte √ Regelmäßige Datenwiederherstellungs-Tests √ unterbrechungsfreie Stromversorgung (USV) √ Virenschutz √ Firewall √ Schutz gegen „malicious code" √ definierte Meldewege (auch mit dem Dienstleister) √ Notfallpläne	3. Availability and resilience (Art. 32 para. 1 b GDPR) **Availability Control** *Protection against accidental or deliberate destruction or loss;* √ Fire and smoke detection systems √ Fire extinguisher for server room √ Air conditioning of the server room √ Server room temperature monitoring √ Use of RAID systems √ Backup concepts & recovery concepts √ Regular data recovery tests √ uninterruptible power supply (UPS) √ Virus protection √ Firewall) √ Protection against malicious code √ defined reporting channels (also with the service provider) √ Emergency plans
Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO); √ Backup-Konzepte & Recovery-Konzepte √ Sicherstellung einer schnellen Beschaffung von Hardware durch Einkauf/Partner	**Rapid recoverability (Art. 32 para. 1 c GDPR);** √ Backup concepts & recovery concepts √ Ensuring fast procurement of hardware by purchasing/partners
4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO) **Datenschutz-Management** √ Datenschutz-Management-System √ Verpflichtung der Mitarbeiter auf Vertraulichkeit √ Richtlinien und Konzepte zu Datensicherheit und Datenschutz (einschließlich Information Security Policy, HR Policy, Datenschutz-Management Konzept, Information Security Summary)	4. Procedures for regular review, assessment and evaluation (Art. 32 para. 1 d GDPR; Art. 25 para. 1 GDPR) **Data-Privacy-Management / Data Protection Management** √ Data Protection Management System √ Employee commitment to confidentiality √ Guidelines and concepts on data security and data protection (including Information Security Policy, HR Policy, Data Protection Management Concept, Information Security Summary)
Incident-Response-Management (Vorfalls-Reaktions-Management, Notfallpläne) ***√ Risikobewertung*** ***√ Notfallpläne***	**Incident-Response-Management (emergency plans)** √ Risk assessment √ Emergency plans
Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO) ***√ Berechtigungskonzepte*** ***√ Need-To-Know-Policy***	**Data Protection by Design and Default (Art. 25 para. 2 GDPR)** √ Authorization concepts √ Need-To-Know-Policy

Auftragskontrolle Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers; √ Verträge zur Auftragsverarbeitung (Art. 28 DSGVO) √ Eindeutige Vertragsgestaltung mit Partnerunternehmen √ formalisiertes Auftragsmanagement √ strenge Auswahl der Dienstleister √ Sicherer Datenträgertransport durch entsprechende Dienstleister √ Vorabüberzeugungspflicht √ Nachkontrollen √ Sichere Datenlöschung nach erfolgtem Auftrag √ Standarisierte Prozesse bei der Verarbeitung von Auftragsdaten √ Standard Change Management Prozess (nach ITIL) √ Überwachung der Prozesse	**Order Control** No commissioned data processing within the meaning of Art. 28 DS-GVO without corresponding instructions from the client; √ Contracts for order processing (Art 28 GDPR) √ Clear contract design with partner companies √ Formalized order management √ Strict selection of service providers √ Secure data medium transport through appropriate service providers √ Obligation of prior conviction √ Follow-up checks via Business System. √ Secure data deletion after the job has been completed/after 30 days or under conditions of the contract, or new instruction to delete by the customer. √ Standardized processes for processing of order data √ Standard Change Management Process (according to ITIL) √ Monitoring of the processes
5. Weitere Anmerkungen / Verweise / Dokumente √ Zertifizierung der KLDiscovery Ontrack GmbH nach ISO 27001 √ Zertifizierungen von Drittanbietern (z.B. Rechenzentren nach ISO 27001)	5. Further remarks / references / documents √ In addition, the technical-organizational measures of the subcontracted data processors apply √ Certification of KLDiscovery Ontrack according to ISO 27001 √ Certification of Third Parties (according to ISO 27001)

Data Processing Agreement 6.3

Standard Contractual Clauses

(Controller to Processor (Module Two)

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter “entity/ies”) transferring the personal data, as listed in Annex I.A. (hereinafter each “data exporter”), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each “data importer”)

have agreed to these standard contractual clauses (hereinafter: “Clauses”).

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses.

In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non- compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub- processors at least fourteen (14) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub- processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub- processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to

that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all

responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) [This section applies where the data exporter listed in Annex 1.A. is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[This section applies where the data exporter listed in Annex 1.A. is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[This section applies, where the data exporter listed in Annex 1.A. is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

(where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without

prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Ireland.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I

LIST OF PARTIES

Data exporter(s): [Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]

1. Name: The customer that is stated in the Order is data exporter for the purpose of these SCC.

Address: Customer's address stated in the Order

Contact person's name, position and contact details: The customer that authorized the Order

Activities relevant to the data transferred under these Clauses: Processing and hosting of data for data recovery and related services as stated in the order…

Signature and date: as stated in the Order

Role (controller/processor): Controller

Data importer(s):

2. Name: KLDiscovery Ontrack, LLC

Address: 9023 Columbine Road, Eden Prairie, MN 55347, USA.

Contact person's name, position and contact details: Shannon Gaughan (Commercial Counsel) / Gideon Kaplan (Associate General Counsel): Shannon.guaghan@kldiscovery.com / Gideon.kaplan@kldiscovery.com

Activities relevant to the data transferred under these Clauses: Hosting and processing of Personal Data .

Signature and date: Data importer's contact person stated above

Role (controller/processor): Processor

2. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Natural persons, such as Customers, Employees, Suppliers of Data Exporter or other data delivered by Data Exporter.

Categories of personal data transferred

Information relating to identified or identifiable natural persons, including pictures and photographs, contractual relationships and/or customer history, billing and payment data or other categories of data delivered by Data Exporter.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

If sensitive data should be transferred, it will be processed using the same processing methods as set out in these standard contractual clauses, using appropriate safeguards.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

One off, or as often as instructed by the data exporter.

Nature of the processing

The applicable Order content, mainly data recovery and connected services.

Purpose(s) of the data transfer and further processing

The purpose of the data transfer and processing results from the Service Terms and Service Description to the applicable Order, usually in connection with Data Recovery or related Services

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

The term required to complete the Order and, if applicable, after termination of the Order, provided, that any such processing is carried out in connection with the services provided under the Order.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

./.

COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

Supervisory Offices, depending on Data Exporter as defined in Clause 13:

https://ec.europa.eu/justice/article-29/structure/data-protection-authorities/index_en.htm

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter.

The technical and organizational measures at Data Importer's location will be shared upon request of the Data Exporter.

ANNEX III – LIST OF SUB-PROCESSORS

EXPLANATORY NOTE:

This Annex must be completed, in case of the specific authorisation of sub-processors (Clause 9(a), Option 1).

The controller has authorised the use of the following sub-processors:

Name: None

Address: Not applicable.

Contact person's name, position and contact details: Not applicable

Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorized): Not applicable.

ANNEX IV TO THE STANDARD CONTRACTUAL CLAUSES – SUPPLEMENTARY PROTECTIONS

In addition to the provisions of the Controller-to-Processor Standard Contractual Clauses, the following supplementary protections shall apply:

Definitions

For the purposes of this Annex IV, the following definitions apply:

(i) "Back Door" means any technical or organisational measures or mechanisms designed to enable any public authorities, or other third parties, to gain access to any of the data importer's systems, or to any Relevant Personal Data, including by circumventing the data importer's security measures;

(ii) "Disclosure Order" means any legally binding demand for access to, or disclosure of, any Relevant Personal Data, made by any public authority, in any jurisdiction, to the data importer;

(iii) "Group" means any legal entity under common control with, controlled by, or control the data importer;

(iv) "Relevant Authority" means a public authority that makes a Disclosure Order; and

(v) "Relevant Personal Data" means any personal data (as defined in these Controller-to-Processor Standard Contractual Clauses)

received by the data importer, or any of its sub-processors, under these Clauses.

Supplementary Protections

1. No back doors

The data importer hereby confirms that:

(i) it has not created any Back Doors in any infrastructure, technical environment, review platforms or other system used to host and/or process Personal Data of the data exporter;

(ii) it has not intentionally created or changed its business processes in a manner that facilitates access to its infrastructure, technical environment, review platforms or others systems or to any Relevant Personal Data; and

(iii) to the best of the data importer's knowledge, applicable laws and government policies applicable to the data importer:

(A) do not require the data importer to create or maintain any Back Doors; and

(B) do not require the importer to be in possession of, or to disclose or provide, any encryption keys in relation to any Relevant Personal Data.

2. Enhanced audit rights

In addition to, and without prejudice to, the audit rights afforded to the data exporter under the auditing provisions of the Data Processing Agreement, and Clause 8.9(c) these Controller-to-Processor Contractual Clauses, to the extent permitted by applicable law, the data exporter, or its appointed representatives, shall be permitted, on no less than 48 hours' written notice, to conduct an audit of the data importer's relevant systems (and the systems of any sub-processors where such sub-processors within the data importer's Group), whether in person or, to the extent practicable, by remote means, for the sole purpose of determining whether any Relevant Personal Data have been disclosed in response to any Disclosure Order. This additional right to audit shall be at the sole cost and expense of the data exporter who shall determine whether and if such audit shall take place. The data importer shall, where requested by the data exporter, take reasonable steps to assist the data exporter in conducting such audits including the provision of technical personnel to assist the data exporter in conducting the audit, supervised and controlled access to data importer's infrastructure, technical environment, review platforms or other systems (provided such access does not impact any other client of the data importer or require the disclosure of confidential information relating to such clients) and copies of relevant documents that may assist the data exporter in conducting and assessing the findings of such audit.

3. Notification and Transparency

To the extent permitted by applicable law, the data importer shall regularly (and at least once every 24 hours) publish a message via a secure URL, accessible at https://www.ontrack.com/en-gb/legal/transparency-report ("Transparency Page") informing the data exporter that, as at the time of the published message, it has not received a Disclosure Order. The data importer shall, for the term of processing of Relevant Personal Data under these Controller-to-Processor Contractual Clauses, continue to publish such information on the Transparency Page.

4. Obligation to Challenge

In the event that the data importer receives a Disclosure Order, the data importer shall promptly review the validity and enforceability of such Disclosure Order under applicable law and if, after a careful assessment, the data importer concludes that there are plausible grounds for challenging the Disclosure Order, and that such a challenge has a reasonable likelihood of succeeding, the data importer shall use reasonable efforts to bring such a challenge (including, where appropriate, through interim proceedings). To the extent that, notwithstanding any challenge, the data importer is obliged to disclose any Relevant Personal Data to the Relevant Authority, the data importer shall take all reasonable measures to ensure that it discloses the minimum amount of Relevant Personal Data required by applicable law.

5. Obligation to Notify

In the event that the data importer receives a Disclosure Order, the data importer shall:

(i) to the extent that the Disclosure Order contradicts the requirements of these Controller-to-Processor Contractual Clauses, inform the Relevant Authority that the Disclosure Order is incompatible with its obligations under these Controller-to-Processor Contractual Clauses, and that the Disclosure Order therefore exposes the data importer to conflicting legal obligations;

(ii) to the extent permitted by applicable law, notify the data exporter of the Disclosure Order; and

(iii) where the data importer is legally able to inform the data exporter of the Disclosure Order, provide all reasonable assistance to the data exporter to defend, challenge and/or limit the scope of the Disclosure Order and shall take all reasonable instructions from the data exporter regarding the Disclosure Order including choice of counsel by the data exporter. Where the data importer is permitted to notify, and therefore take instructions from the data exporter regarding the Disclosure Order, the data exporter shall be responsible for any reasonable costs and expenses incurred by the data importer in carrying out the data exporter's instructions.

6. Policies and procedures

The data importer shall implement and maintain adequate internal policies with clear allocation of responsibilities for data transfers, reporting channels and standard operating procedures for handling Disclosure Orders.

7. Disclosure of Records

The data importer shall create and maintain a written record of:

(i) each Disclosure Order; and

(ii) the response to each Disclosure Order, together with details of the analysis of the Disclosure Order, the reasons for any response to the Disclosure Order,

and shall make such records available to the data exporter on request, to the extent permitted by applicable law, subject to appropriate redactions.

8. Standards

The data importer shall adopt the security standards set out in Annex II, including but not limited to the ISO 27001 standard, and shall implement all appropriate security measures with due regard to the state of the art, in accordance with the levels of risk associated with the categories of Relevant Personal Data processed and the likelihood of Disclosure Orders in relation to such Relevant Personal Data.

9. Policy Review

The data importer shall implement a regular review of the measures it has taken to protect Relevant Personal Data, including its applicable policies and procedures, to assess the suitability of those measures, and identify and implement additional or alternative measures when reasonably necessary.

10. Onward Transfers

Where the data exporter provides instructions to data importer for the onward transfer of Relevant Personal Data to a sub-processor, the data importer shall use commercially reasonable efforts to obtain, from that sub-processor, an agreement that provides an equivalent level of protection for Relevant Personal Data, as is set out in this Annex IV, prior to the onward transfer of Relevant Personal Data to that sub-processor. Where the data importer is unable to obtain equivalent measures as those set out in this Annex IV, the data importer shall not transfer any Relevant Personal Data to the sub-processor without the prior written authorization of the data exporter. It is acknowledged at all times that, where the data importer is unable to obtain equivalent measures as those set out in this Annex IV, any authorization by the data exporter shall be solely at the data exporter's legal risk.

11. Compensation or other legal remedies

It is acknowledged and accepted by the data exporter and data importer that the decision to transfer any Relevant Personal Data shall be solely taken by the data exporter, or the data exporter's end client, as the case may be, and nothing in this Annex IV or more generally following a data exporter decision to transfer Relevant Personal Data shall impose, or create, any liability on the data importer to any Data Subject or the data exporter arising from such a decision.

Ontrack by KLDiscovery

Data Recovery

Provisions applicable in relation to transfers of Personal Data governed by the Data Protection Act 2018 (UK)

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

VERSION B1.0, in force 21 March 2022

ThisAddendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

Table 1: Parties

Start date		
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: Legal name of the customer stated in the Order Trading name (if different): Main address (if a company registered address): Address as stated in the Order Official registration number (if any) (company number or similar identifier): As stated in the Order	Full legal name: Legal name of the customer stated in the Order Trading name (if different): Main address (if a company registered address): Address as stated in the Order Official registration number (if any) (company number or similar identifier): As stated in the Order
Key Contact	Full Name (optional): the person that authorised the order. Job Title: as stated in the Order Contact details including email: As stated in the Order	Full Name (optional): Gideon Kaplan / Shannon Gaughan Job Title: Associate General Counsel / Commercial counsel Contact details including email: Gideon.kaplan@kldiscovery.com / Shannon.gaughan@kldiscovery.com
Signature (if required for the purposes of Section 2)	Signed for and on behalf of the Exporter set out above Signed: by the customer authorizing the Order Date of signature: as the Date of the Order Full name: As stated on the Order Job title: as stated on the Order	Signed for and on behalf of the Importer set out above Signed: by the Key Contact of KLDiscovery Ontrack, LLC Date of signature: June 20, 2023 Full name: Gideon Kaplan Job title: Associate General Counsel

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information. Date: The Date of the Order Reference (if any): Other identifier (if any): none

Table 3: Appendix Information

"Appendix Information" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: (i) The customer that is stated in the Order ; (ii) KLDiscovery Ontrack, LLC

Annex 1B: Description of Transfer: The purpose of the data transfer and processing results from the Service Terms and Service Description to the applicable Order, usually in connection with data recovery or related services

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data:

As set out in the Data Processing Agreement which incorporates this Addendum.

Annex III: List of Sub processors (Modules 2 and 3 only):

As set out in the Data Processing Agreement which incorporates this Addendum.

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes Which Parties may end this Addendum as set out in Section 19:

Importer

Exporter

Part 2: Mandatory Clauses

Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.

ANWENDUNG DER STANDARDVERTRAGSKLAUSELN ZUR ÜBEREINSTIMMUNG MIT DER SCHWEIZERISCHEN GESETZGEBUNG

Damit die Standardvertragsklauseln ("SCC") der schweizerischen Gesetzgebung entsprechen und somit geeignet sind, ein angemessenes Datenschutzniveau für die Übermittlung von Personendaten aus der Schweiz in ein Drittland gemäß Artikel 6 Absatz 2 Buchstabe a des schweizerischen Bundesgesetzes über den Datenschutz vom 19. Juni 1992 ("DSG") und, nach Inkrafttreten, gemäß Art. 16 Absatz 2 Buchstabe d des künftigen revidierten Bundesgesetzes über den Datenschutz vom 25. September 2020 ("revDSG") gelten zusätzlich die folgenden Bestimmungen:

1. Die Vertragsparteien vereinbaren, den GDPR-Standard für alle Datenübermittlungen zu übernehmen.

2. Verweise auf die GDPR sind als Verweise auf das DSG (bzw. nach dessen Inkrafttreten auf das revFADP") zu verstehen.

3. Bis zum Inkrafttreten der revDSG sind auch die Daten von juristischen Personen durch diese DSGVO und das SCC geschützt.

4. Aufsichtsbehörde:

(a) wenn die Datenübermittlung ausschließlich dem DSG oder dem revDSG unterliegt: die zuständige Aufsichtsbehörde ist der Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter ("EDÖB"); oder

(b) wenn die Datenübermittlung sowohl der DSGVO als auch dem DSG unterliegt: die zuständige Aufsichtsbehörde ist der EDÖB für Datenübermittlungen, die unter das DSG oder die revDSG fallen, und die zuständige EU-Aufsichtsbehörde für Datenübermittlungen, die unter die DSGVO fallen;

5. Anwendbares Recht für vertragliche Ansprüche nach Ziff. 17 SCC:

(a) wenn die Datenübermittlung ausschließlich dem DSG unterliegt: Schweizer Recht; oder

(b) wenn die Datenübermittlung sowohl der DSGVO als auch dem DSG unterliegt: deutsches Recht; oder (c) wenn die Datenübermittlung sowohl der DSGVO als auch dem DSG unterliegt: deutsches Recht.

6. Gerichtsstand für Klagen zwischen den Parteien gemäß Klausel 18 b SCC :

(a) wenn die Datenübermittlung ausschließlich dem DSG unterliegt: Zürich, Schweiz; oder

(b) wenn die Datenübermittlung sowohl unter die DSGVO als auch unter das DSG fällt: Stuttgart, Deutschland

Im Zusammenhang mit der gerichtlichen Zuständigkeit für Ansprüche, die sich aus diesem SCC ergeben, ist der Begriff "Mitgliedstaat" nicht so auszulegen, dass betroffene Personen in der Schweiz von der Möglichkeit ausgeschlossen werden, ihre Rechte an ihrem gewöhnlichen Aufenthaltsort (Schweiz) einzuklagen.

APPLICATION OF THE STANDARD CONTRACTUAL CLAUSES TO COMPLY WITH SWISS LEGISLATION

In order for the Standard Contractual Clauses ("SCC") to comply with Swiss legislation and thus be suitable for ensuring an adequate level of protection for transfers of personal data from Switzerland to a third country in accordance with Article 6 paragraph 2 letter (a) of the Swiss Federal Act on Data Protection dated 19 June 1992 ("FADP") and, once entered into force, in accordance with Art. 16 paragraph 2 letter d of the future revised Swiss Federal Act on Data Protection dated 25 September 2020 ("revFADP"), the following additional provisions shall apply:

1. The Parties agree to adopt the GDPR standard for all data transfers.

2. References to the GDPR are to be understood as references to the FADP (respectively, once it entered into force, to the "revFADP").

3. Before the revFADP enters into force, data pertaining to legal entities are also protected by this DPA and the SCC.

4. Supervisory authority:

(a) where the data transfer is exclusively subject to the FADP or revFADP: the competent supervisory authority is the Swiss Federal Data Protection and Information Commissioner ("FDPIC"); or

(b) where the data transfer is subject to both the GDPR and the FADP: the competent supervisory authority is the FDPIC for data transfers governed by the FADP or revFADP, and the competent EU supervisory authority for data transfer governed by the GDPR;

5. Applicable law for contractual claims under Clause 17 SCC:

(a) where the data transfer is exclusively subject to the FADP: Swiss law.; or

(b) where the data transfer is subject to both the GDPR and the FADP: Irish law.

6. Place of jurisdiction for actions between the parties pursuant to Clause 18 b SCC:

(a) where the data transfer is exclusively subject to the FADP: Zurich, Switzerland; or

(b) where the data transfer is subject to both the GDPR and the FADP: Dublin, Ireland

In the context of jurisdiction for claims arising out of this SCC, the term "Member State" shall not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland).

Zusätzliche Bedingungen Mobilgerät-Entsperrdienst

Diese zusätzlichen Bedingungen für den Mobilgerät-Entsperrdienst („Zusätzliche Entsperrbedingungen") ergänzen die Allgemeinen Geschäftsbedingungen für den Ontrack Datenwiederherstellungsdienst (https://www.ontrack.com/de-de/agbs) („Dienstbedingungen") und werden Ihnen im Zusammenhang mit einer Aufforderung zum Entsperren des im Informationsblatt angegebenen Mobilgeräts („Gerät") zur Verfügung gestellt, um das Extrahieren und/oder Dekodieren von Daten und Informationen von diesem Mobilgerät zu ermöglichen („Mobilgerät-Daten") (zusammen der „Entsperrdienst"). Diese zusätzlichen Entsperrbedingungen gelten nur für eine Bestellung für den Mobilgerät-Entsperrdienst.

Sie bestätigen hiermit, dass die in diesen zusätzlichen Entsperrbedingungen enthaltenen Verpflichtungen und Erklärungen unwiderruflich sind und dass Ontrack den Entsperrdienst in Abhängigkeit von den nachstehend aufgeführten Verpflichtungen und Erklärungen bereitstellt.

1. Diese zusätzlichen Entsperrbedingungen werden gemäß den Dienstbedingungen zwischen Ihnen und Ontrack in Bezug auf eine Bestellung (wie in den Dienstbedingungen definiert) für den Entsperrdienst abgeschlossen. Im Falle eines Konflikts oder einer Inkonsistenz zwischen diesen zusätzlichen Entsperrbedingungen und den Dienstbedingungen haben diese zusätzlichen Entsperrbedingungen Vorrang vor den Dienstbedingungen.

2. Ontrack startet den Entsperrdienst nach Zahlung der anfänglichen Einrichtungsgebühr (siehe Zahlungstabelle oben). Die anfängliche Einrichtungsgebühr wird nicht erstattet und entspricht den angemessenen anfänglichen Kosten von Ontrack für die Einrichtung und Implementierung des Entsperrdienstes. Nach Abschluss des Entsperrdienstes wird die Bearbeitungsgebühr von Ontrack in Rechnung gestellt und ist innerhalb von 30 (dreißig) Tagen nach Rechnungsstellung zu zahlen. Das Passwort für das Gerät und der Zugriff auf die Mobilgerät-Daten werden erst bereitgestellt, wenn Sie die Rechnung für die Bearbeitungsgebühr bezahlt haben. Wenn Sie die Bestellung stornieren und weitere Gebühren anfallen (siehe Abschnitte 3 bis 5 unten), ist die Stornierungsgebühr innerhalb von 30 (dreißig) Tagen nach Rechnungsstellung zu zahlen. Das Gerät wird erst zurückgegeben, wenn die Stornierungsgebühr bezahlt ist. Ontrack behält sich das Recht vor, Verspätungszinsen zum gesetzlichen Satz zu verlangen, falls die Zahlung nicht rechtzeitig erfolgt.

3. Stornierung als Verbraucher: Dieses Formular berechtigt Ontrack, den Mobilgerät-Entsperrdienst sofort zu starten. Wenn Sie Verbraucher sind und eine Bestellung aufgeben, haben Sie eine Frist von 14 Tagen, um die Bestellung zu stornieren. In diesem Fall behält Ontrack die Einrichtungsgebühr ein, da dies die angemessenen anfänglichen Kosten von Ontrack für die Einrichtung und Implementierung des Mobilgerät-Entsperrdienstes darstellt. Nach 14 Tagen können Verbraucher die Bestellung stornieren, zahlen Ontrack jedoch eine Gebühr von 1.566 € (einschließlich Mehrwertsteuer). Eine Stornierung ist zulässig, bis Ontrack bestätigt, dass der Mobilgerät-Sperrdienst erfolgreich abgeschlossen wurde, woraufhin die Bearbeitungsgebühr fällig und zahlbar wird.

4. Stornierung als Geschäftskunde: Wenn Sie ein Geschäftskunde sind, beträgt die Stornierungsgebühr 1.566 € (einschließlich Mehrwertsteuer). Eine Stornierung ist zulässig, bis Ontrack bestätigt, dass der Mobilgerät-Sperrdienst erfolgreich abgeschlossen wurde, woraufhin die Bearbeitungsgebühr fällig und zahlbar wird.

5. Es werden weder für Verbraucher- noch Geschäftskunden Stornierungsgebühren erhoben, wenn Ontrack den Mobilgerät-Entsperrdienst nicht innerhalb von 120 Tagen nach der Bestellung erfolgreich abschließt. Ontrack behält jedoch die Einrichtungsgebühr ein. Um zu stornieren, sollten alle Kunden Ontrack über die angegebenen Kontaktdaten per E-Mail oder Telefon kontaktieren oder die Stornierungsformular-Vorlage auf unserer Website verwenden.

6. Sie erkennen hiermit an und garantieren Ontrack, dass: (i) Sie rechtlich in der Lage sind, verbindliche Verträge abzuschließen; (ii) Sie die volle Autorität, Befugnis und Kapazität haben, diesen zusätzlichen Entsperrbedingungen zuzustimmen, und wenn Sie ein Geschäftskunde sind (definiert in den Servicebedingungen), Sie die entsprechende rechtliche Befugnis haben, die zusätzlichen Entsperrbedingungen einzugehen. (iii) Sie den Entsperrdienst nicht in Bezug auf Rechtsfälle bei Scheidung, Nachlass oder Strafverfahren nutzen möchten; (iv) alle Informationen, die Sie Ontrack im Zusammenhang mit der Bestellung zur Verfügung stellen, wahr, genau, vollständig und nicht irreführend sind; (v) Sie der rechtmäßige Eigentümer des Geräts sind oder die ausdrückliche Genehmigung des Eigentümers des Geräts haben, Ontrack die Erlaubnis zur Ausführung des Entsperrdienstes zu erteilen; (vi) der Besitz der Mobilgerät-Daten durch Ontrack keine Verpflichtungen oder Rechte Dritter verletzt; (vii) Ihre Lieferung des Geräts und/oder der Mobilgerät-Daten an uns nicht gegen geltendes Recht verstößt; und (ix) Ihr Gerät kein Material enthält, das gegen geltendes Recht verstößt. Wir behalten uns das Recht vor, dokumentarische Nachweise über Ihr Eigentum oder Ihren Rechtsanspruch zur Autorisierung des Entsperrdienstes anzufordern, einschließlich Kaufbelegen für das Gerät, rechtsverbindlichen Testamenten und Sterbeurkunden, und wir behalten uns das Recht vor, den Entsperrdienst ohne Erhalt solcher Nachweise auszusetzen bzw. nicht zu starten.

7. Sie erkennen an und stimmen zu, dass die Bereitstellung des Entsperrdienstes möglicherweise nicht erfolgreich ist und dass Ontrack das Gerät möglicherweise nicht erfolgreich entsperren kann. Der Entsperrdienst wird „wie gesehen“ bereitgestellt, ohne Zusicherung oder Gewährleistung hinsichtlich der Genauigkeit des Entsperrdienstes, seiner Gültigkeit, Nützlichkeit oder Vollständigkeit bereitgestellt.

8. Sie verpflichten sich hiermit, das entsperrte Gerät oder die Mobilgerät-Daten ausschließlich für Ihren eigenen Gebrauch zu verwenden. Sie werden das entsperrte Gerät oder die Mobilgerät-Daten nicht für rechtswidrige Zwecke verwenden, und Ontrack haftet nicht für die Verwendung des Geräts oder der Mobilgerät-Daten, die Sie nach Abschluss des Entsperrdienstes erhalten haben.

9. Sie erkennen an, dass der Freischaltdienst von einem Lieferanten von Ontrack, Cellebrite, bereitgestellt wird. Sie entbinden Cellebrite ausdrücklich und unwiderruflich von allen Klagen, Klagegründen, Gerichtsverfahren, Verpflichtungen und Schäden, die ab dem Datum dieses Vertrags und danach im Zusammenhang mit der Bereitstellung des Freischaltdienstes entstehen, unabhängig davon, ob es sich um vertragliche, gewohnheitsmäßige oder gesetzliche Rechte, oder solchen aus dem Grundsatz der Billigkeit, handelt. Nichts in diesem Abschnitt schließt jedoch aus, dass Sie nach geltendem Recht Ansprüche gegen Ontrack geltend machen können.

10. Sie erkennen ausdrücklich an, verstehen und erklären sich damit einverstanden, dass die Entsperrdienste die Entsperrung, die Erlangung des Passcodes, die Entschlüsselung, den Zugriff und/oder die Extraktion von Informationen oder Daten (einschließlich Übertragung, Speicherung, Kopieren oder Analysen) erfordern können, die auf einem elektronischen Gerät, einschließlich eines tragbaren elektronischen Geräts wie einem Mobiltelefon oder Tablet, Computersystemen, Programmen, Anwendungen, Servern, Telekommunikations- oder elektronischen Kommunikationssystemen, Medien, geistigem Eigentum (einschließlich, aber nicht beschränkt auf urheberrechtsfähigem Material, Geschäftsgeheimnissen und Know-how) durchgeführt werden.

11. Sie werden Ontrack, seine Direktoren, leitenden Angestellten, Aktionäre, Mitarbeiter und Servicepartner („Ontrack-Entschädigungsberechtigte“) von allen Forderungen, Ansprüchen, Klagen, Verlusten, Haftungsansprüchen, Schäden, Kosten und Ausgaben freistellen und schadlos halten, die gegen einen der Ontrack-Entschädigungsberechtigten geltend gemacht oder vorgebracht werden oder die dem Ontrack-Entschädigungsberechtigten als Folge einer Verletzung oder als Folge einer vermeintlichen Verletzung Ihrer Verpflichtungen im Rahmen dieser zusätzlichen Freigabebedingungen entstehen oder entstehen können.

12. Ontrack übernimmt keine Verantwortung für etwaige Beschädigungen oder physische oder sonstige Schäden oder Zerstörungen des Geräts oder für die Aufhebung von Herstellergarantien in Bezug auf das Gerät, entweder: bevor Ontrack das Gerät erhält; oder im Zuge der Bereitstellung des Entsperrdienstes durch Ontrack, wenn solche Schäden, Zerstörungen, Beschädigungen oder Ungültigkeit dadurch entstehen, dass Ontrack den Entsperrdienst gemäß den zusätzlichen Entsperrbedingungen ausführt.

© KLDiscovery 2023
KLDiscovery Ontrack GmbH
MISC ONT DE_Terms and Conditions for Ontrack Services_Oct 2023